Mesopotamian journal of Computer Science
Vol. **(2024)**, 2024, **pp**. 71–121
DOI: https://doi.org/10.58496/MJCSC/2024/007; ISSN: 2958-6631
https://mesopotamian.press/journals/index.php/cs

Review Article

A Survey on Artificial Intelligence in Cybersecurity for Smart Agriculture: State-of-the-Art, Cyber Threats, Artificial Intelligence Applications, and Ethical Concerns

Guma Ali [1,5*], Maad M. Mijwil[2], Bosco Apparatus Buruga[3], Mostafa Abotaleb [4], Ioannis Adamopoulos[6]

[1] *Department of Computer and Information Science, Faculty of Technoscience, Muni University, Arua, Uganda*

[2] *Computer Techniques Engineering Department, Baghdad College of Economic Sciences University, Baghdad, Iraq*

[3] *Department of Library and Information Services, Muni University, Arua, Uganda*

[4] *Department of System Programming, South Ural State University, Chelyabinsk, Russia*

[5] *Department of Computer Science, Faculty of Science, Islamic University in Uganda, Arua Campus, Arua, Uganda*

[6] *Hellenic Republic, Region of Attica, Department of Environmental hygiene and Public Health and Sanitarian inspections, Greece*

ARTICLE INFO

Article History

Received 03 May 2024
Accepted 28 Jun 2024
Published 20 Jul 2024

Keywords

Smart Agriculture
Artificial Intelligence
Cybersecurity
Ethical Concerns
Cyber threats

ABSTRACT

Wireless sensor networks and Internet of Things devices are revolutionizing the smart agriculture industry by increasing production, sustainability, and profitability as connectivity becomes increasingly ubiquitous. However, the industry has become a popular target for cyberattacks. This survey investigates the role of artificial intelligence (AI) in improving cybersecurity in smart agriculture (SA). The relevant literature for the study was gathered from Nature, Wiley Online Library, MDPI, ScienceDirect, Frontiers, IEEE Xplore Digital Library, IGI Global, Springer, Taylor & Francis, and Google Scholar. Of the 320 publications that fit the search criteria, 180 research papers were ultimately chosen for this investigation. The review described advancements from conventional agriculture to modern SA, including architecture and emerging technology. It digs into SA's numerous uses, emphasizing its potential to transform farming efficiency, production, and sustainability. The growing reliance on SA introduces new cyber threats that endanger its integrity and dependability and provide a complete analysis of their possible consequences. Still, the research examined the essential role of AI in combating these threats, focusing on its applications in threat identification, risk management, and real-time response mechanisms. The survey also discusses ethical concerns such as data privacy, the requirement for high-quality information, and the complexities of AI implementation in SA. This study, therefore, intends to provide researchers and practitioners with insights into AI's capabilities and future directions in the security of smart agricultural infrastructures. This study hopes to assist researchers, policymakers, and practitioners in harnessing AI for robust cybersecurity in SA, assuring a safe and sustainable agricultural future by comprehensively evaluating the existing environment and future trends.

1. INTRODUCTION

The rapid growth of the world's population, combined with intense competition, exploitation of natural resources, climate change, environmental challenges, and natural disasters, has posed severe risks to agricultural output and urbanization, increasing demand for food and agricultural products. According to the Food and Agriculture Organization, the global population will be 10 billion by 2050, with 7 billion people living in urban areas; therefore, 70% more food must be produced to feed the population [1][2]. Integrating innovative technologies into agricultural practices to boost productivity and create the necessary food supply has resulted in new concepts known as "smart agriculture" [1][3]. Smart agriculture, better known as precision agriculture or Agriculture 5.0, is a concept that integrates cutting-edge smart technologies, mechatronics and autonomous systems, protocols, data-driven solutions, and computational paradigms to improve agricultural processes, increase the volume and quality of agricultural and food products, and optimize the utilization of resources, and enhance the efficiency, sustainability, and productivity of farming practices [4-6]. It leverages several emerging technologies like smart agricultural equipment, smart sensors, drones and unmanned aerial vehicles (UAVs), Internet of Things (IoT), cloud computing, wireless sensor networks (WSNs), agricultural robotics, radio frequency identification (RFID), global positioning systems (GPS), big data analytics, satellite imaging and remote sensing, Blockchain technology, AI, geographic

*Corresponding author. Email: a.guma@muni.ac.ug

information system (GIS) and mapping technologies, additive manufacturing, and others to monitor, manage, and optimize agricultural operations [7-9].

Smart agriculture employs a variety of sensors, including ground-based, aerial, satellite-based, and IoT devices, which are installed, worn, or implanted in various parts of the farm to collect agricultural data on livestock health, machinery, crop condition, pH levels, humidity, temperature, nutrient levels, weather, growth stages, pest infestations, and soil condition. The collected data is transmitted to remote analytics servers or the cloud via wireless communication technologies (e.g., Bluetooth, ZigBee, Long Range (LoRa) radio technology, NarrowBand Internet of Things (NB-IoT), SigFox, Wireless Fidelity (Wi-Fi), and fifth generation (5G), or satellite communication) for storage and analysis. A predetermined model, sophisticated analytics approaches, and decision rules are used to identify insights from the stored real-time and historical data on farm conditions. Farmers utilize the information gained via the application layer to make informed decisions regarding crop management, irrigation timing, spraying, pest and disease control, fertilization, and resource allocation [10-13]. The main objective of SA is to transform farms into connected and smart ecosystems by seamlessly integrating cutting-edge technologies, data analytics, and AI to improve crop production and sustainability, minimize resource waste, reduce environmental impact, improve overall profitability, increase efficiency and profitability, and assist farmers in making data-driven decisions [5][14-16]. According to Naidoo and Munga [17], the worldwide SA market value is expected to increase from US$16.2 billion in 2023 to US$25.4 billion by 2028. North America has the most extensive smart agricultural market, followed by Europe, Japan, China, South Korea, India, Brazil, Argentina, Cuba, and South Africa. There are many applications and use cases of smart agricultural technology, such as monitoring climate conditions, environment and field monitoring, crop health monitoring, precision agriculture, greenhouse automation, livestock and poultry monitoring and management, and others [11][18-20]. Smart agriculture offers several benefits: better traceability and transparency, data-driven decision-making, improved food safety and traceability, reduced operational costs, resource optimization and efficiency, and many more [21-23].

Despite the numerous potential benefits offered by SA, the new paradigm is susceptible to advanced persistent threats, agroterrorism, autonomous system hijacking, backdoor attacks, blockchain attacks, brute-force attacks, endpoint attacks, Cloud attacks, data breaches, denial-of-service (DoS) and distributed DoS (DDoS) attacks, eavesdropping attacks, evasion attacks, insider attacks, IoT breaches, malware injection attacks, man-in-the-middle (MiTM) attacks, phishing attacks, poisoning attacks, session hijacking, radio frequency jamming attacks, ransomware attacks, and others [17][22][24][25]. These cyber-attacks have severe consequences for farmers, agricultural enterprises, and organizational infrastructures, including financial losses, identity theft, service disruption, reputational damage, crop yield, and quality reduction, supply chain disruption, data breaches, and privacy concerns, environmental damage, food safety risks, and loss of trust and confidence [25][26]. Several traditional security and data privacy measures are employed in AgriTech to counteract these cyber-attacks. They include data encryption, access control, firewalls, multi-factor authentication, regular updates and patch management, intrusion detection, data anonymization and aggregation, risk assessment, identity-based cryptography, intrusion prevention systems, intrusion detection systems, regular security audits, and vulnerability assessments, digital signatures, data loss prevention systems, incident response plan, and security training [22][27-29]. These traditional cybersecurity techniques depend on preset rules and signatures to detect and prevent known cyber risks and attacks in SA, thus making them static and unresponsive to new cyber-attacks [29]. As a result, integrating emerging technologies such as AI and machine learning is essential for improving and reshaping the cybersecurity environment in SA [2].

In SA, AI implements techniques like machine learning, deep learning, natural language processing, and reinforcement learning in cybersecurity to analyze vast amounts of agricultural data collected from sensors, drones, robots, and other IoT devices to detect anomalies, predict potential attacks in real-time, instantly respond to security breaches, and guarantee smart and computerized cyber defense [24][30-32]. Islam et al. [33] reported that the worldwide market value of AI in cybersecurity is expected to rise from US$8.8 billion in 2020 to US$38.2 billion by 2026 at a 23.3% compound annual growth rate within the period. Some AI applications in cybersecurity include anomaly detection, behavioral analysis, botnet detection, endpoint security, fraud detection, and many more [34-38]. By leveraging AI in cybersecurity, smart agricultural systems can automate and advance threat prediction, offer better endpoint protection, ensure better vulnerability management, easy botnet detection, early and faster detection of new cyber threats and risks, fast response, higher accuracy, lower cost, better threat intelligence, improved decision-making, and reduced false positives [34][39].

Several reviews on the use of AI in cybersecurity have been published in recent years. However, to our knowledge, no comprehensive review describes AI techniques for improving cybersecurity in SA. Thus, this study aimed to survey AI applications in cybersecurity for SA. The contributions of this study are:

- To provide a state-of-the-art review of SA's evolution, architecture, emerging technologies, and applications.
- To conduct an in-depth literature study on cyber threats and challenges facing SA.
- To investigate and synthesize AI approaches in cybersecurity for SA.
- To explain how AI may be used in SA to enhance cybersecurity.
- To examine the ethical implications of employing AI in cybersecurity for SA.

The paper is organized into the following sections: Section 2 discusses the materials and methods used in the review. Section 3 examines the state-of-the-art of SA (i.e., evolution, architecture, emerging technologies, and applications) and the cyber threats and challenges in smart agriculture explored in Section 4. Section 5 describes cybersecurity in smart agriculture, and Section 6 explains artificial intelligence in SA (i.e., artificial intelligence techniques, AI applications in SA cybersecurity, case studies and examples of AI applications in SA cybersecurity, and ethical concerns of using AI in cybersecurity). Finally, Section 4 concludes the study.

2. MATERIALS AND METHODS

This study comprehensively surveys the use of AI in cybersecurity for SA. This method enables the comprehensive collection, assessment, and synthesis of existing literature, resulting in an extensive understanding of current trends, challenges, and advancements. The relevant literature used in the survey was gathered from Journal articles, conference proceedings, book chapters, magazines, and websites using relevant keywords from different academic databases and digital libraries like Nature, Wiley Online Library, MDPI, ScienceDirect, Frontiers, IEEE Xplore Digital Library, IGI Global, Springer, Taylor & Francis, and Google Scholar. The research considered the relevant literature published between January 2021 and July 2024 written in English and focused on scientific and technical research, particularly in AI, cybersecurity, and SA. A set of keywords and phrases related to AI, cybersecurity, and SA was used to search academic databases and digital libraries. The search terms included “Cybersecurity Challenges in SA” OR “AI” AND “Cybersecurity” AND “SA” OR “Machine Learning” AND “Cybersecurity” AND “Precision Agriculture” OR “Deep Learning” AND “Cyber Threats” AND “Agriculture Technology” OR “AI” AND “Cyber Attacks” AND “Smart Farming” OR “Application of AI in Cybersecurity” AND “Advantages of using AI in Cybersecurity” OR “Ethical Concerns in Application of AI in Cybersecurity” AND their intersections, were used to extract the relevant literature for the study. The Boolean operators “AND” and “OR” were employed to filter the search results and ensure relevant material inclusion.

The exclusion criteria included research papers that were not in English, not directly related to the research focus, and papers with insufficient methodological details or lacking empirical evidence. The literature search biases were mitigated using a test-retest approach, comprehensive search strategies, transparent reporting, peer review, critical appraisal, sensitivity analyses, conflict of interest disclosure, meta-analysis, and ongoing monitoring. Relevant research data from the selected studies were extracted using predefined key information such as (1) Title, authors, and publication year, (2) Objectives and research questions, (3) AI techniques used, (4) Cybersecurity applications (e.g., threat detection, risk assessment), (5) SA applications (e.g., precision farming, IoT integration), and (6) Results and conclusions. A total of 180 relevant research papers were reviewed, of which 01 were from Nature, 03 from Wiley Online Library, 39 from MDPI, 10 from ScienceDirect, 02 from Frontiers, 63 from IEEE Xplore Digital Library, 02 from IGI Global, 05 from Springer, 02 from Taylor & Francis, and 53 from Google Scholar. These research papers were analyzed, evaluated, and classified according to their relevance to the AI applications in cybersecurity for SA. Fig. 1 depicts the distribution of digital libraries according to the year of publication.

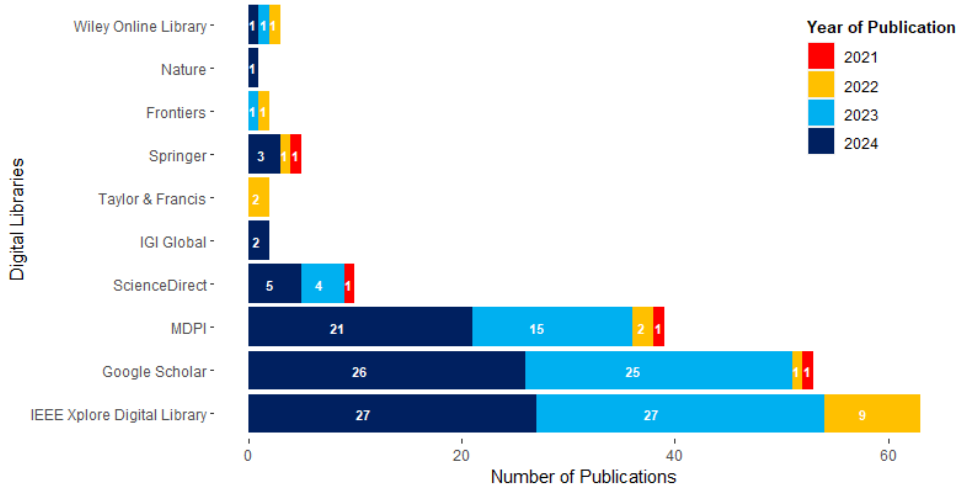

Fig. 1. Depicts the distribution of digital libraries according to the year of publication.

The data extracted from the selected literature were synthesized and analyzed using qualitative synthesis and thematic analysis. The analysis focused on AI technique categorization, identification of common cybersecurity threats, and assessing the effectiveness of AI solutions in addressing these threats in SA contexts. The findings presented in the survey were confirmed by consulting with subject experts, cross-referencing findings with previous literature studies, and critically analyzing the strength of the conclusions reached. Each research paper was evaluated for quality based on the methodology’s

robustness, the validity and reliability of the findings, and their contribution to AI in cybersecurity for SA. A scoring system was used to rate the studies so that only high-quality research papers were included in the final analysis. Since this study reviews existing literature, no primary data was collected; therefore, ethical approval was unnecessary. However, ethical standards were upheld by crediting all sources correctly and avoiding plagiarism.

The study acknowledges potential limitations, such as (1) the possibility of missing relevant studies that are not indexed in the selected databases, (2) publication bias: research with good outcomes is more likely to get published, (3) the survey may not thoroughly investigate the ethical implications of deploying AI in cybersecurity for SA, (4) a lack of quantitative analysis or empirical data might undermine the survey's results, as qualitative assessments may not provide adequate proof for the assertions presented, (5) while the survey may include theoretical applications, there may be an insufficient emphasis on real-world implementation and practical difficulties such as cost, scalability, and user acceptance, and (6) rapid advancements in AI and cybersecurity may outpace the literature.

3. STATE-OF-THE-ART-OF-SMART-AGRICULTURE

The study begins by exploring the evolution (Section 3.1), architecture (Section 3.2), emerging technologies (Section 3.3), and applications (Section 3.4) of SA.

3.1 Evolution of Agriculture

The evolution of agriculture from 1.0 to 5.0 comes with technological advancements and changes in farming practices that transformed food production, distribution, and consumption. Agriculture has evolved in five stages, with each stage bringing innovations [40]:

3.1.1 Agriculture 1.0: The Pre-Industrial Era

Agriculture 1.0, also known as the pre-industrial era, was between 1784 and 1870 and was dominated by (1) heavy reliance on human and animal labor, (2) use of essential hand tools such as hoes, sickles, and plows, (3) most farming was for local consumption with only a tiny surplus for trade, (4) diverse cropping systems for food security, (5) small-scale farms run by families, and (6) the use of simple canals or buckets to water the farms [40-43]. This traditional farming results in poor productivity and efficiency, little technological innovation, and a heavy reliance on natural weather patterns [20][44].

3.1.2. Agriculture 2.0: The Industrial Era

Agriculture 2.0, also known as the industrial era, was between the 18th Century and early 20th Century [40]. It was distinguished by (1) the introduction of machinery like the seed drill, mechanical reaper, and steam-powered tractors, (2) increased productivity and efficiency as a result of mechanization, (3) the use of machines, fertilizers, and better seeds in larger-scale farming to produce a surplus for trade, and (4) the utilization of scientific concepts to increase agricultural yields and livestock breeding [41]. Machinery boosted efficiency, reduced the need for human labor, and raised agricultural productivity, increasing food security and economic growth [20]. Resource waste, chemical pollution, environmental destruction, and excessive energy consumption became issues [42-44].

3.1.3. Agriculture 3.0: The Green Revolution

Agriculture 3.0, the green revolution, emerged in the Mid-20th Century (1940s-1960s). This era was characterized by (1) widespread use of chemical fertilizers, pesticides, and herbicides to boost crop productivity, (2) increase and improvement of irrigation techniques, (3) increased use of tractors, combines, and other machinery, (4) development of high-yield, disease-resistant crop varieties that led to increase in global food production, (5) better farm management practices, and (6) use of earth observation satellites, GPS, and computer science technologies in agriculture [40-42][45]. These innovations boosted food production and reduced food shortages. It also caused environmental damage and health problems owing to increased chemical use. Biotechnological advances enabled crop genetic modification to increase yield and disease resistance [20][43][45].

3.1.4 Agriculture 4.0: The Digital Revolution

Agriculture 4.0, also known as the digital revolution era, was between the late 20th Century and the early 21st Century. It incorporated cutting-edge technologies such as precision agriculture, virtual and augmented reality, big data analytics, 3D printing, IoT devices, quantum computing, drones, satellites, smart farming technologies, WSN, cloud computing platforms, AI, blockchain, and robotics to enhance farming practices, improve efficiency and productivity, make informed decisions about crop management and resource allocation, automate various farm tasks, lessen the environmental impact, promote sustainable development, and monitor and control crop and livestock health in real-time [20][43][45].

3.1.5 Agriculture 5.0: The Sustainable and Smart Agriculture

Agriculture 5.0, also known as sustainable and SA is the next evolutionary stage that employs cutting-edge technologies and innovative techniques to handle agricultural sector challenges while increasing sustainability, efficiency, and production. It uses AI and machine learning, IoT, big data and analytics, vertical and urban farming, advanced robotics and automation,

biotechnology and genetic engineering, non-terrestrial networks, and blockchain technology to optimize resources, increase productivity and sustainability, improve food security and climate resilience, improve transparency and efficiency in the food supply chain, and boost consumer engagement and trust in food systems [45][46]. Agriculture 5.0 has resulted in a paradigm change towards a more data-driven, technology-enabled, and sustainable approach to farming, able to meet rising food demand while reducing agriculture's environmental effect. It also incorporates green concepts and the widespread use of renewable energy and energy harvesting technology to lower total agriculture costs while helping the environment [45-47]. Fig. 2 illustrates the evolution of Agriculture from 1.0 to 5.0.

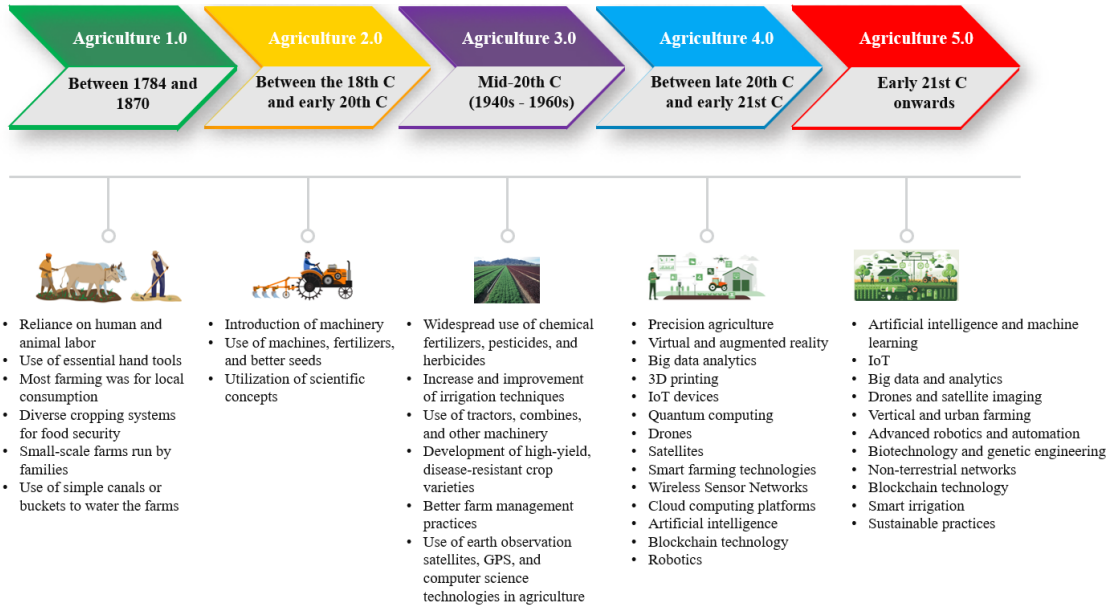

Fig. 2. Shows how agriculture evolved from 1.0 to 5.0, with each stage's technical breakthroughs and changes.

3.2 Smart Agriculture Architecture

The smart agricultural architecture comprises eight (8) layers: perception or sensing, networking and data communication, edge, fog, cloud, analytics, control, and application. These layers support various functions in SA, which are described below.

3.2.1 The perception or sensing layer

The perception or sensing layer is the hardware layer consisting of the physical devices, sensor technologies, GPS, cameras, WSN, RFID systems, agricultural robots, UAV, and actuators deployed throughout the agricultural environment or in greenhouse buildings to capture information on the farm and monitor the plants, livestock, or environmental factors [22][23][48]. These smart sensors include environmental sensors (e.g., temperature, humidity, precipitation, wind speed), soil sensors (e.g., moisture, pH, nutrient levels), and crop sensors (e.g., spectral imaging, biomass measurement). The actuators manage irrigation systems, machinery, and other equipment. RFID tags contain data about the animal identification number. GPS enables the geolocation of agricultural machines and farm supplies, which may aid precision farming systems. The perception layer's data is uploaded to the cloud for storage and data analysis, which helps in intelligent agricultural decision-making [49-52].

3.2.2 Networking and data communication layer

The networking and data communication layer sends data acquired by the perception layer to the cloud for analysis, which is subsequently routed to the application layers. It provides control commands from the control layer to the application layer, allowing intelligent crop management and growth control [49]. Data transmission channels include wired, wireless, short or long-distance mechanisms such as Wireless Fidelity (Wi-Fi), Narrowband-IoT (NB-IoT), Sigfox, Long-Range Wide Area Network (LoRaWAN), Bluetooth, ZigBee, fifth-generation (5G), satellite communication, Near Field Communication (NFC), and Global Positioning System/General Packet Radio Service (GPS/GPRS) [10][23][53][54].

3.2.3 Edge Layer

The edge layer sits between the network and the applications and end devices. It handles IoT device services, data processing, and real-time intelligent decision-making [22]. The edge layer consists of security features, data filters, decision-making capabilities, diverse processing, an in-out interface, and a gateway that are responsible for pre-processing and analyzing data from devices, enhancing data transmission performance, lowering computing load, and passing data to a higher layer for

further processing [11][23][44][52]. For example, the edge layer is used in rural farms without enough network connectivity to ease the processing problem [8][55].

3.2.4 Fog layer

The Fog layer processes and analyzes agricultural data supplied by IoT sensors locally and near the sensor layer to minimize latency for agriculture applications and services while reducing the use of cloud computing [54][56]. It consists of the Static Fog Zone and the Mobile Fog Zone. The Static Fog Zone, placed at the field level, houses agents, microservices, and digital twins, providing localized data storage and computation capabilities for instant farm data analysis and access to internal Application Programming Interfaces for farm data retrieval. The mobile fog nodes collect data directly from the farm's sensors, actuators, harvesters, tractors, drones, and agricultural robots [8][51].

3.2.5 Cloud layer

The cloud layer, comprised of computing resources with high throughput and storage capacity, is used to manage agriculture data received from the sensor or fog layer and process, analyze, and store it to improve agricultural service quality [52][57][58]. It also consists of connected virtual servers communicating with different layers over the Internet. The cloud layer can access external resources such as growth stage estimators, weather services, routing services, and disease detection tools. It also offers farm data anonymization services. It enables AI and machine learning to analyze agricultural data collected from IoT sensors, drones, or satellites to aid in growth stage assessment, weather forecasting, and disease detection and provide useful decision-making information [8][59].

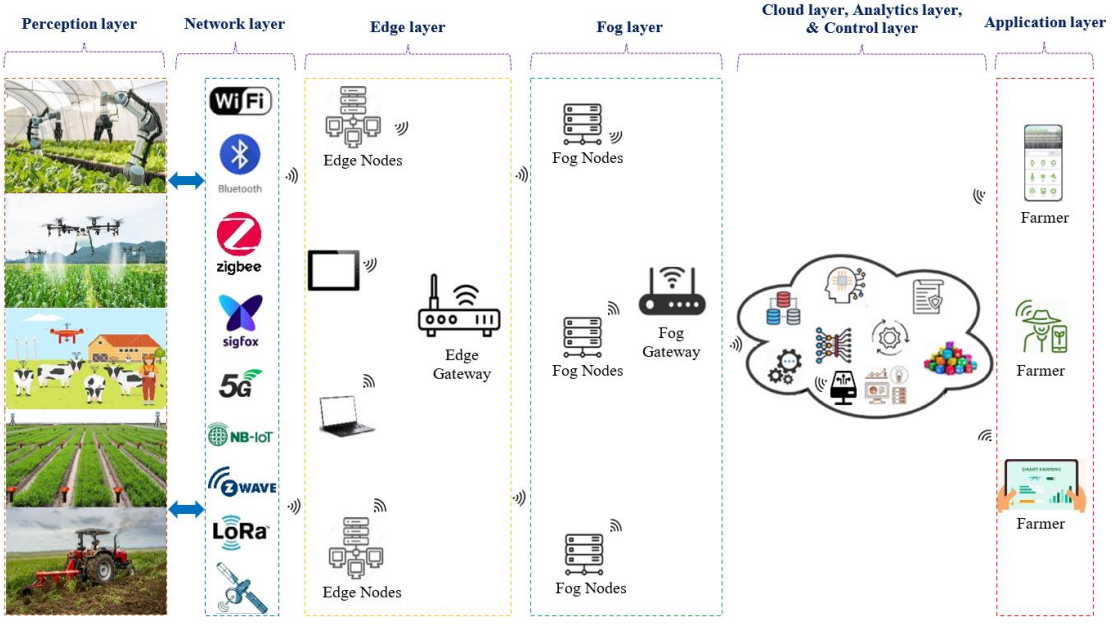

Fig. 3. Shows the main layers in the SA architecture.

3.2.6 Analytics layer

The cloud data analysis layer includes several analytical methodologies, including descriptive, predictive, and prescriptive analytics. Artificial intelligence models and machine learning algorithms are used to mine and analyze massive sensor and agricultural data stored in the cloud, predict crop yields, disease outbreaks, and pest infestations, process spatial information about soil type and nutrient levels, and correlate them with field, and optimal farming practices, which are used for decision-making and then provided to the control layer [48][49][60].

3.2.7 Control layer

The control layer implements the SA system's decision-making function and the different controllers on the farm. It accepts control commands from the SA system and activates the different controllers in the farm to apply fertilizer, spray drugs, irrigate, and generate alarms in case of failure of the farmland network system [49].

3.2.8 Application layer

This layer provides user-friendly interfaces in web-based dashboards, mobile applications, or desktop software for farmers to use the smart agricultural system [48]. It can be accessed on smart devices like personal computers, laptops, smartphones, tablets, and other smart devices that enable farmers to monitor all aspects of crop growth remotely, manage agricultural

activities like spraying, irrigation, and fertilization, and facilitate digital communication with agricultural experts, suppliers, Agroscientists, traders, government officials, businesses, and other stakeholders [49]. Farmers may use the apps to monitor livestock stress levels, identify the root cause of stress, maximize asset use, provide agricultural messages, and provide advice [52]. Fig. 3 depicts the main layers in the SA architecture.

3.3 Emerging Technologies in Smart Agriculture

Smart agriculture employs emerging technologies to increase production, efficiency, and sustainability. The major cutting-edge technologies for the effective development and deployment of smart agricultural systems are:

3.3.1 Wireless sensor networks (WSNs)

The capabilities of WSNs, such as impact sensing, location-based services, and real-time monitoring, have made them the most essential component, resulting in broad adoption in SA. Wireless sensor networks are spatially dispersed sensor nodes that gather and transmit data on environmental variables such as soil moisture, humidity, and temperature [61]. They consist of low-cost, tiny sensors linked to a communication system that collect essential environmental variables such as air quality, temperature, humidity, and pressure and transfer the sensed data to other nodes, providing farmers with real-time agricultural data [6][43][62]. The market value of wireless sensor networks is estimated at US$38.99 billion in 2018 and is predicted to rise to US$148.67 billion by 2026, growing at a Compound Annual Growth Rate (CAGR) of 18.3% from 2019 to 2026. In agriculture, wireless sensor networks enable real-time and continuous monitoring of climatic parameters in an agricultural field, such as soil acidity, moisture, humidity, and light, allowing farmers to make decisions about irrigation schedules, fertilizer application, and pest management, all of which have a significant impact on crop growth, quality, and productivity [61]. They analyze soil, monitor weather, determine yield productivity, detect crop and livestock disease early, monitor crops, sustain agricultural yields, reduce waste, and conserve water while maintaining crop quality [43][63].

3.3.2 Internet of Things (IoT)

The IoT is one of the most significant technical developments in SA, and its use has transformed farming methods by boosting resilience and sustainability via remote object connectivity. Gyamfi et al. [20], Ongadi [27], and Mijwil et al. [64] define the IoT as a network of interconnected physical devices equipped with sensors, monitoring equipment, actuators, and software across the agricultural landscape, resulting in a network of interconnected elements that aid in agricultural data collection, exchange, analysis, and decision-making in real-time. Advancements in communication technologies and wireless networks, such as 5G, LoRaWAN, NB-IoT, Sigfox, ZigBee, and Wi-Fi, are facilitating the use of IoT in SA [65]. IoT devices, such as soil sensors and weather stations, actuators, smart irrigation systems, drones, robotics, and livestock trackers, are implemented in agricultural systems to collect real-time data on various parameters, such as soil conditions, crop health, greenhouses, weather patterns, livestock health, and equipment status, which are transmitted to the server through wireless or wired network [43][66]. They monitor farming conditions remotely and allow the analysis of extensive real-time data from heterogeneous sensors and devices strategically positioned in the field to enable farmers and agricultural managers to make intelligent and well-informed decisions [27][46][67]. According to Vailshery [68], the global market value for agricultural industrial Internet of Things (IIoT), which includes agricultural management platforms, supply chain and inventory management solutions, GPS services and field mapping services, agricultural monitoring services, micro-farming solutions, was US$4.02 billion in 2021 and is expected to reach US$7 billion by 2025 as SA becomes more widely adopted. Smart agriculture employs IoT for livestock monitoring, precision farming, weather tracking, system control, soil management, weed management, pest management, supply chain management, and water conservation [6][69][70]. Farmers use the acquired data to make decisions about irrigation, fertilization, and pest management [27].

3.3.3 Smart sensors

Smart sensor systems have recently transformed the agriculture industry by giving real-time data required for effective farm management. Nitin and Gupta [43] define sensors in SA as small, intelligent, and advanced devices that combine sensing technologies, wireless connection, and data processing capabilities that aid in general farm management. Wire and wireless intelligent sensors are widely used in agriculture to collect data on plants, animals, soil, and the ecosystem. They play an essential role in farming and are a vital component of the IoT [43][71][72]. The global market value for agricultural sensors is projected to quadruple from 2021 to 2027, reaching around US$3 billion [73]. Various agricultural sensors, such as soil moisture sensors, temperature and humidity sensors, drone-fitted sensors, light sensors, water content sensors, nutrient sensors, agricultural robot-fitted sensors, air quality sensors, weather sensors, weed seeker sensors, and crop health sensors, can be planted in the farm and livestock to scan and collect, store, and disseminate relevant agricultural data [74-76]. Smart sensors are used in agriculture to (1) monitor soil, climate, and crop health, (2) manage water and livestock, and (3) monitor irrigation, pest infestations, and weed locations for efficient resource management, improve plant growth and crop yield, and contribute to food security and sustainable development [43][63][72][74][77].

3.3.4 Agricultural robotics

Agricultural robotics transforms SA by speeding plant breeding and increasing data-driven farming with much lower labor inputs through task-appropriate sensing and actuation. Agricultural robotics refers to robotic systems and automation

technologies that work autonomously in agricultural practices to undertake tasks previously performed by humans [50]. They include autonomous tractors, field robots, scarecrows, livestock robots, robotic harvesters, greenhouse robots, and drones utilized in agriculture to increase efficiency, accuracy, and sustainability [20][27][74]. The market value of agricultural robotics is expected to reach US$13.5 billion in 2023 and US$40.1 billion by 2028, with a CAGR of 24.3% between 2023 and 2028. It consists of machinery, IoT, electronics, integration of automatic control technology, WSNs, fine mechanical technology, AI and machine-learning algorithms, computer technology, cameras, and actuators and sensors used to plant, weed, harvest, monitor crops, irrigate the farm, manage soil and pests, detect disease, and spray the farm and animals, thereby enhancing accuracy, reducing the need for manual labor, and improving operations [4][43][46][74]. Crop and soil management, irrigation management, soil cultivation, seed sowing, disease detection, weeding detection, crop yield estimation, mowing, crop harvesting, crop pest detection, pesticide spraying, reducing manual labor, improving efficiency, and picking and sorting products and packaging are some of the uses and benefits of agricultural robotics [1][7][75][78].

3.3.5 Smart agricultural drones

Smart agricultural drones transform farming methods by harnessing innovative technology to improve agricultural efficiency, precision, and sustainability. They also give farmers a bird's eye perspective of their fields and valuable information for efficient crop and livestock management. According to Mowla et al. [50], smart agricultural drones, also known as agri-drones, are UAVs designed and equipped with advanced technologies such as remote sensing sensors, GPS, IoT, GIS, weather forecasting technology, 3D cameras, robotic systems, AI and machine learning algorithms, and imaging systems to collect data, monitor crops and animals, and improve farming and agricultural practices. The market value of agricultural drones for precision agriculture is expected to rise from US$13.9 billion in 2021 to US$40.7 billion by 2026 [79]. Agricultural drones equipped with cameras and sensors may collect high-resolution aerial imagery, allowing farmers to identify problem areas, monitor crops and animals, detect pests, map fields, and make informed decisions [4][27][80]. They make aerial data collecting easier, allowing for a quick and comprehensive overview of the agricultural environment when equipped with IoT-WSNs [50]. Smart agricultural drones are used to monitor crop health, analyze soil health, manage irrigation, plant, seed, spray pesticides and fertilizers, predict yield, reduce reliance on imported chemical inputs, monitor and manage livestock, detect weeds and diseases, and field-level phenotyping, leading to increased efficiency, accuracy, and sustainability of agricultural operations, make informed decision-making through data analytics and machine learning, and improve farm management [7][52][75][77][78].

3.3.6 Satellite imaging

Satellite imaging collects agricultural data using remote sensing techniques, allowing for better monitoring and management of agricultural activities and promoting sustainable agriculture capable of feeding a rapidly growing world population. Satellite imaging is a cutting-edge technique that employs satellite-based remote sensing to monitor and control agricultural activities. It collects high-resolution images of agriculture using satellites, providing significant information about crop and animal health, soil conditions, water consumption, and other essential elements impacting agricultural productivity [81]. The worldwide market value for satellite imaging in agriculture is estimated at US$507.05 million in 2022 and is expected to reach US$1071.47 million by 2031, growing at an 8.78% CAGR from 2023 to 2031. Satellite imaging integrates with other technologies such as IoT, sensors, GIS, and decision support systems, allowing farmers to make more informed planting, fertilizing, irrigation, and harvesting decisions. It also helps farmers detect patterns, abnormalities, and future problems [4][27].

3.3.7 Geographic Information System (GIS) and mapping technologies

Geographic information systems and mapping technologies are transforming global agriculture by harnessing sophisticated technology to increase production and sustainability. A geographic information system in SA is a technology framework that collects, analyzes, and visualizes spatial and geographic data related to agricultural fields and activities. It is utilized in SA to understand field variability better and enhance resource utilization [4]. It comprises (1) remote sensing, GPS technology, and field sensors for data collection, (2) spatial analysis and predictive modeling for data analysis, (3) mapping and dashboards for visualization, and (4) precision farming and risk management to support decision-making and help farmers and agricultural experts to make informed decisions. The GIS market was valued at US$8814.84 million in 2022 and is expected to reach US$14210.1 million by 2028, expanding at an 8.28% CAGR over the forecast period. Farmers employ GIS applications to collect, organize, and analyze geographical data on soil types, elevation, yield history, and previous weather trends on their farms, allowing them to make data-driven decisions [6].

3.3.8 Global Positioning System (GPS)

According to Naidoo and Munga [17], a GPS is a satellite-based navigation system that enables farmers to accurately position, time, and collect real-time data from precise locations anywhere to improve farming practices. In SA, GPS provides exact position data via satellite signals. The GPS market is expected to be worth US$94.25 billion in 2023 and US$417.56 billion by 2033, growing at a CAGR of 16.10% between 2024 and 2033. GPS receivers mounted on tractors, drones, agricultural machinery and equipment, and handheld devices receive signals from several satellites. The receiver determines

how long each satellite's signal takes to reach it. The GPS receiver employs trilateration to determine its location, which includes latitude, longitude, and altitude. Farmers may use precise position information to navigate, guide, and map their farms. It enables farmers to efficiently apply seeds, fertilizers, herbicides, insecticides, and water to specific areas and improve farming activities [82].

3.3.9 Fifth-Generation (5G) communication technology

The advent of 5G mobile communication technology within IoT-WSNs has transformed the agriculture industry by lowering costs and increasing crop and livestock resource use. In SA, 5G communication technology is the latest advancement in mobile network technology established in 2017 with promising features such as high throughput, low latency, high reliability, increased scalability, and energy efficiency to boost agricultural technology and information through seamless connection, data exchange, and operation among sensors, actuators, farm machinery, people across the agricultural value chains, and facilitate real-time analysis [4][45][77][83]. The global market value for 5G technology is estimated at US$5.53 million in 2020 and is expected to reach US$667.79 billion by 2026 [84]. The 5G communication technology provides for remote and rural connections, giving farmers access to technology and services. It enables the deployment of IoT sensors and devices, as well as drones and UAVs with sensing capabilities, to gather agricultural data from above and speed up the use of big data in SA [85-89]. It enables 5G-connected farm robots to execute precise and efficient harvesting, watering, and fertilization, and farmers to track and control live crop attacks using 5G sensors and GPS technology [86][90].

3.3.10 Cloud computing

Implementing IoT and WSN technology in SA has permitted the collection of massive amounts of agricultural data, posing storage issues. The agriculture industry has significantly grown its use of cloud computing due to its infrastructure, platforms, software, hardware, and storage services. According to Nitin and Gupta [43], cloud computing in SA is an Internet-based infrastructure that provides software, storage, infrastructure, and platforms via wireless communication to improve agricultural practices through better data management, analysis, and real-time decision-making. It stores, processes, and analyzes vast data generated by agricultural technology, such as IoT sensors, drones, machinery and equipment embedded with GPS and other sensors, and satellite imagery [17]. The global cloud services revenue in 2021 was US$340.4 billion and is predicted to rise to US$768.5 billion by 2026, rising at a CAGR of 17.7% between 2021 and 2026. Cloud platforms utilized in SA include Google Earth Engine, Akasai, IBM Bluemix, Microsoft Azure, Amazon Web Services, and Alibaba [17]. Cloud computing provides scalable storage and processing capacity to analyze and process IoT agricultural data on remote servers, allowing scalability and accessibility [46][75][77]. It provides low-cost data storage for agricultural applications, helps farmers improve agricultural practices, allows smart farms to access resources continuously, and connects external and internal services to create an intelligent and advanced marketplace [43].

3.3.11 Blockchain technology

Blockchain technology is transforming the SA industry by increasing the transparency, efficiency, and security of agricultural transactions and data management by documenting transactions across a network, allowing for more effective and sustainable smart farming practices. Blockchain in SA entails using decentralized, immutable, distributed ledger systems to record encrypted transactions in a chain of blocks, track assets via a secure global corporate network, and improve agricultural practices ranging from supply chain management to farm management [65][91]. It comprises a growing collection of documents called blocks securely linked together in a consistent chronological sequence using hash values. Each block contains transaction information, such as the sender and recipient information, transaction size, timestamp, and hash value of the previous block. The timestamp confirms that the transaction data was present when the block was generated. The blocks efficiently create a chain because each contains information about the previous block, making them interconnected. Therefore, once a transaction has been recorded, it cannot be deleted or modified without the users' consensus, thus creating an immutable ledger that tracks data records. Blockchain seeks to reduce the involvement of third parties like banks and brokers in transactions [91]. The worldwide market value of blockchain in the food and agricultural business is predicted to be US$140 million in 2020, with a projected growth of US$1.5 billion in 2026. Ethereum, Hyperledger Fabric, Corda, IBM Food Trust, and VeChain are popular blockchain technologies utilized in SA to record, store, and distribute agricultural data [92]. Blockchain technology is used in SA to improve transparency, traceability, reliability, and efficiency across agricultural processes and increase mutual trust among supply chain parties [65][75]. Crucial data, such as soil health, weather patterns, and agricultural yields, may be stored immutably via blockchain, providing farmers and other industry participants with a dependable source of information. It can automate the process while creating confidence among all parties involved [91-93].

3.3.12 Digital twins

Digital twins have emerged as a significant opportunity for SA by accurately depicting agricultural objects and processes, simulating future scenarios, and introducing new farming technologies for efficient and sustainable agriculture. According to Escribà-Gelonch et al. [94], Kalyani et al. [95], and Tagarakis et al. [96], a digital twin in SA is a virtual representation of physical agricultural systems, processes, or objects that uses real-time data from the physical entities to simulate, monitor, optimize, and forecast real-world agricultural operations resulting to increased efficiency, productivity, and sustainability.

Agricultural data is collected by digital twins using sensors, drones, satellites, and IoT devices implanted in farms, livestock, and agricultural machinery. The acquired data is sent to a central database or cloud platform for processing using big data analytics, AI, and machine learning. The digital twins market is estimated to be worth US$10.1 billion in 2023 and US$110.1 billion in 2028, rising at a 61% CAGR throughout the forecast period [96]. The technology has altered SA techniques by simulating farming cycles such as soil conditions, irrigation, fertilization, weather patterns, crop growth, nutrient management, and insect infestations and using real-time data to improve decision-making [8] [97-100].

3.3.13 Big data analytics

Big data analytics is a transformational approach to SA, employing enormous datasets and powerful analytical tools to improve agricultural practices and comprehend data-intensive agricultural processes for decision-making. According to Otieno [101], big data analytics in SA refers to the processing and analysis of massive agricultural datasets using modern analytical tools to improve farming operations. The global market value of big data analytics in agriculture is estimated to be US$817.57 million in 2021 and is expected to reach US$1709.17 million by 2031, growing at a CAGR of 7.65% between 2021-2031. Big data analytics in SA begins with gathering agricultural data from IoT devices and sensors, drones and UAVs, satellite imaging, weather stations, agricultural machinery, and market information. Data from numerous sources is integrated into a single dataset and is then cleaned, formatted, and merged to guarantee consistency and usability. The massive amounts of data are stored in cloud-based data lakes or warehouses, making them scalable and easily accessible. The data is then processed and analyzed, and the results are displayed in charts, graphs, and maps to help farmers see and understand trends and patterns. Predictive analytics is applied to the collected dataset, using machine learning and weather forecasting models to analyze historical data and predict future outcomes (e.g., crop yields, pest infestations, and disease outbreaks) and weather conditions to assist farmers in planning their activities. Prescriptive analytics uses optimization algorithms and decision support systems to prescribe appropriate planting periods, irrigation schedules, and fertilization programs and provide farmers with actionable information and recommendations for effective resource management. Precision farming, crop monitoring and management, and operational efficiency are then decided upon and implemented [20][46][75]. Farmers and agronomists use the extracted meaningful insights to improve agricultural operations, increase crop yields, reduce costs, optimize irrigation and fertilization, understand soil conditions and pest infestations, minimize environmental impact, and identify trends for better decision-making [4][46][75].

3.3.14 Additive manufacturing

The advent of additive manufacturing, also known as three-dimensional (3D) printing, is transforming the agricultural sector by enabling reverse engineering and increasing the availability of physically reconstructed models. This technique has enabled designers to create complicated components, highly configurable products, and effective waste minimization. Ganetsos et al. [102] and Lakkala et al. [103] define 3D printing as an emerging computer-controlled innovation that rapidly fabricates 3D solid objects such as products using a digital computer-aided design file by adding materials layer-by-layer. The technologies include 3D printing, 3D scanning, and customized and standalone applications [104]. The worldwide additive manufacturing market was valued at US$23,841.25 million in 2021 and is expected to reach US$ 82,556.49 million by 2027, growing at a CAGR of 23.0% over the forecast period. Additive manufacturing contributes to SA by enabling the creation of sophisticated, customizable components and equipment on demand. 3D-printed sensors and devices are used in agriculture, water security, food processing, and food handling [105]. 3D printing technology has increased the adaptability of agricultural sensors and supports healthy, sophisticated, sustainable farming. The potential function of 3D printed sensors in food security, including food safety and quality monitoring, is to offer consistent access to healthy, inexpensive food [105].

3.3.15 Agricultural biotechnology and genetic engineering

Agricultural biotechnology and genetic engineering are emerging as beacons of hope in SA, using modern technologies to boost agricultural output, efficiency, and sustainability. Agricultural biotechnology refers to the use of scientific tools and techniques such as genetic engineering, molecular markers, biofertilizers and biopesticides, molecular diagnostics, vaccines, and tissue culture to modify and improve plants and animals, reduce chemical input dependency, improve pest and disease resistance, and increase nutritional value [66][106][107]. Genetic engineering in agriculture refers to biotechnology to deliberately modify an organism’s genetic material, Deoxyribonucleic Acid, to add desirable traits or qualities that increase crop production. The goal is to develop crops and livestock with desired characteristics such as increased growth rates, agricultural nutritional value, and pest resistance. The global agricultural biotechnology market is valued at US$38,918.85 million in 2023 and will increase to US$66,646.82 million by 2030, with a CAGR of 9.38% between 2023 and 2030. Genetic engineering and biotechnology enable the development of crops that can tolerate abiotic challenges, including drought, salinity, and severe temperatures. Genetically modified crops represent the most crucial advancement in agricultural biotechnology. These crops have been modified to increase yields, boost nutritional content, and resist pests and diseases, lessening the need for chemical pesticides and fertilizers [4][18][46][106].

3.3.16 Renewable energy solutions

Renewable energy solutions in SA entail combining clean energy technology with innovative agricultural methods to increase production, sustainability, and efficiency. Renewable energy sources like solar, solid biomass, wind, geothermal, renewable natural gas, hydropower, ocean resources, biogas, and liquid biofuels minimize reliance on fossil fuels while minimizing environmental damage [75][108]. The worldwide renewable energy market was estimated at US$856.08 billion in 2021 and is predicted to reach US$2,025.94 billion by 2030, with a 9.6% CAGR between 2022 and 2030. The demand for electricity in SA has risen due to agricultural technology, such as electric tractors and agricultural robots, and renewable energy has the potential to be integrated into agricultural activities to give a more sustainable alternative [108]. Renewable energy solutions are frequently modular and adaptable, allowing farmers to increase energy output as necessary, which improves agricultural operations' resilience, providing a reliable energy supply even in remote or off-grid places [109]. In SA, renewable energy applications include distributed electricity generation, hybrid energy systems, greenhouses, solar dryers, space cooling and heating, biochar production, saltwater desalination, wind-powered water pumps, solar-powered irrigation systems, soil heating, agricultural product drying, solar-powered agricultural machinery, bioenergy, and farm robots. These applications increase agricultural operations' efficiency and sustainability while reducing farming activities' environmental impact [108].

3.3.17 Smart Agriculture applications

Smart agriculture apps transform agricultural practices by providing real-time monitoring and predictive analytics and automating agricultural management systems through cutting-edge technologies such as IoT, data analytics, machine learning, and remote sensing. These smart agricultural apps are digital solutions integrating current technology, such as data analytics, IoT devices, machine learning, and cloud computing, to improve farming methods and boost efficiency, production, and sustainability. The apps use data from sensors, drones, GPS devices, and weather stations to give farmers helpful information [17][27]. The global market value for precision farming software was US$1.48 billion in 2023 and is expected to reach US$4.03 billion by 2032, increasing at a CAGR of 12.0% between 2023 and 2032. Crop management, livestock management, soil and irrigation management, farm management systems, weather forecasting, data analytics, and decision support are among the key features of smart agricultural applications [27][110]. Some of the most prominent smart agricultural apps include Cropio, FarmLogs, AgriWebb, FarmLogs, Trimble Ag Software, CropX, and John Deere Operations Center. The SA platform enables agricultural experts to process data quickly and adjust their actions in real-time by recommending the most profitable planting plan based on crop rotation, historical data collected from satellite images, and technical recommendations for growing specific crop types [4][17]. The apps let farmers access real-time data, monitor field conditions, and remotely manage farm operations [82]. It helps farmers analyze data, monitor field conditions, manage resources, and plan activities like planting, harvesting, and irrigation [5][27][110].

3.3.18 Artificial Intelligence

Artificial intelligence is revolutionizing SA through learning capabilities to provide multidimensional agro-intelligent solutions, increasing productivity and transforming the delivery and management of agricultural practices. Zhang and Qiao [74] and Hua et al. [111] define AI as the field of computer science that simulates human-like intelligent behavior and critical thinking in devices to make them intelligent and efficient for performing tasks that need skilled human intelligence. In SA, AI uses mathematical logic and computing programs to analyze vast historical agricultural data to discover valuable insights that help make farm decisions. The market value of AI in the global agricultural sector is expected to reach US$1.7 billion in 2023 and rise to US$4.7 billion by 2028 [73]. Smart agriculture uses AI through big data analytics, robots, IoT, sensors, cameras, drone technology, and Internet connectivity on geographically distributed fields [74]. Farmers use AI-driven solutions to predict agricultural production potential, enhance resource allocation, monitor crop health, detect crop diseases, monitor animal health, and reduce the risks associated with unexpected environmental circumstances. Robotic harvesters with AI-powered sensors can detect ripe crops, pick fruits and vegetables, and sort products based on size, shape, and quality criteria, increasing efficiency and product quality [66][112-114]. In SA, machine learning algorithms such as decision tree, k-nearest neighbor, CatBoost, Gaussian Naive Bayes, K-means, random forests, support vector machine, neural networks, ensemble models, and artificial neural networks are used for plant disease classification, facilitate real-time insights and recommendations for proper agricultural decision-making, examine the effects of heat stress on livestock and milk yield, predict rainfall, and analyze soil conditions, detect weed, pest and disease identification, aid in crop yield prediction, nutrient deficiencies identification, time-series forecasting, crop health monitoring, automate tasks such as fruit picking, guide precise agriculture procedures, enhance smart farming irrigation, and enable farmers to make educated decisions regarding planting schedules, crop rotations, and pest control techniques [115-118]. Fig. 4 summarizes the emerging technologies used in SA.

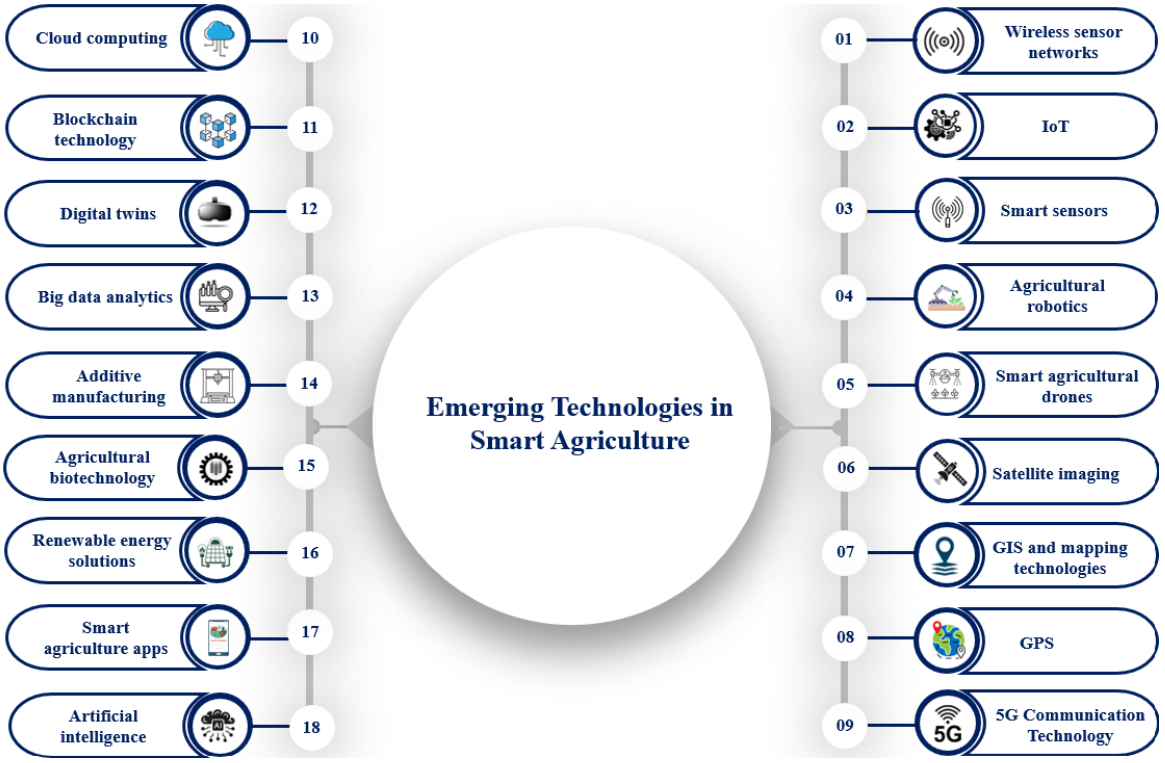

Fig. 4. Summary of the emerging technologies used in SA.

3.4 Application of Smart Agriculture

Smart agriculture applications vary in terms of agricultural systems, techniques, operations, and procedures. It falls into several areas, including:

3.4.1 Monitoring climate conditions

Monitoring climatic conditions is one of the most vital and challenging procedures for attaining optimal production in SA [119]. Continuous weather pattern monitoring is required to organize future occurrences [71]. Smart sensors can help gather real-time weather and climate data. Farmers can use a detailed estimate to determine their crop requirements. The IoT system delivers notifications for any odd changes in environmental parameters, allowing farmers to take preventative steps [40][120]. These systems use a variety of sensors, including temperature, humidity, wind speed, water level, and precipitation gauges, to collect detailed information about the current weather conditions, which is critical for planning planting, harvesting, and disease management [4], anticipating changes in weather patterns, and optimizing planting schedules, irrigation plans, and pesticide applications. Integrating weather monitoring systems into SA platforms boosts resilience to extreme weather events, increases resource efficiency, and promotes sustainable farming practices by aligning agricultural operations with present and predicted weather conditions. It helps reduce the dangers of inclement weather [27]. Weather forecasting improves activity organization, reduces expenses, and increases yields and profits in agriculture [71][121].

3.4.2 Environment and field monitoring

Agricultural ecosystems are monitored and managed using sensors, satellite imaging, drones, and data analytics. Environmental monitoring technology keeps track of environmental factors and field conditions to maintain a favorable agricultural development environment. Several parameters such as temperature, humidity, soil, and water content are constantly monitored; remote sensing technologies employ electromagnetic radiation and measure the reflected radiation. Drones primarily collect geospatial data, perform GIS mapping, and capture high-resolution photos for crop and field analysis. Sensors installed in fields assess soil moisture, temperature, pH, and nutrient content, providing significant information about soil health and fertility. Farmers improve their irrigation and fertilizing operations by monitoring soil conditions over time, ensuring optimal soil conditions for plant development while reducing environmental effects [120]. Environmental monitoring in agriculture is crucial for enhancing crop yields, guaranteeing resource sustainability, and mitigating the consequences of climate change and farming-related environmental harm. It contributes to the quality and

amount of irrigation water; crop diseases and pests are being monitored for their existence and spread, allowing pesticides to be used more effectively and helping to determine the impact of air quality on crop health [80].

3.4.3 Crop health monitoring

Crop health monitoring enables early identification of diseases and pests and agricultural yield optimization, hence decreasing resource usage and encouraging environmental responsibility. It is critical for food security, ecosystems, and economies [71][122]. Crop monitoring is critical for efficient management and higher productivity. Temperature, humidity, soil moisture content, pH, and nutrient concentration can all be detected using different sensors. For automated crop monitoring to be effective, a thorough understanding of the cost-benefit ratio is required to assess whether the system provides overall profits on a given farm [121]. Robots and UAVs with thermal or multispectral sensors continually monitor crop and soil conditions. This facilitates the administration of fertilizer spray and regulated watering. Crop monitoring approaches analyze remote sensing-derived indications by comparing crop status to previous or typical seasons. The more complex functionalities available through automated field management include automated data acquisition, processing, monitoring, decision-making, and management of farm operations, such as crop yields, profits, losses, farm weather prediction, field mapping, and soil nutrient tracking [82].

3.4.4 Precision agriculture

Precision agriculture is a farming strategy that uses technology to increase agricultural yields and efficiency [66]. It is a comprehensive implementation of intelligent concepts and technological applications in agricultural production to achieve accuracy in farming operations, infrastructure intelligence, and industrial development modernization. Precision agriculture employs satellite imaging, GPS, sensors, drones, and other cutting-edge technology to aid management and decision-making and accurately monitor and control crop, soil, and environmental conditions. It extensively uses statistics and information to improve crop quality, yields, and the efficient use of agricultural resources. This enables farmers to administer inputs like water, fertilizer, and insecticides more properly, decreasing waste and environmental impact while increasing yield [1][42][123]. IoT soil sensors and GPS-guided tractors allow farmers to gather instant data on soil conditions, allowing for improved irrigation and fertilization program management [20]. They enable farmers to accurately detect the amount of water, fertilizer, pesticides, and other resources while lowering costs [120]. Remote sensing can help optimize agricultural inputs, increase crop productivity, and reduce waste. It is used for crop monitoring, irrigation management, accurate fertilizer distribution, disease and pest control, and crop yield estimates. The deployment of UAVs has increased the efficiency of remote sensing. Remote sensing technology provides optimum agricultural practices by delivering correct information, which leads to more effective and ecologically friendly farming methods, stressing its importance in precision agriculture. Integrating WSN with UAVs increases crop monitoring, agricultural yields, production modeling, future projections, and decision-making effectiveness [80]. Precision agriculture allows for the early diagnosis of plant diseases and nutritional deficits, facilitates monitoring of various aspects, including crop irrigation, optimal planting phases, and harvesting, and delivers reliable crop status information, which may be obtained from ground and air sources [80].

3.4.5 Livestock and poultry monitoring and management

Livestock management in agriculture is caring for and managing domesticated animals to produce meat, milk, eggs, and other byproducts. It includes fundamental husbandry, animal health and nutrition, pasture management, organic farming, economic sustainability, and sustainable food systems. Livestock management in SA seeks to make agricultural operations more productive, efficient, and sustainable via IoT-enabled technology [44][124]. IoT agricultural sensors may be mounted on farm animals to track their health, movement, and location. It will assist farmers in identifying sick animals and implementing preventive steps to limit their spread. It also reduces labor expenses since the animals may be monitored remotely [40][120]. It provides real-time data monitoring such as breeding status, growth cycle, feeding cycle, and livestock and poultry condition, which can be analyzed to provide insights that help develop more appropriate breeding programs. IoT agricultural sensors can also be integrated with automated equipment to automate feeding and other activities, reducing labor costs while improving cattle and poultry breeding. It can also monitor the chicken buildings' temperature, air quality, and other environmental data. Monitoring the body temperature of individual livestock and poultry allows for satisfactory regulation of the poultry house environment and animal health [125]. Wearable sensors and GPS trackers linked to animals capture data on activity levels, eating patterns, and vital signs, allowing farmers to spot disease or distress early and respond quickly. Automated feeding systems and environmental sensors improve animal comfort and resource efficiency in livestock operations [20][120]. Wearable sensor technologies enable remote management of individual animals, allowing emergency interventions and reacting to time- and labor-intensive problems more efficiently [3]. A wearable collar or tag equipped with sensors tracks the animals' position, temperature, blood pressure, and heart rate, and the data is wirelessly communicated to farming machines almost quickly [66][121].

3.4.6 Greenhouse automation

Greenhouses guarantee the plant's safe growth in a controlled environment where characteristics such as soil moisture percentage, temperature, wind, and sunshine may be adjusted manually or automatically. As a closed building, greenhouses protect plants from unfavorable outside weather conditions such as severe wind, hailstorms, ultraviolet radiation, and insect or pest infestations. The IoT can help fully or partially self-automate the greenhouse [121]. A smart greenhouse can be built utilizing IoT by installing sensors and motors that automatically monitor and modify climatic conditions based on the plants' demands. Adopting this new farming system will automate several processes, including opening and shutting windows, changing the cooling and heating system, and turning on and off light bulbs [126]. Sensors in an IoT-based greenhouse measure and monitor humidity, mist, carbon dioxide levels, ultraviolet intensity, pH and electrical conductivity values, water nutrient solution level, temperature, lighting, pressure, and pesticide quantity for more effective detection and diagnosis. The smart greenhouse has enabled farmers to undertake fieldwork without human inspection while protecting plants from hailstorms, winds, ultraviolet radiation, and bug and pest attacks [82][120]. The IoT improves yield in smart greenhouses by enabling proportional control systems that use sensors to create a controlled environment for the crops they produce. The system is monitored remotely, and data is processed using cloud servers [40].

3.4.7 Smart irrigation systems

According to Gyamfi et al. [20], Pang et al. [42], and Xu et al. [54], smart irrigation systems are highly automated advanced solutions that use data-intensive approaches to optimize water usage through IoT sensors and real-time data analysis. These systems use advanced technologies like IoT, soil moisture sensors, weather-based controllers, wireless connectivity, data processing, fault detection, irrigation control, and intelligent controllers to optimize water usage and ensure efficient and effective irrigation [42][54]. Intelligent irrigation systems rely on sensors, including temperature, moisture, and ultrasonic, which may monitor water level, soil moisture, weather, and plant conditions to use valuable water. These sensors are wirelessly deployed, battery-powered, and have little processing capacity. Based on the sensory data, an actuator is deployed to monitor the weather, soil conditions, vaporization, and plant water usage to alter the irrigation timetable to match the actual site circumstances. Smart irrigation controllers automate irrigation procedures by integrating data from soil moisture sensors and meteorological stations. Aerial systems also monitor soil and moisture content with drone cameras or low-Earth-orbit satellites [4][20]. The goal of irrigation systems in an intelligent agriculture system is to track water requirements so that water flow can be actuated based on collected data and data analytics without human intervention. Smart irrigation technology can reduce costs, increase productivity, improve water efficiency, lower energy costs for water pumps, adjust watering schedules to meet plant needs, and preserve plant health and quality [3][20][50][120].

3.4.8 Crop monitoring

Smart agriculture uses modern technology and data analytics to monitor crops and improve their health, productivity, and management. Crop management is the use of various technologies such as sensor networks, satellite imagery, remote sensing, and data analytics to track and manage crop health, growth, and yields throughout their lifecycle, as well as to improve resource efficiency and ensure sustainable farming practices [19][80]. It uses remote sensing (satellite imagery and drones), IoT sensors (soil sensors and weather stations), GPS and GIS technology, data analytics and AI (predictive analytics and machine learning), field scouting (mobile apps, smartphones, and tablets), and automated machinery (tractors, harvesters, and robots) to give real-time or near-real-time data, helping farmers to identify agricultural issues early [53][80]. This real-time information about the field also aids in timely interventions and improved crop management. It allows farmers to make data-driven decisions to boost crop productivity, resource efficiency, and sustainability in contemporary agriculture [19][80]. Crop monitoring is critical in SA because it helps farmers make precise decisions, conserve resources, increase agricultural output, detect problems early, maximize crop yield, and save costs. It ultimately empowers farmers to make data-driven decisions while minimizing environmental impact [127].

3.4.9 Pest and disease management

Pest and disease management in SA involves using modern technology and data-driven tactics to identify, monitor, and control crop and animal threats more efficiently and sustainably. Remote sensing and imaging, wireless sensors, field scouting, mobile apps, data analytics and AI, automated systems, and robotics are the emerging technologies developed to identify and manage crop pests and diseases through real-time monitoring, modeling, and disease forecasting, thereby increasing overall effectiveness over traditional pest control procedures [71]. Wireless sensor network systems gather and store data on a cloud platform using network protocols, enabling early decisions to avoid pest and agricultural diseases [50]. The IoT in disease management enables farmers to accurately detect, identify, and prevent diseases in agricultural areas and farms, lowering expenses and preventing diseases from spreading prematurely [120]. Plant disease diagnosis improves crop output and food security while lowering agricultural economic losses [80]. Smart insect traps utilize sensors to detect pest activity in the field [4]. IoT-based automated traps collect, count, and describe bug kinds before uploading

the data to the cloud for further study. Early detection and rapid response, crop damage minimization, chemical pesticide reduction, improved crop health, resource conservation, ensuring sustainable and efficient agriculture, cost efficiency, data-driven decision-making, increased agricultural productivity, and environmental stewardship by fostering sustainable practices are all advantages of innovative pest and disease management [122].

3.4.10 Fertilizer management

Fertilizer management in SA employs modern technology to improve fertilizer delivery, ensuring crops receive nutrients appropriately. This strategy boosts crop yields, lowers expenses, and reduces environmental impact. It employs soil sensors to monitor soil moisture, pH, temperature, and nutrient levels in real-time. A thorough chemical examination of soil samples is carried out to evaluate nutrient deficits and soil composition. GPS and GIS mapping are used to generate precise maps of fields to determine differences in soil qualities and crop requirements. Variable rate technology allows farmers to modify the quantity of fertilizer applied in various areas of a field depending on soil and crop data. Drones and satellites assist in gathering photographs and data to analyze crop health, growth phases, and nutritional requirements. Farmers can use the normalized difference vegetation index to determine plant health and biomass and then apply fertilizer. The software systems then evaluate data from sensors, satellite images, and weather forecasts to provide fertilizer application recommendations. Fertilizer management in SA provides better efficiency, cost savings, higher crop yields, and environmental protection [50].

3.4.11 Intelligent agricultural machine

Intelligent agricultural machines in SA are modern equipment and systems that employ numerous technologies to enhance farming methods. These technologies include AI, machine learning, IoT, robotics, and automation. Some intelligent agricultural machines include autonomous tractors and machinery, drones and UAVs, robotic harvesters, precision planters and seeders, smart irrigation systems, automated weeding machines, livestock monitoring systems, soil, and crop sensors, data analytics and farm management software, and supply chain and logistics automation [57]. The objective is to boost efficiency and productivity, reduce costs, increase crop yields, promote sustainability and environmental protection, enable data-driven decision-making, improve soil health and fertility, improve crop and livestock management, traceability and transparency, climate change adaptability, economic growth, and food security.

3.4.12 Smart harvesting

Intelligent harvesting uses innovative technologies to transform the crop collection process in the agriculture industry. Harvesting is the process of collecting ripe crops from fields. Smart harvesting refers to using advanced technologies to automate and optimize gathering crops. Smart harvesting incorporates developing technology like IoT devices, AI, robots, and data analytics. Internet of Things sensor devices collect real-time soil moisture, temperature, and humidity data. The sensors connect via networks, allowing smooth data flow between devices and central systems. Artificial intelligence algorithms analyze data collected by IoT sensors to make informed decisions about the best time to harvest, while machine learning models predict crop readiness and yield based on weather patterns, growth stages, and market conditions [4][120][127]. Autonomous harvesting machines like robots equipped with computer vision and AI can identify ripe crops, pick them precisely, and sort them based on quality [2][43][53]. Smart harvesting maximizes agricultural yields, boosts efficiency, improves crop quality, lowers harvesting labor costs, guarantees sustainability, decreases waste, and improves decision-making [120].

3.4.13 Soil management

Soil is essential in agriculture because crop output is directly proportional to soil quality. Healthy soil is one of the most vital components of a productive agricultural system. As the primary source of nutrients, soil stores water, nitrogen, phosphorus, potassium, and proteins required for optimal crop growth and development. Soil management can mitigate unfavorable elements such as pollutants and pathogens through remote monitoring of soil characteristics such as moisture, temperature, pH value, electrical conductivity, and nutritional content [19][71]. Soil health monitoring is a thorough and lengthy procedure that includes frequent assessments and analyses of many soil characteristics and indicators to determine the soil's overall fertility, structure, and biological activity [80]. Soil management uses modern technology and data-driven methodologies to improve soil health, fertility, and production. These technologies include soil sensors, remote sensing, GPS, GIS, data analytics, soil mapping, data analytics, machine learning algorithms, and automated machinery and robots [4][43][80]. Soil management is crucial because it improves crop yields, soil health, resource efficiency, environmental sustainability, informed decision-making, boosts crop productivity, cost savings, risk management, sustainable land use, soil structure, biodiversity conservation, nutrient management, regulatory compliance, adaptation to climate change, and informed decision-making for farmers and land managers [80].

3.4.14 Crop yield prediction

Crop yield prediction is the application of modern technology and analytical methodologies to anticipate the quantity of crop output in a given area. This method uses a variety of data sources and computer tools to create accurate and timely predictions, which assists farmers, agronomists, and policymakers. Crop yield prediction depends on various factors and situations, including climate, soil condition, seed variety, and fertilizer application [43]. Crop yield prediction has several advantages, including increased efficiency, maximizing crop quality and production, driving marketing initiatives, improving crop management, increasing productivity and sustainability, optimizing resource allocation, and increasing profitability [2].

3.4.15 Weed management

Weed control is a big challenge in modern agriculture since weeds compete with crops for light, water, nutrients, and space, leading to agricultural output losses. Smart agriculture requires integrating contemporary weed management and control approaches with cutting-edge technologies [2]. Nitin and Gupta [43] define weeds as undesired plants that develop spontaneously in a particular environment. Weed management is adopting cutting-edge technology and strategies to effectively manage and minimize weed growth and impact while limiting the use of pesticides and manual labor in agricultural settings. Global positioning systems, remote sensing, and drone technologies precisely monitor, and map weed infestations, allowing farmers to treat particular regions rather than administering herbicides evenly over whole fields. Data from sensors, satellites, and field observations are used to forecast weed growth trends and optimize control tactics. Machine learning and AI systems can aid real-time weed management decisions. Robots and autonomous machinery outfitted with mechanical weeders can locate and eliminate weeds without hurting crops, reducing the demand for chemicals and physical labor. Sensors and imaging technology can identify weeds early in their life cycle, allowing for prompt action before they establish and harm agricultural production [19][81].

3.4.16 Water management

According to Kassim [124] and Victor et al. [80], water management uses modern technology and methods to give the proper amount of water to crops and animals at the right time, thus increasing production and conserving natural resources. Soil moisture sensors assess soil moisture content in real-time, allowing irrigation schedules to be adjusted to minimize overwatering or underwatering. Water management platforms collect and analyze data from various sources to improve water consumption and resource management efficiency. Decision support systems assess sensor data, weather predictions, and other inputs to suggest water management techniques [43][71]. Water management provides numerous benefits, such as helping farmers understand the physical and chemical composition of the water, improved water efficiency, increased crop yields, saving costs, ensuring sustainable water usage, adaptation to climate change, reduced labor requirements, improved soil health, better decision-making, increased resilience, greater food security, and promoted sustainable agriculture [80][120].

3.4.17 Agricultural product quality and safety traceability

Integrating intelligent technology for agricultural product quality and safety traceability has become critical in the rapidly evolving agricultural landscape. Smart agriculture uses advanced technologies like the IoT, blockchain, cloud computing, and data analytics to monitor, document, and manage the whole agricultural product quality and traceability process. Agricultural product quality and safety traceability refers to the methods and technology used to track and document agricultural production, processing, and distribution. This traceability guarantees that the products are safe and of high quality and can be traced back to their source in case of a food safety incident. Blockchain technology provides a secure, immutable ledger for tracking every supply chain step, whereas cloud computing stores and analyzes massive amounts of data gathered from numerous sources. Laboratory testing analyzes soil, water, and product samples to ensure that safety criteria are met. Certification and audits ensure that items adhere to specified quality and safety requirements. Radio-frequency identification and QR codes allow items to be tracked from farm to table [2][43][80]. Agricultural product quality and safety traceability provide numerous benefits, including improved food safety, quality control, increased consumer trust, regulatory compliance, supply chain efficiency, environmental sustainability, improved data utilization, risk management, and competitive advantage [125]. Fig. 5 summarizes the application of SA.

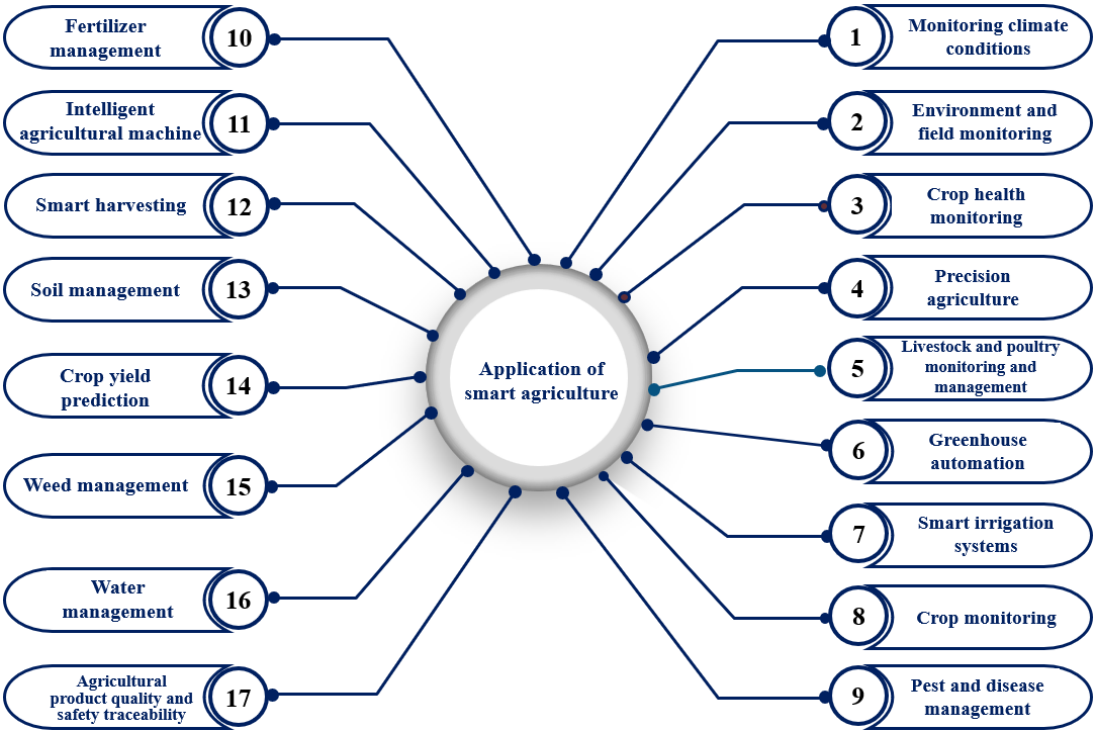

Fig. 5. Summary of the application of SA.

4. CYBER THREATS AND CHALLENGES IN SMART AGRICULTURE

Emerging technologies expose smart agricultural ecosystems to various cybersecurity threats and vulnerabilities. Some of the numerous cyber security threats in SA are:

4.1 Data privacy concerns

Data privacy is a serious issue due to the growing integration of digital technology in agriculture. Smart agriculture collects vast amounts of sensitive data, including crop conditions, livestock health, weather patterns, soil quality, machinery performance, and operational details to improve agricultural productivity and efficiency. This raises farmers' concerns about unauthorized access to, collection of, and sharing of their farm data with third parties by agricultural technology providers. Privacy violations might discourage farmers from adopting new technology, harming numerous stakeholders, the government, and the general public [128]. As this data is obtained, issues concerning who has access to it and how it is utilized become increasingly important [129]. Leakage of such data by unauthorized access or by an insider might pose a threat. For example, disclosing information about agricultural anti-jamming devices can enable an attacker to circumvent these security measures. Leakage of soil, crop, and agricultural procurement information can result in financial losses for farmers if rivals or unfriendly groups utilize it. Smart agriculture uses IoT technology in farms, and the appliances and sensors are typically utilized outside, making them vulnerable to physical assaults. Collecting and transmitting sensitive agricultural data raises concerns about potential security breaches or abuse [130]. Adversaries may target gateways with DoS attacks, disrupting network availability [131]. Misusing agricultural data for unintended objectives, such as targeted marketing or insurance premium changes, might result in privacy breaches. Real-world incidents concerning data privacy in SA include: (1) A prominent agricultural machinery firm, John Deere, has received intense scrutiny for its data policy. The company's equipment gathers detailed data on machine performance, crop yields, and other parameters. Farmers have expressed worry about who controls the data and how it is utilized. Farmers often realized that John Deere's conditions permitted the firm to access, use, and share their data, raising concerns about potential abuse and loss of control over their agricultural information; (2) Deere & Co., another key participant in the agricultural machinery business, has drawn criticism for its plans to monetize farmers' data. Farmers were afraid that their information might be sold to third parties or used to manipulate market circumstances in ways that would hurt their interests, and (3) Farmobile, a provider of data services to farmers, was entangled in a court battle with a former employee over data ownership. The dispute revolved around whether data gathered on farms belonged to the farmers or the firm. This disagreement highlighted the legal difficulties regarding data ownership in agriculture and the importance of explicit, enforceable agreements.

4.2 Data breaches and leakages

As SA evolves, the threat of data breaches and leaks remains a significant worry. The growing use of digital technology in agriculture has sparked worries about data breaches and leaks. Malware, ransomware, and other cyber threats may be used by attackers in SA to hack sensors, drones, robots, cloud services, and farm networks, allowing them to penetrate and leak farmers' personal, agronomic, and proprietary information. Hackers can target these devices and get access to sensitive data, including crop yields, animal health records, and financial information [17][132]. Cybercriminals can use vulnerabilities or defects in smart agricultural systems to steal sensitive and secret data, such as crop models, plant breeders' rights, and IoT-generated data [133]. Confidential data leakage can occur due to farmworker carelessness or intentional data breaches by farm staff, violating confidentiality [129]. Examples of data breaches in SA include (1) vulnerabilities discovered in John Deere's software in 2021, which could allow hackers to access sensitive customer data and remotely control agricultural equipment, and (2) Climate Corporation, a Monsanto subsidiary, collects extensive agronomic data. A breach or release of this data might jeopardize farmers' competitive advantage and Monsanto's unique technology. These data breaches and leaks can have serious repercussions [130].

4.3 Malware injection attack

A malware injection attack occurs when an attacker injects malware into an attached computing device and nodes, which spreads across the system and makes it a compelling target for intruders [44][134]. Due to inadequate security standards, devices such as soil sensors, weather stations, and controlled irrigation systems are frequently used as entry sites for malware. Many IoT devices interact via wireless networks that may lack strong encryption, leaving them vulnerable to eavesdropping and injection attacks. Malware attacks include ransomware, spyware, and botnets. Malware is a prevalent threat in large-scale systems because, in most situations, it acts and propagates autonomously, making it an appealing target for attackers. The majority of these farm setups employ identical software components. As a result, malware that infects one smart farm is likely to infect others, causing a wide range of harm. Once successfully implanted, malware can damage the firmware, destroying the farm control system and causing crop rot, drought, excess fertilizer/pesticides/herbicides, and irregular crop and animal monitoring [123][132]. Many UAVs have software that enables pilots to operate them from various mobile platforms. Bad actors can utilize this software to implant malware payloads into the UAV's memory or the base station, giving attackers total control over the UAV [135]. Examples of malware injection attacks in SA include: (1) In March 2021, Agromart Group, a Canadian agricultural merchant, had a ransomware assault that halted operations. While not a direct attack on smart agricultural devices, the event disrupted the supply chain for agricultural supplies, demonstrating how ransomware may harm the agriculture industry. Similar attacks on automated farming systems might result in interrupted planting or harvesting procedures; and (2) In May 2021, JBS Foods, one of the world's largest meat processing enterprises, was targeted by a ransomware attack, briefly halting operations. This event demonstrated the vulnerability of the food supply system to hackers. If comparable attacks were launched against automated crop production systems, the consequences might be devastating, disrupting the whole agricultural supply chain. These attacks can compromise SA systems' security, integrity, and availability, leading to severe consequences [17][44].

- ***Ransomware attacks***

According to Bui et al. [22] and Naseer et al. [136], a ransomware attack involves malicious actors infiltrating the system via phishing, compromised devices, and weak credentials and encrypting critical data on SA systems, holding it hostage till a ransom, potentially disrupting planting, harvesting, and other critical operations. Many IoT devices in SA, such as sensors and automated systems, may have weak security measures, making them ideal targets for fraudsters. Agricultural businesses frequently use centralized systems to manage data from several devices. Compromising these systems can cause significant disruptions in operations. Adversaries can infect an autonomous tractor with ransomware delivered via a Trojan horse attack, giving them entire control, endangering individuals' physical well-being in the field, and affecting crop productivity and essential infrastructure [15]. Real-world examples of ransomware attacks against SA include: (1) In May 2022, a prominent agricultural machinery producer, AGCO, was targeted by a ransomware attack. It impacted production facilities, limiting the company's capacity to fulfill orders. The interruption substantially impacted the farming business, particularly during the peak planting season; (2) In 2021, a ransomware attack hit a big agricultural cooperative in the United States, interrupting activities during harvest season. The perpetrators wanted a multi-million-dollar ransom; (3) NEW Cooperative, an Iowa-based agricultural services firm, was targeted by a ransomware attack in September 2021. The attack jeopardized the cooperative's capacity to control its supply chain, which included grain, feed, and fertilizer delivery. The hackers employed BlackMatter ransomware and sought a ransom of US$5.9 million. The cooperative took systems offline to limit the attack during the vital harvest season, posing severe dangers to food supply chains. (4) The Agromart Group provides fertilizer, crop protection, seed goods, and other agricultural services in Eastern Canada. On or around 27 May 2020, Agromart Group had a Sodinokibi/Revil ransomware attack, extracting 22,328 data from their systems. When the Agromart Group refused to pay the ransom, the attackers publicized the data breach and auctioned it on the dark Web to the highest bidder [137]. The attack also caused a price drop due to excess wool on the market and generated significant

concerns about the Talman cybersecurity system [22][58]. (5) In 2019, a ransomware attack was launched against a German dairy farm's automated milking equipment. The attackers encrypt the system's data and demand a ransom for its release. The attack disrupted milk production, causing considerable financial losses and operational disruptions. This incident revealed the vulnerability of smart farm systems to ransomware attacks and the possible impact on agricultural output.

- ***Botnet***

Botnets in agricultural systems are networks of infected computers or Internet-connected devices (remote sensors) managed by a central command that might have disastrous effects [134]. Agricultural businesses that deal with drones or robots are vulnerable to these attacks, and botnet attacks commonly target agriculture equipment and semi-autonomous farming operations. A compromised IoT device has the potential to be a botnet for more sophisticated attacks, such as DDoS attacks and information theft, as well as to compromise availability and integrity, which might render the entire smart farming network unusable [134]. Botnets employ compromised devices to commit fraud or wreak havoc without the owner's knowledge or consent. Using Mirai, for instance, puts network devices at risk [138]. A botnet may breach these systems and steal confidential information for nefarious reasons, such as industrial espionage or manipulating market pricing. In SA systems, sensor data manipulation is possible through a botnet. For example, it may change temperature or moisture measurements, resulting in inaccurate pest treatment or irrigation judgments, and can cause crops to be over- or undertreated, affecting their productivity and health. A botnet may try to take over control of autonomous farming equipment, such as drones or automated tractors, in a more focused attack. As attackers take control of these devices, they may disrupt agricultural management activities and harm crops or machinery. The goal of bots is to infect IoT devices within the group by connecting to a server, commonly referred to as a "bot master," which serves as the main control center for hacked devices collectively referred to as the "Botnet of Things (BoT)" [44]. An army of zombies comprised of infected farm IoT devices can quickly breach an IoT-based agriculture system and spread to numerous other networks via various channels, impeding its operation [132]. Real-world examples include the global NotPetya malware epidemic of 2017, which severely disrupted businesses across the board, including several in the agriculture industry.

4.4 Social engineering attacks

The rising digitization and reliance of agriculture on smart technology increases the possibility of social engineering attacks. To obtain illegal access to agricultural systems, data, and processes, social engineering in SA involves manipulating people's behavior and psychology by deceiving them into installing malware or disclosing sensitive information [17]. Rather than taking advantage of technological flaws, it leverages human weakness. By sending unsolicited emails and clicking on malicious websites, attackers exploit unsuspecting farmers to get sensitive information and gain illegal access [133]. This may involve phishing, pretexting, baiting, and other deceptive tactics to get people to divulge private information or provide access to smart agricultural systems. Among the prominent social engineering attacks in SA are attackers posing as agents of prominent agricultural equipment manufacturers who have reportedly offered discounts on smart farming equipment. Under the pretense of installing equipment updates or patches, farmers and agricultural businesses have been duped into divulging personal and financial information or downloading harmful malware. These attacks have compromised confidential information and activities, resulting in monetary losses and illegal access to farm management systems.

- ***Phishing attacks***

According to Bui et al. [22], a phishing attack is a social engineering technique typically involving deceiving farmers into revealing sensitive login credentials, financial details, or access to critical agricultural systems. Phishing scams allow attackers to influence decision-making and internal operations since it is impossible to avoid this attack [17][44][139]. Phishing attacks include email, spear, clone, vishing, and smishing [55]. Phishing emails are another common threat used by hackers to infiltrate agriculture firms. Government technology cites an example where a cybercriminal imitated a vendor payment, sending an email that would funnel funds to the criminal's bank instead. Evil Twin access phishing creates a rouge access point and allows attackers to get access to farmers' credentials on IoT-based agriculture that may be compromised [132]. Real-world incidents of phishing attacks in SA include (1) In 2021, a ransomware attack via phishing emails targeted a U.S.-based agribusiness company. Employees unknowingly clicked on malicious links, leading to the installation of ransomware. This attack halted operations of automated systems for several days, affecting planting schedules and resulting in significant financial loss and reputational damage. (2) In 2018, hackers used phishing emails from the Ukrainian Ministry of Agrarian Policy and Food to target Ukrainian agricultural companies. Upon opening the malicious attachments in the emails, the recipient's computer became infected with malware. Because of the malware, attackers could steal data and perhaps interfere with agricultural activities, and (3) An agricultural supplier received a phishing email that appeared to be from one of its major clients. The email requested sensitive information and access to the supplier's inventory management system. Once access was granted, attackers manipulated inventory records, resulting

in delays and shortages in the supply chain and disrupting farming operations reliant on timely deliveries of seeds and fertilizers.

4.5 Denial-of-Service (DoS) and Distributed DoS (DDoS) attacks

Denial-of-service and distributed denial-of-service attacks in SA pose severe threats to the efficiency and dependability of automated agricultural systems. According to Padhy et al. [44], Alam [123], and Bibi et al. [138], a denial-of-service attack occurs when an adversary attempts to render smart agricultural systems inaccessible to an intended farmer by flooding it with false requests until the normal request cannot be completed. Because of security flaws, the attacker can initiate this attack via the Web or a subsystem [44]. A distributed denial-of-service attack occurs when cybercriminals flood a target SA system, server, or network with fake Internet traffic from multiple sources that the system cannot handle, causing it to slow down, crash, or become inaccessible [129][140]. In the context of SA, these attacks can target IoT devices, sensors, control systems, and data storage and management systems, and adversaries can use DDoS attacks to disrupt service and then insert fraudulent data, potentially compromising food safety, agri-food supply chain efficiency, and agricultural production [24]. Because a farm has numerous interconnected nodes, IoT devices may be utilized to conduct large-scale DoS attacks at any time [58]. Network infrastructure vulnerabilities, such as routers and gateways, may also be used to execute DoS attacks, resulting in massive disruptions. When DoS attacks target centralized control systems that manage diverse agricultural activities, they become single points of failure [55][71]. These attacks can disrupt the normal operations of numerous units within a single agricultural operation; nevertheless, they can also disrupt legitimate cyber services in various domains [136]. Distributed denial-of-service attacks necessitated botnets of previously exploited agricultural systems, such as IoT devices, and deployed smart and autonomous agricultural machinery, which can be controlled by a command-and-control server known as the “zombies” [133]. As a result, farms equipped with smart devices become part of this “zombie” network, risking losing control over their resources. When an attacker uses several infected devices to undertake DDoS attacks, such as flooding botnet requests across smart farming servers or routers, numerous services may become unavailable [22]. Denial-of-service attacks on servers housing SA historical data logs and other agricultural advisory systems would keep smart farmers unaware of timely insect infestation prevention measures [141]. In the smart farming field, an attacker can halt greenhouse operations from accessing any agricultural service by jamming the network or spamming agri-apps with phony requests; therefore, the lack of availability of the offered services can create disruption and potentially loss of consumer confidence and income [63][133]. Examples of DoS attacks in SA include (1) On 6 November 2022, Maple Leaf Foods, Canada’s most enormous, prepared meats and poultry producer, revealed a system outage caused by a cybersecurity issue. The corporation took rapid action but noted that “complete recovery of the outage would take time and result in some operational and service delays” [137]; and (2) WATTPoultry, a Canadian agri-food media outlet, predicted that the DoS attack on the corporation would cost at least CA$23 million. This estimate was based on the financial data from the company’s fourth quarter of fiscal year 2022, which showed a net loss of CA$ 41.5 million [137]. (3) A DDoS attack includes flooding a cloud-based agriculture management platform with traffic, leaving it momentarily unreachable and affecting farm operations. The hostile deployment of disruptive behavior extends to agricultural robots and actuators, causing operational downtime [15].

4.6 Man-in-the-middle (MitM) attacks

According to Alam [123], Bibi et al. [138], and Sarowa et al. [139], a man-in-the-middle attack in SA is a cyberattack in which an attacker intercepts and potentially alters the communication between two parties, such as sensors, actuators, and control systems, without either party being aware that the communication link has been compromised. It is typically accomplished via unsecured wireless networks, where the communication path is insufficiently secure. It can result in packet capture, allowing unauthorized users to access information from the insecure communication channel. Once the attacker has access, they may quickly escalate their privileges and acquire access to the system to perform unauthorized modifications without the users’ knowledge [55]. These attacks might target the system’s secrecy or integrity [134]. Real-world examples of MitM attacks in SA include (1) In 2022, attackers launched a MitM attack against tractor telemetry systems in the United Kingdom, capturing and manipulating real-time data sent between the tractor and farm management software. This tampering resulted in erroneous data logging, disrupting autonomous farming operations; (2) In 2021, a security evaluation found MitM attacks on precision agricultural sensors in Canada, which might intercept and modify data from moisture sensors. This alteration resulted in inaccurate watering recommendations, affecting crop health and output; (3) In 2020, attackers launched a MitM attack against greenhouse management systems in the Netherlands. By intercepting and manipulating sensor data, they might change ambient variables such as temperature and humidity, negatively influencing plant development.

4.7 Replay attacks

In SA, a replay attack occurs when an adversary intercepts and maliciously re-transmits legitimate data or commands across agricultural network devices or systems [22][123]. This attack leverages flaws in communication protocols or security mechanisms to perform unauthorized operations or acquire control of the vulnerable machine. Sensors in a smart agricultural system collect data on soil moisture, temperature, humidity, and other environmental variables. This information is wirelessly transferred to a central control system for processing and decision-making. The attacker intercepts genuine data packets or commands sent between equipment or systems in the smart agricultural infrastructure. This interception can occur in various ways, including eavesdropping on wireless conversations and intercepting data across the network. Using the collected data, the attacker resends or replays these packets or commands to the target system, potentially producing erroneous readings or driving the system to take inappropriate actions. Because the data seems authentic and comes from reputable sources, the system may handle it without detecting malicious intent [22]. Real-world examples of replay attacks in SA include (1) In 2020, a security investigation of precision agricultural systems in the United States discovered weaknesses that may be exploited via replay attacks. Attackers might use GPS signals to misguide autonomous tractors, resulting in inefficient farm operations and significant crop loss; and (2) In 2019, researchers showed a replay attack on greenhouse climate management systems, modifying temperature and humidity settings. The attack caused inadequate growth conditions, affecting agricultural productivity.

4.8 Eavesdropping attacks

Eavesdropping attacks in SA entail the illegal interception and listening of communication or data exchanged between IoT devices, sensors, and systems in the agricultural environment. Different connection technologies linking different nodes on the smart agricultural network and wireless networking that transmits unencrypted data render these systems vulnerable to data breaches. Such attacks can jeopardize data confidentiality and have a wide range of severe implications. Eavesdropping attacks often begin with the attacker identifying prospective targets inside the smart agricultural system, such as sensors, controllers, or communication hubs. The attacker investigates the communication protocols utilized by the target devices to determine how data is conveyed. Wireless interception requires the attacker to be within range of the wireless signals. This might include being physically close to agricultural fields or facilities. The attacker needs access to the wired network infrastructure to conduct network sniffing, including physical infiltration or exploiting network vulnerabilities. The attacker captures transmitted data using packet sniffing tools, radio frequency capture equipment, or compromised devices. Data is collected and processed to derive relevant information such as sensor readings, operational directives, and sensitive agricultural data. The attacker collects sensitive data about agricultural operations, including crop health indices, soil conditions, and proprietary farming practices. The attacker might exploit the collected data to control or disrupt agricultural activities, such as changing watering schedules or tampering with automated machinery. Real-world broad instances and scenarios demonstrate the possibility of eavesdropping attacks, such as: (1) In 2017, researchers showed how easily drones might be intercepted and controlled. They demonstrated that the communication between the drone and its controller may be intercepted and controlled. Agricultural drones that monitor crop health and deliver treatments are vulnerable to similar attacks, with intercepted communications potentially leading to data theft or operational problems; and (2) In 2016, a cyber-attack on a water treatment facility in the United States entailed listening in on unencrypted communications between control systems. The attackers can monitor and alter water treatment operations. Similar eavesdropping tactics might intercept communications between irrigation systems and control units in SA, causing possible disturbances.

4.9 Insider attacks

Insider attacks in SA are security breaches or malicious activities carried out by individuals or entities with authorized access to SA systems, networks, or data within the agricultural technology infrastructure who abuse their privileges for malicious purposes [22]. These attacks can come from employees, contractors, suppliers, or any other trusted entity within the business that has been provided access to firm data and systems, resulting in unlawful access, data theft, and network exploitation. Employees can use their privileged access to the agritech system to steal or manipulate data [17]. It can significantly affect agricultural operations, data integrity, and overall system security [22][55][142]. Insider attacks in SA include data theft and unauthorized access, sabotage and data manipulation, intellectual property theft, unlawful transactions, insider espionage, and credential theft and misuse. The perception layer of IoT-based SA is particularly vulnerable to insider attacks, which can introduce eavesdropping interferences by inserting an external agent in disguise [55]. Real-world examples of insider attacks in SA include (1) In 2022, an insider with access to pest control systems in a smart agricultural setting changed the schedule and dose of pesticide sprays. This alteration impacted pest management efficacy and may have increased pest resistance; (2) In 2021, an insider event in smart irrigation systems resulted in an employee manipulating irrigation schedules and settings without authority. This prohibited conduct resulted in poor water distribution, causing crop stress and yield decline; and (3) In 2020, an employee with access to

livestock monitoring devices purposefully corrupted the data collecting procedure. This move interrupted animal health and activity monitoring, which might jeopardize animal welfare and agricultural output.

4.10 Supply chain attacks

Supply chain attacks in SA encompass malicious operations that target many components of the agricultural supply chain, such as farm equipment and software, as well as data management systems. Suppliers may accidentally incorporate vulnerabilities into hardware, software, or firmware components that attackers can use to compromise the entire system. Potential vulnerabilities in SA supply chains include IoT devices, sensors, software, firmware, data management systems, supply chain components, and third-party vendors and suppliers. An attack on farm equipment and fertilizer providers might damage critical equipment at a critical time. It can alter the amount of nutrients in fertilizers, causing crops to suffer rather than thrive. The supplier's security flaws, such as vulnerability to phishing attempts and the theft of privileged credentials, represent a danger to protecting sensitive information. These vulnerabilities can propagate across the organization's processes and systems, mainly if they originate at the start of the supply chain [71]. Hackers targeting agritech supply chains with lower security might get access to more sensitive data, eventually reaching their intended target [17]. If a third-party attacker disrupted the operation of an existing smart agricultural system, food security would be jeopardized, and the equipment manufacturer's reputation would suffer [143]. While supply chain attacks in SA have not garnered as much attention as those in other sectors, there have been incidences that show the vulnerabilities in this industry, such as (1) The 2021 ransomware assault on JBS, the world's largest meat processing business, exposed flaws in the food supply chain. Such catastrophes can impair food supply and agricultural activities; and (2) In 2021, a cyberattack targeted a major seed distributor, interrupting operations and delaying seed deliveries to farmers. The hack impacted the agricultural input supply chain, exposing weaknesses in essential components of SA.

4.11 Side-channel attacks

A side-channel attack in SA refers to indirect information leakage from a system to collect sensitive data or disrupt its functioning. These attacks do not target the system's primary communication channels or direct data pathways, instead relying on ancillary features like power consumption, electromagnetic emissions, or timing information [123][134]. Side-channel exploits the physical features of the hardware, software, or communication media to harvest sensitive information from the target device's internal working and operation [57]. It can jeopardize the integrity, confidentiality, and availability of data and agricultural management and automation systems. A successful side-channel attack may expose private keys, contaminating sensitive data such as agricultural production estimates, livestock data, sensor data, and meteorological information [22]. Side-channel attacks may represent a hazard to SA in the following scenarios: (1) An attacker positions a power monitoring device near a soil moisture sensor. By studying power usage patterns, they determine moisture levels and adjust the watering schedule to disturb agricultural growth. This can result in inappropriate watering, compromising crop health and productivity; and (2) An attacker utilizes electromagnetic analysis to intercept and decode orders delivered to automated farming equipment, including tractors and irrigation systems. This allows the attacker to change or disturb the device's operation, resulting in operational inefficiency or damage.

4.12 Advanced persistent threats (APTs)

Advanced persistent threats in SA are sophisticated, targeted cyber-attacks that obtain and keep illegal access to an agricultural organization's systems and networks for a lengthy period without detection [134]. These attacks are frequently carried out by well-funded and competent opponents, such as nation-states, organized criminal organizations, and hacktivists, to steal sensitive data, disrupt operations, or cause economic and environmental harm. Advanced persistent attacks provide one of the most severe challenges to smart farming and precision agriculture since they encompass nearly every level of the cyber-kill chain. Most APT attacks on smart farming and precision agriculture aim to get covert, long-term access to food chain and production network data. Advanced persistent threat organizations want to strike critical targets, including greenhouses, animals, and smart farms. They rely on sophisticated tactics to achieve their objectives, including zero-day vulnerabilities, phishing attacks, and social engineering [134].

4.13 Radio-frequency jamming attacks

Radio-frequency jamming attacks are the purposeful interruption of communication signals between IoT devices, sensors, and control systems. Such attacks can interrupt a smart farm's routine operations by blocking or significantly weakening wireless connections required for monitoring and managing agricultural activities. Radio-frequency jamming attacks pose a substantial danger to SA, which increasingly relies on wireless communication for various applications such as sensor networks, automatic irrigation systems, drone surveillance, etc. It can interfere with these communications, potentially leading to breakdowns in crucial agricultural operations. Attackers utilize radio frequency jammers, devices that broadcast powerful radio signals at the same frequency as the targeted communication channels, drowning out genuine messages. Smart agriculture systems frequently use

wireless communication protocols such as Wi-Fi, Bluetooth, Zigbee, LoRa, and cellular networks. Each of them uses specific frequency ranges that jammers can target. Radio-frequency jamming attacks in SA fall into four categories: constant, deceptive, random, and reactive. The rapid growth of the 5G network increases vulnerability to jamming attacks, particularly in mobile sensor networks. Intermittent GPS signal loss at Harbin airport due to a jamming attack at a pig farm highlights the risk of hackers repurposing such devices, as the jammer was originally used to prevent criminal gangs from dropping disease-infected packages onto the herd, forcing farmers to sell contaminated meat at a lower price [22]. Attackers may jam global navigation satellite systems (GNSS) for malicious objectives by placing several distributed low-power jammers to disrupt GNSS across large areas, preventing smart farming equipment from operating correctly [123]. Signal jamming, particularly radio jamming, poses a significant risk to agriculture by disrupting vital systems such as remote imagery for crop monitoring, GPS for precision agriculture, and communication devices for collaboration. As a result of this interruption, location may be inaccurate, data collection may be halted, communication may be disturbed, and there is a risk of damage or loss [136]. Notable instances and case studies demonstrating radio-frequency jamming attacks in SA include a California research center subjected to repeated radio-frequency jamming attempts aimed at smart agricultural research projects in a reported occurrence. The institution employed a variety of wireless technologies to monitor experimental plots, including soil moisture sensors, weather stations, and controlled watering systems. The jammer attacks caused periodic data loss and system malfunctions. The study team used spectrum analyzers to determine the jamming frequencies and sources. They also improved their communication infrastructure by using more robust protocols and implementing redundancy in essential systems.

4.14 Rogue device deployment attack

A rogue device deployment attack in SA involves introducing illegal devices into the agricultural IoT network to disrupt operations, steal data, or inflict other harm. These rogue devices can impersonate regular devices, intercept or modify messages, or inject malicious payloads into the system. These attacks use flaws in network security, physical access restrictions, or supply chain management to introduce devices capable of disrupting operations, stealing data, or jeopardizing the integrity of agricultural processes. These attacks include illegal access and device introduction, data interception and manipulation, operational interruption, malware introduction, malicious intent, stealth, and persistence. In agricultural IoT network setups, an attacker may install illegal sensing equipment and clone the already infected sensing device to capture critical information and connect it to other network nodes [123]. An intruder adds harming nodes into the automated agricultural field, disrupting the system's smooth operation. This attack might be initiated by seizing a node and replicating it, and it is often intended to alter or modify data-shuttered devices and programs [44][132]. While fewer recorded occurrences of rogue device deployment in SA may exist, specific pertinent examples and scenarios demonstrate the potential threats. (1) Drones can be used to place unapproved devices in fields. For example, a drone may drop a rogue sensor or communication device into a field to intercept or manipulate data transmitted by legitimate sensors, and (2) Rogue devices may be inserted into smart tractors or harvesters during production or maintenance. These gadgets might serve as a conduit for malware, allowing attackers to take control of machines, interrupt operations, or steal critical data.

4.15 Sensing device capture attack/Node tampering

Sensing devices play an essential role in SA by collecting data on environmental conditions, crop health, and other aspects. However, these devices are susceptible to attacks and interruptions, including capture attempts, node manipulation, and jamming. A capture attack occurs when an adversary intercepts and eavesdrops on communications between sensing devices and the central control system. This can jeopardize sensitive data such as agricultural production forecasts, environmental conditions, or patented farming methods [123]. Node tampering is sensing devices' physical or software modification to change their operation or obtain sensitive data. For example, an attacker may tamper with soil moisture sensors to provide misleading readings, resulting in improper irrigation choices and significant crop damage. In SA, sensing device capture attacks and node tampering are defined as unlawful physical access to sensors or nodes in the agricultural IoT network. These attacks seek to interrupt the system's regular operation, steal data, or initiate malicious activity. Smart systems designed for small or big farms may include equipment located outside. Many of these gadgets lack tamper-resistant enclosures since doing so would be prohibitively costly. The absence of tamper-resistant enclosures exposes the device to interactions with external agents such as people, animals, or agricultural equipment. Farm equipment, such as a tractor, may strike the device, causing temporary or permanent physical harm and resulting in data corruption, unavailability, or device damage. Hacking IoT sensors and manipulating the data they gather can impact the broader decision-making system and disrupt the entire food supply chain [139]. Node capture or outages pose a considerable danger to agricultural sensor networks and IoT systems, leading to poor resource management, reduced agricultural yields, and financial losses [55][136]. A node capture compromises the system's integrity and may interfere with decision-making [22]. Real-world cases of sensing device capture attacks/node tampering in SA include: (1) In 2019, researchers carried out a simulated attack on an intelligent greenhouse to investigate the vulnerabilities of IoT devices in agriculture. They showed how attackers may physically acquire and tamper with sensors to change environmental data such as temperature and humidity, resulting in

poor growth conditions and crop loss; and (2) According to allegations from 2017, Israeli agricultural fields were targeted by cyber-attacks to interrupt irrigation systems. Attackers modified data from soil moisture sensors, resulting in over- or under-irrigation, which affected agricultural output and quality.

4.16 Spoofing attack

A spoofing attack in SA involves an adversary deceiving a system or device into accepting false data by impersonating a valid source. Spoofing in wireless sensor network nodes is sometimes accomplished by producing a clone of a legitimate node and accessing the network as an impostor [55]. It can impair IoT devices, sensors, and automated system functions, resulting in faulty decision-making. The three types of spoofing attacks in SA are GPS spoofing, sensor spoofing, and network spoofing. Data sent from a drone to a central controller in SA can be intercepted and altered. Several trials have shown how easily this weakness may be exploited, allowing bad actors to control the drone entirely [135]. Some real-world instances of spoofing attacks in SA are: (1) Researchers at the University of Virginia discovered that GPS signals used by autonomous tractors might be faked, causing the gear to operate erroneously. The trials demonstrated how an attacker might mislead the tractor into taking erroneous tracks, possibly causing agricultural damage, resource waste, and even endangering neighboring personnel or animals; and (2) In 2019, cybersecurity researchers exposed the vulnerability of autonomous farm machinery to GPS spoofing. They ran tests on an autonomous tractor, successfully deceiving its navigation system by broadcasting bogus GPS signals. The tractor diverted from its intended course, resulting in crop loss, ineffective field coverage, and significant safety risks if such attacks were carried out purposefully.

4.17 Agroterrorism

Agroterrorism in SA is the deliberate use of biological agents, chemicals, or cyber-attacks by adversaries to disrupt agricultural operations, cause economic loss, impair public health, and instill fear and uncertainty. Adversaries can utilize viruses, bacteria, fungi, and insects to harm crops, animals, and humans and transmit infectious diseases and influenza [133]. An easy agroterrorism strike might ruin any smart farm’s ambition to be a dependable food provider, weakening supply chain confidence [71]. Attackers use IoTs to hurt or persuade many to distrust or disrupt IoT-enabled agriculture. Many IoT-based agriculture systems will fail, and the increased pesticide supply from smart sprinklers can impact food quality [132]. Real-world incidences of agroterrorism in SA are very uncommon. However, there have been prominent cases and examples, such as (1) In 2021, JBS, the world's largest meat processing corporation, was hit by ransomware, forcing it to close its facilities in the United States, Canada, and Australia. The hack interrupted meat supply routes, resulting in significant financial losses and exposing weaknesses in the food supply system; and (2) Ukraine has seen multiple cyberattacks on critical infrastructure, especially the agriculture industry. These attacks were intended to disrupt supply systems and cause economic instability. The attacks highlighted agricultural systems' vulnerabilities to cyber warfare, which terrorists may use to disrupt food production and delivery.

4.18 False data injection attack

A false data injection attack in SA entails an attacker intentionally inserting incorrect data into agricultural data collection and processing systems via compromised sensors, IoT, and other network devices to disrupt operations, manipulate outcomes, or cause harm [22]. Adversaries carry out fake data injection attacks using various means, including sensor manipulation, network penetration, software exploitation, and physical tampering. This can jeopardize the integrity and honesty of data utilized in decision-making, negatively impacting agricultural operations and outcomes. The attack aims to flood smart agricultural systems with fake data. Feeding false telemetry data from compromised IoT devices to IoT-based systems would result in inaccurate analytics and choices, causing complete disruption and wasting time and resources [133]. High voltage grid Passover can generate a strong electromagnetic field in vast fields that might harm IoT-based agriculture devices and cause distortion or data corruption. With IoT-based agriculture, the accuracy of the data is compromised, and the farmer receives incorrect updates about the farm; agriculture productivity needs to be improved due to a lack of prompt response [132]. False data injection attacks target data integrity [134].

4.19 Signature wrapping attacks

In SA, signature-wrapping attacks exploit flaws in handling digital signatures to change or fabricate data without invalidating the original signature. This can be accomplished by exploiting deficiencies in implementing XML Signature, JSON Web Tokens (JWT), and other secure communication protocols. These attacks could undermine the integrity and validity of data exchanged between numerous components in SA, including sensors, actuators, control systems, and cloud services. The attack might have severe ramifications in SA, where data integrity and authenticity are critical for automated decision-making and system operations. A sensor in a smart agricultural system collects soil moisture data and sends it to a centralized control system. The data is wrapped in an XML document that has been digitally signed to ensure validity. An attacker intercepts the XML document during transit. The attacker replicates the signed <SensorData> element and wraps it in a new unsigned <Wrapper> element. The

attacker changes the unsigned portion of the document to incorporate fake soil moisture data. The control system validates the signature using the original signed <SensorData> element, which remains intact and valid. However, the control system interprets the harmful text from the unsigned section of the document, resulting in improper irrigation choices. Signature-wrapping attacks attempt to modify the message structure of a signature without invalidating it. Attackers might try signature-wrapping attacks by modifying sensor data from the farm within the messages [22].

4.20 Reconnaissance attacks

Reconnaissance attacks in SA involve gathering information about agricultural systems, networks, and devices to uncover possible weaknesses that might be exploited in future attacks. Such attacks are typically the initial stage in a bigger cyberattack plan, with the attacker aiming to fully understand the target environment before initiating more invasive acts such as data breaches, DoS attacks, or other malicious activities. Reconnaissance attacks may be passive or active. Passive reconnaissance involves attackers listening to unencrypted communications between devices and systems without actively interfering. This can provide insights into data flows, device interactions, and system setups. Attackers employ tools to search for open ports and services operating on networked devices, which can assist in discovering possible access points and weaknesses. Attackers get information by leveraging human factors, such as duping workers into disclosing sensitive information or utilizing publicly available data from social media or websites. During active reconnaissance, attackers transmit packets to devices and systems to determine their replies, settings, and vulnerabilities. This may involve port scanning, banner grabbing, and vulnerability scanning. Actively engaging with devices allows attackers to detect and exploit weak security setups, obsolete software, and other weaknesses. Reconnaissance attacks acquire information about a target. The information gathered can then be utilized to carry out a targeted attack against a device or network. Reconnaissance attacks include packet sniffing, ping sweeping, port scanning, phishing, social engineering, and Internet information searches [138]. Examples of reconnaissance attacks in SA include a smart farm that connects IoT sensors and automated equipment over a wireless network. Devices on the network include soil moisture monitors, weather stations, irrigation controls, and autonomous tractors. An attacker scans the farm's wireless network with tools such as Nmap or Angry IP Scanner, looking for active IP addresses and open ports. The attacker lists the services operating on the detected devices, seeking common ones like Hypertext Transfer Protocol, Secure Shell, and Message Queuing Telemetry Transport. By examining the services and ads, the attacker determines the types and models of devices in use and their firmware versions. The attacker thoroughly maps the farm's network, noting vital equipment and potential access points. With knowledge of device kinds and firmware versions, the attacker may look for known vulnerabilities and organize targeted attacks.

4.21 SQL injection attacks

SQL injection attacks occur when an adversary injects malicious SQL code into input fields, allowing them to modify database searches and obtain unauthorized access to data or even compromise the entire farm system [129][140]. It exploits application software vulnerabilities by manipulating input fields to insert malicious SQL code into the application's database queries [22][132]. Smart agricultural systems frequently use databases to gather, store, and analyze data from various sources, including sensors, weather stations, and automated machinery. If these systems are not adequately protected, attackers can use SQL queries to obtain unauthorized access to the database, change data, or execute arbitrary instructions. SQL injection vulnerabilities can majorly affect SA, as several sensors, controllers, and databases are linked together to govern agricultural operations. A robust SQL injection attack might corrupt or change agricultural data, posing a significant danger to IoT devices, particularly those utilized in agriculture [136]. Real-world examples of SQL injection threats in SA include. In 2018, Agrisync, a software platform for agricultural service providers, faced a security problem involving a SQL injection attack. The attack targeted Agrisync's online application weaknesses, possibly exposing sensitive client information to unauthorized access.

4.22 IoT breaches

Internet of Things breaches in SA are security events in which IoT devices and systems used in agricultural contexts are infiltrated by hostile actors. Many IoT devices in SA lack strong security measures and may have default passwords, unencrypted communication, or out-of-date firmware, leaving them open to attacks such as illegal access, data breaches, or manipulation. Smart agriculture IoT breaches include illegal access, data manipulation, DoS attacks, ransomware attacks, and supply chain vulnerabilities. Attacks on a precision farm's IoT network might interrupt the services supplied, coordination, and communication throughout the farm. The botnet, buffer overflow, malware, DDoS, DNS spoofing, and Phantom attacks are some threats that target IoT networks [144]. Several prominent occurrences and research on IoT breaches in SA include: (1) In 2020, ransomware attacks targeted agricultural enterprises, notably those that use IoT devices for precision farming. Attackers encrypted crucial data and demanded ransom payments to regain access. Such attacks can hinder agricultural operations by rendering critical data and control systems unavailable, resulting in financial losses and delays in farming activities; and (2) In 2018, a water management system used in agriculture was hacked, allowing attackers to control irrigation schedules and water distribution. This vulnerability

illustrated how hackers might inflict considerable crop harm by manipulating water delivery patterns, such as overwatering or depriving crops of required irrigation.

4.23 Malicious hardware injection

Malicious hardware injection in SA is the purposeful insertion of compromised hardware into the agricultural system to inflict harm, disrupt operations, or steal critical data. It can be carried out by supply chain compromise, physical access, interception and replacement, unauthorized peripheral devices, backdoor implants, wireless interception, and electromagnetic interference. This attack can seriously compromise smart agricultural systems' integrity, availability, and confidentiality, which rely significantly on networked equipment and sensors to function efficiently. If attackers have direct access to physical agricultural products, recovering system control becomes considerably more difficult, including the optical distortion of cameras in autonomous equipment and the destruction of IoT sensors used for monitoring duties [133]. Real-world instances of malicious hardware insertion in SA include (1). In 2021, the US Department of Homeland Security researched the possibility of agro-terrorism, including introducing harmful hardware into agricultural systems. The study identified situations in which hacked technology may be utilized to disrupt food production and distribution channels. The study focused on the national security consequences of malicious hardware injection in agriculture, such as economic and social instability caused by interrupted food supply. (2) In 2020, Purdue University completed detailed security research on numerous IoT devices used in smart farming. The investigation discovered that many devices are vulnerable to hardware manipulation and malicious software insertion. The findings highlighted the importance of using tighter security measures when developing and deploying IoT devices in agriculture to prevent malicious hardware infiltration and assure data integrity.

4.24 Autonomous system hijacking and disruption

Autonomous system hijacking and disruption in SA are malevolent operations that attempt to manipulate or disrupt the autonomous systems that handle various agricultural processes. These systems include robots, drones, automated machines, and IoT gadgets that require little human interaction [132]. Cybercriminals can hijack and impair autonomous systems in SA using tactics such as GPS spoofing and jamming, illegal remote access, malware infections, insiders, remote access exploits, and IoT vulnerability exploitation. Several farming tasks employ autonomous technologies, such as drones and robots. Drones may spray pesticides and fertilizers, while robots might help with weeding and disease detection. If malevolent actors take over an autonomous system, including tractors, robotics, and drones, they can remotely operate and use farm equipment without permission. This attack might have various consequences, including the system's inability to fulfill a task, complete damage, or crop damage [44][132][139]. Real-world examples of autonomous system hijacking and disruption in SA include: In 2020, a cyber-attack attacked Israeli water management systems, including agricultural irrigation systems. The assailants sought to increase the amount of chlorine in the water supply. Although the attack targeted more extensive water management infrastructure, it demonstrated the possibility of similar attacks on automated irrigation systems in agriculture, which might result in agricultural loss and environmental degradation.

4.25 Unauthorized Access

Smart agriculture uses networked devices and systems, such as IoT sensors, drones, and automated machinery, to increase efficiency and productivity. However, this interconnectedness creates weaknesses that unauthorized parties can exploit. Unauthorized access in SA is defined as accessing agricultural systems, data, or physical assets without sufficient authority. It can be caused by network intrusion, data breach, control system compromise, or physical access, and attackers can get unauthorized access to agricultural systems, data, or physical assets by hacking, social engineering, insider, weak authentication, and malware. Several agricultural methods, however, employ gateways with minimal or no access restrictions [44]. Attackers can impersonate verified individuals and infiltrate the smart farming system. Unauthorized access to this system may result in severe consequences such as data loss, alteration, unavailability of settings, device disconnections, or even the destruction of the smart agricultural agriculture system [55][63]. Real-world examples of illegal access in SA include (1) The FBI’s Cyber Division said that a feed milling firm that provides agricultural services had two cybersecurity incidents in February 2022. In this case, an unauthorized actor accessed the firm’s system, but the company recognized and stopped the efforts before encryption could occur [137]. (2) In 2019, a ransomware outbreak struck a dairy farm in Germany. The breach aimed at the farm’s automated milking equipment, encrypted its data and demanded ransom for it to be released. The attackers used system weaknesses to obtain unauthorized access. The attack hampered milk production, causing significant financial losses for the farm.

4.26 Backdoor attack

A backdoor attack in SA occurs when hackers inject hidden backdoors into agricultural technology's hardware, software, or communication systems to obtain illegal access to, control over, or manipulation of critical agricultural infrastructure. These backdoors can then acquire unwanted access, control, or data from the farming systems. Backdoor attacks in SA can take several

forms, including compromised software updates, communication protocol vulnerabilities, insider threats, physical tampering, supply chain attacks, remote exploitation, and social engineering. Real-world examples of backdoor attacks in SA include (1) In a 2020 study, Purdue University researchers did a complete security audit of IoT devices in agriculture. They discovered vulnerabilities, such as backdoor access points and unsafe communication routes. Attackers might use these vulnerabilities to obtain unauthorized access to IoT devices in SA systems, jeopardizing data integrity and system security. (2) In 2017, cybersecurity experts uncovered severe flaws in John Deere tractors, including weaknesses that might allow remote access to control systems.

4.27 Sybil attacks

A Sybil attack in SA occurs when a malevolent party creates many phony identities or nodes inside an agricultural network to obtain an unfair advantage, disrupt operations, or alter data. The attacker injects several fake sensor nodes into the network. These nodes may look authentic, but the attacker controls them. The attacker gets control of existing devices and causes them to function as several independent nodes. Fake nodes give inaccurate data, such as soil moisture levels, temperature, and humidity, resulting in poor decision-making. Sybil nodes can outvote genuine nodes in networks that rely on consensus, such as blockchain-based systems, disrupting the consensus process. Fake nodes can use network bandwidth and power resources, causing inefficiencies and higher operating expenses. Overloading the network with traffic from several bogus nodes might render authentic nodes unable to connect correctly. Fake nodes can capture sensitive data from authentic nodes, potentially resulting in privacy breaches and theft. This attack can seriously weaken the confidence and functioning of a distributed system, such as those used in precision farming, IoT-based monitoring, and self-driving agricultural machinery. These attacks have severe effects because they can modify data, interrupt processes, or trick the system into doing dangerous activities. It allows many requests from the same identity to be approved, resulting in a 51% attack [123].

4.28 Black-hole attack

A black-hole attack in SA is a security vulnerability in which hostile nodes in a WSN falsely present themselves as having the best route to a specific location. When other nodes submit data packets through this rogue node, the packets are intercepted and discarded, interrupting the connection between genuine nodes. The rogue node claims to have the quickest or most efficient path to the target, deceiving genuine nodes into routing their packets via it. The attacker exploits flaws in routing protocols such as Ad hoc on-demand distance vector and dynamic source routing to spread false route information. Once the data packets pass via the rogue node, they are captured. The rogue node discards (drops) any incoming packets rather than sending them to their intended destination [123]. Real-world examples of black-hole attacks in SA include: (1) An attacker inserts a black-hole node into the communication network of autonomous tractors. Control commands are routed through the malicious node, which drops them, causing the tractors to operate erratically or cease to function, resulting in operational delays, potential machinery damage, and increased maintenance costs; and (2) A malicious node in a network of soil moisture sensors falsely advertises itself as having the shortest path to the data aggregation point. It subsequently discards all the data packets it receives, resulting in inadequate moisture data collection, erroneous irrigation schedules, overwatering or underwatering crops, and, ultimately, lower yield.

4.29 Cloud computing attacks

Cloud computing attacks in SA are hostile actions that target cloud-based systems and services used to manage agricultural data and operations. Smart agriculture relies on cloud computing for data storage, processing, and analysis, making it susceptible to cyber-attacks. Cloud computing attacks in SA include data breaches, DoS attacks, MitM attacks, malware, account hijacking, insider threats, and vulnerable interfaces. It exploits cloud resources and may abuse cloud capabilities like auto-scaling and on-demand service. False statistics supplied by the cloud regarding the farm may prevent the farmer from making well-informed and timely decisions [132]. Internet service providers or wireless connections connect the cloud to the gateway. Interrogating a gateway allows a network attacker to create fake cloud requests. The attacker may utilize these requests to modify precision agriculture parameters, influence inquiries for sensitive services, or interpret system data. The Sensor-Cloud paradigm is vulnerable to various attacks, such as cloud data theft, DoS/DDoS attacks, wrapping attacks, and MitM attacks [133]. Real-life instances of cloud computer attacks in SA include: In 2017, Amazon Web Services (AWS) had a significant outage in its S3 storage service, which impacted various websites and services that used AWS infrastructure. Cloud service outages, whether caused by technical problems or deliberate attacks, can impact smart agricultural systems that use cloud platforms for data storage and processing.

4.30 Cloud data leakage

Cloud data leakage in SA is the illegal exposure or disclosure of sensitive agricultural data housed in cloud-based platforms. As SA depends more on cloud computing for data storage, processing, and analysis, data leakage becomes a severe threat. This data may contain sensitive information regarding crop health, soil conditions, farming methods, financial transactions, and proprietary

technology. Misconfigured access controls, insider threats, cyber-attacks, and third-party services can all result in cloud data leaks in SA. The consequences of such data breaches are serious since they can result in competitive disadvantages, operational interruptions, and a loss of confidence among stakeholders [44][132].

4.31 Physical attack

Physical attacks in SA are purposeful activities that aim to harm or disrupt the physical infrastructure of smart agricultural systems. Physical tampering with IoT devices, such as sensors or automated machinery, can disrupt operations, alter data, or cause equipment failure, resulting in financial losses or safety risks. Common physical attacks in SA are hardware tampering, communication network disruption, physical attacks on data centers and control units, vandalism, theft, sabotage, interference with automated systems, environmental damage, and animal interference [44][63]. Real-world instances and examples of physical attacks in SA include (1) In 2020, a series of thefts targeting agricultural machinery, including tractors and other equipment, took place in rural regions of the United Kingdom. Thieves targeted critical equipment left unguarded in fields and storage facilities. Farmers experienced financial losses due to stolen equipment and operational interruptions during important farming seasons. (2) In 2019, claims surfaced of purposeful tampering with irrigation infrastructure in rural Australia. This included damage to pipelines, valves, and pumps, which was thought to be driven by disagreements over water access and usage rights. Farmers reported water shortages, crop stress, and yield decreases due to damaged irrigation systems.

4.32 Artificial intelligence attacks

Artificial intelligence attacks in SA involve exploiting vulnerabilities or manipulating AI-powered systems and algorithms to disrupt or compromise agricultural operations. It includes data poisoning, adversarial attacks, model evasion, model theft, DoS attacks, privacy breaches, and manipulation of recommendations [133]. Machine learning models make intelligent decisions in the smart farming infrastructure sector. However, machine learning is subject to adversarial attacks, which mislead the model and force it to make attacker-intended predictions. Poisoning attacks target the machine learning model's training data. The attacker inserts malicious data into the training set to alter the model's behavior while training. Evasion attacks, also known as adversarial example attacks, perturb the input data and cause the model to make incorrect predictions. The attacker may make minor changes to the input features to cause the model to make an incorrect decision. In agriculture, an evasion attempt might entail changing environmental sensor data (temperature, humidity) or satellite images to modify the model's crop health assessment or water requirements [22]. Real-world examples of AI attacks in SA include (1) In 2021, Purdue University researchers identified the susceptibility of precision agricultural systems to data poisoning attacks. They might trick AI-driven irrigation systems into overwatering or underwatering crops by inserting misleading data into soil sensors. (2) Researchers from the University of California, Berkeley, investigated adversarial attacks on AI models used in crop monitoring systems. They showed that by carefully modifying drone images, AI systems might be tricked into misclassifying healthy crops as unhealthy or vice versa. Such attacks might lead to improper agricultural management decisions, compromising crop output and quality.

- **Evasion attacks**

Evasion attacks in SA are adversarial attacks in which the attacker alters input data to avoid or circumvent security measures, protocols, or detection mechanisms to obtain unauthorized access to agricultural systems or data without raising alarms. These attacks use flaws in the design or implementation of smart farming technology, allowing malicious parties to avoid detection and carry out evil operations [140]. It may target various smart agricultural components and systems, including sensors, communication networks, and data processing techniques. To carry out evasion attacks, attackers exploit weak authentication, tamper with sensor data, change protocols, and hide harmful activity. In agriculture, an evasion attack might entail manipulating environmental sensor data (temperature, humidity) or satellite images to influence the model's crop health assessment or water needs. There have been reported instances and probable circumstances where such attacks may or have occurred, such as in 2016, the Mirai botnet utilized default credentials to infect and manipulate IoT devices, including irrigation controls and environmental sensors. The botnet conducted massive DDoS attacks, interrupting Internet services and widespread outages. The Mirai attack showed how attackers may use weak authentication protocols to hack IoT devices, including those used in SA systems.

- **Data poisoning attack**

Data poisoning attacks in SA involve manipulating the data used by agricultural systems such as sensors, drones, or AI algorithms to compromise their performance or integrity. Sensors in SA collect data on various environmental parameters, including temperature, humidity, and soil moisture. Attackers might use these sensors to give fake readings, resulting in inaccurate judgments by automated systems [140]. In SA, machine learning algorithms are frequently used to estimate crop output, identify pests, and optimize irrigation. By adding fraudulent data during training, attackers might degrade the model's comprehension and force it to make inaccurate predictions or recommendations. Many current agricultural systems are automated, with data inputs driving autonomous decision-making. By poisoning the data these systems utilize, attackers might control their behavior, resulting in suboptimal or even hazardous consequences such as inaccurate pesticide

application or wasteful water consumption. Data poisoning and sensor poisoning are the two main types of poisoning attacks. Data poisoning involves altering the data used to train or calibrate an IoT device. This can be accomplished by entering fake data into the system or changing existing data. Data poisoning is intended to cause the device to produce erroneous findings. Sensor poisoning includes messing with an IoT device's sensors. This can be accomplished by physically modifying or hacking into the sensors' software. Sensor poisoning aims to cause the gadget to gather incorrect data. Attacks using poisoning have a significant impact on IoT systems. They can cause devices to malfunction, generate incorrect data, or even let the attacker gain control of the device [92]. As machine learning becomes more widespread in everyday life, attacks such as data poisoning impair the quality and consistency of the training data on which the model is trained, affecting machine learning performance [123][144]. While data poisoning attacks in SA are a relatively recent worry, certain occurrences and research papers have revealed the possible vulnerabilities in agricultural systems, such as (1) Research released in 2021 looked at the susceptibility of machine learning algorithms used to predict crop yields to data poisoning attacks. The researchers proved that introducing harmful data into training datasets allowed them to alter the model's predictions, resulting in incorrect yield estimations. (2) In 2020, there were allegations of hackers attacking weather stations and environmental sensors to modify temperature, humidity, and precipitation data. Attackers who input fake meteorological data into agricultural systems may fool farmers into making poor decisions, potentially resulting in crop failure or financial loss.

4.33 Blockchain attacks

Blockchain attacks in SA refer to malicious actions aimed at exploiting vulnerabilities within blockchain-based systems or leveraging weaknesses in their implementation. Blockchain technology is increasingly used in agriculture for various purposes, including supply chain transparency, food traceability, and smart transaction contracts. Some possible blockchain attacks in SA include 51% attacks, Sybil attacks, smart contract vulnerabilities, and privacy and data breaches [133]. Attacks could involve falsifying data or manipulating blockchain records to misrepresent agricultural products' origin, quality, or handling practices [133].

4.34 Tracing attack

A tracing attack in SA occurs when hostile actors attempt to trace or follow the transfer of sensitive information within agricultural systems, such as crop yield statistics, supply chain records, or operational operations. These attacks can jeopardize data security, integrity, and privacy, posing several dangers and repercussions for farmers, agricultural enterprises, and the sector [134].

4.35 Protocol attacks

Protocol attacks in SA aim to exploit vulnerabilities in communication protocols used by IoT devices, sensors, and systems. These attacks target the rules and processes that govern how devices, sensors, and systems communicate and interact, posing various dangers and repercussions for agriculture operations. Some typical protocol attacks that disrupt SA include MitM attacks, protocol spoofing, DoS attacks, protocol fuzzing, protocol manipulation, and traffic analysis. Numerous attacks may be tried against the network dynamic data exchange protocol widely used in agricultural monitoring networks. Unauthorized surveillance may jeopardize the security of critical agricultural data [136]. Real-world incidents of protocol attacks in SA include (1) Attackers exploiting vulnerabilities in wireless communication protocols such as Wi-Fi, Bluetooth, or Zigbee, which are used by IoT devices to gain unauthorized access to agricultural networks or intercept sensitive data; and (2) Adversaries manipulating agricultural control protocols, such as Supervisory Control and Data Acquisition or Message Queuing Telemetry Transport, to tamper with automated farming processes or disrupt critical operations.

4.36 Measure infusion forgery

Measure infusion forgery in SA is a cyber-attack in which an attacker injects false or misleading data into the system that monitors and regulates agricultural activities. The attacker first gathers information about the agricultural system, identifying potential vulnerabilities in sensor networks, communication protocols, or data storage systems, and exploiting weaknesses such as unencrypted communication channels, poorly protected devices, or lack of authentication mechanisms, and directly accessing sensors or network devices in the field and penetrating the network through remote vulnerabilities, such as unsecured wireless communication. Data can be changed at the sensor level by interfering with the device or running malicious software. They intercept and manipulate data packets sent between sensors and central control systems and exploit software weaknesses in data processing systems to change data values. This can significantly influence decision-making processes and result in inaccurate outcomes when managing agricultural operations [44]. Real-world instances of measure infusion forgery in SA include: (1) an attacker might intercept and manipulate data from soil moisture sensors to indicate greater moisture levels than in a smart irrigation system. This might result in under-irrigation, which stresses plants and reduces agricultural output. Falsely low readings may result in over-irrigation, wasting water, and perhaps injuring the plants or soil structure; and (2) Sensors and IoT devices detect pests and diseases in crops. If an attacker

injects fake data showing a pest infestation, the system may apply extra pesticides, raising expenses and perhaps inflicting environmental harm.

4.37 Buffer overflow

A buffer overflow in SA occurs when more data is written to a buffer, i.e., a temporary storage region in memory, than it can retain. This extra data may overwrite nearby memory, resulting in unexpected behavior, system failures, or security vulnerabilities [140]. Buffer overflows are a severe risk to any computerized system, including those employed in SA, because they can interrupt operations and jeopardize security. Attackers obtain access to the corporate system by exploiting software faults and illegal usage. It causes problems for IoT-based farm systems [132].

4.38 RFID-based attacks

Radio Frequency Identification (RFID) technology is commonly utilized in SA to track and manage livestock, equipment, and crop inventories. However, RFID systems are subject to various threats, jeopardizing the integrity, confidentiality, and availability of agricultural data and operations. RFID-based attacks corrupt RFID tags and signals, resulting in replay attacks, spoofing, eavesdropping, cloning, MitM, kill tags, side-channel attacks, and illegal access. IoT-based agriculture will cease to work or be hacked by attackers or criminals [132]. Real-world examples of RFID-based attacks in SA include (1) RFID tags, widely used for livestock tracking in Australia. If attackers clone RFID tags, they can replace genuine tags on stolen animals. This gives the impression that the stolen cattle is real, aiding theft and complicated recovery attempts; (2) RFID devices are used to monitor and manage access to valuable agricultural equipment. Attackers can utilize relay attacks to increase the range of genuine RFID tags, allowing unauthorized access and equipment theft.

4.39 Account hijacking

Account hijacking in SA is unlawful access and control of user accounts that manage and run agricultural systems and equipment. These accounts are often owned by farmers, agronomists, or technicians who utilize SA platforms to monitor and control operations such as irrigation, fertilization, pest control, and equipment management. Attackers can hijack smart agricultural network accounts by phishing, weak passwords, credential stuffing, MitM attacks, and malware. Several IoT gadgets have insufficient security or send data in plain text over the Internet. When a packet is recorded after a consumer has been authenticated, a hacker can hijack an account [136].

4.40 Routing attacks

In SA, a routing attack is a malicious activity that attempts to hack or influence the routing protocols and procedures utilized inside agricultural networks. Routing protocols are critical for routing data packets between equipment, sensors, and systems in smart agricultural networks. These attacks use routing protocol weaknesses to redirect, halt, or change data flow, possibly interrupting operations, jeopardizing data integrity, or allowing unwanted access to network resources. Cybercriminals use route hijacking, route interception, and routing table poisoning. Agriculture routing hacks include unauthorized modifications to networked data channels. Such attacks may threaten the security of agricultural operations, causing erroneous data routing and interrupting critical activities [132][136]. Table 1 summarizes SA's cyber threats, challenges, and targeted security principles.

TABLE I. SUMMARIZES THE CYBER THREATS TO SA AND TARGETED SECURITY PRINCIPLES.

S/No	Reference	Cyber threat	Description	Targeted Principle					
				C	I	A	Au	N	P
1	[129-131]	Data privacy concerns	It raises farmers' concerns about unauthorized access to, collection, and sharing of their farm data with third parties by agricultural technology providers. Leakage of such data by unauthorized access or by an insider might pose a threat.	✓	✓	✓	×	✓	✓
2	[17][129][132]	Data breaches and leakages	Cybercriminals can use vulnerabilities or defects in smart agricultural systems to steal sensitive and secret data, such as crop models, plant breeders' rights, and IoT-generated data.	✓	✓	✓	✓	✓	✓
3	[44][123][132]	Malware injection attack	A malware injection attack occurs when an attacker injects malware into an attached computing device and nodes, which spreads across the system and makes it a compelling target for intruders.	✓	✓	✓	✓	✓	✓
4	[15][22][136] [137]	Ransomware attacks	A ransomware attack involves malicious actors infiltrating the system via phishing, compromised devices, and weak credentials, encrypting critical data on SA systems, holding it hostage till a ransom, and potentially disrupting planting, harvesting, and other critical operations.	✓	✓	✓	×	✓	×

5	[44][132][138]	Botnet	A network of infected computers or Internet-connected devices (remote sensors)—managed by a central command might have disastrous effects. A compromised IoT device has the potential to be a botnet for more sophisticated attacks, such as DDoS attacks and information theft.	✓	✓	✓	×	✓	×
6	[17]	Social engineering attacks	It involves manipulating people's behavior and psychology by deceiving them into installing malicious programs, disclosing sensitive information, or providing access to smart agricultural systems.	✓	✓	✓	✓	✓	✓
7	[17][22][44][139]	Phishing attacks	It is a social engineering technique that typically involves deceiving farmers into revealing sensitive login credentials, financial details, or access to critical agricultural systems.	✓	✓	✓	✓	✓	×
8	[24][44][123][138]	DoS and DDoS attacks	These attacks can target IoT devices, sensors, control systems, and data storage and management systems, and adversaries can use DDoS attacks to disrupt service and then insert fraudulent data, potentially compromising food safety, agri-food supply chain efficiency, and agricultural production.	✓	✓	✓	×	×	✓
9	[123][138][139]	MitM attacks	It is a cyberattack in which an attacker intercepts and potentially alters the communication between two parties, such as sensors, actuators, and control systems, without either party knowing the communication link has been compromised.	✓	✓	✓	✓	✓	×
10	[22][123]	Replay attacks	It occurs when an adversary intercepts and maliciously re-transmits legitimate data or commands across agricultural network devices or systems.	✓	✓	✓	✓	✓	×
11	[133]	Eavesdropping attacks	It entails the illegal interception and listening of communication or data exchanged between IoT devices, sensors, and systems in the agricultural environment.	✓	✓	✓	✓	✓	✓
12	[22]	Insider attacks	These are security breaches or malicious activities carried out by individuals or entities with authorized access to SA systems, networks, or data within the agricultural technology infrastructure who abuse their privileges for malicious purposes.	✓	✓	✓	✓	✓	✓
13	[17][71]	Supply chain attacks	It encompasses vulnerabilities in hardware, software, or firmware components that attackers can use to compromise the agricultural supply chain system.	✓	✓	✓	✓	✓	✓
14	[57][123]	Side-channel attacks	It exploits the physical features of the hardware, software, or communication media to harvest sensitive information from the target device's internal working and operation. It collects illegal information on deploying an IoT-based farm system by monitoring hardware metrics such as electric current or voltage.	✓	✓	✓	✓	✓	✓
15	[134]	APTs	These are sophisticated, targeted cyber-attacks that obtain and keep illegal access to an agricultural organization's systems and networks for a lengthy period without detection to steal sensitive data, disrupt operations, or cause economic and environmental harm.	✓	✓	✓	✓	✓	✓
16	[22][123][142]	Radio-frequency jamming attacks	It is the purposeful interruption of communication signals between IoT devices, sensors, and control systems. Such attacks can interrupt a smart farm's routine operations by blocking or significantly weakening wireless connections required for monitoring and managing agricultural activities.	✓	✓	✓	×	×	✓
17	[44][123][132]	Rogue device deployment attack	It involves introducing illegal devices into the agricultural IoT network to disrupt operations, steal data, or inflict harm.	✓	✓	✓	✓	✓	✓
18	[22][123][136][139]	Sensing device capture attack/Node tampering	These are unlawful physical access to sensors or nodes in the agricultural IoT network to interrupt the system's regular operation, steal data, or initiate malicious activity.	✓	✓	✓	✓	✓	✓
19	[55][135]	Spoofing attack	It involves an adversary deceiving a system or device into accepting false data by impersonating a valid source and accessing the network as an impostor.	✓	✓	✓	✓	✓	✓
20	[71][132]	Agroterrorism	It is the deliberate use of biological agents, chemicals, or cyber-attacks by adversaries to disrupt agricultural	✓	✓	✓	×	×	✓

			operations, cause economic loss, impair public health, and instill fear and uncertainty.						
21	[22]	False data injection attack	It entails an attacker intentionally inserting incorrect data into agricultural data collection and processing systems via compromised sensors, IoT, and other network devices to disrupt operations, manipulate outcomes, or cause harm.	✓	✓	✓	✓	✓	✓
22	[22]	Signature wrapping attacks	It exploits flaws in handling digital signatures to change or fabricate data without invalidating the original signature. This can be accomplished by exploiting deficiencies in implementing XML Signature, JWT, and other secure communication protocols.	✓	✓	×	✓	✓	✓
23	[138]	Reconnaissance attacks	It involves gathering information about agricultural systems, networks, and devices to uncover possible weaknesses that might be exploited in future attacks.	✓	✓	✓	✓	✓	✓
24	[22][132][136]	SQL injection attacks	It occurs when an adversary injects malicious SQL code into input fields, allowing them to modify database searches and obtain unauthorized access to data or even compromise the entire farm system.	✓	✓	✓	✓	✓	✓
25	[144]	IoT breaches	These are security events in which IoT devices and systems used in agricultural contexts are infiltrated by hostile actors.	✓	✓	✓	✓	✓	✓
26	[133]	Malicious hardware injection	It is the purposeful insertion of compromised hardware into the agricultural system to inflict harm, disrupt operations, or steal critical data.	✓	✓	✓	✓	✓	✓
27	[44][132][139]	Autonomous system hijacking and disruption	These malicious operations attempt to manipulate or disrupt the autonomous systems that handle various agricultural processes.	✓	✓	✓	✓	✓	✓
28	[44][63]	Unauthorized Access	It refers to accessing agricultural systems, data, or physical assets without sufficient authority.	✓	✓	✓	✓	✓	✓
29	[22]	Backdoor attack	It occurs when hackers inject hidden backdoors into agricultural technology's hardware, software, or communication systems to obtain illegal access to, control over, or manipulation of critical agricultural infrastructure.	✓	✓	✓	✓	✓	✓
30	[123]	Sybil attack	It occurs when a malevolent party creates many fake identities or nodes inside an agricultural network to obtain an unfair advantage, disrupt operations, or alter data.	✓	✓	✓	✓	✓	✓
31	[123]	Black-hole attack	It is a security vulnerability in which hostile nodes in a WSN falsely present themselves as having the best route to a specific location.	✓	✓	✓	✓	✓	✓
32	[44][132]	Cloud computing attacks	These malicious actions target cloud-based systems and services that manage agricultural data and operations.	✓	✓	✓	✓	✓	✓
33	[44][132]	Cloud data leakage	It is the illegal exposure or disclosure of sensitive agricultural data housed in cloud-based platforms.	✓	✓	✓	✓	✓	✓
34	[44][55][63]	Physical attacks	These purposeful activities aim to harm or disrupt the physical infrastructure of smart agricultural systems.	✓	✓	✓	✓	✓	✓
35	[22]	AI attacks	These involve exploiting vulnerabilities or manipulating AI-powered systems and algorithms to disrupt or compromise agricultural operations.	✓	✓	✓	✓	✓	✓
36	[22][44][140]	Evasion attacks	These are adversarial attacks in which the attacker alters input data to avoid or circumvent security measures, protocols, or detection mechanisms to obtain unauthorized access to agricultural systems or data without raising any alarms.	✓	✓	✓	✓	✓	✓
37	[92][123][140] [144]	Data poisoning attack	It involves manipulating the data used by agricultural systems such as sensors, drones, or AI algorithms to compromise their performance or integrity.	✓	✓	✓	✓	✓	✓
38	[133]	Blockchain attacks	It refers to malicious actions aimed at exploiting vulnerabilities within blockchain-based systems or leveraging weaknesses in their implementation.	✓	✓	✓	✓	✓	✓
39	[134]	Tracing attack	It occurs when hostile actors attempt to trace or follow the transfer of sensitive information within agricultural systems, such as crop yield statistics, supply chain records, or operational operations.	✓	✓	✓	✓	✓	✓
40	[136]	Protocol attacks	It aims to exploit vulnerabilities in communication protocols used by IoT devices, sensors, and systems.	✓	✓	✓	✓	✓	✓

41	[44]	Measure infusion forgery	It is a cyber-attack in which an attacker injects false or misleading data into the system that monitors and regulates agricultural activities.	✓	✓	✓	✓	✓	✓
42	[132][140]	Buffer overflow	It occurs when more data is written to a buffer than it can retain. This extra data may overwrite nearby memory, resulting in unexpected behavior, system failures, or security vulnerabilities.	✓	✓	✓	✓	✓	✓
43	[132]	RFID-based attacks	It corrupts RFID tags widely used for livestock tracking and signals, resulting in replay attacks, spoofing, eavesdropping, cloning, MitM, kill tags, side-channel attacks, and illegal access.	✓	✓	✓	✓	✓	✓
44	[136]	Account hijacking	It is the unlawful access and control of user accounts that manage and run agricultural systems and equipment.	✓	✓	✓	✓	✓	✓
45	[132][136]	Routing attacks	It is a malicious activity that attempts to hack or influence the routing protocols and procedures utilized inside agricultural networks.	✓	✓	✓	✓	✓	✓
Confidentiality (C), Integrity (I), Availability (A), Authentication (Au), Non-Repudiation (N), Privacy (P)									

5. CYBERSECURITY IN SMART AGRICULTURE

The agriculture industry is becoming more reliant on technology, from SA to supply chain management, and the data generated by these systems might be lucrative to cyber criminals. Still, agricultural systems are linked; thus, compromising one system might result in a security compromise across the entire network. Adequate agritech cyber security necessitates a comprehensive approach considering the industry's specific threats and challenges [17]. In SA, cyber security refers to the tools, measures, and practices used to protect and defend agricultural systems, networks, and electronic data from digital attacks, unauthorized access, damage, breaches, and other malicious activities [32][145]. Confidentiality, integrity, availability, privacy, authentication, and non-repudiation principles are critical for protecting data and SA systems.

- *Confidentiality* guarantees that only authorized personnel can access, alter, or delete sensitive information. This means that agritech firms should ensure that only authorized workers can access data. It safeguards sensitive agricultural data, such as proprietary farming techniques, crop yields, and financial information, against unauthorized access and possible espionage;
- *Integrity* guarantees that information is correct, complete, and untampered with. It ensures that data such as sensor readings, weather predictions, and inventory records are accurate and reliable to make effective decisions and run operations efficiently. Any lost or corrupted data might cause substantial downstream disruption;
- *Availability* guarantees that authorized users have access to information and resources when they need them. It enables continuous access to essential systems and data for monitoring and managing agricultural operations, which is required for prompt decision-making and productivity;
- *Privacy* safeguards individuals' personal information and ensures it is used and shared correctly. It protects the personal information of farmers, workers, and consumers and adheres to data protection legislation;
- *Authentication* checks the identification of users and systems to guarantee that access is restricted to authorized entities. It guarantees that only legitimate users can access sensitive agricultural systems and data, limiting illegal access and potential abuse; and
- *Non-repudiation* ensures that no party in communication can reject the legitimacy of their signature on a document or message they created. It verifies the origin and integrity of data and communications, which is required for accountability and traceability in agricultural supply chain transactions and interactions [15][17][22][146].

Cybersecurity in SA includes network security, cloud security, endpoint security, mobile security, IoT security, application security, and zero trust [33]. It establishes policies, processes, and technological methods to protect, detect, correct, and defend against damage, illegal use, modification, or exploitation of information and communication systems and their data [32]. Cybersecurity measures protect sensitive data, such as farmer information, agricultural data, financial records, intellectual property, and trade secrets [147], reduce risk, and keep systems secure and operable [17]. In response to unprecedented cyber threats and challenges in SA, AI-based cybersecurity technologies have evolved to assist security teams in effectively mitigating risks and improving security [32][148].

6. ARTIFICIAL INTELLIGENCE

Artificial intelligence has evolved into a helpful instrument in the cybersecurity industry. Kaur et al. [32], Mijwil et al. [149], and Aldoseri et al. [150] define AI as a field of computer science that creates computer systems capable of doing activities that need human intellect, such as learning, problem-solving, decision-making, and natural language

understanding. Artificial intelligence systems do this via various techniques and approaches, many of which are inspired by how the human brain functions, which provides services for computer vision, pattern recognition, expert systems, language processing and translation, speech recognition, biometric systems, robots, the IoT, and other related areas. It has advanced data analytics capabilities and can rapidly, efficiently, and precisely analyze large volumes of electronic data. Artificial intelligence systems can forecast future cyber-attacks based on historical threats, even if they alter [151]. It enhances defensive systems through continual learning and modification, allowing real-time detection and response to danger. Artificial intelligence integration in agriculture enables cybersecurity solutions to protect critical smart agricultural systems and data, reducing cyber-attack threats and increasing security in IoT ecosystems. Artificial intelligence techniques include machine learning, deep learning, natural language generation, expert systems, intelligent agents, speech recognition, text analytics, and natural language processing.

6.1 Artificial Intelligence Techniques for Smart Agriculture

With the increasing frequency of cyberattacks and threats in SA, using AI techniques, specifically machine learning, deep learning, reinforcement learning, and natural language processing, has become critical in improving current cybersecurity methods when combined with other technological methods [152][153].

6.1.1 Machine learning

According to Bala et al. [154], Jouini et al. [155], and Capodieci et al. [156], machine learning is a branch of AI that creates algorithms and statistical models capable of extracting and analyzing essential datasets, identifying new patterns, and making data-driven predictions or decisions. Machine learning techniques also include rules and methods for detecting or predicting new data patterns or practices [154]. Supervised, unsupervised, semi-supervised, and reinforcement learning are the categories of machine learning techniques [147][153]. (1) Supervised learning algorithms train algorithms using labeled datasets with predetermined input and output. It uses classification and regression algorithms [147][153][155]; (2) Unsupervised learning algorithms detect patterns and correlations in unlabeled data without using predetermined categories or labels. Unsupervised machine learning approaches are used when training data lacks annotations or classification. Clustering is among the unsupervised learning strategies most often utilized [147][153][155]; (3) Semi-supervised learning employs both labeled and unlabeled data to maximize efficiency and accuracy. It uses labeled and unlabeled data to train models, making it especially beneficial when labeled data is few, but unlabeled data is plentiful. Semi-supervised learning provides a compelling approach to improving algorithms with less human effort and more accuracy. It uses a variety of approaches, including generative models, graph-based models, mixture models, entropy minimization, and semi-supervised support vector machines [153][155]; and (4) Reinforcement learning is a machine learning strategy in which an agent interacts with its surroundings to improve its learning through experience [153]. It involves learning by interaction with the environment rather than training the model on a pre-defined dataset. Q-learning is an essential algorithm in reinforcement learning [155]. Reinforcement learning creates more dynamic and adaptable security systems to manage new and emerging threats [30][153]. Machine learning algorithms use statistical approaches to analyze data to find trends and cyber risks. These algorithms are trained to recognize harmful activities and behaviors. It allows regression, classification, clustering, dimensionality reduction, and boosting [153].

6.1.2 Deep learning

Deep learning is a kind of machine learning that employs artificial neural networks to interpret complex input such as images or voice [150]. It is inspired by neural networks, which may simulate the human brain with several layers of interconnected nodes and perform analytical learning by evaluating data such as text, pictures, and audio [157]. Many applications train deep learning models on large datasets, which helps them perform better on higher-level tasks [156]. It is suitable for supervised, semi-supervised, and unsupervised learning and has demonstrated considerable promise in enhancing the accuracy and efficiency of cybersecurity systems, notably in image and speech recognition [153]. Artificial neural networks, attention mechanisms, autoencoders, convolutional neural networks, deep belief networks, deep neural networks, fully connected layers, generative adversarial networks, graph neural networks, long short-term memory, recurrent neural networks, recursive neural networks, residual networks, restricted Boltzmann machines, and stacked autoencoders are deep learning algorithms utilized in SA applications [153][158]. Deep learning algorithms are employed in cybersecurity to identify malware, phishing, and fraud [30]. Deep learning algorithms have shown promise in increasing the precision of cyberattack detection by autonomously accumulating hierarchical properties from unprocessed data [159].

6.1.3 Natural language processing

Rizvi [30] and Aldoseri et al. [150] define natural language processing as a technique of AI that allows computers to perceive, interpret, and synthesize human language, including voice and text, to enhance security measures. It includes the creation of algorithms and strategies that allow computers to perceive, interpret, and synthesize human language in meaningful ways. Natural language processing allows computers to connect with people using natural language and accomplish tasks including language translation, sentiment analysis, text summarization, speech recognition, and language

creation. It is utilized in cybersecurity to identify possible vulnerabilities in unstructured data sources such as social media feeds and online forums [30], and it can help identify and manage spam and other social engineering threats [160]. Natural language processing may be used with machine learning and deep learning models to categorize email content and detect phishing attacks efficiently.

6.2 Applications of AI in Smart Agriculture Cybersecurity

The use of AI in cybersecurity for SA is a growing field that integrates cutting-edge technology to improve the security and efficiency of farming operations. The primary areas where AI is employed in cybersecurity for SA are as follows:

6.2.1. Intrusion/anomaly detection and prevention

Intrusion detection systems that analyze network data are critical for preventing unwanted access and malicious activity while guaranteeing confidentiality on smart farm networks. However, due to increased data volume and network traffic, traditional intrusion detection systems solutions may struggle to keep up with the changing nature of cyber threats and encounter issues on the IoT platform. Classical intrusion detection systems analyze and filter network data using preset signatures, rule-based techniques, and well-known domain protocols. As a result, they are impoverished at identifying new risks, such as zero-day attacks. Thus, deploying AI in an agricultural IoT setting is essential. Artificial intelligence algorithms can evaluate agricultural IoT equipment's network traffic patterns and real-time data streams to find anomalies that might suggest an intrusion or cyber threat. For example, abrupt changes in sensor readings or unusual communication patterns might be reported for additional examination [39]. Artificial intelligence may also employ machine learning algorithms to understand a network's or system's usual behavior and detect deviations from it [147][161]. The most appropriate use for AI models, particularly machine learning and deep learning, is to detect abnormalities and improve the efficacy and accuracy of intrusion detection systems for agricultural IoT. Machine learning models, primarily supervised learning algorithms, may be trained using past data to distinguish between normal and aberrant patterns. Intrusion detection systems powered by AI algorithms, such as anomaly detection or behavior-based models, can more quickly identify and respond to cyber threats than previous approaches, lowering the risk of a successful attack [36]. Random forest, gradient boosting, ada boost, decision tree, and extremely randomized trees are machine learning techniques that may be trained to recognize existing threats and anticipate future ones by evaluating massive volumes of data from numerous sensors and devices [162]. Machine learning-based anomaly detection systems can minimize random sensor malfunction, robot or drone system hijacking, camera image distortion incidents, and data penetration anomalies [139]. Deep learning may help enhance intrusion detection by analyzing network traffic and recognizing patterns that indicate an attack. Deep learning algorithms may be trained using massive datasets of typical network traffic and known attack patterns. Once trained, the algorithm can examine network data in real-time and identify abnormalities that indicate an attack [153]. Fuzzy logic and neural networks are utilized for host-based and anomaly detection because their model can evaluate network data using basic data mining techniques and track suspicious traffic back to its origin [28][130] [163][164].

6.2.2. Efficient threat detection and response

Artificial intelligence and machine learning have evolved as effective threat detection systems, utilizing supervised, unsupervised, and reinforcement learning. Artificial intelligence-powered systems continuously monitor and analyze massive amounts of data from various sensors, such as soil sensors, weather stations, and drones, and automatically detect and classify known and unknown threats that would be difficult or impossible for a human to detect, as well as automatically and instantly respond to threats [35][37][165][166]. Agricultural firms use AI to manage better, protect their networks and devices, and discover and mitigate risks. These systems may scan network traffic using machine learning techniques, find patterns that suggest a possible attack, and evaluate user behavior to detect suspicious activity [30][147][167]. Artificial intelligence and machine methods techniques for threat detection include deep learning, convolutional neural networks, recurrent neural networks [168], and natural language processing techniques for analyzing unstructured data [161].

6.2.3. Malware detection

The fast spread of malware, such as viruses, worms, and Trojan horses, seriously threatens smart agricultural systems and networks. It is intended to exploit weaknesses and undermine the integrity of agricultural systems, resulting in data breaches, financial losses, and operational interruptions with catastrophic repercussions. As more malware is generated for hidden purposes, signature-based detection approaches are insufficient for critical cybersecurity since they rely on a preset database of known malware signatures [163]. As a result, machine learning methods, which use the power of AI, show promise in automating malware identification at the system level. Artificial intelligence employs heuristic analysis, recognizing patterns and behaviors associated with harmful code to detect possible malware [37][153]. Artificial intelligence models can be trained on large datasets of known malware samples and benign software, enhancing their capacity to discriminate between the two. Machine learning's intrinsic ability to examine massive volumes of data and uncover patterns suggesting dangerous behavior can provide suitable and timely detection capabilities [147][167][169]. Automated system-level malware detection using machine learning algorithms in smart agricultural networks and systems

helps to identify and mitigate malware attacks [20][147][163]. Deep learning identifies malware by studying a program's behavior rather than its code, a behavioral detection technique [28][153]. Neural networks and deep convolutional neural networks are deep learning models that can assess complicated and high-dimensional data, increasing malware detection [170].

6.2.4. DDoS/Botnet detection

Traditional DDoS mitigation systems often fall short of battling attackers' ever-changing plans because they cannot evaluate complicated or identify zero-day DDoS attacks. Botnets allow attacks such as DDoS to access the target agricultural IoT device and its network since they may be managed via command-and-control software. However, in the fight against DDoS attacks, AI techniques have shown promise in combating botnets. Artificial intelligence-based botnet detection approaches can identify newer or undiscovered botnets without needing pre-built botnet signatures, improving the ability to detect, analyze, and respond to these threats and guaranteeing the security and continuity of agricultural operations [29][163]. Artificial intelligence systems can continually analyze network traffic for abnormal patterns or behaviors that might suggest a DDoS attack [171]. Machine learning algorithms can distinguish between typical traffic fluctuations and malicious behavior. Artificial intelligence can evaluate time-series data to find temporal trends and abnormalities that might indicate a botnet or a DDoS attack. When AI systems identify a DDoS attack or botnet activity, they can automatically begin actions such as rate limiting, blocking malicious IP addresses, and isolating afflicted devices. Artificial intelligence can dynamically alter security measures based on the identified threat's severity, resulting in a more personalized and effective response.

6.2.5. Fraud detection

Artificial intelligence-driven techniques are used in SA to improve fraud detection, resulting in a safer, more transparent, and more efficient agricultural environment. Artificial intelligence systems examine vast amounts of data from numerous sources, such as bank transactions, supply chain records, and sensor data, to detect abnormalities that might suggest fraudulent activity [30][161]. It can monitor the behavior of several entities, including suppliers, farmers, and consumers, to detect unusual acts that may indicate fraud [165]. Artificial intelligence algorithms can be trained to spot fraud trends and indications using historical data classified as fraudulent or non-fraudulent [153]. Machine learning algorithms can identify fraud by examining patterns and trends in financial data [147]. Deep learning can detect fraud by examining massive transaction databases and discovering fraudulent patterns. Trained deep-learning systems can identify these patterns and flag questionable transactions [153].

6.2.6. Behavioral analysis

Artificial intelligence and machine learning can monitor user activity and identify abnormalities that may indicate a security breach. Behavioral analytics assist firms in detecting emerging risks and often occurring vulnerabilities [31]. Artificial intelligence systems can monitor network traffic and device activity in real-time, identifying unexpected patterns that might suggest security breaches [35][39]. User behavior analytics powered by machine learning examines user activity, emphasizing aberrant behavior that may indicate illegitimate access or compromised accounts. Machine learning models can help define baselines for predicted device and user behavior. Deviations from these baselines might raise alarms about possible cyber dangers [30][37][147][161][166]. Artificial intelligence systems can monitor the behavior of sensors, actuators, and linked devices, detecting unusual activity that might indicate a cyber-attack or malware infection.

6.2.7. Network security

Improving network security in SA is critical for any complete cybersecurity strategy. Artificial intelligence is primed to transform this environment, serving as a powerful catalyst for improving performance and efficacy in those domain names. Artificial intelligence systems monitor network traffic and device activity in real-time, looking for unexpected patterns that suggest security vulnerabilities [37]. It can automate responses to identified attacks, such as isolating compromised devices, blocking malicious IP addresses, and notifying administrators to avoid additional harm [170]. Artificial intelligence can detect trends and abnormalities in network traffic, such as odd data transfers, access patterns, or device interactions, that might signal malicious behavior [37][172].

6.2.8. Threat intelligence

Artificial intelligence-powered threat intelligence helps to secure agricultural systems by delivering timely and accurate insights into potential threats. Artificial intelligence systems may automatically collect data from various sources, including network logs, device logs, social media, and threat databases, to provide a complete picture of possible risks [161]. It can work with existing farm management and cybersecurity systems to collect essential data without disrupting operations. Machine learning algorithms can monitor device, user, and network traffic behavior patterns to detect anomalies that might suggest a security issue [165]. Artificial intelligence-driven solutions may collect and analyze massive amounts of threat intelligence data from several sources to discover new threats, trends, and vulnerabilities, hence improving proactive

security measures [30][37][167][172]. Artificial intelligence can assess the danger of prospective threats by evaluating their likelihood and effect, prioritizing responses, and allocating resources. It can help agricultural entities and cybersecurity groups share threat intelligence, enhancing protection systems. Artificial intelligence can also help standardize threat intelligence data formats, making sharing and comprehending information across several platforms and organizations easier.

6.2.9. Phishing and spam detection

As SA depends more on digital communication channels and connected devices, the likelihood of phishing attacks and spam messages increases. Phishing attacks try to get sensitive information from unsuspecting victims, including usernames, passwords, credit card numbers, and debit card information [163]. Artificial intelligence is critical in phishing and spam detection for SA, protecting agricultural operations from harmful emails, texts, and communications [163]. It improves phishing and spam detection for SA by utilizing advanced approaches in content analysis, pattern recognition, and real-time monitoring. Natural language processing techniques aid in comprehending written and spoken language, making it easier to detect phishing emails and fraudulent correspondence [163][167][173]. By combining AI with machine learning models, threat intelligence, and behavioral analytics, agricultural operations may efficiently prevent the dangers of phishing attacks and spam emails. This proactive strategy protects the security and integrity of digital communications in SA, preventing interruptions and risks to production. Artificial intelligence examines the content of emails and messages to detect phishing, spam, and questionable links. It validates sender identities and examines email headers for spoofing or fabrication, guaranteeing that communications originate from authentic sources. Artificial intelligence systems examine user and system behavior to identify abnormalities, such as strange email sending patterns or abrupt increases in email traffic, which might suggest a phishing campaign or spam attack. It may identify trends in phishing emails, such as faked domains, urgent demands, and deceptive URLs, which improves detection accuracy [31][35][167]. Artificial intelligence can also examine email images and attachments by scanning for malware signatures and comparing them to threat intelligence databases to detect phishing attempts, such as implanted malware or false visuals intended to deceive users.

6.2.10. Security automation

Artificial intelligence assists agricultural operations in minimizing risks and responding quickly to security threats by automating threat detection, incident response, vulnerability management, and compliance checks. This proactive strategy increases cybersecurity defenses and promotes digital technology's sustainable and secure agricultural deployment. It can automate regular tasks performed by security analysts during security measures. Analyzing historical data can help automate procedures more successfully. Artificial intelligence algorithms utilize this data to develop a model, which may then be used to locate associated online activity. With this approach, AI systems respond to threats without human intervention [170]. Artificial intelligence-powered systems can automate security processes, including installing security updates, developing security rules, and producing security reports. Artificial intelligence-powered chatbots and virtual assistants can automate typical security operations such as password reset and account management and provide consumers with immediate support in resolving security-related concerns [30]. Machine learning can assist with repetitive and time-consuming security procedures and automate network traffic inspection, ransomware prevention, virus removal, and network log analysis [35] [174].

6.2.11. User authentication

Artificial intelligence improves user identification procedures in SA, ensuring safe access to digital systems, devices, and data. Authentication is critical to protecting agricultural operations from illegal access and cyber threats. Implementing AI in cybersecurity enables agricultural enterprises to protect passwords better and user accounts through authentication. Artificial intelligence-driven solutions offer sophisticated capabilities that increase the accuracy, reliability, and usability of authentication processes. Biometric authentication, behavioral analysis, and face recognition are all examples of AI technologies that may improve user authentication methods. These strategies make it more difficult for unauthorized users to access systems and sensitive data [167]. Artificial intelligence-powered authentication systems can use machine learning algorithms to analyze user behavior, identify potential anomalies, detect fraudulent activities, and prevent unauthorized access, thereby improving access control measures [147]. Artificial intelligence may be used to build advanced biometric authentication systems that recognize people based on their distinct physical and behavioral features, considerably lowering the danger of unwanted access [147].

6.2.12. Vulnerability management

Artificial intelligence is essential in SA vulnerability management as it addresses the vital requirement to find, analyze, prioritize, and eliminate vulnerabilities in agricultural systems and networks. Vulnerability management is a vital part of cybersecurity that entails finding, analyzing, and prioritizing the vulnerabilities in a system or network before taking action to eliminate or mitigate such vulnerabilities. This technique assists agricultural enterprises in lowering the risk of a cyberattack and mitigating the possible consequences of a breach. Artificial intelligence and machine learning aid in

automating and expediting the vulnerability management process, allowing agricultural enterprises to discover and remediate vulnerabilities more quickly and efficiently [28][168]. As SA depends more on networked devices, sensors, and data-driven technologies, cyber threats become more prevalent, necessitating comprehensive vulnerability management to ensure robust cybersecurity. Agricultural systems can use machine learning algorithms to analyze network traffic, find trends, and discover system vulnerabilities [161][165]. Artificial intelligence techniques can help uncover software and system vulnerabilities by automating the scanning and analysis of code, configurations, and infrastructure, enabling enterprises to prioritize and fix vulnerabilities before exploiting them [167]. Machine learning can automatically identify and prioritize vulnerabilities in agricultural software systems or network infrastructure. Machine learning algorithms can analyze network traffic, find trends, and detect system vulnerabilities [161]. It can assist security teams in identifying high-risk vulnerabilities and prioritizing patching or remediation efforts before they are exploited [35]. Artificial intelligence could revolutionize the vulnerability management landscape by shifting the focus away from reactive methods and toward proactive and predictive approaches [172].

6.2.13. Automated incident response

Artificial intelligence is crucial in automating incident response for SA, allowing for faster detection, investigation, and mitigation of cybersecurity problems. Automated incident response is critical for reducing the effect of security breaches while protecting the integrity of agricultural operations. Machine learning algorithms are used to spot patterns of suspicious activity or known attack signatures, and events are classified depending on their severity and impact. Artificial intelligence systems can speed up incident response by automatically analyzing and correlating security events, providing real-time warnings when security issues are discovered, recommending remediation actions, increasing cybersecurity team efficiency, and reducing response times [30][167][175]. Artificial intelligence automates procedures such as isolating affected devices, blocking rogue IP addresses, quarantining malicious IoT devices, shutting down compromised servers, and deploying security upgrades to reduce the effect of events and the time necessary to respond [161].

6.2.14. Adaptive and predictive security

Adaptive and predictive security uses AI-powered systems to continually monitor risks, forecast future attacks, and alter defense mechanisms in agricultural operations. Artificial intelligence and machine learning models can constantly learn from new data and adapt to changing threats, making them more successful in detecting and responding to new attack vectors. Predictive analytics may also assist in anticipating possible security hazards using past data and patterns [35][167]. Artificial intelligence-driven adaptive and predictive security improves the resilience and efficacy of cybersecurity measures in SA by allowing for proactive threat detection, dynamic reaction actions, and ongoing defensive strategy refinement. Agricultural operations may reduce risks, protect vital assets, and preserve operational continuity in the face of emerging cyber threats by utilizing behavioral analytics, predictive analytics, and adaptive security measures. This proactive strategy promotes the secure adoption and long-term expansion of digital technology in agriculture, guaranteeing resilience to growing cybersecurity problems.

6.2.15. End-point security

End-point security is essential for protecting against cyber-attacks targeting IoT devices, frequently scattered throughout varied and sometimes distant agricultural areas. Artificial intelligence monitors end-point devices for anomalous behavior patterns that may indicate potential threats, such as unauthorized access attempts or abnormal data transfers [174]. Artificial intelligence-powered solutions employ machine learning algorithms to detect abnormalities from typical device behavior, allowing for early identification of malware infestations, blocking malicious activities on individual devices or compromised end-points, and enhancing overall SA system security [35]. Artificial intelligence can scan end-point devices for known malware signatures and patterns, detecting and preventing harmful software before it harms. It monitors end-point devices and performs real-time network traffic analysis to discover and respond to security risks. It also checks the integrity of end-point devices by scanning program settings, file integrity, and system activities for evidence of tampering or illegal modifications.

6.2.16. Insider threat detection

Insider threats to agricultural businesses can be severe, resulting in data breaches, sabotage, and intellectual property theft. Artificial intelligence improves insider threat detection in SA using advanced behavioral analytics, machine learning algorithms, and contextual analysis to identify and manage risks posed by authorized personnel with nefarious intentions. Artificial intelligence-powered solutions assist agricultural operations in protecting sensitive data, intellectual property, and essential infrastructure from insider threats by monitoring user activity, identifying anomalies, and initiating automatic reactions. This proactive strategy promotes the secure adoption and long-term expansion of digital technology in agriculture while assuring resilience against insider threats and operational continuity. Artificial intelligence examines user behavior to identify abnormalities that indicate insider risks, such as unlawful data access or unusual system interactions.

6.2.17. Reduce false positives

Artificial intelligence plays a vital role in decreasing false positives in cybersecurity for SA, solving the difficulty of precisely recognizing serious threats while minimizing the incidence of wrong warnings, which can cause unneeded interruptions and waste. Artificial intelligence-powered solutions improve the accuracy and efficacy of cybersecurity operations in SA by eliminating false positives. It reduces the incidence of unnecessary warnings while enhancing identification and reaction to serious security risks [147]. This proactive strategy improves cybersecurity resilience and promotes the secure adoption and long-term expansion of digital technologies in agriculture, assuring the protection of vital assets and data from emerging cyber threats.

6.2.18. Risk assessment

Artificial intelligence is significant in cybersecurity risk assessment for SA, providing increased capabilities for identifying, analyzing, and mitigating possible hazards associated with digital technology, networked systems, and data-driven processes. It improves risk assessment in cybersecurity for SA by utilizing sophisticated analytics, machine learning algorithms, and real-time monitoring capabilities to efficiently detect, prioritize, and mitigate security issues. Machine learning algorithms can examine system settings, vulnerabilities, and other data to determine the likelihood and effect of cyber-attacks [147]. By incorporating AI-driven risk assessment into cybersecurity policies, agricultural operations may manage risks proactively, secure essential assets and data, and preserve operational continuity in the face of increasing cyber threats. This proactive strategy promotes the secure adoption and long-term expansion of digital technology in agriculture, guaranteeing resilience to cyber hazards while protecting agricultural production and innovation.

6.3 Case Studies and Examples

Implementing AI-driven cybersecurity solutions in agricultural settings is still a relatively new field, but several notable case studies and examples demonstrate these technologies' potential and effectiveness in improving security efficiency and significantly benefiting agricultural operations. Some of the success stories and significant lessons learned are:

John Deere has effectively integrated AI-driven cybersecurity into its precision agricultural systems. It uses AI to monitor and analyze data from multiple sensors on tractors and other equipment, ensuring safe data transfer and protecting against cyber-attacks. This solution has enhanced data integrity, resulting in more accurate decision-making and optimal agricultural techniques. Farmers can trust safe data, encouraging further usage of precision agricultural systems. Continuous monitoring and real-time threat detection are critical to ensuring the security of networked devices. Artificial intelligence algorithms must be updated regularly to respond to evolving dangers [176].

Cargill, a worldwide leader in food and agriculture, has started the Digital Saathi program in India. This venture offers farmers AI-driven advice services via a mobile app, including real-time data on crop health, weather predictions, and market pricing. Farmers reported higher crop yields and market prices for their produce. The project increased confidence and openness in the agricultural process. The mobile app includes AI-driven security measures to safeguard user data and enable secure communication with backend servers. Securing mobile applications and communication channels is crucial for winning farmers' trust while protecting the security and integrity of their data [177].

A coalition of Dutch agricultural enterprises and academic organizations collaborated on a smart greenhouse project that used AI and IoT. The greenhouses were outfitted with sensors that monitored environmental conditions and optimized plant development. The initiative increased agricultural yields by 15% while reducing resource usage by 20%. Artificial intelligence algorithms optimized lighting, temperature, and humidity conditions in real-time. Artificial intelligence-powered anomaly detection systems were utilized to scan network traffic and sensor data for possible cyber threats. Regular security audits and upgrades were performed to ensure the system's integrity. Continuous monitoring and preemptive threat identification are critical for maintaining the integrity of integrated agricultural systems and avoiding interruptions [178].

Climate Corporation's FieldView product employs AI to deliver insights into crop management while maintaining cybersecurity through AI-driven threat identification and response. Farmers trust the platform because of its capacity to analyze large volumes of data securely. Farmers that use FieldView benefit from trustworthy data analytics, which leads to higher agricultural yields and improved resource management. The platform's sophisticated cybersecurity features safeguard sensitive data, foster confidence, and promote adoption. Ensuring data privacy and integrity is crucial for obtaining farmers' trust. Artificial intelligence-driven cybersecurity must be easily incorporated into the platform to provide a safe and user-friendly experience [179].

Several vineyards in California have installed AI-powered smart irrigation systems that optimize water use using soil moisture sensors and weather predictions to provide real-time data. These systems employ AI to detect and respond to cyber-attacks, guaranteeing a safe operation. Precision irrigation management has resulted in considerable water savings and enhanced grape quality in the vineyards. Cybersecurity safeguards have averted interruptions and assured uninterrupted, dependable functioning. The use of AI in both operational efficiency and cybersecurity can yield significant benefits. Educating users on cybersecurity in IoT applications is critical for effective implementation [180].

Several lessons were learned from integrating AI in cybersecurity for SA, among which include the following:

- Data integrity and confidentiality are critical in agricultural contexts because data is used to make essential choices. Artificial intelligence-powered cybersecurity solutions must emphasize data protection to provide dependable and accurate insights.
- Agricultural operations frequently involve real-time data analysis and decision-making. Artificial intelligence-powered cybersecurity systems are capable of real-time monitoring and fast reaction to possible attacks.
- Farmers and agricultural workers require education and training on cybersecurity's value and deploying AI-driven solutions properly. This helps them establish trust and promotes the use of innovative technology.
- The scalability of AI-driven cybersecurity solutions is critical for managing the growing number of IoT devices and sensors in SA. Solutions must be flexible to growing cyber threats and compatible with varied agricultural technology.
- Collaboration between technology suppliers, cybersecurity specialists, and agricultural stakeholders is critical. Sharing expertise and best practices can assist in creating more effective and resilient AI-driven cybersecurity solutions.
- While innovation in SA is critical, it should not be at security's price. Designing new safe technologies can help prevent vulnerabilities and develop user confidence.

The success stories and lessons learned from applying AI-driven cybersecurity solutions in agricultural settings highlight the benefits and limitations of integrating these technologies. The agriculture business can benefit from AI by focusing on data protection, real-time threat detection, user education, and cooperation. These efforts will help to create more resilient and sustainable farming techniques, ultimately supporting the larger aims of SA.

The application of AI in cybersecurity for SA offers various advantages, such as real-time threat detection and response, improved accuracy and precision, enhanced data security, operational efficiency, cost savings, scalability, enhanced regulatory compliance, increased trust and adoption, improved threat intelligence, automation, extensive data processing, fast response, identifying emerging threats, better endpoint protection, better vulnerability management, reduced fake positives, automated incident response, and cybersecurity danger assessment [25][153][166].

6.4 Ethical Concerns of Using AI in Cybersecurity

Integrating AI into cybersecurity for SA involves several ethical concerns that must be carefully explored to guarantee that these technologies are deployed responsibly and moderately. Some of the ethical issues are:

6.4.1.Data privacy

The rise of AI in cybersecurity raises concerns about the possible misuse of farmers' data. Artificial intelligence algorithms frequently require access to vast and sensitive datasets for training. If not managed appropriately, the algorithm may unintentionally reveal or exploit this personal data, resulting in privacy violations and breaches of confidentiality. The algorithm can invade privacy, mainly if not created with solid privacy safeguards, raising ethical concerns regarding data usage and permission. Besides, AI threat scanners may access and monitor files, emails, mobile and endpoint devices, people, and network traffic data, resulting in a privacy paradox. This issue is inherent since these technologies rely on the data given by the user [38]. Organizations may lessen the risk of privacy breaches by anonymizing personal data before feeding it into AI systems while still gaining insights from the data. Furthermore, ethical considerations should govern the development and implementation of AI systems, guaranteeing fairness, openness, and respect for individual privacy rights [38][167].

6.4.2.Artificial intelligence bias and fairness

Artificial intelligence systems may accidentally propagate biases in training data, resulting in unfair or discriminating outputs. For example, AI algorithms trained on biased or unrepresentative datasets may inherit and exacerbate prior biases, resulting in unjust or discriminating outputs with severe consequences in cybersecurity [38][161][167]. If the machine learning model is taught using biased judgments, the bias can solidify and intensify over time, creating a self-reinforcing loop. Biased security algorithms may discriminate against individuals based on gender, color, ethnicity, or other protected characteristics, which might have serious consequences, such as arbitrarily targeting people for security measures or denying access to essential services. If people perceive security systems as discriminatory, they are less inclined to trust and assist in security efforts. This might affect the overall effectiveness of security measures [35]. It is critical to ensure that all farmers, regardless of size, location, or resources, have access to AI-driven cybersecurity solutions to avoid growing the gap between giant agribusinesses and small-scale farmers. Ensuring impartial data and model development is essential for developing fair and ethical AI in cybersecurity. Agricultural organizations must work to uncover and eliminate training data biases through data pretreatment, bias identification, and algorithmic fairness testing. Organizations may create equal and impartial AI systems by encouraging diversity and inclusion in dataset collecting and model training. Developing bias detection and mitigation tools, establishing diverse and representative datasets, and promoting transparency and accountability in AI development processes are examples of industry efforts and best practices for mitigating bias in cybersecurity systems. Organizations may use fairness-aware algorithms and strategies to reduce bias in AI models,

resulting in more equal outcomes across demographic groups and circumstances. It is vital to constantly review machine learning models for bias and evaluate their efficacy across diverse demographic categories. Bias problems can be identified and addressed through frequent audits and feedback mechanisms. Human monitoring and intervention are vital for ensuring fairness and avoiding unfair outcomes. Human specialists should examine and approve machine learning algorithms' judgments, particularly in specific scenarios [35].

6.4.3.Transparency and accountability

Many AI systems, particularly those that use deep learning, function as "black boxes," making it impossible to comprehend how they reach certain conclusions. This lack of transparency might undermine accountability and confidence in AI systems, particularly in crucial areas such as cybersecurity, where decisions must be explained and comprehensible [38]. Determining who is liable for AI systems' judgments, particularly in cybersecurity breaches, presents a serious ethical dilemma. Accountability and trust are vital in data security applications, as is knowing how an algorithm makes decisions. Explainable AI (XAI) is required for security professionals to trust and assess the results of AI-powered cybersecurity solutions. By giving insights into how AI algorithms arrive at their findings, XAI allows security analysts to comprehend the reasoning behind AI-generated warnings, recommendations, or judgments. This transparency promotes trust and confidence in AI systems, enabling security professionals to make educated decisions and take appropriate action in the face of security problems. Likewise, organizations and industry groups advocate adopting XAI principles and standards to ensure that AI systems are trustworthy and accountable [35][38][167]. Making AI systems' decision-making processes more understandable can help to increase trust and accountability.

6.4.4.Adversarial attacks

Adversaries are looking at new ways to mislead AI systems via adversarial attacks. These attacks use false data input modification to drive AI algorithms to make poor judgments, rendering the systems less reliable and potentially inefficient [161][163]. This is especially dangerous in cybersecurity, where attackers might circumvent AI-based security measures by exploiting algorithmic flaws. If AI models are not resistant to adversarial attacks, they can weaken the effectiveness of cybersecurity measures and jeopardize system security. Because machine learning models are fragile, minor changes to training data can result in incorrect predictions, delayed detection of attacks, infrastructure damage, financial loss, or even death [35]. Some research has demonstrated the possibility of poison attacks on training data, where attackers tamper with some users' biometric templates, impersonate a specific user, and deceive face authentication [163]. Artificial intelligence systems must be safeguarded from adversarial attacks and resistant to manipulation and hacking [167], and research on robust AI and counter-adversarial strategies is critical [35].

6.4.5.Cybersecurity risk of AI

Using AI to monitor agricultural activities may blur the distinction between cybersecurity and surveillance, creating ethical concerns about the scope and intent of surveillance methods. Artificial intelligence has cleared the door for building conversational agents, such as chatbots, that can communicate with people via messaging interfaces. Highly complex chatbots, such as ChatGPT, may precisely simulate human discussions. However, its utilization poses major cybersecurity threats that must be addressed [161]. Artificial intelligence models are trained on current data, so they may need help recognizing new threats previously recorded.

6.4.6.Interpretability and explainability

The AI training process frequently acts as a black box with minimal transparency in its inner workings based on the input information, making it difficult to determine or understand the logic behind these models' actions. This lack of interpretability can make it difficult to explain why an AI system made a specific cybersecurity decision, which is a significant concern for organizations because they need to be able to trust the decisions made by artificially intelligent systems to choose the best course of action in response to an alert [37][161][163]. Users must understand how and why AI reached a specific result [167].

6.4.7.Data quality and availability

Artificial intelligence systems rely on vast data to train and enhance performance and high-quality data to learn and make accurate predictions. However, obtaining high-quality and representative data can be difficult and limited [37][161], and data in the cybersecurity field is frequently inconsistent and noisy, making it difficult for AI systems to learn novel capabilities [35][37].

6.4.8.Lack of regulatory framework

Artificial intelligence technology typically advances faster than legislative frameworks, resulting in governance and oversight deficiencies. Establishing comprehensive legislation addressing the ethical use of AI in cybersecurity is critical. Adhering to existing standards while lobbying for new legislation that addresses the particular issues of AI in cybersecurity can help to ensure ethical technology use. There is no legislative framework to oversee the use of AI in cybersecurity,

making it challenging for enterprises to grasp their legal and ethical responsibilities when adopting systems built on AI [161]. Evaluating various smart agricultural systems may be difficult owing to the lack of standards and best practices for using AI in cybersecurity [37]. Creating and following ethical principles for employing AI in cybersecurity can help guarantee that these technologies are used in a way that respects human rights and promotes societal good.

6.4.9. Limited scalability

As cybersecurity risks evolve, the amount of data that must be examined increases. Artificial intelligence systems can be resource-intensive, making it difficult to scale them to suit the demands of big agricultural businesses [37][161].

6.4.10. Limited cybersecurity experts

Using AI in cybersecurity is a fascinating and promising field that may provide firms a considerable advantage in recognizing and responding to possible cyber-attacks. Implementing AI-based systems necessitates specific skills and experience in high demand. Because of the scarcity of cybersecurity specialists capable of developing, operating, and maintaining AI-based systems, agricultural organizations find it challenging to adopt and execute these systems successfully [161]. Agricultural businesses must engage in training and development programs to create a competent workforce capable of administering and sustaining AI-based agricultural systems.

6.4.11. Human oversight and control

Exaggerating AI's capabilities may provide a false sense of security. Excessive dependence on AI without human oversight may lead to missed threats, false positives, or vulnerabilities that AI fails to resolve [167]. Because AI-based cybersecurity solutions are not a solution, they require human inspection and involvement [37]. Humans should be allowed to challenge or overturn AI decisions to ensure the system is operated by moral principles [167]. Security analysts must be trained in how they work and be able to intervene when required to guarantee that AI-based systems make correct and appropriate judgments [37].

6.4.12. Human error

Artificial intelligence for cybersecurity might be challenging due to human error. For example, cybersecurity specialists may misinterpret or reject alerts generated by an AI system, failing to detect or respond to a cyber-attack [37].

7 CONCLUSIONS

This extensive survey delves into the convergence of AI and cybersecurity in SA, emphasizing the significant progress and advances. Technological advancements have accelerated the move from traditional to SA, allowing for more efficient, productive, and sustainable farming operations. The exploration of smart agricultural architecture and new technologies highlights the revolutionary potential of these breakthroughs in solving global food security issues. However, as dependence on digital technology grows, so do cyber-attacks, which can compromise the integrity and operation of smart agricultural systems. This survey has mapped out the landscape of these cyber threats, giving a clear picture of the vulnerabilities and hazards that must be reduced to preserve agricultural facilities.

Artificial intelligence applications in cybersecurity provide promising answers to these challenges by improving threat detection, prevention, and response methods. It also provides options for improving data integrity, confidentiality, and availability in smart agricultural ecosystems. The benefits of incorporating AI into SA cybersecurity include increased threat detection accuracy, real-time monitoring, optimizing operational efficiency and productivity, fostering sustainable farming practices for the future, and proactive defense strategies. These advantages are critical for ensuring smart agricultural systems' data integrity, operational efficiency, and overall resilience. Furthermore, the ethical considerations about employing AI in cybersecurity for SA must be addressed. Data privacy, AI bias, and the possibility of misusing AI technology demand a balanced strategy emphasizing moral concerns alongside technological advancement.

While incorporating AI into cybersecurity for SA has enormous promise, a comprehensive approach incorporating technological, security, and ethical elements is required. Future research should focus on (1) developing cost-effective, scalable, and privacy-preserving AI solutions tailored to the unique needs of the agricultural sector; (2) developing robust, transparent, and ethically sound AI solutions that can effectively secure smart agricultural systems; (3) continuing research and development investment that is critical to advance further AI technologies tailored for cybersecurity in SA; (4) encouraging collaboration among researchers, practitioners, and stakeholders in agriculture and cybersecurity to exchange insights, best practices, and lessons gained; (5) implementing a multi-layered defense strategy to strengthen the security infrastructure of smart agricultural systems; (6) paying close attention to data privacy regulations and ethical considerations when deploying AI solutions in SA; (7) establishing mechanisms to track emerging threats and vulnerabilities in smart agricultural networks and devices; and (8) providing comprehensive education and training programs for farmers, agronomists, and agricultural professionals. By accepting these recommendations and capitalizing on AI technology's revolutionary potential, the agricultural industry can improve its cybersecurity posture while ensuring the sustainability and efficiency of smart agricultural systems in the digital era.

Funding
The authors had no institutional or sponsor backing.

Conflicts Of Interest
The authors disclosure statement confirms the absence of any conflicts of interest.

Acknowledgment
The authors extend appreciation to the institution for their unwavering support and encouragement during the course of this research.

References
[1]. S. Balyan, H. Jangir, S. N. Tripathi, A. Tripathi, T. Jhang, and P. Pandey, "Seeding a Sustainable Future: Navigating the Digital Horizon of Smart Agriculture," *Sustainability*, vol. 16, no. 2, pp. 1–21, 2024. https://doi.org/10.3390/su16020475

[2]. J. U. M. Akbar, S. F. Kamarulzaman, A. J. M. Muzahid, A. Rahman, and M. Uddin, "A Comprehensive Review on Deep Learning Assisted Computer Vision Techniques for Smart Greenhouse Agriculture," *IEEE Access*, vol. 12, pp. 4485–4522, 2024. https://doi.org/10.1109/access.2024.3349418

[3]. A. Pagano, D. Croce, I. Tinnirello, and G. Vitale, "A Survey on LoRa for Smart Agriculture: Current Trends and Future Perspectives," *IEEE Internet of Things Journal (Online,* vol. 10, no. 4, pp. 3664–3679, 2023. https://doi.org/10.1109/jiot.2022.3230505

[4]. M. Pradeep, and A. K. Tyagi, "Smart Sensor-Based Smart Agriculture for Better Crop Production in This Smart Era," In AI Applications for Business, Medical, and Agricultural Sustainability. *IGI Global*, pp. 236–266, 2024. https://doi.org/10.4018/979-8-3693-5266-3.ch009

[5]. Z. D. Atasoy, "An evaluation of the examples of mobile smart agriculture applications in Turkiye," *BIO Web of Conferences*, vol. 85, pp. 1–7, 2024. https://doi.org/10.1051/bioconf/20248501046

[6]. D. Kalfas, S. Kalogiannidis, O. Papaevangelou, K. Melfou, and F. Chatzitheodoridis, "Integration of Technology in Agricultural Practices towards Agricultural Sustainability: A Case Study of Greece," *Sustainability*, vol. 16, no. 7, pp. 1–24, 2024. https://doi.org/10.3390/su16072664

[7]. M. A. Rahu, S. Karim, S. M. Ali, G. M. Jatoi, and N. D. Sohu, "Integration of wireless sensor networks, internet of things, artificial intelligence, and deep learning in smart agriculture: A Comprehensive survey," *Journal of Innovative Intelligent Computing and Emerging Technologies (JIICET),* vol. 1, no. 1, pp. 8–19, 2024.

[8]. Y. Kalyani, L. Vorster, R. Whetton, and R. Collier, "Application Scenarios of Digital Twins for Smart Crop Farming through Cloud–Fog–Edge Infrastructure," *Future Internet*, vol. 16, no. 3, pp. 1–16, 2024. https://doi.org/10.3390/fi16030100

[9]. D. Rongwei, "Smart Precision Feeding system for dairy cows based on amplitude iterative pruning algorithm," *2024 5th International Conference on Mobile Computing and Sustainable Informatics (ICMCSI),* Lalitpur, Nepal, 18-19 January 2024, pp. 415–420. https://doi.org/10.1109/icmcsi61536.2024.00065

[10]. A. Hashmi, G. U. Mir, K. Sattar, S. S. Ullah, R. Alroobaea, J. Iqbal, and S. Hussain, "Effects of IoT Communication Protocols for Precision Agriculture in Outdoor Environments," *IEEE Access*, vol. 12, pp. 46410–46421, 2024. https://doi.org/10.1109/access.2024.3381522

[11]. A. Ahmed, I. Parveen, S. Abdullah, I. Ahmad, N. Alturki, and L. J. Menzli, "Optimized Data Fusion with Scheduled Rest Periods for Enhanced Smart Agriculture via Blockchain Integration," *IEEE Access*, vol. 12, pp. 15171–15193, 2024. https://doi.org/10.1109/access.2024.3357538

[12]. M. Akbari, A. Syed, W. S. Kennedy, and M. Erol-Kantarci, "AoI-Aware Energy-Efficient SFC in UAV-Aided Smart Agriculture Using Asynchronous Federated Learning," *IEEE Open Journal of the Communications Society*, vol. 5, pp. 1222–1242, 2024. https://doi.org/10.1109/ojcoms.2024.3363132

[13]. M. Barjaktarović, M. Santoni, and L. Bruzzone, "Design and Verification of a Low-Cost Multispectral Camera for Precision Agriculture Application," *IEEE Journal of Selected Topics in Applied Earth Observations and Remote Sensing*, vol. 17, pp. 6945–6957, 2024. https://doi.org/10.1109/jstars.2024.3377104

[14]. M. A. U. Haq, J. P. Sankar, F. Akram, and H. A. M. Malik, "Harvesting Prosperity: AI-Powered Solutions for Household Poverty Reduction through Smart Agriculture,"*2024 IEEE 1st Karachi Section Humanitarian Technology Conference (KHI-HTC),* Tandojam, Pakistan, 08-09 January 2024, pp. 1–5. https://doi.org/10.1109/khi-htc60760.2024.10482025

[15]. C. Eleftheriadis, G. Andronikidis, K. Kyranou, E. M. Pechlivani, I. Hadjigeorgiou, and Z. Batzos, "Machine learning for cybersecurity frameworks in smart farming," *2024 28th International Conference on Information Technology (IT),* Zabljak, Montenegro, 21-24 February 2024, pp. 1–5. https://doi.org/10.1109/it61232.2024.10475711

[16]. A. M. Haval, and F. H. Rahman, "Application of machine learning techniques and the Internet of Things for smart, sustainable agriculture," *BIO Web of Conferences*, vol. 82, pp. 1–11, 2024. https://doi.org/10.1051/bioconf/20248205021

[17]. N. Naidoo, and N. Munga, "Cyber Security in Smart Agriculture Technology," Snode Technologies. https://www.snode.com/resources/snode-agri-tech-white-paper.pdf (accessed June 15, 2024).

[18]. M. Dayoub, S. Shnaigat, R. A. Tarawneh, A. Al-Yacoub, F. Al-Barakeh, and K. Al-Najjar, "Enhancing Animal Production through Smart Agriculture: Possibilities, Hurdles, Resolutions, and Advantages," *Ruminants*, vol. 4, no. 1, pp. 22–46, 2024. https://doi.org/10.3390/ruminants4010003

[19]. B. Fulkar, S. Mendhe, and P. G. Patil, "Artificial Intelligence Cultivation: Transforming agriculture for a smart and Sustainable future," *2024 2nd International Conference on Intelligent Data Communication Technologies and Internet of Things (IDCIoT)*, Bengaluru, India, 04-06 January 2024, pp. 960–964. https://doi.org/10.1109/idciot59759.2024.10467857

[20]. E. K. Gyamfi, Z. ElSayed, J. Kropczynski, M. A. Yakubu, and N. Elsayed, "Agricultural 4.0 Leveraging on Technological Solutions: Study for Smart Farming Sector," *arXiv (Cornell University)*, pp. 1–9, 2024. https://doi.org/10.48550/arxiv.2401.00814

[21]. S. Sharma, M. Tomar, and R. Tyagi, "Artificial Intelligence and Vedic Scripture in Digital Agriculture for Global Economy," *2024 International Conference on Intelligent and Innovative Technologies in Computing, Electrical and Electronics (IITCEE)*, Bangalore, India, 24-25 January 2024, pp. 1–6. https://doi.org/10.1109/iitcee59897.2024.10467916

[22]. H. T. Bui, H. Aboutorab, A. Mahboubi, Y. Gao, N. H. Sultan, A. Chauhan, M. Z. Parvez, Bewong, R. Islam, Z. Islam, S. Camtepe, P. Gauravaram, D. M. Singh, A. Babar, and S. Yan, "Agriculture 4.0 and Beyond: Evaluating Cyber Threat Intelligence Sources and Techniques in Smart Farming Ecosystems," *Computers and Security*, vol. 140, pp. 1–32, 2024. https://doi.org/10.1016/j.cose.2024.103754

[23]. I. Guevara, S. Ryan, A. Singh, C. Brandon, and T. Margaria, "Edge IoT Prototyping Using Model-Driven Representations: A Use Case for Smart Agriculture," *Sensors*, vol. 24, no. 2, pp. 1–20, 2024. https://doi.org/10.3390/s24020495

[24]. T. H. H. Aldhyani, and H. Alkahtani, "Cyber Security for Detecting Distributed Denial of Service Attacks in Agriculture 4.0: Deep Learning Model," *Mathematics*, vol. 11, no. 1, pp. 1–19, 2023. https://doi.org/10.3390/math11010233

[25]. R. Nautiyal, R. S. Jha, S. Kathuria, R. Singh, A. Kathuria, and V. Pandey, "Artificial Intelligence Indulgence in Protection of Cybercrime," *2023 3rd International Conference on Pervasive Computing and Social Networking (ICPCSN)*, Salem, India, 19-20 June 2023, pp. 518–522. https://doi.org/10.1109/icpcsn58827.2023.00090

[26]. B. Guembe, A. A. Azeta, S. Misra, V. C. Osamor, L. F. Sanz, and V. Pospelova, "The emerging threat of AI-driven cyber attacks: a review," *Applied Artificial Intelligence*, vol. 36, no. 1, pp. e2037254-2376-e2037254-2409, 2022. https://doi.org/10.1080/08839514.2022.2037254

[27]. P. A. Ongadi, "A Comprehensive examination of security and privacy in precision Agriculture technologies," *GSC Advanced Research and Reviews*, vol. 18, no. 1, pp. 336–363, 2024. https://doi.org/10.30574/gscarr.2024.18.1.0026

[28]. G. De Jesus Coelho Da Silva, and C. B. Westphall, "A survey of large language models in cybersecurity," *arXiv (Cornell University)*, pp. 1–16, 2024. https://doi.org/10.48550/arxiv.2402.16968

[29]. Á. González, M. M. Espino, A. C. M. Román, Y. H. Fernández, and N. C. Pérez, "Ethics in Artificial Intelligence: an Approach to Cybersecurity," *Inteligencia Artificial*, vol. 27, no. 73, pp. 38–54, 2024. https://doi.org/10.4114/intartif.vol27iss73pp38-54

[30]. M. Rizvi, "Enhancing cybersecurity: The power of artificial intelligence in threat detection and prevention," *International Journal of Advanced Engineering Research and Sciences*, vol. 10, no. 5, pp. 055–060, 2023. https://doi.org/10.22161/ijaers.105.8

[31]. M. Muzammil, "Artificial Intelligence and Machine Learning in Cyber Security," Aalpha. https://www.aalpha.net/articles/artificial-intelligence-and-machine-learning-in-cyber-security/#:~:text=AI%20in%20cybersecurity%20involves%20the,automated%20and%20smart%20security%20defenses. (accessed April 8, 2024).

[32]. R. Kaur, D. Gabrijelčič, and T. Klobučar, "Artificial intelligence for cybersecurity: Literature review and future research directions," *Information Fusion*, vol. 97, pp. 1–29, 2023. https://doi.org/10.1016/j.inffus.2023.101804

[33]. S. Islam, Md. A. Hayat, and Md. F. Hossain, "Artificial Intelligence for Cybersecurity: Impact, Limitations and Future Research Directions," *Journal of Emerging Trends and Novel Research*, vol. 1, no. 12, pp. a297–a319, 2023.

[34]. A. O. Adewusi, U. I. Okoli, T. Olorunsogo, E. M. Adaga, D. O. Daraojimba, and O. Chimezie, "Artificial intelligence in cybersecurity: Protecting national infrastructure: A USA review," *World Journal of Advanced Research and Reviews*, vol. 21, no. 1, pp. 2263–2275, 2024. https://doi.org/10.30574/wjarr.2024.21.1.0313

[35]. T. A. Inbamala, and A. Rengarajan, "The Role of Machine Learning in Detecting and Preventing Data Breaches," *International Journal of Innovative Research in Computer and Communication Engineering*, vol. 12, no. 02, pp. 1025–1030, 2024. https://doi.org/10.15680/ijircce.2024.1202050

[36]. M. Malatji, and A. Tolah, "Artificial intelligence (AI) cybersecurity dimensions: a comprehensive framework for understanding adversarial and offensive AI," *AI And Ethics*, pp. 1–29, 2024. https://doi.org/10.1007/s43681-024-00427-4

[37]. M. S. Nour, and A. S. Said, "Harnessing the power of AI for effective cybersecurity defense," *2024 6th International Conference on Computing and Informatics (ICCI)*, New Cairo - Cairo, Egypt, 06-07 March 2024, pp. 1–5. https://doi.org/10.1109/icci61671.2024.10485059

[38]. A. D. Sontan, and S. Samuel, "The intersection of Artificial Intelligence and cybersecurity: Challenges and opportunities," *World Journal of Advanced Research and Reviews*, vol. 21, no. 2, pp. 1720–1736, 2024. https://doi.org/10.30574/wjarr.2024.21.2.0607

[39]. M. Humayun, N. Tariq, M. Alfayad, M. Zakwan, G. Alwakid, and M. Assiri, "Securing the Internet of Things in Artificial Intelligence Era: A Comprehensive Survey," *IEEE Access*, vol. 12, pp. 25469–25490, 2024. https://doi.org/10.1109/access.2024.3365634

[40]. A. A. AlZubi, and K. Galyna, "Artificial Intelligence and Internet of Things for Sustainable Farming and Smart Agriculture," *IEEE Access*, vol. 11, pp. 78686–78692, 2023. https://doi.org/10.1109/access.2023.3298215

[41]. S. Polymeni, S. Plastras, D. N. Skoutas, G. Kormentzas, and C. Skianis, "The Impact of 6G-IoT Technologies on the Development of Agriculture 5.0: A Review," *Electronics*, vol. 12, no. 12, pp. 1–24, 2023. https://doi.org/10.3390/electronics12122651

[42]. Y. Pang, F. Marinello, P. Tang, H. Li, and Q. Liang, "Bibliometric Analysis of Trends in Smart Irrigation for Smart Agriculture," *Sustainability*, vol. 15, no. 23, pp. 1–23, 2023. https://doi.org/10.3390/su152316420

[43]. Nitin, and S. B. Gupta, "Artificial Intelligence in Smart Agriculture: Applications and Challenges," *Current Applied Science and Technology*, vol. 24, no. 2, pp. 1–24, 2024. https://doi.org/10.55003/cast.2023.254427

[44]. S. Padhy, M. Alowaidi, S. Dash, M. Alshehri, P. P. Malla, S. Routray, and H. Alhumyani, "AgriSecure: A Fog Computing-Based Security Framework for Agriculture 4.0 via Blockchain," *Processes*, vol. 11, no. 3, pp. 1–27, 2023. https://doi.org/10.3390/pr11030757

[45]. S. Fountas, B. Espejo-García, A. Kasimati, M. Gemtou, H. Panoutsopoulos, and E. Anastasiou, "Agriculture 5.0: Cutting-Edge Technologies, Trends, and Challenges," *IT Professional*, vol. 26, no. 1, pp. 40–47, 2024. https://doi.org/10.1109/mitp.2024.3358972

[46]. M. S. E. De La Parte, S. Lana-Serrano, M. M. Elduayen, and J. Martínez-Ortega, "Spatio-Temporal Semantic Data Model for Precision Agriculture IoT Networks," *Agriculture*, vol. 13, no. 2, pp. 1–28, 2023. https://doi.org/10.3390/agriculture13020360

[47]. A. Holzinger, I. Fister, Jr, I. Fister, H. Kaul, and , S. Asseng "Human-Centered AI in Smart Farming: Towards Agriculture 5.0," *IEEE Access*, vol. 12, pp. 62199–62214, 2024. https://doi.org/10.1109/access.2024.3395532

[48]. N. N. Thilakarathne, M. S. A. Bakar, P. E. Abas, and H. Yassin, "Towards making the fields talks: A real-time cloud enabled IoT crop management platform for smart agriculture," *Frontiers in Plant Science*, vol. 13, pp. 1–25, 2023. https://doi.org/10.3389/fpls.2022.1030168

[49]. G. Zhu, and T. D. Palaoag, "Implementation and Evaluation of Smart Agriculture System based on Big Data Analytics," *2023 9th International Conference on Systems and Informatics (ICSAI)*, Changsha, China, 16-18 December 2023, pp. 1–4. https://doi.org/10.1109/icsai61474.2023.10423334

[50]. M. N. Mowla, N. Mowla, A. F. M. S. Shah, E. Alsusa, and T. Shongwe, "Internet of Things and Wireless Sensor Networks for Smart Agriculture Applications- A Survey," *IEEE Access*, vol. 11, pp. 145813–145852, 2023. https://doi.org/10.1109/access.2023.3346299

[51]. S. Mishra, S. K. Nayak, and R. N. Yadav, "An Energy Efficient LoRa-based Multi-Sensor IoT Network for Smart Sensor Agriculture System," *2023 IEEE Topical Conference on Wireless Sensors and Sensor Networks*, Las Vegas, NV, USA, 22-25 January 2023, pp. 28–31. https://doi.org/10.1109/wisnet56959.2023.10046242

[52]. S. P. Singh, G. Dhiman, S. Juneja, W. Viriyasitavat, G. Singal, N. Kumar, and P. Johri, "A New QoS Optimization in IoT-Smart Agriculture Using Rapid-Adaption-Based Nature-Inspired Approach," *IEEE Internet of Things Journal*, vol. 11, no. 3, pp. 5417–5426, 2024. https://doi.org/10.1109/jiot.2023.3306353

[53]. M. O. Yerebakan, and B. Hu, "Human–Robot Collaboration in Modern Agriculture: A Review of the Current Research Landscape," *Advanced Intelligent Systems*, pp. 1–25, 2024. https://doi.org/10.1002/aisy.202300823

[54]. X. Xu, R. Patibandla, A. Arora, M. Al-Razgan, E. M. Awwad, and V. O. Nyangaresi, "An Adaptive Hybrid (1D-2D) Convolution-based ShuffleNetV2 Mechanism for Irrigation Levels Prediction in Agricultural Fields with Smart IoTs," *IEEE Access*, pp. 1–19, 2024. https://doi.org/10.1109/access.2024.3384473

[55]. E. Kariri, "IoT Powered Agricultural Cyber-Physical System: Security Issue Assessment," *IETE Journal of Research*, pp. 1–11, 2022. https://doi.org/10.1080/03772063.2022.2032848

[56]. G. Singh, and J. Singh, "A Cost Effective IoT-Assisted Framework Coupled with Fog Computing for Smart Agriculture," *2023 IEEE 8th International Conference for Convergence in Technology (I2CT)*, Pune, India, 7-9 April 2023, pp. 1–8. https://doi.org/10.1109/i2ct57861.2023.10126231

[57]. A. Alahmadi, S. U. Rehman, H. Alhazmi, D. G. Glynn, H. Shoaib, and P. Solé, "Cyber-Security Threats and Side-Channel Attacks for Digital Agriculture," *Sensors*, vol. 22, no. 9, pp. 1–14, 2022. https://doi.org/10.3390/s22093520

[58]. S. Condran, M. Bewong, Z. Islam, L. Maphosa, and L. Zheng, "Machine Learning in Precision Agriculture: A Survey on Trends, Applications and Evaluations Over Two Decades," *IEEE Access*, vol. 10, pp. 73786–73803, 2022. https://doi.org/10.1109/access.2022.3188649

[59]. M. S. Farooq, O. O. Sohail, A. Abid, and S. Rasheed, "A Survey on the Role of IoT in Agriculture for the Implementation of Smart Livestock Environment," *IEEE Access*, vol. 10, pp. 9483–9505, 2022. https://doi.org/10.1109/access.2022.3142848

[60]. B. K. Shukla, N. Maurya, and M. Sharma, "Advancements in Sensor-Based Technologies for Precision Agriculture: An Exploration of Interoperability, Analytics and Deployment Strategies," *Engineering Proceedings*, vol. 58, no. 1, pp. 1–6, 2023. https://doi.org/10.3390/ecsa-10-16051

[61]. E. S. Hassan, A. A. Alharbi, A. S. Oshaba, and A. El-Emary, "Enhancing smart irrigation efficiency: a new WSN-Based localization method for water conservation," *Water*, vol. 16, no. 5, pp. 1–17, 2024. https://doi.org/10.3390/w16050672

[62]. A. Soussi, E. Zero, R. Sacile, D. Trinchero, and M. Fossa, "Smart Sensors and Smart Data for Precision Agriculture: A Review," *Sensors*, vol. 24, no. 8, pp. 1–32, 2024. https://doi.org/10.3390/s24082647

[63]. S. Ahmadi, "A Systematic Literature Review: Security Threats and Countermeasures in Smart Farming," *TechRxiv*, pp. 1–16, 2023. https://doi.org/10.36227/techrxiv.22029974.v1

[64]. M. M. Mijwil, I. Bala, G. Ali, M. Aljanabi, M. Abotaleb, R. Doshi, K. K. Hiran, and E.-S. M. El-Kenawy, "Sensing of Type 2 diabetes patients based on Internet of Things solutions: an extensive survey," In Modern Technology in

Healthcare and Medical Education: Blockchain, IoT, AR, and VR, *IGI Global*, pp. 34–46, 2024. https://doi.org/10.4018/979-8-3693-5493-3.ch003

[65]. E. M. B. M. Karunathilake, A. T. Le, S. Heo, Y. Chung, and S. Mansoor, "The Path to Smart Farming: Innovations and Opportunities in Precision Agriculture," *Agriculture*, vol. 13, no. 8, pp. 1–26, 2023. https://doi.org/10.3390/agriculture13081593

[66]. C. T. Nautiyal, P. Nautiyal, G. Papnai, H. Mittal, K. Agrawal, Shivani, Vishesh, and R. Nandini, "Importance of Smart Agriculture and Use of Artificial Intelligence in Shaping the Future of Agriculture," *Journal of Scientific Research and Reports*, vol. 30, no. 3, pp. 129–138, 2024. https://doi.org/10.9734/jsrr/2024/v30i31864

[67]. K. Taji, and F. Ghanimi, "Enhancing security and privacy in smart agriculture: a novel homomorphic signcryption system," *Results in Engineering*, vol. 22, pp. 1–14, 2024. https://doi.org/10.1016/j.rineng.2024.102310

[68]. L. S. Vailshery, "Agricultural Industrial Internet of Things (IIoT) market size worldwide from 2020 to 2025," Statista. https://www.statista.com/statistics/1222813/worldwide-agricultural-industrial-iot-market-value/ (accessed April 19, 2024).

[69]. S. Tiwari, A. Sharma, A. Jain, D. Gupta, M. Goňo, R. Goňo, Z. Leonowicz, and M. Jasiński, "IOT-Enabled Model for Weed Seedling Classification: An Application for Smart Agriculture," *AgriEngineering*, vol. 5, no. 1, pp. 257–272, 2023. https://doi.org/10.3390/agriengineering5010017

[70]. S. Terence, J. Immaculate, A. Raj, and J. Nadarajan, "Systematic Review on Internet of Things in Smart Livestock Management Systems," *Sustainability*, vol. 16, no. 10, pp. 1–37, 2024. https://doi.org/10.3390/su16104073

[71]. S. Arya, S. Tripathi, A. Srivastava, S. Aggarwal, N. Soni, and S. A. Ansar, "Double-Edged Agriculture 4.0: Hodiernal expedient technologies and Cyber-Security Challenges," *2023 6th International Conference on Contemporary Computing and Informatics (IC3I)*, Gautam Buddha Nagar, India, 14-16 September 2023, pp. 313–320. https://doi.org/10.1109/ic3i59117.2023.10398136

[72]. A. Tyagi, Z. A. Mir, and S. Ali, "Revisiting the Role of Sensors for Shaping Plant Research: Applications and Future Perspectives," *Sensors*, vol. 24, no. 11, pp. 1–21, 2024. https://doi.org/10.3390/s24113261

[73]. M. Shahbandeh, "Global market value of agricultural sensors 2021-2027, by application," Statista. https://www.statista.com/statistics/1306915/global-market-of-agricultural-sensors-by-application/ (accessed April 19, 2024).

[74]. B. Zhang, and Y. Qiao, "AI, Sensors, and Robotics for Smart Agriculture," *Agronomy*, vol. 14, no. 6, pp. 1–3, 2024. https://doi.org/10.3390/agronomy14061180

[75]. W. K. Alazzai, M. Obaid, B. S. Abood, and L. Jasim, "Smart Agriculture Solutions: Harnessing AI and IoT for Crop Management," *E3S Web of Conferences*, vol. 477, pp. 1–7, 2024. https://doi.org/10.1051/e3sconf/202447700057

[76]. D. Kaplun, S. Deka, A. Bora, N. Choudhury, J. Basistha, B. Purkayastha, I. Z. Mazumder, V. V. Gulvanskii, K. K. Sarma, and D. D. Misra, "An intelligent agriculture management system for rainfall prediction and fruit health monitoring," *Scientific Reports*, vol. 14, no. 1, pp. 1–23, 2024. https://doi.org/10.1038/s41598-023-49186-y

[77]. A. Issa, S. Majed, S. Ameer, and H. M. Al–Jawahry, "Farming in the Digital Age: Smart Agriculture with AI and IoT," *E3S Web of Conferences*, vol. 477, pp. 1–6, 2024. https://doi.org/10.1051/e3sconf/202447700081

[78]. G. Mohyuddin, M. A. Khan, A. Haseeb, S. Mahpara, M. Waseem, and A. M. Saleh, "Evaluation of Machine Learning approaches for precision Farming in Smart Agriculture System - A comprehensive Review," *IEEE Access*, vol. 12, pp. 60155–60184, 2024. https://doi.org/10.1109/access.2024.3390581

[79]. J. Lindner, "UAV Industry Statistics," GITNUX. https://gitnux.org/uav-industry/#:~:text=More%20than%2070%25%20of%20drone,USD%2040.7%20billion%20by%202026. (accessed April 19, 2024).

[80]. N. Victor, P. K. R. Maddikunta, D. R. K. Mary, M. Ramalingam, R. Chengoden, T. R. Gadekallu, N. Rakesh, Y. Zhu, and J. Paek, "Remote Sensing for Agriculture in the Era of Industry 5.0 – A survey," *IEEE Journal of Selected Topics in Applied Earth Observations and Remote Sensing*, vol. 17, pp. 5920–5945, 2024. https://doi.org/10.1109/jstars.2024.3370508

[81]. H. Qu, and W. Su, "Deep Learning-Based Weed–Crop Recognition for Smart Agricultural Equipment: A Review," *Agronomy*, vol. 14, no. 2, pp. 1–28, 2024. https://doi.org/10.3390/agronomy14020363

[82]. D. Muthumanickam, C. Poongodi, K. Ramalingam, S. Pazhanivelan, and R. Kaliaperumal, "Smart Farming: Internet of Things (IoT)-Based Sustainable Agriculture," *Agriculture*, vol. 12, no. 10, pp. 1–26, 2022. https://doi.org/10.3390/agriculture12101745

[83]. G. Gkagkas, D. J. Vergados, A. Michalas, and M. Dossis, "The Advantage of the 5G Network for Enhancing the Internet of Things and the Evolution of the 6G Network," *Sensors*, vol. 24, no. 8, pp. 1–18, 2024. https://doi.org/10.3390/s24082455

[84]. P. Taylor, "5G technology market revenues worldwide 2020-2026," Statista. https://www.statista.com/aboutus/our-research-commitment/3282/petroc-taylor (accessed April 19, 2024).

[85]. J. Liu, L. Shu, X. Lu, and L. Shu, "Survey of Intelligent Agricultural IoT Based on 5G," *Electronics*, vol. 12, no. 10, pp. 1–46, 2023. https://doi.org/10.3390/electronics12102336

[86]. M. A. Khan, A. Khan, M. Abuibaid, and J. Huang, "Harnessing 5G networks for enhanced precision Agriculture: challenges and potential solutions," *2023 International Conference on Smart Applications, Communications and Networking (SmartNets)*, Istanbul, Turkiye, 25-27 July 2023, pp. 1–6. https://doi.org/10.1109/smartnets58706.2023.10215761

[87]. A. Gunawan, B. G. G. Odang, K. Honggiarto, and F. L. Cahyadi, "Understanding the Uses and Potential of IoT with 5G Technology compared to 4G LTE: A Systematic literature review," *2023 International Conference on Information*

Management and Technology (ICIMTech), Malang, Indonesia, 24-25 August 2023, pp. 101–106. https://doi.org/10.1109/icimtech59029.2023.10277995

[88]. J.P. Ferreira, V.C. Ferreira, S.L. Nogueira, J.M. Faria, and J.A. Afonso, "A Flexible Infrastructure-Sharing 5G Network Architecture Based on Network Slicing and Roaming," *Information*, vol. 15, no. 4, pp. 1-15, 2024. https://doi.org/10.3390/info15040213

[89]. P. Tang, Q. Liang, H. Li, and Y. Pang, "Application of Internet-of-Things Wireless Communication Technology in Agricultural Irrigation Management: A Review," *Sustainability*, vol. 16, no. 9, pp. 1–19, 2024. https://doi.org/10.3390/su16093575

[90]. S.R. Raja, B. Subashini, and R.S. Prabu, "5G Technology in Smart Farming and Its Applications," In: Balasubramanian, S. Natarajan, G. Chelliah, P.R. (eds) Intelligent Robots and Drones for Precision Agriculture. Signals and Communication Technology. *Springer*, 2024. https://doi.org/10.1007/978-3-031-51195-0_12

[91]. G. K. Akella, S. Wibowo, S. Grandhi, and S. Mubarak, "A Systematic Review of Blockchain Technology Adoption Barriers and Enablers for Smart and Sustainable Agriculture," *Big Data and Cognitive Computing*, vol. 7, no. 2, pp. 1–22, 2023. https://doi.org/10.3390/bdcc7020086

[92]. A. Aliyu, and J. Liu, "Blockchain-Based Smart Farm Security Framework for the Internet of Things," *Sensors*, vol. 23, no. 18, pp. 1–13, 2023. https://doi.org/10.3390/s23187992

[93]. O. H. Abdelkader, H. Bouzebiba, D. Pena, and A. P. Aguiar, "Energy-Efficient IoT-Based Light Control System in Smart Indoor Agriculture," *Sensors*, vol. 23, no. 18, pp. 1–20, 2023. https://doi.org/10.3390/s23187670

[94]. M. Escribà-Gelonch, S. Liang, P. van Schalkwyk, I. Fisk, N. V. D. Long, and V. Hessel, "Digital Twins in Agriculture: Orchestration and Applications," *Journal of agricultural and food chemistry*, vol. 72, no. 19, pp. 10737–10752, 2024. https://doi.org/10.1021/acs.jafc.4c01934

[95]. Y. Kalyani, L. M. Vorster, R. Whetton, and R. W. Collier, "Application Scenarios of Digital Twins for Smart Crop Farming through Cloud–Fog–Edge Infrastructure," *Future Internet*, vol. 16, no. 3, pp. 1–16, 2024. https://doi.org/10.3390/fi16030100

[96]. A. C. Tagarakis, L. Benos, G. Kyriakarakos, S. Pearson, C. G. Sørensen, and D. Bochtis, "Digital Twins in Agriculture and Forestry: A Review," *Sensors*, vol. 24, no. 10, pp. 1–26, 2024. https://doi.org/10.3390/s24103117

[97]. N. Peladarinos, D. Piromalis, V. Cheimaras, E. Tserepas, R. A. Munteanu, and P. Papageorgas, "Enhancing smart Agriculture by Implementing Digital Twins: A Comprehensive review," *Sensors*, vol. 23, no. 16, pp. 1–38, 2023. https://doi.org/10.3390/s23167128

[98]. W. Purcell, and T. Neubauer, "Digital Twins in Agriculture: A State-of-the-art review," *Smart Agricultural Technology*, vol. 3, pp. 1–11, 2023. https://doi.org/10.1016/j.atech.2022.100094

[99]. P. Catala-Roman, E. A. Navarro, J. Segura-Garcia, and M. Garcia-Pineda, "Harnessing Digital Twins for Agriculture 5.0: A Comparative Analysis of 3D Point Cloud Tools," *Applied Sciences*, vol. 14, no. 5, pp. 1–19, 2024. https://doi.org/10.3390/app14051709

[100]. L. Wang, "Digital Twins in Agriculture: A Review of Recent Progress and Open Issues," *Electronics*, vol. 13, no. 11, pp. 1–26, 2024. https://doi.org/10.3390/electronics13112209

[101]. M. Otieno, "An extensive survey of smart agriculture technologies: Current security posture," *World Journal of Advanced Research and Reviews*, vol. 18, no. 3, pp. 1207–1231, 2023. https://doi.org/10.30574/wjarr.2023.18.3.1241

[102]. T. Ganetsos, A. Κάνταρος, N. Gioldasis, and K. Brachos, "Applications of 3D Printing and Illustration in Industry," *2023 17th International Conference on Engineering of Modern Electric Systems (EMES)*, Oradea, Romania, 09-10 June 2023, pp. 1–4. https://doi.org/10.1109/emes58375.2023.10171656

[103]. P. Lakkala, S. R. Munnangi, S. Bandari, and M. A. Repka, "Additive manufacturing technologies with emphasis on stereolithography 3D printing in pharmaceutical and medical applications: A review," *International Journal of Pharmaceutics*: X, vol. 5, pp. 1–16, 2023. https://doi.org/10.1016/j.ijpx.2023.100159

[104]. M. Javaid, A. Haleem, R. P. Singh, R. Suman, and S. Rab, "Role of additive manufacturing applications towards environmental sustainability," *Advanced Industrial and Engineering Polymer Research*, vol. 4, no. 4, pp. 312–322, 2021. https://doi.org/10.1016/j.aiepr.2021.07.005

[105]. D. J. S. Agron, and W. S. Kim, "3D Printing Technology: Role in Safeguarding Food Security," *Analytical chemistry*, vol. 96, no. 11, pp. 4333–4342, 2024. https://doi.org/10.1021/acs.analchem.3c05190

[106]. D. Shikha, K. A. V. Sindhura, M. Rastogi, B. Saritha, S. N. Satapathy, S. Srivastava, and A. K. Kurdekar, "A Review on Propelling Agricultural Practices with Biotechnology into a New Era," *Journal of Advances in Biology and Biotechnology*, vol. 27, no. 3, pp. 99–111, 2024. https://doi.org/10.9734/jabb/2024/v27i3725

[107]. L. Badadyan, "Research and Recent Achievements in Agriculture and Biotechnology with Innovative Technologies Application," *E3S Web of Conferences*, vol. 493, pp. 1–11, 2024. https://doi.org/10.1051/e3sconf/202449301010

[108]. S. Gorjian, O. Fakhraei, A. Gorjian, A. Sharafkhani, and A. Aziznejad, "Sustainable Food and Agriculture: Employment of Renewable Energy Technologies," *Current Robotics Reports*, vol. 3, no. 3, pp. 153–163, 2022. https://doi.org/10.1007/s43154-022-00080-x

[109]. A. Bathaei, and D. Štreimikienė, "Renewable Energy and Sustainable Agriculture: Review of Indicators," *Sustainability*, vol. 15, no. 19, pp. 1–24, 2023. https://doi.org/10.3390/su151914307

[110]. S. Mandal, A. Yadav, F. A. Panme, K. M. Devi, and S. K. SM, "Adaption of smart applications in agriculture to enhance production," *Smart Agricultural Technology*, vol. 7, pp. 1–11, 2024. https://doi.org/10.1016/j.atech.2024.100431

[111]. D. Hua, N. Petrina, N. Young, J. Cho, and S. K. Poon, "Understanding the factors influencing acceptability of AI in medical imaging domains among healthcare professionals: A scoping review," *Artificial Intelligence in Medicine*, vol. 147, pp. 1–14, 2024. https://doi.org/10.1016/j.artmed.2023.102698

[112]. M. M. Mijwil, O. Adelaja, A. Badr, G. Ali, B. A. Buruga, and P. Thapa, "Innovative Livestock: A Survey of Artificial Intelligence Techniques in Livestock Farming Management," *Wasit Journal of Computer and Mathematics Science*, vol. 2, no. 4, pp. 99–106, 2023. https://doi.org/10.31185/wjcms.206

[113]. S. Majumder, Y. Khandelwal, and K, Sornalakshmi. "Computer Vision and generative AI for yield prediction in digital agriculture," *2024 2nd International Conference on Networking and Communications (ICNWC),* 02-04 April 2024, Chennai, India, pp.1–6. https://doi.org/10.1109/icnwc60771.2024.10537337

[114]. F. Salehi, "The Role of Artificial Intelligence in Revolutionizing the Agriculture Industry in Canada," *Asian Journal of Research and Review in Agriculture*, vol. 6, no. 1, pp. 70–78, 2024.

[115]. K. R. Reddy, S. Arshiya, S. L. Surabhi, M. Subhashini, V. Manasa, and K. Haripriya, "Renewable Energy Integration into Cloud and IoT Based Smart Agriculture," *International Journal of Progressive Research in Engineering Management and Science (IJPREMS*, vol. 4, no. 4, pp. 1689–1696, 2024. https://www.ijprems.com/

[116]. M. Del-Coco, M. Leo, and P. Carcagnì, "Machine Learning for Smart Irrigation in Agriculture: How Far along Are We?," *Information*, vol. 15, no. 6, pp. 1–23, 2024. https://doi.org/10.3390/info15060306

[117]. P. Thongnim, V. Yuvanatemiya, and P. Srinil, "Smart Agriculture: Transforming Agriculture with Technology," In Communications in computer and information science. *Springer Nature*, pp. 362–376, 2024. https://doi.org/10.1007/978-981-99-7240-1_29

[118]. E. E. K. Senoo, L. Anggraini, J. A. Kumi, L. B. Karolina, E. Akansah, H. A. Sulyman, Mendonça, I. and M. Aritsugi, "IoT Solutions with Artificial Intelligence Technologies for Precision Agriculture: Definitions, Applications, Challenges, and Opportunities," *Electronics*, vol. 13, no. 10, pp. 1–89, 2024. https://doi.org/10.3390/electronics13101894

[119]. K. Bezas, and F. Filippidou, "The Role of Artificial Intelligence and Machine Learning in Smart and Precision Agriculture," *Indonesian Journal of Computer Science*, vol. 12, no. 4, pp. 1576–1588, 2023.

[120]. B. Subedi, and G. Sharma, "Smart Agriculture: Components, Processes, Challenges, and Future Perspectives," *Journal of Data Mining and Management*, vol. 8, no. 2, pp. 28–40, 2023.

[121]. M. Papri, D. Subhankar, C. Arindam, and D. Santosh, "Advanced Technologies in Smart Agriculture: Applications and Challenges," In M. Sagar, G. J. Dinkar, and D. Santosh (Eds). Advances in Agricultural Technology. *Griffon*, pp. 81-99, 2023.

[122]. S. K. Phang, T. Chiang, A. Happonen, and M. M. L. Chang, "From Satellite to UAV-Based Remote Sensing: A Review on Precision Agriculture," *IEEE Access*, vol. 11, pp. 127057–127076, 2023. https://doi.org/10.1109/access.2023.3330886

[123]. S. Alam, "Security concerns in smart agriculture and blockchain-based solution," *2022 OPJU International Technology Conference on Emerging Technologies for Sustainable Development (OTCON)*, Raigarh, Chhattisgarh, India, 08-10 February 2023, pp. 1–6. https://doi.org/10.1109/otcon56053.2023.10113953

[124]. M. R. M. Kassim, "Applications of IoT and blockchain in smart agriculture: architectures and challenges," *2022 IEEE International Conference on Computing (ICOCO)*, Kota Kinabalu, Malaysia, 14-16 November 2022, pp. 253-258. https://doi.org/10.1109/icoco56118.2022.10031697

[125]. M. Niu, and T. Shi, "Application and Development of Smart Agriculture based on Internet of Things," *Frontiers in Computing and Intelligent Systems*, vol. 3, no. 3, pp. 55–58, 2023. https://doi.org/10.54097/fcis.v3i3.8566

[126]. E. Bouali, M. R. Abid, E. Boufounas, T. A. Hamed, and D. Benhaddou, "Renewable Energy Integration into Cloud and IoT-Based Smart Agriculture," *IEEE Access*, vol. 10, pp. 1175–1191, 2022. https://doi.org/10.1109/access.2021.3138160

[127]. R. Rani, J. Sahoo, S. Bellamkonda, S. Kumar, and S. K. Pippal, "Role of Artificial Intelligence in Agriculture: An Analysis and Advancements with Focus on Plant Diseases," *IEEE Access*, vol. 11, pp. 137999–138019, 2023. https://doi.org/10.1109/access.2023.3339375

[128]. J. Kaur, S. M. H. Fard, M. Amiri-Zarandi, and R. Dara, "Protecting farmers' data privacy and confidentiality: Recommendations and considerations," *Frontiers in Sustainable Food Systems*, vol. 6, pp. 1–9, 2022. https://doi.org/10.3389/fsufs.2022.903230

[129]. G. Ali, M. M. Mijwil, B. A. Buruga, and M. Abotaleb, "A Comprehensive Review on Cybersecurity Issues and Their Mitigation Measures in FinTech," *Iraqi Journal for Computer Science and Mathematics*, vol. 5, no. 3, pp. 45–91, 2024. https://doi.org/10.52866/ijcsm.2024.05.03.004

[130]. V. Kumar, K. V. Sharma, N. Kedam, A. Patel, T. R. Kate, and U. Rathnayake, "A comprehensive review on smart and sustainable agriculture using IoT technologies," *Smart Agricultural Technology*, vol. 8, pp. 1–23, 2024. https://doi.org/10.1016/j.atech.2024.100487

[131]. S. Dargaoui, M. Azrour, A. E. Allaoui, A. Guezzaz, S. Benkirane, A. Alabdulatif, and F. Amounas, "Internet-of-Things-Enabled Smart Agriculture: security enhancement approaches," *2024 4th International Conference on Innovative Research in Applied Science, Engineering and Technology (IRASET),* Fez, Morocco, 16-17 May 2024, pp. 1–5. https://doi.org/10.1109/iraset60544.2024.10548705

[132]. S. Rudrakar, and P. Rughani, "IoT Based Agriculture (AG-IoT): A detailed study on architecture, security and forensics," *Information Processing in Agriculture*, pp. 1–18, 2023. https://doi.org/10.1016/j.inpa.2023.09.002

[133]. O. Friha, M. A. Ferrag, Λ. Μαγλαράς, and L. Shu, "Digital Agriculture Security: Aspects, Threats, Mitigation Strategies, and Future Trends," *IEEE Internet of Things Magazine*, vol. 5, no. 3, pp. 82–90, 2022. https://doi.org/10.1109/iotm.001.2100164

[134]. A. Yazdinejad, B. Zolfaghari, A. Azmoodeh, A. Dehghantanha, A. Dehghantanha, E. D. G. Fraser, A. G. Green, C. Russell, and E. Duncan, "A Review on Security of Smart Farming and Precision Agriculture: Security Aspects, Attacks, Threats and Countermeasures," *Applied Sciences*, vol. 11, no. 16, pp. 1–24, 2021. https://doi.org/10.3390/app11167518

[135]. T. Koduru, and N. P. Koduru, "An Overview of Vulnerabilities in Smart Farming Systems," *Journal of Student Research*, vol. 11, no. 1, pp. 1–14, 2022. https://doi.org/10.47611/jsrhs.v11i1.2303

[136]. A. Naseer, M. Shmoon, T. Shakeel, S. U. Rehman, A. Ahmad, and V. Gruhn, "A Systematic Literature review of the IoT in agriculture - global adoption, innovations, security privacy challenges," *IEEE Access*, vol. 12, pp. 60986–61021, 2024. https://doi.org/10.1109/access.2024.3394617

[137]. A. Kulkarni, W. Ying-Jie, M. Gopinath, D. Sobien, A. Rahman, and F. A. Batarseh, "A Review of Cybersecurity Incidents in the Food and Agriculture Sector," *arXiv (Cornell University)*, pp. 1–34, 2024. https://doi.org/10.48550/arxiv.2403.08036

[138]. I. Bibi, A. Akhunzada, and N. Kumar, "Deep AI-Powered Cyber Threat Analysis in IIoT," *IEEE Internet of Things Journal*, vol. 10, no. 9, pp. 7749–7760, 2023. https://doi.org/10.1109/jiot.2022.3229722

[139]. S. Sarowa, V. Kumar, B. Bhanot, and M. Kumar, "Enhancement of security posture in smart farming: challenges and proposed solution," *2023 International Conference on Device Intelligence, Computing and Communication Technologies, (DICCT)*, Dehradun, India, 17-18 March 2023, pp. 155–159. https://doi.org/10.1109/dicct56244.2023.10110208

[140]. G. Ali, and M. M. Mijwil, "Cybersecurity for Sustainable Smart Healthcare: State of the Art, Taxonomy, Mechanisms, and Essential Roles," *Mesopotamian Journal of CyberSecurity*, vol. 4, no. 2, pp. 20–62, 2024. https://doi.org/10.58496/MJCS/2024/006

[141]. S. Qazi, B. A. Khawaja, and Q. U. Farooq, "IoT-Equipped and AI-Enabled Next Generation Smart Agriculture: A Critical Review, Current Challenges and Future Trends," *IEEE Access*, vol. 10, pp. 21219–21235, 2022. https://doi.org/10.1109/access.2022.3152544

[142]. F. Kuntke, V. N. Romanenko, S. Linsner, E. Steinbrink, and C. Reuter, "LoRaWAN security issues and mitigation options by the example of agricultural IoT scenarios," *Transactions on Emerging Telecommunications Technologies*, vol. 33, no. 5, pp. 1–20, 2022. https://doi.org/10.1002/ett.4452

[143]. S.P. Priyadharshini, and P. Balamurugan, "Unmanned aerial vehicle in the smart farming Systems: Types, applications and Cyber-Security threats," *2022 International Conference on Innovative Computing, Intelligent Communication and Smart Electrical Systems (ICSES)*, Chennai, India, 15-16 July 2022, pp. 1–9. https://doi.org/10.1109/icses55317.2022.9914070

[144]. S. R. A. Balaji, S. P. Rao, and P. Ranganathan, "Cybersecurity challenges and solutions in IoT-based precision farming systems," *2023 IEEE 14th Annual Ubiquitous Computing, Electronics and Mobile Communication Conference (UEMCON)*, New York, NY, USA, 12-14 October 2023, pp. 0237–0246. https://doi.org/10.1109/uemcon59035.2023.10316154

[145]. O. S. Albahri, and A. H. Alamoodi, "Cybersecurity and Artificial intelligence Applications: A bibliometric analysis based on Scopus database," *Mesopotamian Journal of CyberSecurity*, vol. 2023, pp. 158–169, 2023. https://doi.org/10.58496/mjcsc/2023/018

[146]. M. A. Ali, and A. Alqaraghuli, "A Survey on the Significance of Artificial intelligence (AI) in Network cybersecurity," *Babylonian Journal of Networking*, vol. 2023, pp. 21–29, 2023. https://doi.org/10.58496/bjn/2023/004

[147]. J. P. Bharadiya, "AI-Driven Security: How Machine Learning Will Shape the Future of Cybersecurity and Web 3," *American Journal of Neural Networks and Applications*, vol. 9, no. 1, pp. 1–7, 2023. https://doi.org/10.11648/j.ajnna.20230901.11

[148]. M. M. Mijwil, M. Aljanabi, and ChatGPT. "Towards Artificial Intelligence-Based Cybersecurity: The Practices and ChatGPT Generated Ways to Combat Cybercrime," *Iraqi Journal for Computer Science and Mathematics*, vol. 4, no. 1, pp. 65–70, 2023. https://doi.org/10.52866/ijcsm.2023.01.01.0019

[149]. M. M. Mijwil, G. Ali, and E. Sadıkoğlu, "The Evolving Role of Artificial Intelligence in the Future of Distance Learning: Exploring the Next Frontier," *Mesopotamian Journal of Computer Science*, vol. 2023, pp. 98–105, 2023. https://doi.org/10.58496/mjcsc/2023/012

[150]. A. Aldoseri, K. Al-Khalifa, and K. Hamouda, K. Re-Thinking Data Strategy and Integration for Artificial Intelligence: Concepts, Opportunities, and Challenges," *Applied Sciences*, vol. 13, no. 12, pp. 1–33, 2023. https://doi.org/10.3390/app13127082

[151]. M. Akhtar, and T. Feng, "An overview of the applications of Artificial Intelligence in Cybersecurity," *EAI Endorsed Transactions on Creative Technologies*, vol. 8, no. 29, pp. 1–8, *2021*. https://doi.org/10.4108/eai.23-11-2021.172218

[152]. B. B. Naik, A. Mehta, H. Yagnik, and M. Shah, "The impacts of artificial intelligence techniques in augmentation of cybersecurity: a comprehensive review," *Complex and Intelligent Systems*, vol. 8, no. 2, pp. 1763–1780, 2021. https://doi.org/10.1007/s40747-021-00494-8

[153]. M. Ozkan-Okay, E. Akin, Ö. Aslan, S. Koşunalp, T. Iliev, I. Stoyanov, and I. Beloev, "A Comprehensive Survey: Evaluating the Efficiency of Artificial Intelligence and Machine Learning Techniques on Cyber Security Solutions," *IEEE Access*, vol. 12, pp. 12229–12256, 2024. https://doi.org/10.1109/access.2024.3355547

[154]. I. Bala, I. A. Pindoo, M. M. Mijwil, M. Abotaleb, and W. Yundong, "Ensuring Security and Privacy in Healthcare Systems: A Review Exploring Challenges, Solutions, Future Trends, and the Practical Applications of Artificial Intelligence," *Jordan Medical Journal*, vol.58, no.2, pp.250-270, 2024. https://doi.org/10.35516/jmj.v58i2.2527

[155]. O. Jouini, K. Sethom, A. Namoun, N. Aljohani, M. H. Alanazi, and M. N. Alanazi, "A Survey of Machine Learning in Edge Computing: Techniques, Frameworks, Applications, Issues, and Research Directions," *Technologies*, vol. 12, no. 6, pp. 1–34, 2024. https://doi.org/10.3390/technologies12060081

[156]. N. Capodieci, C. Sanchez-Adames, J. Harris, and U. Tatar, "The impact of generative AI and LLMs on the cybersecurity profession," *2024 Systems and Information Engineering Design Symposium (SIEDS)*, Charlottesville, VA, USA, 03-03 May 2024, pp. 448–453. https://doi.org/10.1109/sieds61124.2024.10534674

[157]. A. H. Halbouni, T. S. Gunawan, M. H. Habaebi, M. Halbouni, M. Kartiwi, and R. Ahmad, "Machine Learning and Deep Learning Approaches for CyberSecurity: A Review," *IEEE Access*, vol. 10, pp. 19572–19585, 2022. https://doi.org/10.1109/access.2022.3151248

[158]. J. Ruan, G. Liang, J. Zhao, H. Zhao, J. Qiu, F. Wen, and Z. Dong, "Deep learning for cybersecurity in smart grids: Review and perspectives," *Energy Conversion and Economics*, vol. 4, no. 4, pp. 233–251, 2023. https://doi.org/10.1049/enc2.12091

[159]. S. Mohammed, A. Al-Jumaily, J. S. Mandeep, V. P. G. Jiménez, A. S. Jaber, Y. S. Hussein, M. M. Al-Najjar, and D. Al-Jumeily, "Evaluation Feature Selection with Using Machine Learning for Cyber-Attack Detection in Smart Grid: Review," *IEEE Access*, vol. 12, pp. 44023–44042, 2024. https://doi.org/10.1109/access.2024.3370911

[160]. M. A. Khder, S. Shorman, D. A. Showaiter, A. S. Zowayed, and S. I. Zowayed, "Review Study of the Impact of Artificial intelligence on Cyber Security," *2023 International Conference on IT Innovation and Knowledge Discovery (ITIKD)*, Manama, Bahrain, 08-09 March 2023, pp. 1–6. https://doi.org/10.1109/itikd56332.2023.10099788

[161]. R. R. Shanthi, N. K. Sasi, and P. Gouthaman, "A new era of cybersecurity: the influence of artificial intelligence," *2023 International Conference on Networking and Communications (ICNWC)*, Chennai, India, 05-06 April 2023, pp. 1–4. https://doi.org/10.1109/icnwc57852.2023.10127453

[162]. A. Rachini, C. Fares, M. A. Assaf, B. Jamal, and R. Khatoun, "AI-Powered Network Intrusion Detection: a new frontier in cybersecurity," *2023 24th International Arab Conference on Information Technology (ACIT)*, Ajman, United Arab Emirates, 06-08 December 2023, pp. 1–8. https://doi.org/10.1109/acit58888.2023.10453733

[163]. U. U. Ibekwe, U. M. Mbanaso, and N. A. Nnanna, "A Critical Review of The Intersection of Artificial Intelligence and Cybersecurity," *2023 2nd International Conference on Multidisciplinary Engineering and Applied Science (ICMEAS)*, Abuja, Nigeria, 01-03 November 2023, pp. 1–6. https://doi.org/10.1109/icmeas58693.2023.10379362

[164]. R. Allafi, and I. R. Alzahrani, "Enhancing Cybersecurity in the Internet of Things Environment Using Artificial Orca Algorithm and Ensemble Learning Model," *IEEE Access*, vol. 12, pp. 63282–63291, 2024. https://doi.org/10.1109/access.2024.3390093

[165]. T. Guemmah, H. E. Fadili, and S. Hraoui, "A review and synthesis for framing the use of artificial intelligence in cybersecurity," *2023 7th IEEE Congress on Information Science and Technology (CiSt)*, Agadir - Essaouira, Morocco, 16-22 December 2023, pp. 44–49. https://doi.org/10.1109/cist56084.2023.10409914

[166]. P. S. Dandge, U. I. Dawre, and R. F. Shirshikar, "Artificial intelligence in cyber security," *Journal of Advanced Zoology*, vol. 44, no. S-8, pp. 69–72, 2023.

[167]. P. Ramya, S. V. Babu, and G. Venkatesan, "Advancing Cybersecurity with Explainable Artificial intelligence: A review of the latest research," *2023 5th International Conference on Inventive Research in Computing Applications (ICIRCA)*, Coimbatore, India, 03-05 August 2023, 1351–1357. https://doi.org/10.1109/icirca57980.2023.10220797

[168]. M. Elbes, S. Hendawi, S. AlZu'bi, T. Kanan, and A. Mughaid, "Unleashing the full potential of artificial intelligence and machine learning in cybersecurity vulnerability management,"*2023 International Conference on Information Technology (ICIT)*, Amman, Jordan, 09-10 August 2023, pp. 276–283. https://doi.org/10.1109/icit58056.2023.10225910

[169]. N. Peppes, T. Alexakis, E. Daskalakis, K. Demestichas, and E. Adamopoulou, "Malware Image Generation and Detection Method Using DCGANs and Transfer Learning," *IEEE Access*, vol. 11, pp. 105872–105884, 2023. https://doi.org/10.1109/access.2023.3319436

[170]. M. Lourens, A. P. Dabral, D. Gangodkar, N. Rathour, C. N. Tida, and A. Chadha, "Integration of AI with the Cybersecurity: A detailed systematic review with the practical issues and challenges," *2022 5th International Conference on Contemporary Computing and Informatics (IC3I)*, Uttar Pradesh, India, 14-16 December 2022, pp. 1290–1295. https://doi.org/10.1109/ic3i56241.2022.10073040

[171]. K. Garg, K. S. Gill, R. Chauhan, D. Rawat, and D. Banerjee, "Distributed Denial of Services (DDOS) botnet attack prevention in internet of things (IoT) devices using AI," *2023 3rd International Conference on Smart Generation Computing, Communication and Networking (SMART GENCON)*, Bangalore, India, 29-31 December 2023, pp. 1–5. https://doi.org/10.1109/smartgencon60755.2023.10442302

[172]. M. Mahfuri, S. Ghwanmeh, R. Almajed, W. Alhasan, M. Salahat, J. H. Lee, and T. M. Ghazal, "Transforming Cybersecurity in the Digital Era: The Power of AI," *2024 2nd International Conference on Cyber Resilience (ICCR)*, Dubai, United Arab Emirates, 26-28 February 2024, pp. 1–8. https://doi.org/10.1109/iccr61006.2024.10533072

[173]. B. S. Alfurhood, D. P. Mankame, M. Dwivedi, and N. Jindal, "Artificial Intelligence and Cybersecurity: Innovations, Threats, and Defense Strategies," *Journal of Advanced Zoology*, vol. 44, no. S2, pp. 4715–4721, 2023.

[174]. S. A. Alawadhi, A. S. Zowayed, H. Abdulla, M. A. Khder, and B. J. A. Ali, "Impact of artificial intelligence on information security in business," *2022 ASU International Conference in Emerging Technologies for Sustainability and Intelligent Systems (ICETSIS)*, Manama, Bahrain, 22-23 June 2022, pp. 437–442. https://doi.org/10.1109/icetsis55481.2022.9888871

[175]. U. Upadhyay, A. Kumar, S. Roy, U. Rawat, and S. Chaurasia, "Defending the Cloud: Understanding the role of explainable AI in intrusion detection Systems," *2023 16th International Conference on Security of Information and Networks (SIN)*, Jaipur, India, 20-21 November 2023, pp. 1–9. https://doi.org/10.1109/sin60469.2023.10475080

[176]. E. Mendonça, "John Deere revolutionizes agriculture with AI and automation," *ASSEMBLY*. https://www.assemblymag.com/articles/97831-john-deere-revolutionizes-agriculture-with-ai-and-automation (accessed July 10, 2024).

[177]. M. Hamilton, "An AI-Powered app fights climate change while revolutionizing farming," The Rockefeller Foundation. https://www.rockefellerfoundation.org/insights/grantee-impact-story/an-ai-powered-app-fights-climate-change-while-revolutionizing-farming/ (accessed July 10, 2024).

[178]. S. Hemming, "Autonomous Greenhouse Challenge 4th Edition," WUR. https://www.wur.nl/en/research-results/research-institutes/plant-research/greenhouse-horticulture/show-greenhouse/autonomous-greenhouse-challenge-4th-edition.htm (accessed July 10, 2024).

[179]. A. McClerren, "Using AI to power the digital transformation of agriculture," Bayer. https://www.bayer.com/en/agriculture/ai-for-agriculture (accessed July 11, 2024).

[180]. Zeptogreens. "Smart Agriculture for Vineyards: Precision in Wine Production," Linkedin. https://www.linkedin.com/pulse/smart-agriculture-vineyards-precision-wine-production-ntc4c/ (accessed July 11, 2024).