Mesopotamian journal of Computer Science
Vol. **(2024)**, 2024, **pp**. 53–103
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. Figure 1 depicts the distribution of digital libraries according to the year of publication.

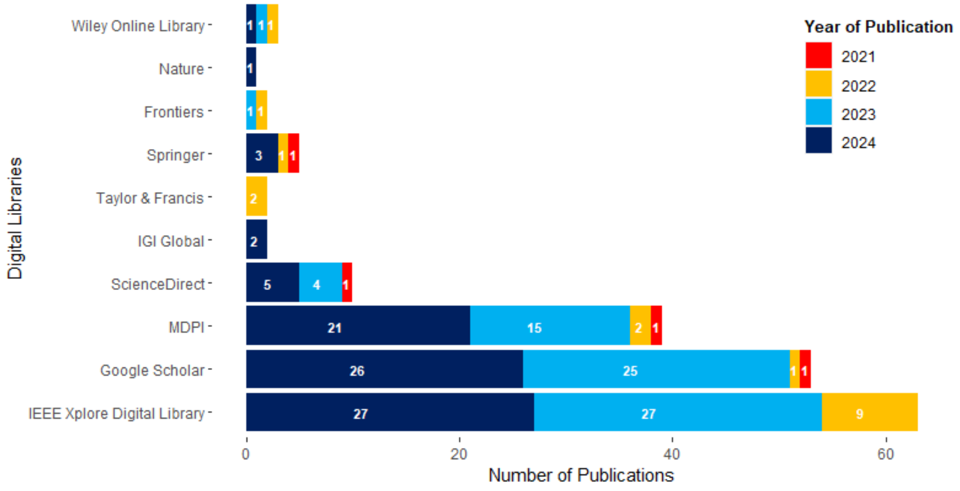

Fig. 1. Depicts the distribution of digital libraries according to the year of publication.

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