City Research Online

City, University of London Institutional Repository

Citation: Maraveas, C., Rajarajan, M., Arvanitis, K. G. & Vatsanidou, A. (2024). Cybersecurity threats and mitigation measures in agriculture 4.0 and 5.0. Smart Agricultural Technology, 9, 100616. doi: 10.1016/j.atech.2024.100616

This is the accepted version of the paper.

This version of the publication may differ from the final published version.

Permanent repository link: https://openaccess.city.ac.uk/id/eprint/34120/

Link to published version: https://doi.org/10.1016/j.atech.2024.100616

Copyright: City Research Online aims to make research outputs of City, University of London available to a wider audience. Copyright and Moral Rights remain with the author(s) and/or copyright holders. URLs from City Research Online may be freely distributed and linked to.

Reuse: Copies of full items can be used for personal research or study, educational, or not-for-profit purposes without prior permission or charge. Provided that the authors, title and full bibliographic details are credited, a hyperlink and/or URL is given for the original metadata page and the content is not changed in any way.

City Research Online: http://openaccess.city.ac.uk/ publications@city.ac.uk

Cybersecurity Threats and Mitigation Measures in Agriculture 4.0 and 5.0

Chrysanthos Maraveas[1]*, Muttukrishnan Rajarajan[2], Konstantinos D Arvanitis[3], Anna Vatsanidou[4]

[1] Farm Structures Lab, Department of Natural Resources and Agricultural Engineering, Agricultural University of Athens, Greece

[2] Institute for Cyber Security, Department of Engineering, City, University of London, London, UK

[3] Farm Machine Systems Lab, Department of Natural Resources and Agricultural Engineering, Agricultural University of Athens, Greece

[4] Department of Agricultural Development, Agrofood and Management of Natural Resources, School of Agricultural Development, Nutrition & Sustainability, National and Kapodistrian University of Athens, Psahna, Evia, Greece

*Corresponding Author: maraveas@aua.gr

Abstract

The primary aim of this study was to explore cybersecurity threats in agriculture 4.0 and 5.0, as well as possible mitigation strategies. A secondary method was employed involving narrative review in which many studies on cybersecurity were sampled and analyzed. The study showed that the main risks that increase cybersecurity threats to agricultural organizations include poor cybersecurity practices, lack of regulations and policies on cybersecurity, and outdated IT software. Moreover, the review indicated that the main cybersecurity threat in agriculture 4.0 and 5.0 involves denial of service attacks that target servers and disrupt the functioning of relevant smart technologies, including equipment for livestock tracking, climate monitoring, logistics and warehousing, and crop monitoring. The analysis also revealed that malware attacks occur when hackers change the code of a system application to access sensitive farm-related data and may alter the operations of the digitized systems. Some of the impacts of cybersecurity breaches were noted to include data loss, reduced efficiency of digitized systems, and reduced food security. A crucial mitigation strategy against cybersecurity threats includes using advanced technologies such as artificial intelligence (AI), blockchain, and quantum computing to improve malware detection in Internet of Things (IoT) digital equipment and ensure faster response to any threats. The other mitigation measures include training employees on best cybersecurity practices and creating guidelines and regulatory standards on best cybersecurity practices.

Keywords: Cybersecurity, threats, security, agriculture, mitigation, artificial intelligence

1.0 Introduction

1.1 Background

Different industries in the contemporary world are characterized by the increased adoption of digital technologies. Toussaint, Krima, and Panetto (2024) describe the phenomenon as the fourth industrial revolution or Industry 4.0, where the industry world is digitally transformed. A feature of Industry 4.0 is the increased application of digital technologies, including the Internet of Things (IoT), communication technologies, and industry standards that enhance the automation and real-time exchange of data in manufacturing processes (Suleiman et al., 2022). As such, Industry 4.0 transforms traditional production methods to improve processes.

1.1.1 Agriculture 4.0 and 5.0 systems

A subset of Industry 4.0 is Agriculture 4.0, which describes the integration of emerging technologies such as IoT, artificial intelligence (AI), and big data into the agricultural production chain (Da Silveira, Lermen, and Amaral, 2021). Haloui et al. (2024) add to Da Silveira, Lermen, and Amaral (2021) and observe that Agriculture 5.0 involves the development of smart innovations that enable farmers to boost their production at a lower environmental effect while resolving the political and social problems faced in food production systems. Various applications of Agriculture 4.0 and 5.0 in the modern agricultural ecosystem have also been widely documented. For example, Rose and Chilvers (2018) describe the increased use of precision agriculture to ensure fertilizers, pesticides, and herbicides are used appropriately and applied at the right time. Lu et al. (2022) reiterate Rose and Chilvers (2018) and explain that precision fertilization and irrigation technology are important in achieving efficient global agriculture through integrating information technology in the production chain. The insights from Rose and Chilvers (2018) and Lu et al. (2022) emphasize that the outcomes of implementing precision agriculture include increased productivity and reduced wastage of essential fertilizers and water resources in farms. A diagrammatic representation of Agriculture 4.0 and 5.0, showing the integration of simulation and technology systems, is in Figure 1.

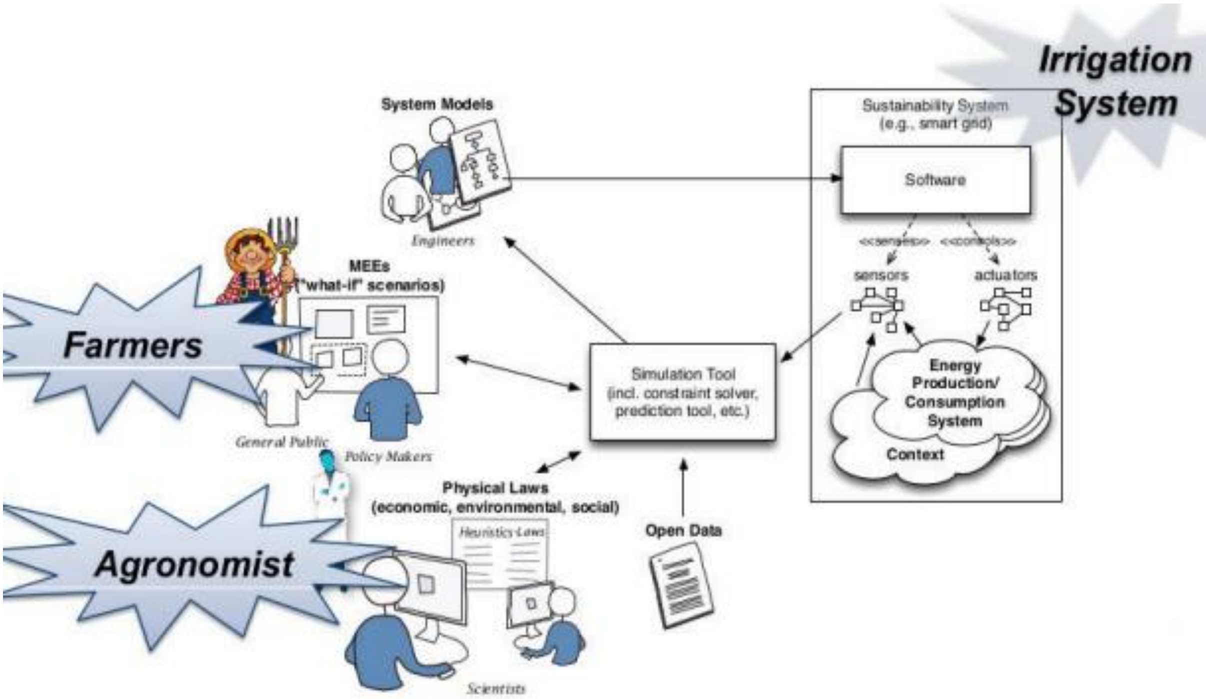

Figure 1. Agriculture 4.0 and 5.0 system framework (Barreto and Amaral, 2018).

In another study, Pukrongta, Taparugssanagorn, and Sangpradit (2024) supported Rose and Chilvers (2018) and Lu et al. (2022) where they showed that precision agriculture improved yield detection, monitoring diseases in crops, and detecting stress and water levels in crops. Precision agriculture has also been adopted to improve the yield of livestock. A case example was Monteiro, Santos, and Gonçalves (2021), who observed that precision livestock farming enabled farmers to monitor animals to enhance their growth, improve milk production, and detect diseases. The insight from these studies indicates that precision agriculture, as an application of Agriculture 4.0, facilitates the increase in yield and production of both crops and livestock. As such, farmers can obtain more value from agriculture by relying on the insights from advanced technologies.

Further applications of Agriculture 4.0 and 5.0 include the use of robotics and IoT to automate different farming activities and reduce the cost overheads incurred. Yépez-Ponce et al. (2023) suggest that robotics are adopted in agriculture to automate processes such as fumigation, the application of chemicals, and harvesting to reduce costs and improve the efficiency of the processes. In such a scenario, advanced robots are adopted in large-scale farms to automate manual processes to ensure lower costs and higher efficiency in undertaking activities such as harvesting and the application of chemicals. Hartanto et al. (2019) support Yépez-Ponce et al. (2023) where they report the use of unmanned aerial vehicles (UAVs) as mobile robots that automate farming tasks and facilitate data collection where aspects such as soil moisture and nitrogen quantity can be obtained using sensors. As a result, farmers can make more informed decisions to improve productivity and address issues faced by crops. Gokool et al. (2023) reiterated Hartanto et al. (2019) and also showed that UAVs were applied in monitoring crop growth and development, guiding the management of fertilizer application, and undertaking crop mapping. Figure 2 illustrates the diverse sources of data collected from IoT devices in a smart greenhouse.

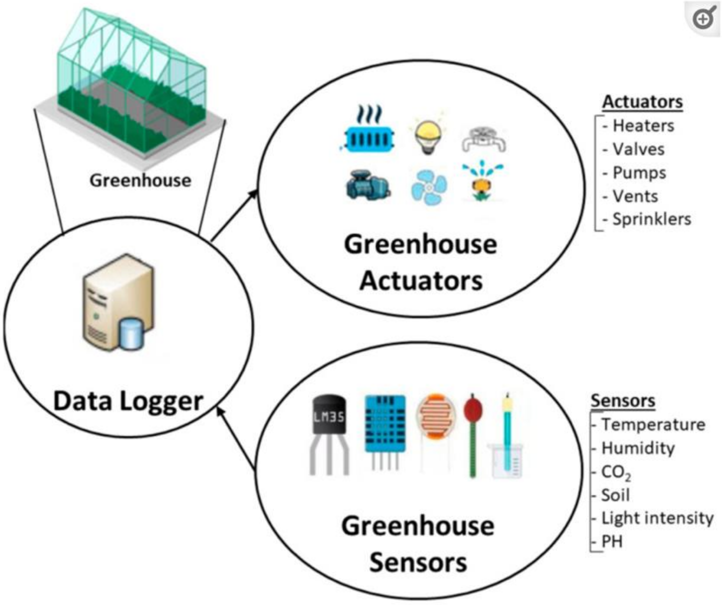

Figure 2. Data sources in a smart greenhouse with multiple IoT sensors (Soussi et al., 2024)

As shown in Figure 2, the data sources in a smart greenhouse are diversified, where different types of sensors are used to collect data, such as temperature, light intensity, humidity, and pH (Soussi et al., 2024). Further cybersecurity risks also arise as the data is transferred to the cloud, where nefarious actors can launch attacks to compromise the data's confidentiality, integrity, and availability. In another study, Zhao, Wang, and Pham (2023) reported that the use of UAVs embedded with IoT sensors enabled farmers to collect data on aspects such as crop status, soil preparation, and detection of insects and pests. The outcome of adopting robotics and IoT sensors within the farm is an increase in the overall production and crop yield due to improved detection of pests, efficient application of fertilizers, and monitoring of different aspects that enhance production, including soil preparation and irrigation efficacy.

1.1.2 Cyber-security threats in Agriculture 4.0 and 5.0

Despite the potential for technologies to improve production in agriculture 4.0 and 5.0, several challenges may be experienced. In particular, Demestichas et al. (2020) indicated that incorporating information and communication technologies (ICT) in agriculture 4.0 and 5.0 can be accompanied by cyber-security threats where cyber-criminals engage in the theft of money as well as business secrets, intellectual properties, and other non-tangible assets from agricultural companies. In other cases, cyber-attacks may interfere with the operations of smart agricultural systems, such as drones used for spraying crops or the remote control of heating and cooling systems in farms (Barreto and Amaral, 2018). Some of the agricultural companies that have made global headlines due to cyber-attacks in recent years include JBS, which is one of the largest meatpackers, the Australian beverage company named Lion, and the Florida water system (Alahmadi et al., 2022). The cyber-security risks in agriculture 4.0 and 5.0 are exacerbated by the trend showing that agricultural companies are not investing adequately in the relevant cybersecurity systems, which means that attacks targeting the sector have a high payoff potential and can attract more cyber-attackers (Barreto and Amaral, 2018).

The increase in cyber-security risk targeting smart agricultural systems has been attributed to different factors. Zanella, da Silva, and Albini (2020) explain that smart agriculture is affected by cyber threats due to factors such as the use of open wireless networks for data transmission, which leads to easier exploitation by malicious actors. Demestichas, Peppes, and Alexakis (2020) support Zanella, da Silva, and Albini's (2020) report that smart agriculture is at risk of cybercrime due to the increasing accessibility to smart technology where multiple points of access are available for hackers to exploit. In this regard, the threat surface is increased where data from the farm can be accessed at home and the office. Yazdinejad et al. (2021) add to Demestichas, Peppes, and Alexakis (2020) where they report that smart agricultural systems employ measures that expose the reliability of the system by exposing them to remote control while the sensors lack computational resources that support security methods such as cryptography. The direct implication is that due to the numerous threats linked to Agriculture 4.0 and 5.0 applications, cybersecurity causes significant data and financial losses for farmers. Ahmadi (2023) observed that cybersecurity threats in smart agriculture compromise privacy and confidentiality, leading to the disclosure of critical information.

Therefore, identifying comprehensive strategies that can be adopted by farmers to secure their smart agricultural systems is critical to supporting security in their farming applications.

1.2 Research Aim and Objectives

The core focus of this review article is to investigate the cybersecurity threats challenging Agriculture 4.0 and 5.0 and the technological mitigation strategies adopted to address them. The novelty of the research arises from the fact that it is the first review article that adopts a comprehensive approach to investigate the cybersecurity threats facing Agriculture 4.0 and 5.0 applications and identify mitigation strategies utilized to overcome the issues. The examination of diverse review articles showcases the various cybersecurity risks affecting Agriculture 4.0, while minimal studies have focused on the strategies that can also be adopted to address them. The objectives of this review article include the following:

i. To investigate the cybersecurity threats facing agriculture 4.0 and 5.0.

ii. To critically examine technological solutions adopted to mitigate cybersecurity threats in agriculture 4.0 and 5.0.

iii. To critically assess the limitations of cybersecurity mitigation measures and explore the future directions in the area.

1.3 Paper Outline

The rest of the article is organized into four sections. The subsequent section elaborates on the narrative review methodology adopted in the article. The third section introduces cybersecurity threats faced in Agriculture 4.0 and 5.0. In the fourth section, the results obtained in the review article are discussed to address the research question and the research objectives. The final section concludes the review article and outlines the implications of the research.

2.0 Methodology

2.1 Research Method

The methodology adopted in the current research is the narrative secondary review. According to Demiris, Oliver, and Washington (2019), a narrative review involves the thorough examination of published studies on a given research topic to summarize current knowledge and known issues. The rationale for conducting a narrative review in the current research arises from its appropriateness in summarizing current knowledge insights on the threats of cybersecurity in agriculture 4.0 and 5.0 and the various technological mitigation measures that are being adopted to address the issues. The researcher observes that the topic has been broadly published in different scientific journals, and a narrative review of the secondary sources provides a feasible methodology to address the research objectives.

Basheer (2022) also reveals that narrative reviews are adopted in exploring under-researched topics to establish new insights and unusual perspectives in robustly researched fields. Therefore, the narrative review will allow the researcher to identify future research directions on the selected topic. Sukhera (2022) outlines a stepwise process adopted in conducting a narrative review, including framing the research question, developing a search strategy to clarify boundaries and scope, selecting research studies, and conducting the analysis. The different steps are showcased in the subsequent sections.

2.1 Framing the Research Question

The main research question guiding the review article was stated as follows;

What cybersecurity threats challenge agriculture 4.0 and 5.0, and what technological mitigation strategies are adopted to address them?

The research question explores the various threats of cybersecurity in agriculture 4.0 and 5.0 where modern technologies are employed, their adverse consequences, and the various mitigation strategies adopted to address them.

2.2 Development of the Search Strategy

With the research question clarified, the subsequent process involved developing a search strategy to identify keywords, databases, and the inclusion and exclusion criteria adopted in selecting relevant articles. Neilson and Premji (2023) explain that developing a search strategy ensures that the search process is replicable by outlining the search terms, such as keywords and syntax, including Boolean operators and field codes. The narrative review identified databases such as Science Direct, MDPI, Scopus, and Springer Nature to identify relevant articles. The selected databases were adopted based on their effectiveness in ensuring updated articles on the research topic were identified. Additionally, the Google Scholar website was used to locate relevant articles on the topic.

The subsequent phase involved deriving keywords related to the research topic, which included Agriculture 4.0, Agriculture 5.0, AI, IoT, ML, Cybersecurity, Threats, Mitigation, and Strategies. The keywords were combined using Boolean logic operators AND/OR to broaden the scope of the search process. MacFarlane, Russell-Rose, and Shokraneh (2022) observe that combining keywords using the Boolean operators widens the search and identifies more articles related to the research topic. The combined search phrases in the review article were detailed as follows;

"Cybersecurity" AND "Threats" AND "Agriculture 4.0" AND "Agriculture 5.0" AND "Mitigation" AND "Measures"

"Cybersecurity" AND "Threats" OR "Risks" AND "Agriculture 4.0" AND "Agriculture 5.0" AND "AI" AND "IoT" AND "Mitigation" AND "Measures" OR "Strategies"

2.3 Selection of Studies

The third phase involves the selection of studies that adhere to the set inclusion and exclusion criteria. Table 1 showcases the inclusion and exclusion criteria adopted to guide the selection of the studies.

Table 1. Inclusion and exclusion criteria

Focus	**Inclusion**	**Exclusion**
Scope	Studies focused on cybersecurity threats challenging agriculture 4.0 and 5.0, and the technological mitigation strategies are adopted to address them.	Studies have not focused on cybersecurity threats challenging agriculture 4.0 and 5.0 and the technological mitigation strategies adopted to address them.
Period	2017-2024	Before 2017
Language	English	All non-English languages
Type	Peer-reviewed journal articles	Grey literature, blogs

As showcased in Table 1, the inclusion criteria focused on a narrow scope regarding the cybersecurity threats challenging agriculture 4.0 and 5.0 and the technological mitigation strategies adopted to address them. The studies were required to be current and related to the research topic within the period 2017 to 2024. The limit ensured that updated insights would be generated on the topic. The selected studies were also published in English to eliminate the need for further translation, which required more time to complete. The studies were also peer-reviewed journal articles. The exclusion criteria eliminated all studies published beyond the scope of the research where the articles did not consider the cybersecurity threats challenging agriculture 4.0 and 5.0 and the technological mitigation strategies adopted to address them. Studies published before 2017 on personal websites and blogs were eliminated.

The conducted search generated 2,587 records from databases such as Science Direct, MDPI, Scopus, and Springer Nature. By employing the inclusion and exclusion criteria, the research narrowed down to 213 studies that are elaborated in the critical review and analysis. A summary of the themes, subthemes, and codes from the sampled articles is shown in Appendix 2.

2.4 Critical Appraisal

A critical appraisal in secondary research is crucial in assessing the reliability, quality, and relevance of sampled articles (Tod et al., 2022). The underlying aim of critical assessment is to ensure that the articles selected are relevant in addressing the developed research question and objectives. For this narrative review, the SANRA tool (Scale for the Quality Assessment of Narrative Review Articles) developed by Baethge et al. (2019) was used to assess the quality of the sampled articles. The critical appraisal process is shown in Appendix 1. The appraisal process considered six aspects, with each aspect being rated on a scale of 0-2. The first point involved the article's importance for the reader, where the content of the paper aligns with the current research. The second point involved the sampled article depicting a clear aim and questions to ensure that it is focused on the topic of research. The third aspect was a description of the literature search, where there is a need for a clear literature search for secondary papers considered. The fourth aspect involves proper referencing, where key statements are all supported by citations. (Baethge et al., 2019). The fifth aspect involves scientific reasoning, in which adequate scientific evidence is used to back various arguments in the paper. The last aspect entails appropriate data presentation in which data outcomes are clearly shown to reveal how objectives are addressed. After assessing the sampled articles, it was noted that all of them were of high quality, with a score of 10 or more out of the possible 12. Therefore, all the identified sources were considered for analysis.

2.5 Data Analysis

The current study employed a thematic analysis technique to identify trends in the various studies sampled. The first step of the analysis involved going through the sampled articles to familiarize themselves with the general objectives and key findings obtained (Campbell et al., 2021). The second step involved coding the data by identifying repeated ideas in different articles that are aligned with the objectives of the current study (Naeem et al., 2023). During the coding process, the authors' similar and contrasting views on cybersecurity threats and mitigation in agriculture were identified and highlighted. The third step involved grouping the codes into themes to ensure a broad consideration of different codes (Braun and Clarke, 2023). The themes were named appropriately, and the write-up was done in several chapters, with each chapter considering a specific theme from the analysis.

2.6 Ethical Considerations

Two main ethical principles were considered in this research. The first principle involved transparency, which entails providing clear steps on how articles were searched, critically appraised, and selected. Transparency is crucial in secondary research because it enables readers to replicate the study and verify or improve on its findings (Moravcsik, 2020). For this study, transparency was applied by showing inclusion and exclusion criteria, article search process and output, and the critical appraisal process. The second ethical principle considered was integrity, which involves applying correct referencing and accurate reporting of data (Bell et al., 2022). Research integrity is crucial in secondary research to improve the quality of evidence and ensure the reliability of results since the conclusions made are based on data that can be traced and verified.

2.7 Limitations

The first limitation of this research was the propagation of bias since the author did not gather first-hand data and, hence, did not have control over the findings from the dataset.

As such, bias in the analysis by original authors may also be incorporated into this study. The second limitation of this study is that the data gathered from published sources may not reveal recent trends in cybersecurity in agriculture, especially due to the rapidly changing AI landscape. Therefore, the data may only reveal past issues on cybersecurity problems and solutions, leading to less accurate conclusions.

2.8 Summary

The current chapter presented a summary of steps taken in executing this research. This study employed a narrative review design with a comprehensive search strategy. After applying the selection criteria and SANRA assessment tool, 212 articles were sampled for review. Thematic analysis was considered when analyzing the gathered data to develop relevant themes. The ethical principles considered in this study included integrity and transparency.

3.0 Cybersecurity Threats in Agriculture 4.0 and 5.0

In this section, the examination of the underlying issues leading to cybersecurity risks in smart agriculture is undertaken. The discussion also examines the kinds of cybersecurity threats directed at smart agriculture and the associated negative consequences of smart agriculture.

3.1 Definition of Cybersecurity Aspects

A prerequisite to examining the factors increasing cybersecurity risks in agriculture 4.0, the types of risks, and their consequences is to define different security aspects associated with smart farming. The aspects are defined below.

3.1.1 Privacy

Describes the ability of the system to keep data away from unauthorized personnel and to protect it based on individual rights (Hung and Cheng, 2009). Taji and Ghanimi (2024) explain that in smart agriculture, privacy is important to ensure the sensitive information obtained from the farm, such as farming practices, use of land, and crop yields, is protected. Kaur et al. (2022) add to Taji and Ghanimi (2024) and reveal that privacy is also important in precision agriculture, where different types of data are collected from sensors, drones, and data analysis technologies. As such, the farmer raises concerns about whether the data collected from the different technologies can be accessed by unauthorized third parties as well as technology providers. However, unlike confidentiality, Kaur et al. (2022) argue that privacy is also concerned with ensuring that the collected data is protected in alignment with the requirements set by the legislation and government.

3.1.2 Integrity

Property of the data being complete and accurate where no modifications are expected to have occurred during transmission or storage processes (Lundgren and Möller, 2017). In smart agriculture, Awan et al. (2020) argue that providing a guarantee of the integrity of the collected data is important to ensure accurate decisions can be made in different farming areas.

3.1.3 Confidentiality

Describes the property where information is not disclosed to other unauthorized entities, processes, or individuals (Qadir and Quadri, 2016). In smart agriculture, Kaur et al. (2022) posit that the concerns of confidentiality align with privacy and emphasize that the data collected from the farmers and the farm-related activities ought to be protected from unauthorized access by other entities.

3.1.4 Availability

Describes the property of the data being easily accessible and usable upon demand by authorized entities (Yee and Zolkipli, 2021). In smart agriculture, the concept ensures that rightful entities within the farm can access any data they require upon demand.

3.1.5 Non-Repudiation

Describes the property of agreeing to adhere to an obligation where actors cannot refute their responsibility (Wheeler, 2011). As such, this concept ensures that users within smart agriculture cannot refute what they do within the system.

3.1.6 Trust

Describes a state where the intention to accept vulnerability is based on the positive expectations of the behavior of others under interdependence and risk conditions (Dhagarra, Goswami, and Kumar, 2020). As a result, farmers trusting the data generated from sensors ensures that they cannot be spoofed by the technologies and can make important decisions using them.

3.2 Factors Increasing Cybersecurity Risks in Agriculture 4.0 and 5.0

The synthesis of diverse empirical literature reveals that cybersecurity risks in Agriculture 4.0 and 5.0 arise due to multiple issues. This topic is divided into three main phases, which include framework, taxonomies, and cyber threats relevant to agriculture. The framework part shows a broad overview of the smart agricultural system and how different layers in the system can be breached. The second phase on taxonomy focuses on the different systems that can contribute to cyber risks, including physical security, external factors, actions of people, and failed internal processes. Lastly, the cyber threat phase indicates the specific cyber threats that can affect smart systems in agriculture compared to other sectors.

Framework

To understand the scope of the cybersecurity threat, the framework for digital technologies used in smart farming infrastructure was identified, as shown in Figure 3 (Friha et al., 2022). Figure 3 indicates that digital systems used in agriculture are based on different layers, including physical, edge, application, service, and network.

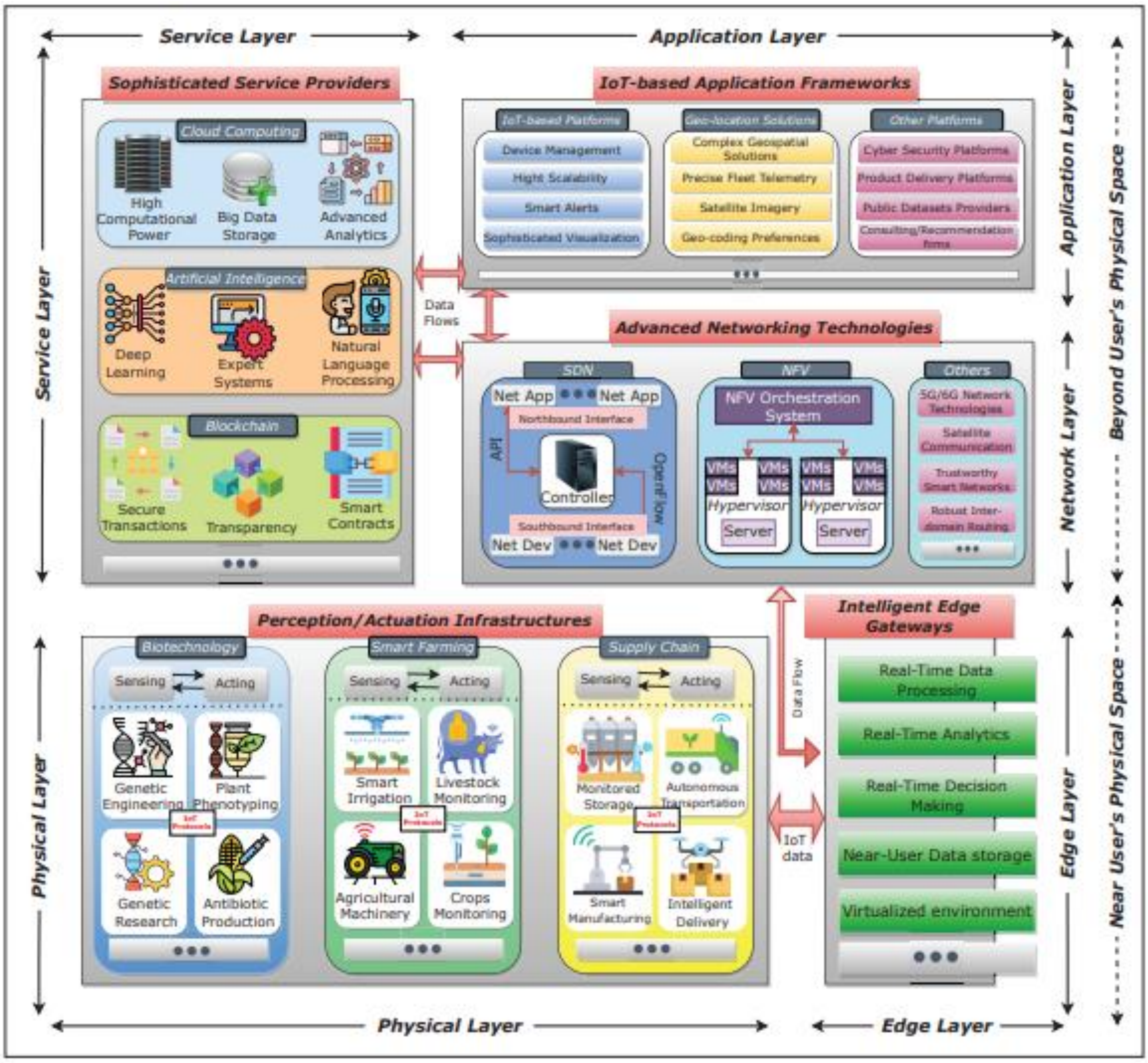

Figure 3. Digital framework for smart agricultural system (Friha et al., 2022)

From Figure 3, one cybersecurity risk entails network attacks that affect the connectedness of IoT devices. In such instances, attacks can disrupt the operation of IoT devices in smart farming activities that use older legacy wireless technologies and unpatched software. Ali et al. (2024) postulate that smart farming employs diverse IoT devices to undertake activities such as monitoring crop production, evaluating the content of soil moisture, and deploying drones to facilitate pesticide spraying. However, IoT devices are associated with high cybersecurity risks due to unpatched firmware or extended use of default passwords, which exposes them to risks of compromise within the IoT network (Ali et al., 2024). Demestichas, Peppes, and Alexakis (2020) add that IoT devices are also at risk of cyberattack due to the vulnerabilities in their communication protocols and their limited computational resources that restrict the implementation of complex cryptographic algorithms. The issues include the lack of security recommendations, the diversity of devices, weak security of the wireless network protocols that are still used (Wi-Fi Protected Access (WPA)), and a general lack of attention to the security of smart devices. As a result, cybercriminals launch attacks that target the vulnerabilities in the IoT devices used in smart agriculture.

Taxonomy of Cyber Threats

Failed Internal Process. A second factor that exposes smart farming technologies to cyberattacks regards weak or absent mechanisms for access control of different farming devices. Buchanan and Murphy (2022) describe an access control attack involving a John Deere tractor where unauthorized access led to the installation of a 1990s vintage video game. The particular case indicated that many smart agriculture technologies that could be accessed remotely lacked robust access control mechanisms and were exposed to data breaches, unauthorized access, and data manipulation. Sontowski et al. (2020) add to Buchanan and Murphy (2022) and demonstrate that cyber attackers can exploit vulnerabilities in the wireless networks used by different smart farming devices to remotely control and disrupt the flow of data from the on-field sensors and the autonomous vehicles such as drones and smart tractors. The exploitation of vulnerabilities within the Wi-Fi networks leads to unauthorized access to crucial farming technologies and may cause adverse consequences during high-risk periods such as harvesting. Rahaman et al. (2024) reiterate Sontowski et al. (2020) and report that unauthorized access is a persistent challenge in smart farming in scenarios where farmers adopt weak access control solutions such as maintaining default passwords. Hackers and other nefarious actors can exploit such weak security protocols to access smart devices and launch attacks on the farm. Some of the smart equipment used in agriculture that can be affected by unauthorized access are shown in Figure 4.

Figure 4. Smart devices used in agriculture 4.0 and 5.0 (Barreto and Amaral., 2018)

The inspection of the various studies underscores the lack of cybersecurity awareness that leads to poor security practices, including the failure to change default passwords. Due to poor cybersecurity training for farmers, devices used in smart farms rely on weak security mechanisms and access control methods and are at risk of being easily exploited by attackers.

Physical Security. The lack of physical security mechanisms is another factor that exposes smart farming devices to cyberattacks, as they can be easily stolen and malicious software installed. Abbasi, Martinez, and Ahmad (2022) align with the argument and report that many smart farming devices, such as sensors and drones, are small in size and lack proper physical security mechanisms on the field. Malicious actors can exploit weak physical security and tamper with them to install firmware and malware to steal data and control them remotely (Abbasi, Martinez, and Ahmad, 2022). Zanella, da Silva, and Albini (2020) add to Abbasi, Martinez, and Ahmad (2022) and report that many smart farming devices lack physical security features such as tamper-resistant boxes. As a result, they are easily tampered with when wild animals collide with them or when they are damaged by other farm equipment, such as tractors, leading to data corruption or unavailability.

Studies show that the increase in cybersecurity risks in agriculture is attributed to the increase in smart farm management techniques, which feature the large utilization of ICT and IoT for communication. The layers in ICT framework targeted during attacks is shown in Figure 5.

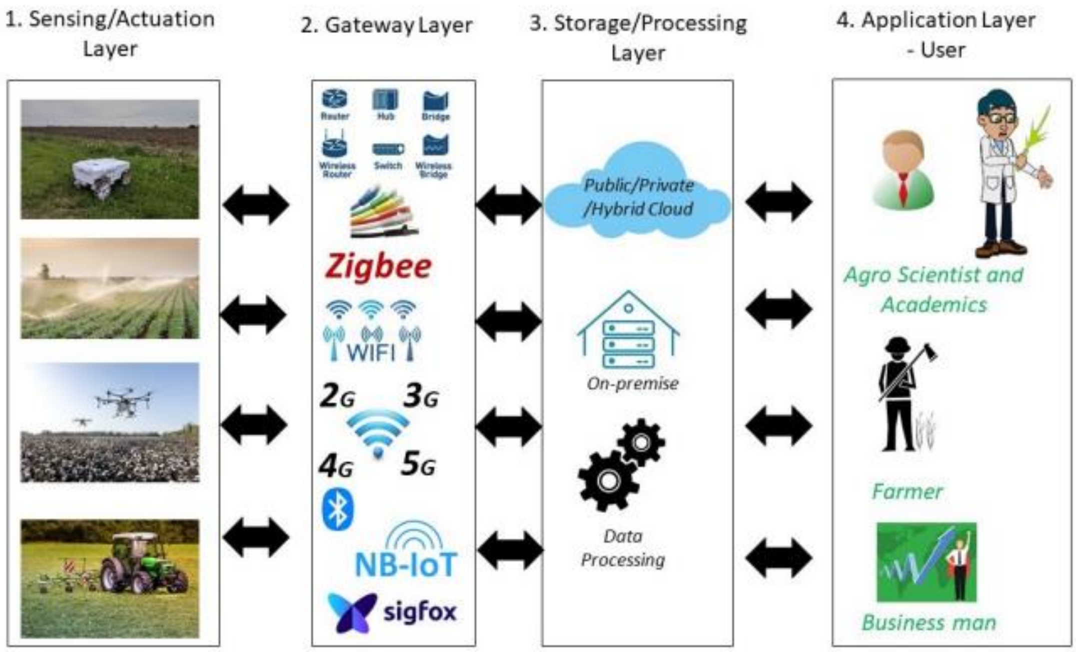

Figure 5. Layers targeted during attacks on smart agricultural systems (Alahmadi et al., 2022)

Concerning the risks of smart technologies in agriculture, Demestichas et al. (2020) pointed out that the rapid evolution of modern agriculture to incorporate smart communication strategies presented serious security issues from potential cyberattacks. The view was supported by Gupta et al. (2020), who also pointed out that the use of smart communication technologies and IoT increased the vulnerability of farming environments to cybersecurity threats. A similar observation was made by Barreto and Amaral (2018) regarding the inherent security risks of smart farming. In that respect, the findings imply that cybersecurity risks in agriculture increase with the massive use of communication technologies. Besides communication technologies, studies further attribute cybersecurity risks in agriculture to the wide use of big data. The proposition was presented by Amiri-Zarandi et al. (2022), who noted that a large volume of agriculture data presented privacy challenges and attracted potential hacking activities by cyber criminals. According to Benmalek (2024), ransomware attacks are the most common cyber threat directed at farm databases. The implication is that the availability of data is regarded as a rich asset by cyberattackers, leading to an increase in cybersecurity issues in smart farming solutions.

Actions of People. In the same breath, Altulaihan et al. (2022) noted that sensitive information theft in agriculture has been accelerated with the increasing usage of IoT devices. Specifically, the study revealed that this specific technology lacks information security features, making it highly targeted. According to Alahmadi et al. (2022), the main contributor to cybersecurity threats in agriculture is the lack of skilled personnel in the sector. The problem has led to increased use of automated systems, which are vulnerable to cyberattacks. Aloqaily et al. (2022) reported that automated systems were susceptible to manipulation from online counterfeit programs, which rendered them ineffective or caused data breaches. The implication is that cybersecurity risks in agriculture are propelled by over-reliance on technological solutions. Meanwhile, Alqudhaibi et al. (2024) attributed the high rate of cybersecurity threats to the absence of proper cyberdefense measures in the agriculture sector. Essentially, most of the digital platforms relied on basic protection protocols that were ineffective against advanced attacks. The failure to install the correct countermeasures was also highlighted by Ahmadi (2023). In that respect, cybersecurity risks are high in the agricultural sector due to the negligence of standard protection measures. The sources point to the overall association of smart-agriculture technology with higher cybersecurity risks.

External Factors. The lack of regulations and cybersecurity policies governing the security of IoT devices used in smart farming further complicates their security and exposes them to cyberattacks. Barreto and Amaral (2018) report that although cybersecurity leads to increased losses for farmers, many large technology providers are still not investing in cybersecurity protection for IoT and smart farming devices. However, Demestichas, Peppes, and Alexakis (2020) contradict Barreto and Amaral (2018) and posit that in other cases, smaller agricultural companies demonstrate their interest in safe security systems but face challenges such as the lack of financial resources and plans to implement security measures against possible cyberattacks. The contradiction suggests that multiple factors affect the implementation of cybersecurity mechanisms in smart agriculture.

Cyber Threats: Comparing Features Influencing Agriculture and Other Sectors

Weather Conditions. A comparison was done on the characteristics of agriculture and other sectors on cyber threats. Agricultural sector has certain unique characteristics that mitigate or amplify cyber threats. The first feature relates to weather conditions. On the one hand, IoT in agriculture such as soil sensors and sensors for detecting pests are exposed to the open air (Demestichas et al., 2020). This means that the sensors can easily be damaged by dust, chemicals, or rain leading to malfunction that reduces their reliability. On the other hand, IoT sensors used in other sectors such as smart homes such as sensors for controlling TVs, fridges, and lighting are kept in sheltered spaces and protected against the harsh weather conditions (Sokullu et al., 2020). Therefore, this means that weather conditions amplify the cyber threats of IoT devices in agricultural sector compared to the other sectors when the smart IoT devices fail to work as expected in harsh weather.

Geographical coverage. The second point of comparison entails geographical coverage. For IoT devices in agriculture, their installation often covers large tracts of land and extends into remote areas to ensure the whole farmland is monitored to detect changes in soil nutrients as well as livestock movements (Barreto and Amaral, 2018). In contrast, IoT devices in smart homes are often placed in enclosed spaces within a few rooms in the house, which means any faulty devices are quickly identified and repaired (Ray et al., 2020). The geographical coverage implies that IoT devices in agriculture are not only difficult to install but also difficult to maintain and ensure consistent network connectivity. The vast area covered also means that the IoT devices can be stolen or damaged due to challenges of ensuring physical security of the devices. Moreover, there is a longer delay of identifying faulty IoT devices distributed in vast areas because of physical effort needed to locate them compared to those in other sectors. This means that geographical coverage amplifies cyber threats in agriculture because of elevated risk of theft, and network connectivity issues.

Hardware and software. The third point of comparison entails hardware and software employed in the industries. Agricultural sector often rely on older equipment and software because they are expensive to acquire compared to those of other systems (Yazdinejad et al., 2021). For example, IoT devices installed in vast area of land cannot be easily replaced and upgraded to new models due to the high costs involved. In contrast, IoT devices in smart homes can easily be replaced due to ease affordability since only a few units are used per household (Oh et al., 2021). Therefore, the extensive use of old equipment and software in agriculture increases cyber threats since the systems may lack protection against the latest cyber risks.

Responsive IoT. The fourth point of comparison entails responsive IoT. On the one hand sectors such as smart homes use IoT devices with voice recognition such as Alexa which provide personalized protection against use by unauthorized personnel. Moreover, the responsive devices ensure that other connected IoT devices can be conveniently controlled (Hafeez et al., 2020). In contrast, IoT devices in agriculture are not responsive which means that users have to physically visit the site to assess their condition in case of any problem in operation (Barreto and Amaral, 2018). This means that unlike other sectors where users can use responsive IoT devices to trouble shoot problems, the agricultural sector requires more manual labour to complete the smart systems which increases the cyber threats due to semi-automation.

A summary of the cybersecurity risks based on layers shown in framework of Agriculture 4.0 and 5.0 is indicated in Table 2.

Table 2. Cybersecurity risks for various layers in Agriculture 4.0 and 5.0

Layer	**Cybersecurity Risk**	**Potential Impact on Agricultural Systems**
Physical	Attackers target gateways that control messages between IoT devices	Attacks can affect the operation of actuators and sensors and disrupt the collection of environmental data spread over the farms.
Edge	Attackers target data and information processing systems	Attacks can lead to costly mistakes due to false data, inaccurate conclusions, and poor decisions by farmers from smart farming systems.
Network	Attackers target communication between IoT devices used to share agricultural data	Attacks can affect sharing of data between different IoT devices and reduced monitoring of smart agricultural equipment in real time.
Cloud	Attackers target cloud storage of agricultural data	Attacks can disrupt access to accumulated data from different farmers, which can reduce the effectiveness of the decision-making process.

Adapted from (Demestichas et al., 2020; Friha et al., 2022).

3.3 Cybersecurity Attacks in Agriculture and Consequences

The discussion in the previous section indicated that different underlying factors increased the vulnerability of cybersecurity risks in Agriculture 4.0 and 5.0, including using outdated applications, lack of proper security infrastructure, and poor cybersecurity practices within the farm. In this section, the discussion is advanced further to elaborate on the different types of cybersecurity attacks faced in smart agriculture. This section is divided into different phases, including framework, taxonomy, and cyberattacks. The framework indicates smart farming (SF) and precision agriculture (PA) components that are affected by cyberattacks. The taxonomy indicates the main points of attack, such as hardware, data or code. Meanwhile, cyberattacks narrows down the discussion to strategies used during the attack, such as ransomware, data leak, or RF jamming.

Framework

The framework for cyberattack in agriculture is shown in Figure 6. Figure 6 illustrates the broad classification of attacks on smart agriculture digital systems. In Figure 6, the broad categorization of cybersecurity attacks in smart farming is detailed where, ranging from attacks on hardware, networks, and equipment to data attacks, attacks on code and support chains, and misuse attacks.

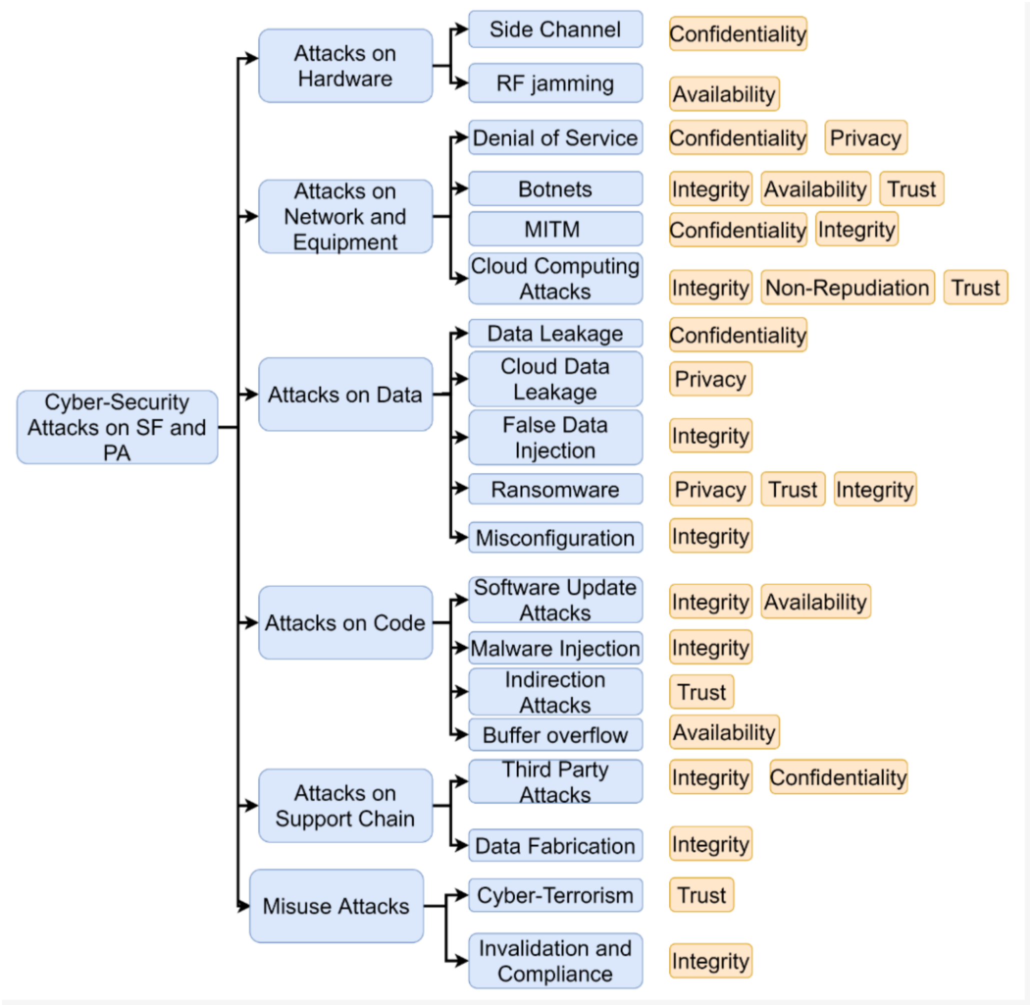

Figure 6. Classification of cybersecurity attacks in smart agriculture (Yazdinejad et al., 2021)

Taxonomy of Targets of Cyber Attacks

***Hardware*.** The hardware attacks are associated with a breach of confidentiality where disclosure of critical data is Yazdinejad et al. (2021) report that hardware attacks are a cybersecurity threat where professional hackers jam side channels and radio frequencies, hence violating the privacy and confidentiality of the cyber-physical systems. Alahmadi et al. (2022) align with Yazdinejad et al. (2021), positing that side-channel attacks are directed at collecting unauthorized information about the implementation of systems through monitoring physical parameters such as voltage and electrical systems. Figure 7 showcases a side-channel attack in digital applications.

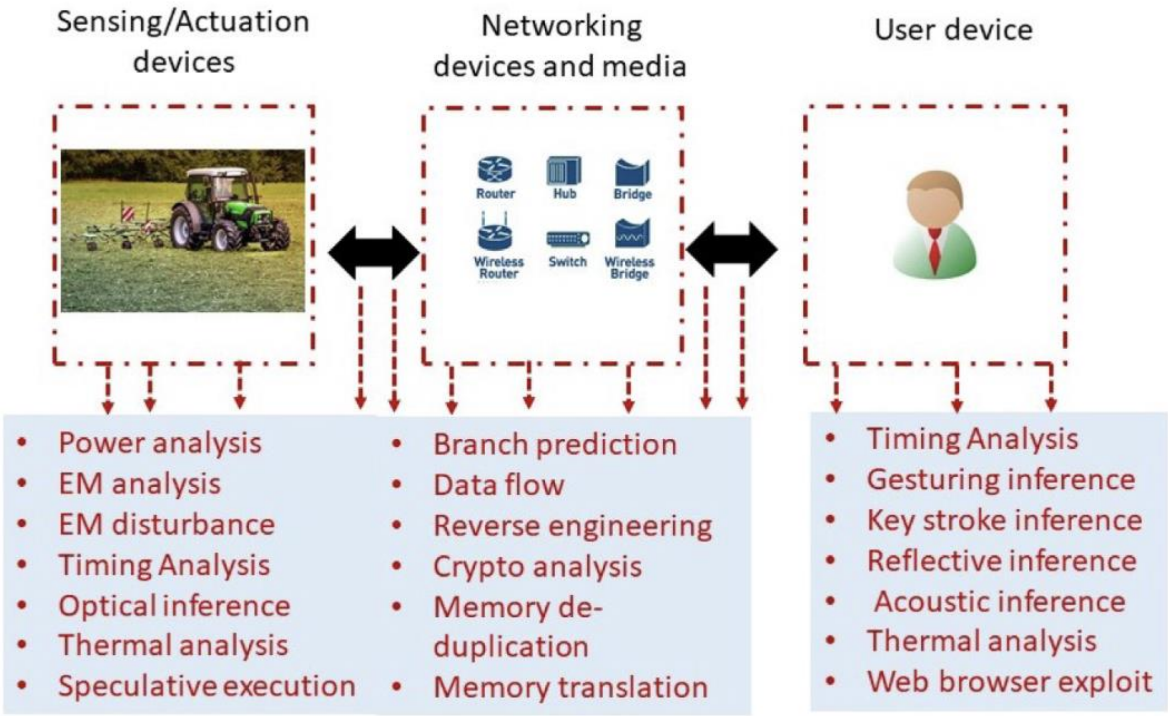

Figure 7. Side-channel attack in digital applications (Alahmadi et al., 2022)

The examination of Figure 7 indicates that side-channel attacks target the channels of communication where hackers extract useful and sensitive information from the operations of the targeted devices. In this view, confidentiality and privacy are breached as the communication that occurs between the sensors embedded in farming devices such as tractors and the wireless router in the farm office is disrupted. Tsague and Twala (2017) support Alahmadi et al. (2022) and report that in side-channel attacks, skillful attackers expose the cryptographic keys involved in the communication between devices by examining leaked information associated with the physical implementation. The consequence of side-channel attacks is that they violate the confidentiality of digital agricultural systems.

A further cybersecurity attack against agriculture 4.0 and 5.0 hardware is the jamming of radio frequencies (RF Jamming). Pirayesh and Zeng (2022) explain that jamming attacks in wireless channels arise due to the open nature of wireless networks and the slow progress achieved in preventing jamming attacks within such networking systems. Yazdinejad et al. (2021) add to Pirayesh and Zeng (2022), where they observe that the jamming networks lead to the lack of availability of communication systems within smart agriculture such as greenhouses. Salameh et al. (2018) support Yazdinejad et al. (2021) and report that jamming attacks are common in IoT, where proactive and reactive approaches are used to attack wireless networks by placing pressure on network resources. The associated consequence of the RF jamming attacks on IoT hardware is violating the availability of different systems within smart agriculture. Ahmadi (2023) adds to Salameh et al. (2018) and Yazdinejad et al. (2021) where they highlight an example of suspending the activities within a greenhouse as the loss of availability, hence causing both disruption of core activities and a lack of customer confidence. As such, farmers who are rightful in using greenhouse services are unable to access them due to their disruption. A summary of attacks on hardware is shown in Table 3.

Table 3. Cybersecurity attacks on hardware

Attack	**Cybersecurity attack**	**Potential Impact on Agricultural Systems**
Side channel	Illegal data gathering from agricultural monitoring equipment	Attacks affect the confidentiality of smart farming systems and theft of business secrets.
RF Jamming	Attackers jam wireless channels.	Attacks disrupt communication of IoT devices and reduce availability of the smart farming systems.

Adapted from (Demestichas et al., 2020; Yazdinejad et al., 2021).

Network and Equipment. Cybercriminals also target networks and connected devices. A common attack is the denial of service (DoS), where users are prevented from accessing resources within the networks, such as servers and communication links (Shah et al., 2022). In further elaboration, Shah et al. (2022) posit that skillful attackers can also launch distributed denial of service (DDoS) attacks by using IoT devices as botnets. In this view, the attackers exploit the vulnerabilities within IoT devices and use them to launch DDoS attacks against different networks. Caviglia et al. (2023) add to Shah et al. (2022) and report that in other instances, attackers use radio frequency jamming (RF) to initiate the DoS attacks where the available spectrums are denied communication to the connected nodes. The direct consequence of the DoS and DDoS attacks is that they deny essential services to the different actors within smart agricultural systems, such as requesting information from servers and sending communication to different devices. As a result, the reliability of the agricultural systems is adversely affected, and rightful entities are unable to use the resources.

Other network attacks in smart agriculture encompass man-in-the-middle (MITM) attacks. Yazdinejad et al. (2021) explain that the MITM attacks adversely affect confidentiality where the attackers store and replay information transmitted over unsecured connections. Koduru and Koduru (2022) add that the MITM attacks generate adverse consequences for the farming systems by also affecting the integrity of the transmitted data due to the likelihood of the data being modified before reaching the set destination. The inaccurate information further affects the reliability of smart agriculture systems. Additionally, cloud computing attacks affect the wireless networks where attackers self-provision on-demand services and resources available on the cloud (Yazdinejad et al., 2021). Close inspection of these types of attacks on wireless networks indicates that they directly violate the trust, integrity, and availability of essential communication channels. As a result, inaccurate data may be transmitted where MITM attacks are initiated, leading to the incorrect provisioning of resources on the farm. The use of inaccurate information may also lead to the compromise of the security of the smart farm systems.

Table 4. Cybersecurity attacks on networks

Attack	**Cybersecurity attack**	**Potential Impact on Agricultural Systems**
Distributed Denial of service (DDoS)	Prevent users from accessing the smart farming system	Attacks affect communication within the farm and reduce the efficiency of smart systems
MITM (Man-in-the-Middle)	Attackers intercept data transmitted from smart farming systems along networks.	Attacks reduce the integrity and confidentiality of smart farming systems.

Adapted from (Alahmadi et al., 2022; Yazdinejad et al., 2021).

Attacks on Data. A further category of cybersecurity threats in smart agriculture targets the stored and transmitted data. During the transit of data from one communication device to another, a risk of data leakage is identified within the cyber-physical systems. Amiri-Zarandi et al. (2022) explain that critical data collected from the farm, such as water management, weather monitoring, and soil health indicators, are transmitted to different storage locations, such as servers. However, where attackers leak the data to unauthorized entities, this leads to risks affecting decision-making and the data being mishandled. Koduru and Koduru (2022) add that in addition to breaching confidentiality, crucial data from farms may also be stolen by nefarious actors and later sold to other companies. As such, there is a need to protect against the leaks of critical farm-related data to avoid theft and to ensure privacy and confidentiality are guaranteed. Ahmadi (2023) adds that attacks in the stored data affect the non-repudiation quality, where attackers repudiate the created data and the production systems within the smart farming systems. The implication is that the repudiation activities by attackers deny appropriate users access to the required services.

The stored data within servers is also at risk of other cybersecurity threats, especially when viruses and malware are used. In their study, Kulkarni et al. (2024) revealed that ransomware attacks in the food and agricultural sector lead to serious consequences where farmers lose finances as they try to recover their farming data. Ransomware attacks are also a threat to food security because they affect the integrity and trust of the data. Demestichas, Peppes, and Alexakis (2020) support this view and reveal that threats such as trojan horses adversely affect the integrity of the data where there is a likelihood of the data being modified by the attackers. The synthesis of these studies suggests that the risks of ransomware and viruses against food security emerge when the modification of data affects the decisions made on the farm. Inaccurate data regarding pest and insect control may lead to poor measures, which in turn cause low agricultural yields. A summary of cybersecurity attacks on data from smart agricultural systems is shown in Table 5.

Table 5. Cybersecurity attacks on data

Attack	**Cybersecurity attack**	**Potential Impact on Agricultural Systems**
Data leakage	Illegal transmission of data to an unauthorized person	Attacks violate confidentiality and reduce the integrity of smart farming systems.
Ransomware	Attackers block access to agricultural data gathered through encryption.	Attacks lead to financial losses by farmers due to blackmail, as well as violations of trust, integrity, and privacy.

Adapted from (Alahmadi et al., 2022; Yazdinejad et al., 2021).

Attacks on Code. Other cyberattacks in smart agriculture have been linked to the applications where hackers affect the code. Yazdinejad et al. (2021) observe that in instances such as software update attacks, the injection of malicious codes violates integrity, while disruption of the update processes halts the overall process. In this view, malicious attackers can disrupt the software update process and prevent important security features from being implemented in the system. Directly, this leads to a consequence where attackers exploit the vulnerabilities and inject malicious code to gain access to the farm-related data (Zidi et al., 2024). The implication is that there is a need to ensure code attacks are minimized to avoid affecting the integrity and trust of the data stored within different devices. Finally, other types of cyberattacks are directed toward smart agriculture, including attacks on the support chain and misuse of physical resources. The attacks are associated with security consequences similar to other types of cybercriminal activities, where the stored data is modified and loses its integrity. The fabrication of the farming data further affects trust and may lead to serious adverse consequences, which also affect food security. A summary of cybersecurity attacks on applications is shown in Table 6.

Table 6. Cybersecurity attacks on applications

Attack	**Cybersecurity attack**	**Potential Impact on Agricultural Systems**
Software update	Disrupt software updates and prevent improved security	Attacks violate the integrity of smart farming systems since the latest cybersecurity protection systems are not installed
Malware injection	Attackers infect devices and nodes using malicious codes	Attacks violate the integrity of smart farming system devices and reduce the efficiency of operations.

Adapted from (Alahmadi et al., 2022; Yazdinejad et al., 2021).

Generally, the transition from traditional to digital technology requires resources, which presents financial implications. In the case of cybersecurity attacks, farms are pushed to install the latest defense systems and upgrade software. According to Mourtzis et al. (2022), the changes stretch the resources of the sector, leading to financial losses in the long run. On the same note, Oruc (2022) pointed out that cybersecurity attacks on unmanned vehicles used in agriculture resulted in huge financial losses, especially when these machines are jammed. The implication is that cyberattacks negatively impact the financial security of the agricultural sector. Another consequence of cybersecurity attacks in agriculture is a loss of confidence and trust in the smart systems. On this point, Pan and Yang (2018) indicated that most farmers opted for conventional farming after facing IoT vulnerability to cyberattacks. The observation was supported by Koduru and Koduru (2022), who also highlighted the implications of IoT's vulnerability to cyberattacks. The study showed that malware infections corrupted the integrity of farm IoTs, leading to substantial loss of time and produce. The implication is that cybersecurity attacks lower interest in utilizing technological solutions in farming. The other consequence of cyberattack is loss of information. About this point, Kulkarni et al. (2024) noted a loss of employees and customers' information following the breach of an agrochemical and agricultural biotechnology corporation's website. According to Macas et al. (2023), one of the goals of attackers has been to compromise the integrity of systems. The implication is that loss of information fuels privacy and security issues among the parties concerned. Maddikunta et al. (2021) noted that cyberattack events prompted a push for advanced data protection systems, testifying to the loss of confidence in normal systems. In some cases, the regulator is forced to upgrade acceptable standards for the industry. The issue of data confidentiality and privacy was also examined by Kaur et al. (2022). The investigators asserted that failure to adopt best practice guidelines and standards influenced data breaches. The implication is that cybersecurity attacks may be used to gauge the protection standards in agricultural applications. In the meantime, Kapoor (2024) reported that cybersecurity attacks in agriculture led to investigations aimed at detecting the existing weak spots and designing better protection models. The implication is that cyberattacks have catalyzed data security advancement in smart farming. On the other hand, Jerhamre et al. (2022) attested to an increase in legal challenges for agricultural organizations that experience cyberattacks. The implication is that organizations can be penalized by government regulators in case of cyberattacks affecting individuals’ data.

4.0 Critical Review and Analysis

The critical review and analysis section showcases results relating to the use of different measures to mitigate cybersecurity threats. This section is also divided into framework, taxonomy and explanations for specific cyber threat mitigation strategies. The framework shows the key points to consider when striving to reduce the risk of cyber threats. Meanwhile the taxonomies show the specific approaches used to address the risks. The measures are organized into six sub-sections, which include generic cybersecurity measures, UAV, AI/IoT, blockchain and robotics, and quantum computing.

Framework

A framework for mitigating cyber threats is shown in Figure 8.

Figure 8. Cyber threats mitigation framework (Yadav, 2024)

From Figure 8, it is noted that mitigating cyber threats requires diverse strategies to address different threats. In particular, the end-user education can help address threats related to weak passwords while IoT security can ensure regular updates of the cyber security system to protect the latest threats. A summary of the threats and mitigation strategies discussed in this section is indicated in Table 7.

Table 7. Mitigation strategy based on potential cybersecurity threats

Context	**Cybersecurity Threats**	**Mitigation strategy in Agricultural Systems**
Data	Unauthorized data access due to the use of default passwords	Train farm employees on creating strong encryptions and good cyber security practice of not sharing passwords. Also install security software and firewalls.
	Injecting false data	Create disaster recovery plan for the smart farm database such as using cloud data systems
Software	Malware attacks	Apply software updates to smart farm systems to ensure the latest cyber threats are detected and blocked. Apply signed software execution policies so that illegal software installation is prevented.
	Third-party attacks	Limit actors who can access the smart farm systems and ensure account privileges only given to users who need them. Also embrace zero-trust approach where users follow onboarding and off boarding procedures and can be traced in case of data breach.
Network	Protocol attacks	Conduct regular scans on software and network devices and remove illegal installations. Use AI tools to detect suspicious activities that can cause data breach.
	Edge-gateways hijacking	Acquire latest smart farm hardware which are more difficult to hack into due to better protective systems. Segregate networks using applications such as firewalls to protect against certain critical information such as finances of the agricultural company.
Service	AI attacks	Regularly audit AI systems for vulnerabilities and check for any problems with bias in decision making. Further training of AI and robotic systems can be done to improve accuracy and modelling abilities of the smart farm cyber threats and mitigation strategies.

Cloud attacks	Apply multi-factor authentication system where remote access to cloud data. This means that passwords and pins are accompanied by physical token-based authentication to verify the individuals accessing the data.

Adapted from (Alahmadi et al., 2022; Yazdinejad et al., 2021).

From Table 7, the cyber threats related to data require mitigations where individuals engaged in data management are trained to improve data encryption and management behavior. Meanwhile, mitigation for networks and software, require more stringent proactive strategies such as signed policies when installing new software as well as regular scanning to remove illegal software. Lastly, mitigation for attacks targeting services such as AI and cloud systems require regular auditing and muti-factor authentication to verify the data and detect any cyber breach. 4.1 Cybersecurity Measures

The first theme elaborated on cybersecurity measures advocated to secure smart farming systems. An overview of the measures indicated that they focused on diverse aspects, including cybersecurity awareness training and education, models and frameworks to guide the development of cybersecurity strategy, and individual strategies for cybersecurity that could be adopted by farmers.

4.1.1 Cybersecurity awareness and training

The evaluation of the studies highlighted the importance of cybersecurity awareness training and education to equip farmers and workers within farms with skills to reduce the risks of cyberattacks. In their research, Al-Emran and Deveci (2024) advocated for appropriate cybersecurity behavior in the metaverse to protect themselves and their organizations from cyberattacks. The arguments stipulated that cybersecurity threats within the virtual environments were similar across different application domains, including business and agriculture, where they exploited the user’s lack of security expertise, diverse human errors, and a lack of standardization for security within virtual environments. Figure 8 showcases the comprehensive list of cybersecurity risks associated with the metaverse.

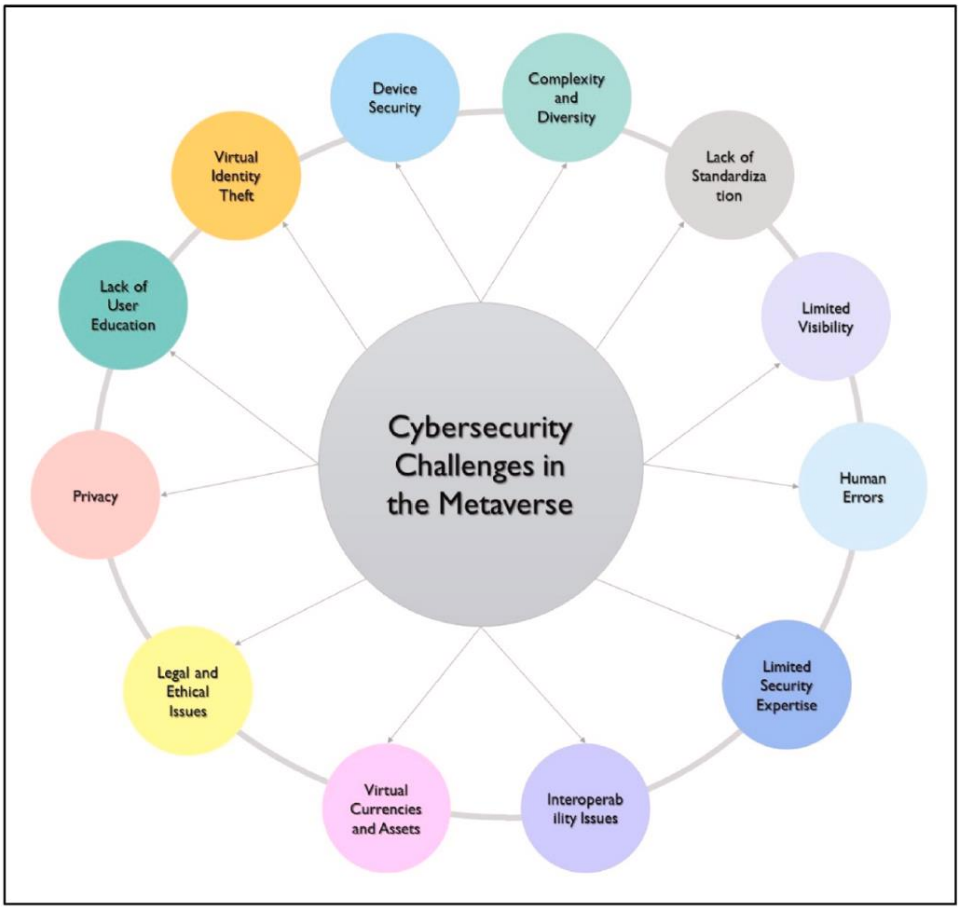

Figure 9. Cybersecurity challenges in the metaverse (Al-Emran and Deveci, 2024)

In Figure 9, the diverse cybersecurity challenges faced in the metaverse were similar to those in smart agriculture, where a lack of user education, lack of standardization, human errors, legal and ethical issues, and interoperability problems were reported. Al-Emran and Deveci (2024) further argued that to address the various cybersecurity threats, a multi-faceted cybersecurity approach was required where users would be educated about the potential risks in the metaverse, including privacy and confidentiality concerns. Adopting similar strategies in smart farming would ensure that farmers were secure from the cybersecurity risks experienced. However, Chaudhary, Gkioulos, and Katsikas (2023) contradicted Al-Emran and Deveci (2024) and posited that in some instances, small-scale enterprises were not engaging in cybersecurity training either due to the lack of financial resources or their attitudes where they viewed cyber-risks to affect only large corporates. The negative attitudes against cybersecurity training hindered efforts to equip SME owners with security skills.

In further review, Chaudhary, Gkioulos, and Katsikas (2023) resonated with Al-Emran and Deveci (2024), where they highlighted the importance of cybersecurity awareness in enhancing cyber defense in small and medium enterprises. The findings highlighted that education could be offered in less formal and less intensive sessions to educate users about general security practices. Zhao et al. (2024a) added to Chaudhary, Gkioulos, and Katsikas (2023) and highlighted the use of innovative games to raise cybersecurity awareness about secure software and cloud security. The findings showed that cybersecurity awareness training was integral for both users in enterprises and software developers, where they were required to demonstrate awareness about existing cyber risks and threats. Baltuttis, Teubner, and Adam (2024) also reiterated Zhao et al. (2024a) and reported that cybersecurity behavior among knowledge workers influenced their approach toward cybersecurity measures. As a result, older employees had a high resilience to cybersecurity while younger individuals were less concerned with risks of cybersecurity. The inferences from the studies implied that organizations could tailor their training programs to ensure employees were educated about the importance of cybersecurity and various ways they could use it to reduce cyber threats.

However, Fatoki, Shen, and Mora-Monge (2024) misaligned with Zhao et al. (2024a), where they revealed that the poor attitudes of non-information technology (IT) users towards cybersecurity reinforced risky behavior. In particular, some of the bad behavior that can elevate the risk of a cybersecurity breach include clicking on malicious links, opening USB drives without scanning for malware, replying to phishing emails, and sharing passwords to company websites with third parties (Arroyabe et al., 2024; Chundhoo et al., 2021; Geil et al., 2018; Ghobadpour et al., 2022; Khan et al., 2019). The results suggest that positively shaping employee behavior is a crucial step toward promoting the cybersecurity of digital systems and reducing the risk of cyberattacks. The insights also showed that conversely, optimism by non-IT users towards cybersecurity improved security, where they demonstrated positive risk communication behavior and cybersecurity education and training (Zhao et al., 2024a). The misalignment implied that providing cybersecurity training and raising awareness about the importance of cybersecurity encouraged the users to minimize threats, while a lack of such training and cybersecurity awareness led to more threats.

4.1.2 Cybersecurity models and frameworks

Further evaluation revealed various cybersecurity models that were advocated to enhance security within cyber-physical systems. The models and frameworks highlighted different strategies that were also important in minimizing cyber threats. In the study by Toussaint, Krima, and Panetto (2024), different cybersecurity frameworks were examined to ensure that various user needs to address risks of data manipulation could be met. The research reviewed diverse cybersecurity frameworks, including the compliance framework that specified guidelines and recommendations to help protect users by ensuring regulatory adherence. A standard-based framework was further used to outline guidelines and best practices to manage and protect organizations, while a comprehensive framework ensured data security across different industry domains (Toussaint, Krima, and Panetto, 2024). The National Institute of Standards and Technology (NIST) framework was further advocated as a comprehensive guideline that provided numerous benefits to organizations, including enhancing technical innovation and allowing organizations to improve gaps in their cybersecurity approaches. The NIST framework is showcased in Figure 10 below.

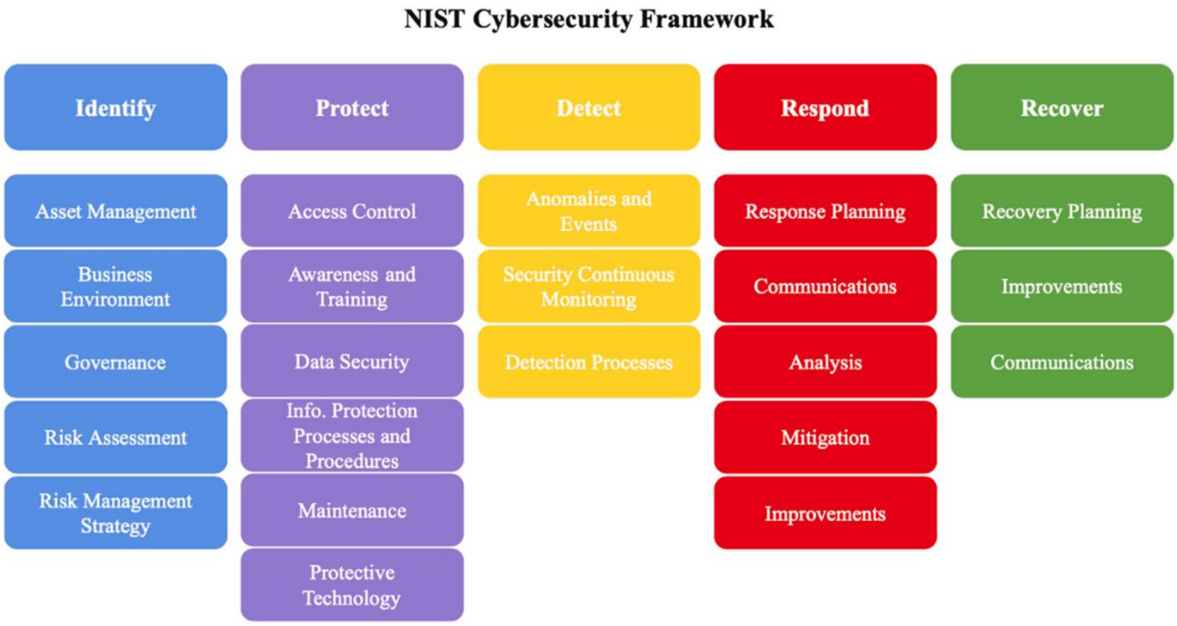

Figure 10. NIST Cybersecurity Framework (Toussaint, Krima and Panetto, 2024)

In Figure 10, the NIST cybersecurity framework is outlined, which highlights various guides to support organizations in developing a comprehensive cybersecurity strategy. A crucial benefit of a robust cybersecurity framework is that it shows best practices to consider in cybersecurity to achieve positive outcomes (Javaid et al., 2022; Klerkx et al., 2019; Peppes et al., 2021; Shaik et al., 2023; Singh et al., 2022). From Figure 5, the first practice is identifying security risks, which may be threats or vulnerabilities to the cybersecurity system. In agricultural context, this step involves unsecure networks which lack the latest cyber protection software or the lack of awareness and education on cybersecurity among staff, The second practice is to create robust protection strategies, which may be in the form of controlling access, creating awareness and training, and installing cybersecurity software. In agriculture context, this involves considering unique challenges in the sector such as long distances of networks and risk of damage due to exposure to harsh weather conditions. The third strategy entails detecting any malware through continuous monitoring, while the fourth strategy involves responding to any cyberattacks if they happen (Toussaint et al., 2024). In agriculture, this requires continuous checking of data from IoT devices against physical data collected from the field to determine whether there is a security breach. However, in case of successful cyberattacks, the company should have plans to recover data and ensure the resilience of its smart systems. The guides involve the identification and evaluation of risks, provision of awareness training to secure processes and procedures, continuous monitoring of the security scenario to detect any anomalies, and specifying guidelines for response and recovery planning.

The other cybersecurity framework commonly used is ISO/IEC 27001 which indicates the strategies companies of different sizes need to consider to boost their capacity to deal with cyber threats. The framework latest model is ISO/IEC 27001:2022 (ISO, 2024). An analysis of the ISO framework indicates that it has many sections that focuses on protection from cyber threats (n = 82), followed by identification of cyber threats (n = 26), and response to the threats (n = 21) (Malatji, 2023). However, ISO/IEC 27001:2022 framework only has a few sections on the detection (n = 18) and recovery from cyberattacks (n = 12). The controls covered in ISO/IEC 27001:2022 which help in protection against cyberattacks include threat intelligence, physical security monitoring, use of cloud services, secure coding, and the use of cloud services (ISO, 2024). In the agricultural context, ISO 27001 can be used as framework for the continuous improvement of the information security management system (ISMS) for smart agriculture devices. When implementing ISO 27001 in agriculture, a PDSA (plan, do, check, act) cycle approach is used because it is linked with many benefits such as defined roles of stakeholders, better risk management and improved information protection (Condolo et al., 2024). A summary of PDSA when implementing ISO 27001 in agricultural sector is shown in Figure 11. The first step involves planning where the key agricultural data and customer information are clarified to understand the information to be safeguarded by the security systems. The second step entails developing a risk management plan based on ISO 27001 recommendations, showing strategies to use to protect against different cyber threats (Condolo et al., 2024). In this stage, the probability of different threats such as phishing stacks, leakage of confidential data, identity theft, or interception of communications are analyzed to decide on how to allocate resources for mitigating cyber threats.

Figure 11. PDCA approach when implementing ISO 27001 (Condolo et al., 2024)

The third stage entails acting, where the necessary preventive or corrective action against cyber threats is taken. The last step entails monitoring ISMS implemented based on ISO 27001 and developing audit to show areas for improvement

4.2 UAV Measures

The second measure to address cybersecurity issues focused on UAV devices where suspicious traffic was detected and attacks were mitigated. The analysis indicated that the development of security models ensured cybersecurity in UAVs. In the study by Khan, Shiwakoti, and Stasinopoulos (2022), a conceptual system dynamics (CSD) model was developed to assess cybersecurity risks in UAVs where issues were identified in human factors, weak security in communication networks, and the lack of regulatory frameworks and legislation to secure the technologies. As such, cyber threats were mitigated by updating the current legal framework, analyzing human behavior, and implementing robust security solutions to mitigate attacks. Ahmad et al. (2024) supported Khan, Shiwakoti, and Stasinopoulos (2022) and proposed an attention-based framework to secure UAVs by leveraging transformer neural network architecture. The framework demonstrated an improvement in accuracy of 86% in predicting the failure of sensors and anticipating their failure 1s to 2s before occurrence. The findings indicated that the framework mitigated cybersecurity risks by predicting and classifying the real-time failure of sensors. In further work, Kim et al. (2021) added that cybersecurity measures in UAVs could be enhanced by integrating AI techniques to detect and classify suspicious traffic and mitigate attacks against the systems. The insights indicated that AI was improving the robustness of cybersecurity solutions to ensure smart agriculture solutions were not affected by cyber-attacks. The view is supported by other researchers who have noted that UAVs rely on wireless communication because they are often controlled remotely, and hence, robust encryption and security systems are needed to protect them from theft and cyber-attacks (Alsamhi et al., 2021; Bashir et al., 2023; Dahlman and Lagrelius, 2019; Li et al., 2024; Ly and Ly, 2021). Moreover, UAVs often use common chips as well as universal protocols, open-source operating systems, and simple software architectures that make them affordable while also elevating their security risks. Therefore, the use of AI-powered cybersecurity can improve detection and response to cyber-attacks when UAVs are used, thereby improving the reliability of smart agricultural systems.

4.3 IoT /AI Measures

The findings highlighted different IoT and AI cybersecurity measures in smart agricultural systems. IoT devices face severe cybersecurity threats since a security breach can disrupt the entire network and affect the operations of all devices connected to the network (Pärn et al., 2024; Smith et al., 2021). From the studies, some of the strategies that can be used to improve IoT cybersecurity include enhancing encryption and authentication, implementing network segmentation, and using patch management and regular updates (Chatfield and Reddick, 2019; Choo et al., 2021; Nagaraju et al., 2022). Authentication and encryption systems can prevent unauthorized access to the system, while regular updates can ensure improved capability of cybersecurity software to manage the latest threats (Prodanović et al., 2020; Pyzynski and Balcerzak, 2021; Saleh, 2024). In agricultural cybersecurity, farm employees can be trained regularly on best cybersecurity practices to ensure they understand the connection between their data management behavior and cyber attacks. The emphasis is to reveal how gathered agricultural data can be used by competitors or other third parties to affect the smart farm operations and encourage them to better manage smart farm online systems. Concerning network segmentation, some studies showed that using cloud computing can ensure sensitive data in a system is stored in the cloud where it cannot be easily accessed even when the system is hacked (Arce, 2020; Pang and Tanriverdi, 2022; Pedchenko et al., 2022; Rao and Elias-Medina, 2024). Based on the findings, it is realized that in protecting IoT devices in agriculture, a combination of strategies is needed to mitigate potential threats since there is no single approach that addresses all the potential cybersecurity risks. A summary of the mitigation strategies for cybersecurity risks is shown in Figure 12.

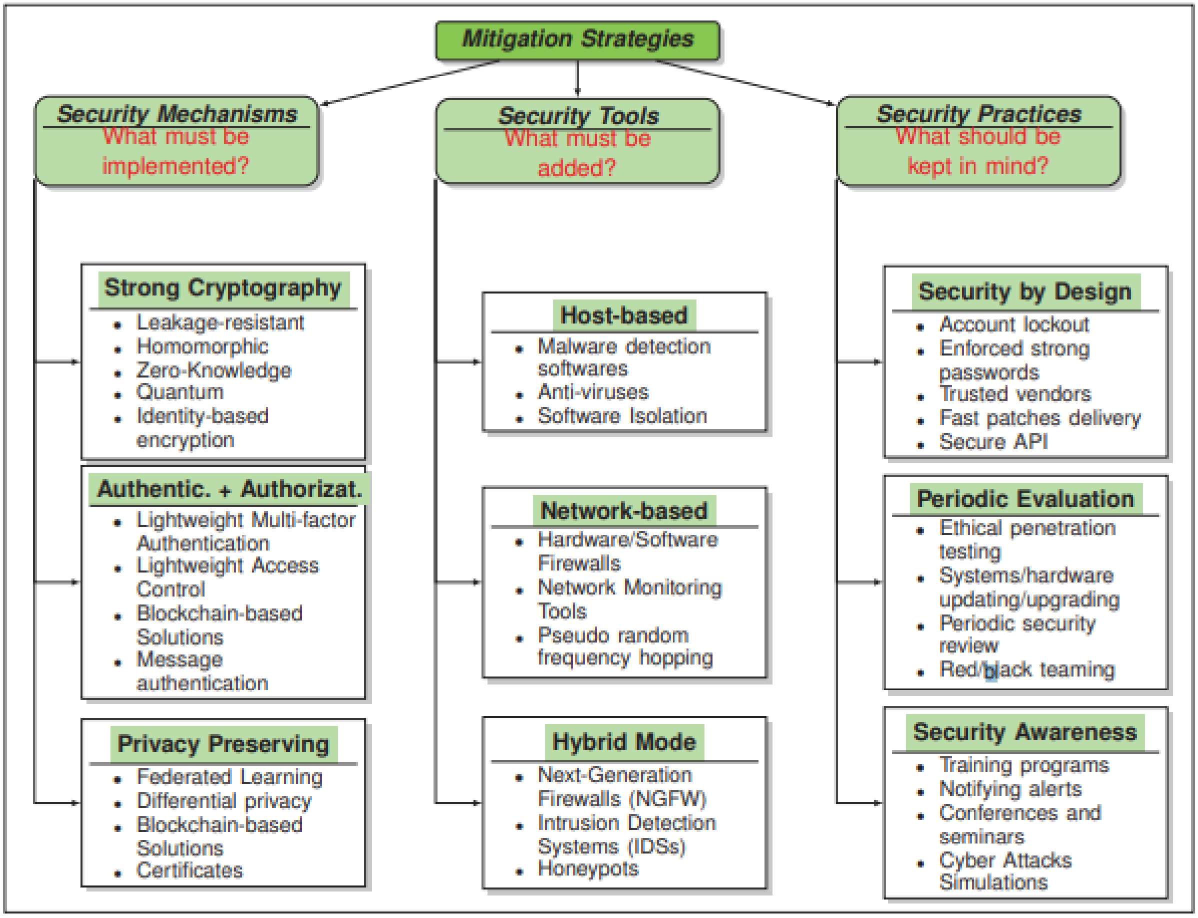

Figure 12. Mitigation strategies for cybersecurity risks (Friha et al., 2022)

Moreover, the findings revealed that the cybersecurity of IoT could be enhanced by using AI algorithms. A crucial benefit of AI technology is that it enables accurate and efficient analysis of large traffic data to identify anomalies, which helps to detect malicious attacks, malware, and phishing attempts (Hasan et al., 2024; Linkov et al., 2019; Sarker et al., 2021). Expounding on this view, Sudharsanan et al. (2024) demonstrated the use of the Xception-based Feedforward Encasement (XBFE) deep learning algorithm as an intrusion detection solution to monitor IoT devices and undertake feature mapping and filter scaling. The findings showed that the feed-forward algorithm improved the accuracy of parameters as a result of training where patterns were learned and matched to attacks. Yang et al. (2023) added to Sudharsanan et al. (2024) and proposed an efficient intrusion detection system based on cloud-edge collaboration where it outperformed the traditional cloud-based methods that did not meet the demands for network load, data privacy, and timely response. The system used the stacked sparse autoencoder (SSAE) to reduce dimensionality and overcome challenges of resource constraints, as well as the temporal convolutional network (TCN) to detect attacks. Findings showed that the IDS for IoT systems reduced the training time and the storage and memory requirement by more than 50%, while the detection accuracy was similar to the centralized trained models. Further work by Shafiq et al. (2020) supported Yang et al. (2023) and demonstrated the effectiveness of machine-learning algorithms in classifying and identifying malicious IoT traffic with a 95% accuracy. Meidan et al. (2020) reiterated Shafiq et al. (2020) and demonstrated that ML-based techniques were effective in detecting specific vulnerable IoT device models connected behind domestic network address translation (NAT). In such studies, ML methods enhanced cybersecurity in IoT devices by classifying and eliminating malicious traffic and identifying vulnerable IoT devices. Pan and Yang (2018) also revealed that ML methods were integrated into the cybersecurity mechanisms of IoT devices to better analyze behaviors related to cybersecurity and identify potential threats. As a result, IoT traffic would be easily classified as suspicious based on user behavior, hence identifying potential misuse.

4.4 Blockchain and Robotics Measures

Blockchain and robotics measures were also recommended to address the cybersecurity issues faced in smart agriculture. In agriculture, robots are used to promote accuracy and sustainability in agriculture, where they are used to apply pesticides and fertilizers in a manner that minimizes wastage and optimizes resource use (Okupa, 2020; Wang et al., 2023). In terms of cybersecurity, robots such as drones are used for remote patrol and monitoring to check IDs, scan faces, detect physical breaches, and intervene in emergencies (Li, 2018; Okey et al., 2023; Stevens, 2020). Jin and Han (2024) reported that despite the unique advantages of robotic arms in precision agriculture, where they reduced labor costs and improved environmental sustainability, they faced cybersecurity challenges when cloud computing was involved in storing sensitive data. Taeihagh and Lim (2019) also indicated that a lack of legal framework on liability in accidents caused by robots has limited its use in different fields, including agriculture. Further security cyber risks arose from the real-time processing of data from robotic arms and issues related to the difficulty in managing the accessibility of large data volumes. However, the cyber security of the robotic systems was improved by using advanced software architectures and improving kinetic algorithms in digital twins to mitigate unnecessary security issues (Jin and Han, 2024). Fosch-Villaronga and Mahler (2021) added to Jin and Han (2024) and showed that cybersecurity risks in robotics used in smart agriculture arose from the lack of existing regulations governing robotics in the European Union. The identified cybersecurity risks included the exploitation of weaknesses in the networks that interconnected the robotics systems and the lack of security of sensitive stored data. Subsequently, Fosch-Villaronga and Mahler (2021) recommended the implementation of policies and legal frameworks to enhance the privacy of communication with robotics and the security of stored data. Additionally, the use of mandatory cybersecurity labels and certifications was advocated to guarantee the security of robotics systems. The findings emphasized the need for cybersecurity regulations to support the use of robots in smart agriculture.

In addition to cybersecurity measures focused on robotics systems, the findings highlighted the role of blockchain-based strategies. Kshetri (2017) demonstrated the effectiveness of blockchain-based identity and access systems to strengthen the efficiency of existing IoT devices used in smart agriculture. Blockchain was also recommended because it promoted the auditing of security transactions and reduced the susceptibility of agricultural systems to hacking. Other benefits linked to blockchain include reduced costs of transactions due to the efficiency of processing and increased accountability and transparency, which ensures that the privacy of users is enhanced since the data can be traced in case any problem arises (Bahassi et al., 2022; Fernandez et al., 2021; Lee, 2020; Sharma et al., 2022; Victor et al., 2024). In this regard, blockchain use in agricultural smart systems can ensure a reliable supply chain as it promotes financial transactions between customers, suppliers, and agricultural companies. In this case, agricultural companies can maintain privacy in dealing with other stakeholders and gain competitive advantage linked to blockchain applications in financial management. Moreover, blockchain can help track different information relating to crop growth, seed quality, and demand by customers which helps to not only improve supply chain efficiency but also decision making on the best crops to consider. The exchange of data and its verification using smart contracts was identified to enrich the privacy of the blockchain networks.

4.5 Quantum Computing Measures

Quantum computing measures were further discussed to secure smart agricultural systems from cyber threats. An overview of the measures showed that researchers combined quantum computing with other existing solutions, including blockchain, traditional encryption, and machine learning. Quantum computing provides the benefits of inherent parallelism and high processing speeds, which optimizes machine learning and improves the efficiency and accuracy of monitoring, detecting, and responding to cyber threats (Bissadu et al., 2024; Maraveas et al., 2024; Onur et al. 2024). The use of quantum computing in cybersecurity is deemed revolutionary because it can solve complex encryptions such as those that use discrete algorithms and integer factorization and, hence, can provide better encryption models than classical techniques (Kavallieratos and Katsikas, 2023; Liu et al., 2023). This means that quantum computing will phase out cryptography in future since the former is more efficient in the encryption of data compared to the latter. In agricultural sector, this means that using quantum computing can enhance detection of data breaches and improve data encryption thereby enhancing the level of cyber security for smart farm systems. With the blockchain measures, Aurangzeb et al. (2024) proposed evaluation criteria to detect cybersecurity attacks in smart grids using quantum voting ensemble models combined with blockchain to secure stored data. The findings indicated that quantum voting improved the analysis of traditional cryptographic systems and enhanced the accuracy of cybersecurity injunctions within the smart grids. The combination of quantum voting and blockchain-preserving storage enhanced the accuracy and privacy of smart grid systems and produced tolerance during cyberattacks. Abdel-latif et al. (2021) supported Aurangzeb et al. (2024), who proposed a system based on quantum-inspired quantum walks that combined blockchain technology to ensure the secure transmission of data between IoT devices. The insights from the system showed that it promoted security against message and impersonation attacks, promoting the cybersecurity of IoT devices. Figure 13 illustrates the proposed quantum-inspired and blockchain-based smart water utility.

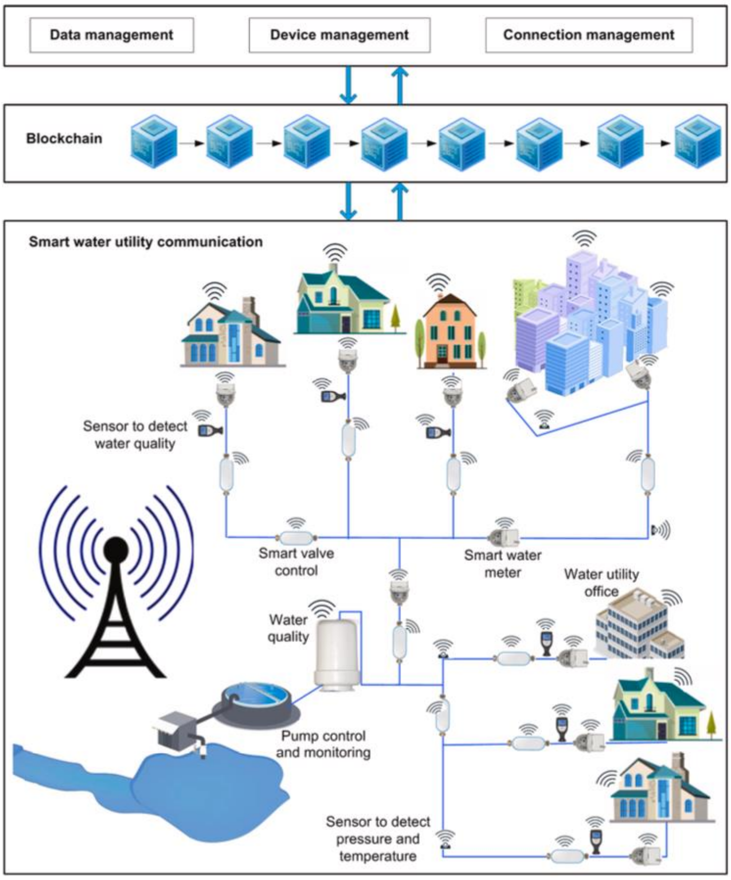

Figure 13. Quantum-inspired and blockchain-based smart water utility (Abdel-latif et al., 2021)

In Figure 13, the combination of quantum computing and blockchain technology to secure a smart water utility against cyberattacks was showcased. The secure transmission of data via blockchain and quantum computing mitigated attacks such as man-in-the-middle and message attacks against the smart water utility and promoted privacy and confidentiality.

Further study showed how quantum computing could be combined with machine learning. In the study by Alomari and Kumar (2024), a framework based on quantum machine learning was proposed that leveraged optical pulses of secure communication to detect post-quantum cyberattacks in IoT systems. The framework used measurable features of optical pulses during qubit transitions to train the quantum machine learning model. The findings from Alomari and Kumar (2024) indicated that although quantum algorithms were utilized to compromise the security of IoT systems, the proposed framework leveraged machine learning to detect and predict such attacks. As such, combining quantum computing and machine learning facilitated the detection and prevention of cyberattacks. In agriculture, the use of quantum computing can help to better detect and block suspicious visits on the smart farming systems which can signal the need for verification by operators, leading to reduced risk of cyber breach.

Quantum computing application in agriculture can also help to improve cybersecurity of smart farm systems by reducing risk of disruptions of communication equipment within the farm. The combination of quantum computing with encryption was identified to secure direct communications. Abdelfatah (2024) demonstrated the effectiveness of a three-factor biometric quantum identity authentication system for biometrics, which relied on classical cryptography systems. The findings indicated that the quantum-based system provided double-layer security using quantum encryption and quantum secure direct communication, hence securing real-time exchange of information. The proposed system addressed the weakness of biometric systems based on classical cryptography, which could be exploited using quantum techniques. Argillander et al. (2023) added to Abdelfatah (2024) and showed that a new material for generating random numbers based on the perovskite light emitting diode (PeLED) could be adopted in cybersecurity applications, hence promoting safer, cheaper, and more environmentally-friendly exchange of digital information. The advantage of the PeLED techniques was that they were cheaply sourced and more environmentally friendly.

4.6 Challenges Implementing Cybersecurity Mitigation Measures

Although the various cybersecurity mitigation techniques, such as AI, IoT, blockchain, and quantum computing technologies, can enhance the protection of technologies used in agriculture, there are certain problems that can hinder their implementation. One challenge highlighted in most studies involves employees' work overload, which contributes to job stress and negative attitudes toward appropriate cybersecurity behavior (Araújo et al., 2024; Daim et al., 2020; Kim and Kim, 2024). Expounding on this point, researchers have explained that when employees lack self-efficacy, they view AI learning and implementation as a threat to their work, fearing job losses if technologies are implemented rather than a challenge to be overcome to improve the cybersecurity of agricultural technologies (Adil et al., 2023; Ahmed et al., 2024; Balaji et al., 2023; Ramos-Cruz et al., 2024; Sott et al., 2021). In this respect, employees experiencing work overload may not comply with additional rules on cybersecurity, thereby hindering the effective implementation of mitigation measures.

The second challenge that can prevent the implementation of cybersecurity mitigation measures involves legal challenges related to data privacy (Choo et al., 2018; El Alaoui et al., 2024; Familoni, 2024; Sarker et al., 2024a; Wurzenberger et al., 2024; Yang et al., 2024). Essentially, AI technologies may use customers' personal data in an unauthorized manner, which raises concerns about how AI should be integrated into different fields, including agriculture (Pawlicki et al., 2024; Sharma and Gillanders, 2022; Sun et al., 2021). Similarly, other studies have revealed that AI has transparency issues, known as black-box problems, where it does not show how data entered into the system is synthesized to provide output (Lin et al., 2018; Sarker et al., 2024b; Yu et al., 2023). In agriculture, this can lead to issues of discrimination against farmers of certain socioeconomic backgrounds due to AI bias. In this respect, AI use in agriculture also presents regulatory concerns that need to be addressed by farmers and relevant companies to avoid problems of AI bias in the data process.

The third challenge in implementing cybersecurity mitigation measures such as quantum computing is technical difficulties, especially where employees lack the skills to use the technologies (Alshaikh et al., 2024; Bui et al., 2024; Raval et al., 2023). The view is supported by many studies highlighting that small and medium-sized companies in developing countries lack the financial capacity to train their staff on advanced technologies such as AI and quantum computing to enhance their ability to use the cybersecurity software in an effective manner (AlDaajeh and Alrabaee, 2024; Channon and Marson, 2021; Duncan et al., 2019). In agreement, other researchers have explained that ransomware is constantly evolving and phishing attacks are becoming more sophisticated, which emphasizes the need for employees to be given continuous training on advanced technologies in cybersecurity mitigation (Nazir et al., 2024; Raj et al., 2024; Venkatachary et al., 2024). The strategy can ensure that employees in the agricultural sector are competent in detecting threats and addressing any vulnerabilities in the technologies.

5.0 Discussion

The current discussion focuses on cybersecurity threats in agriculture and the possible mitigation measures. To understand the smart farming architecture that can be attacked by attacked, the key aspects were based on that of Yazdinejad et al. (2021) shown in Figure 13.

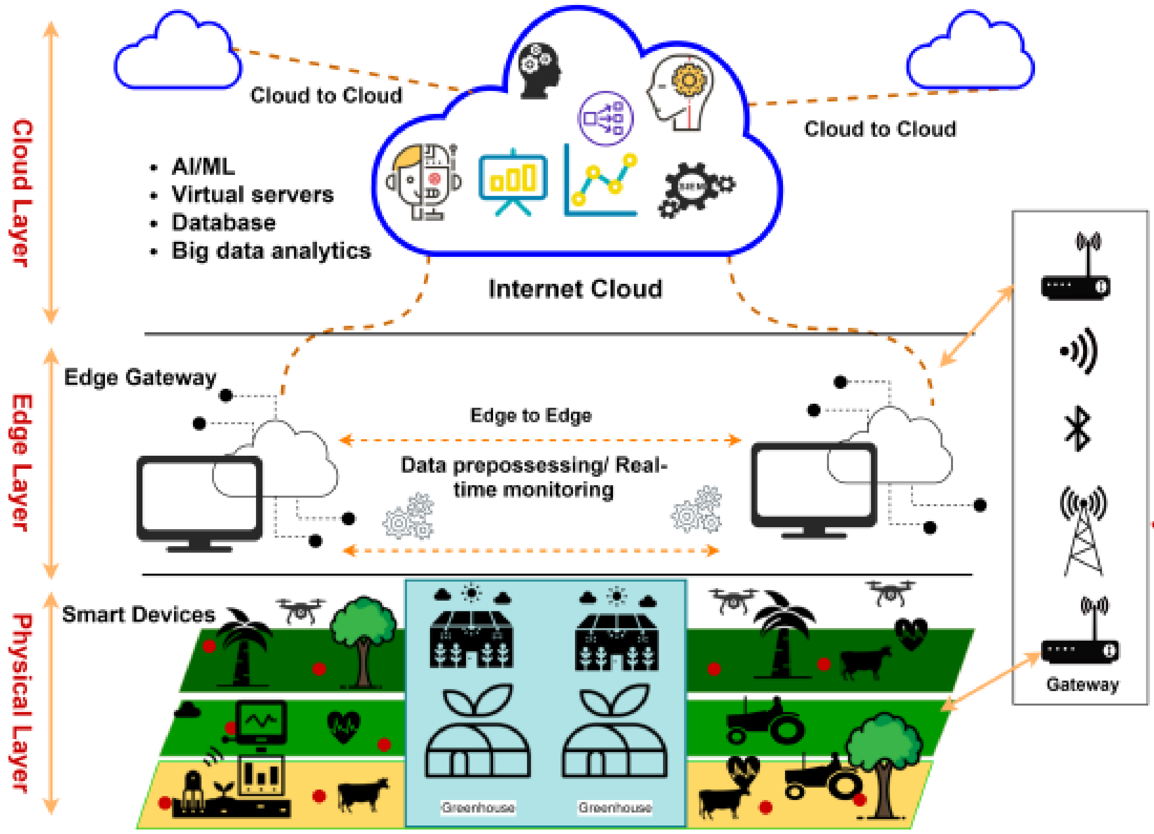

Figure 14. Smart agricultural system infrastructure (Yazdinejad et al., 2021).

From Figure 14, attacks on smart farming systems can target different layers, including cloud, edge, physical, and networks. Therefore, diverse mitigation strategies are required to address the cybersecurity threats at different levels. Besides, a taxonomy related to the cybersecurity issues was shown in Figure 15.

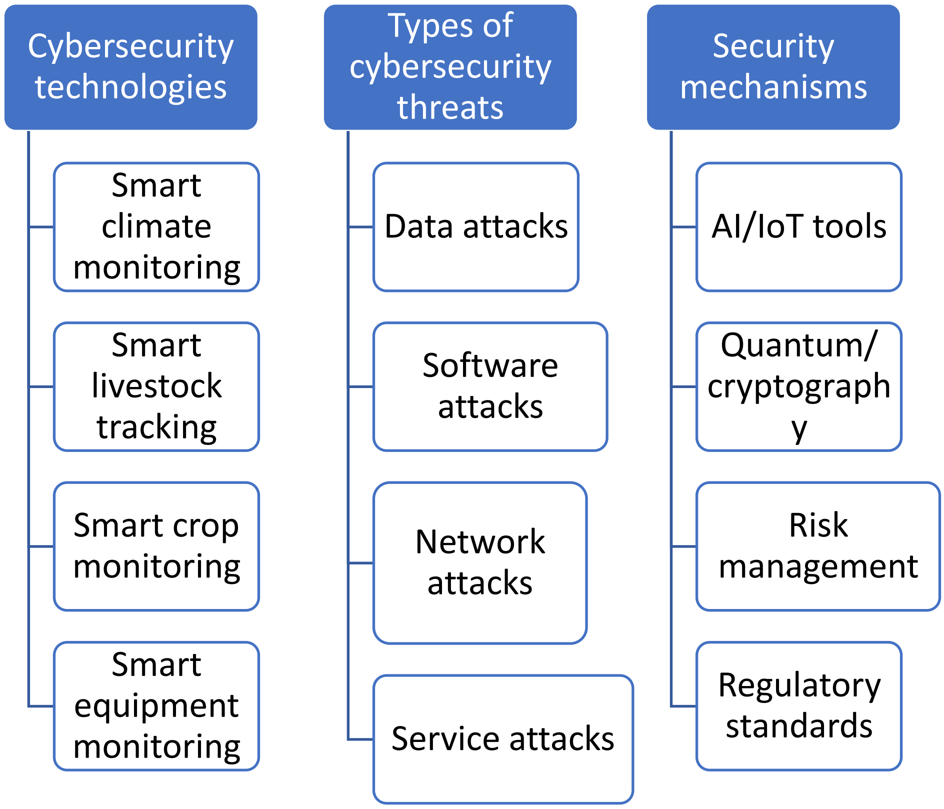

Figure 15: Taxonomy for cybersecurity technologies, threats, and security mechanisms.

5.1 Cybersecurity Threats in Agriculture 4.0 And 5.0

The findings on cybersecurity threats in agriculture 4.0 and 5.0 revealed the types of threats and consequences of attacks on agricultural systems are shown in Table 8. Overall, the results demonstrate that Agriculture 4.0 and 5.0 are still susceptible to cybersecurity threats despite perceived advancement in cyber protective measures.

Table 8. Types of cybersecurity attacks and impacts

Context	Cybersecurity Attacks	Impact on Agricultural Systems
Data	Unauthorized data access due to the use of default passwords	Illegal access to agricultural information such as crop models, livestock conditions, and production volumes is caused by a lack of physical security on agricultural smart equipment.
	Injecting false data	False data fed into the smart agricultural systems can lead to faulty analytics and poor decisions on agriculture leading to losses.
Software	Malware attacks	Ransomware attack by installing illegal software on the agricultural smart systems that interfere with operations. Used for blackmail and extortion.
	Third-party attacks	Third-party service providers can access private data from smart agricultural systems that cause compromise of an organization's confidential information.
Network	Protocol attacks	Vulnerabilities in communication protocols can be attacked through various strategies, such as through radio frequency jamming. Can affect IoT systems and hinder sharing of agricultural information between different devices.
	Edge-gateways hijacking	Hackers can attack compromised edge-gateways, take total control of the agricultural smart systems, and perform malicious actions such as falsifying data and manipulating traffic data. Caused by failure to follow cybersecurity regulations.
Service	AI attacks	Attacks can target data gathered by smart agricultural systems and cause bias in AI training, leading to false predictions by AI and poor decision-making.
	Cloud attacks	Attackers can target IoT-cloud integration, causing cloud-data theft as well as main-in-the-cloud attacks.
	Blockchain attacks	Vulnerabilities in blockchain systems such as transaction privacy leakage, double spending, and smart contracts can be exploited by attackers to affect decision making using smart systems.

For the factors increasing cybersecurity risks in Agriculture 4.0 and 5.0, the first element extracted from the literature was the extended use of default passwords and unpatched firmware (Ali et al., 2024; Demestichas, Peppes and Alexakis, 2020; Ram, Rao, and Ranganathan, 2023). The implication is that some software and firmware accommodate first-time passwords and security keys for long durations. In other words, such systems do not prompt password change from the default. As such, the resultant cybersecurity threat is both system and human-enabled. On that note, regulations should direct manufacturers of smart farming firmware and software to have built-in prompts for password changes upon first login to allow users to set strong passwords. Additionally, password guides should be available to lead users to standardized strong phrases for passwords and security codes. The other contributor to increased cyber threat in Agriculture 4.0 and 5.0 was weak or absent mechanisms for access control of different farming devices (Buchanan and Murphy, 2022; Sontowski et al., 2020; Rahaman et al., 2024). The implication is that attempts by users to address cybersecurity threats are thwarted, where the technology distributor reserves the right to access and adjust the systems. The results show the need for policymakers to review the exclusive rights of smart farming equipment suppliers regarding the provision of opportunities for operators to gain panel control for enhancing cybersecurity protection. To this end, literature suggests that the manufacturer or distributor may have sole rights, which limits the ability to fight cyberattacks and increases threats to the sustainability of Agriculture 4.0 and 5.0.

Lack of physical security was another factor increasing cybersecurity risks in agriculture 4.0 and 5.0 (Abbasi, Martinez, and Ahmad, 2022; Zanella, da Silva, and Albini, 2020). The results showed that some devices were stolen and malicious software was installed. The findings imply that cybersecurity efforts in agriculture 4.0 and 5.0 are crippled by the exposed nature of projects, which readily avail devices to unauthorized persons. Additionally, the result shows that agriculture players have not invested in detailed physical security of their premises, equipment, and systems. In that respect, policymakers are blamed for not emphasizing the bare minimum requirements for securing agricultural premises to protect against potential cyberattack attempts through direct malware introduction. Meanwhile, the findings showed that increased cybersecurity risks in Agriculture 4.0 and 5.0 stemmed from the lack of regulations and cybersecurity policies governing the security of IoT devices used in smart farming (Barreto and Amaral, 2018; Demestichas, Peppes, and Alexakis, 2020). The implication is that the policy section for related cybersecurity measures is not polished. The trend suggests that the industry is relying on random standards, with no one held responsible for failed information protection. The consequence is laxity among technology users, leading to higher rates of cybersecurity attacks in agriculture 4.0 and 5.0. In that regard, future research outlining available regulations is warranted.

On the other hand, the study also addressed the consequences of cybersecurity threats in agriculture 4.0 and 5.0. The findings from the literature revealed that attacks on networks paralyzed communication between the connected devices and denied the rightful users the opportunities to utilize the resources (Shah et al., 2022; Caviglia et al., 2023). The implication is that cybersecurity threats can halt crucial firm activities by locking out communication portals. Such moments present serious downtimes, accompanied by losses in productivity. Generally, radio frequency jamming (RF) to deny communication between devices is meant to interrupt the operational flow in the farm by causing substantial command delays or possible breakdown of the entire smart farming system. For practice, trained personnel should be engaged to disable the network attacks and secure the systems before serious damage is caused. Besides inter-device communication interruption, jamming of network systems was also linked to preventing human access to work devices (Pirayesh and Zeng, 2022; Yazdinejad et al., 2021; Salameh et al., 2018). The literature indicated that network system attacks through radio frequency jamming can block the user interface to lock out human operators from keying commands. The implication is that cybersecurity threats render smart farming useless and may drive farm and processing managers to manual production. The results were similar to that of other studies, which have shown that cybersecurity breaches can cause damage to equipment and stalling of operations, which cumulatively lead to extensive financial losses to the company and damage to its reputation (Boeckl et al., 2019; Drape et al., 2021; Krishna & Murphy, 2017; Lima e al., 2021; Stephen et al., 2023). In this respect, cyber insurance has been fronted as a crucial strategy to deal with potential losses linked to cybersecurity attacks and ensure companies are supported to quickly recover from their difficulties. Moreover, future studies should consider quantifying the extent of damage caused by jamming device communication systems in agricultural settings. The current findings suggest possible extensive losses.

Furthermore, the results indicated that cyberattacks breach the confidentiality of digital agricultural systems when data gets into unauthorized hands (Yazdinejad et al., 2021; Alahmadi et al., 2022). The finding implies that cybersecurity attacks are not merely directed at causing system disruption but can involve data theft. In such cases, information marked private can be exposed to the public. The worst cases highlighted in literature are misuse of the stolen information for extortion or blackmail. Essentially, a relevant policy can protect the affected firms from legal implications if the threat is proven and addressed. Nevertheless, the damage shall have been done, making it necessary to have tight cybersecurity measures in place. The results also indicated that such data breaches may create legal problems for the affected agricultural organizations when the data owners opt for compensation (Jerhamre et al., 2022). The implication is that managers and agricultural investments are not completely safe during data attacks. On that note, a special observation was made that policy and regulation protecting agricultural organizations against related cybersecurity data breach lawsuits are not defined. As such, there is a need for policy improvement to limit the extent of responsibility for an organization in the event of cyber data theft. To this end, further studies are required to explore the available policies for other industries and how they can be applied to digital agricultural systems to promote Industry 4.0 and 5.0.

The results also showed that cybersecurity attacks in agriculture are associated with violations of the trust and integrity of the available systems (Yazdinejad et al., 2021; Koduru and Koduru, 2022). On that note, the implication is that the usage of digital systems in agriculture may drop with an increase in cybersecurity attack incidences. Essentially, potential users will avoid the systems to escape possible losses and delays experienced when the system is under attack. At the same time, customers and employees who value data privacy and confidentiality may refuse to subscribe to technological solutions to protect their information. The finding is similar to those of other researchers who noted that the social and financial costs of cyberattacks may discourage certain companies from transitioning to digital systems as they fear being spied on by hackers and losing sensitive information to competitors (Pechlivani et al., 2023; Vangala et al., 2023; Van Hilten and Wolfert, 2022; Zanasi et al., 2024). In this respect, it is noted that to boost trust in digitization programs, robust cybersecurity strategies should be developed, and awareness and training should be given to employees to enable them to understand how to mitigate any potential cyber-security risks. The findings suggest the need for a strong and elaborate data policy for agricultural smart systems to restore user confidence. Additionally, the systems should have cybersecurity protection update features to prevent perpetual attacks and breakdowns.

Finally, the results also pointed out that cybersecurity attacks in smart agriculture may lead to data loss (Amiri-Zarandi et al., 2022; Ahmadi, 2023). The implication is that attacks on data can take agricultural organizations back to scratch in terms of database management. Whenever data is lost, the organization must begin afresh with little information, which slows down essential processes such as paying suppliers, employees, and bills. The finding was aligned with the views of several authors, who explained that data loss following cyber-attacks could cause loss of intellectual property that gives a company its competitive advantage, cause damage to company's reputation, lead to additional costs related to settlement with hackers or rebuilding damaged software, and legal penalties by regulators (Al Asif et al. (2021; Alferidah and Jhanjhi, 2020; Axelrod et al., 2017; Studiawan et al., 2023; Van Der Linden et al., 2020). In this regard, it is realized that data loss affects not only the company but also other stakeholders invested in them. Also, important contacts are lost in the process, isolating the farm from essential networks. Further, the results suggest that cybersecurity attacks can lead to unbudgeted expenses for creating new databases. At times, debtor records may be lost or compromised, leading to losses. On that note, policymakers should consider compensation frameworks for affected agricultural firms. Most importantly, data backups are essential for all smart agriculture systems.

5.2 Cybersecurity Mitigation Measures

A review of the cybersecurity mitigation measures in the agricultural sector revealed several crucial points. A summary of the key points concerning cybersecurity measures was shown in Table 9.

Table 9Possible cybersecurity mitigation measures for agricultural smart systems

Context	**Cybersecurity Measures**	**Impact on Agricultural Systems**
Data	Strong passwords	Increase security level and reduce risk of illegal access to smart farming systems. Increases privacy, authenticity, and confidentiality
	Two-factor authentication	Keeps the data encrypted and reduces risk of unauthorized individuals accessing data on crop and livestock development as well as production data.
Software	Firmware update	Frequently update the smart farming system software to increase the level of security and reduce the risk of possible attacks.
	Encryption of drives	Encrypt drive to prevent access to critical smart farming software without authorization.

Network	Disable UPnP	Disable UPnP to avoid exposing the network to possible cyber attackers.
	Block unnecessary ports	Block vulnerable and unnecessary ports to ensure individuals cannot physically connect to the smart farming system without authorization.
Service	Account lockout	Account lockout system should be used to ensure only legitimate users use smart farming systems to reduce risk of compromise.
	Periodic assessment of devices	Smart farming systems should be periodically assessed using AI, and new vulnerabilities should be dealt with by upgrading.

The first point from studies such as Shafiq et al. (2020), Sudharsanan et al. (2024), and Yang et al. (2023) was that farmers using many technological devices should employ advanced technologies such as AI for improved detection of malware in IoT devices since they can flag suspicious activities which do not conform to user activity or which bypass security protocols. Moreover, using AI and IoT also allows the integration of data across many devices, including UAV, thereby improving the monitoring of agricultural systems in real-time and faster response to cyber security breaches (Kim et al., 2021). The findings implied that to encourage the uptake of AI/IoT systems in agriculture and reduce the risk of cybersecurity breaches, technology companies, farmers, and government agencies should collaborate to improve internet installation and support infrastructure for farmers, especially those in rural areas who may not access the services. The strategy is particularly important because successful cybersecurity mitigation can encourage more farmers to go digital by selling produce online, seeking online loans, and expanding their agricultural operations. The obtained findings were consistent with those of many researchers (Camacho, 2024; Chan et al., 2019; Ferrag et al., 2021; Kang, 2023; Sumathy et al., 2023; Zhao et al., 2024b), who also noted that AI could analyze data from different sources simultaneously and provide notifications for cybersecurity threats in real time thereby enabling faster response to any emerging threat. However, one policy implication of using AI in cybersecurity is that further analysis of the AI output should be done to verify them since AI is affected by ethical issues of discrimination and bias (Hofstetter et al., 2020; Holzinger et al., 2024; Kusyk et al., 2019; Liu and Murphy, 2020). AI operation heavily depends on the nature of data used in its training, and hence, poor quality data can reduce the effectiveness of its output. Therefore, one practical implication is that when using AI in smart agriculture, a large and diversified dataset should be employed to improve the accuracy of outputs.

The second finding was that cybersecurity threats can be mitigated by using blockchain and quantum computing measures to enhance the encryption of passwords and minimize issues of hacking. Several studies emphasized that quantum computing techniques improved the privacy and accuracy of smart grid systems due to faster processing power, which can ensure secure transmission of data between IoT devices while also ensuring better detection of any attacks (Abdel-latif et al., 2021; Alomari and Kumar, 2024). The results implied that cybersecurity mitigation can prevent identity theft issues, which can cause financial losses to farmers and threaten their farming activities. Besides, using quantum computing and blockchain strategies can prevent issues of supply chain disruption and delays in food distribution that are linked to cybersecurity breaches. The findings were aligned with the views of several authors (Etemadi et al., 2020; Padhy et al., 2023; Rangan et al., 2022; Torky and Hassanein, 2020) who explained that the use of blockchain and quantum computing enhanced security, safety and transparency of data systems thereby reducing food supply chain risks. The result implies that apart from improving security, cybersecurity technology can enhance transparency, which enhances trust among stakeholders in the agriculture supply chain, leading to improved collaboration and outcomes. Therefore, one policy implication of the finding in cybersecurity is that blockchain and quantum computing technologies should be fronted as crucial standards for compliance for farmers seeking to develop smart systems integrating payment infrastructure. The strategy can ensure that even where farmers lack knowledge of cybersecurity, they are guided on best practices to ensure safety in payments, which reduces the risk of financial losses through hacking.

The third finding was that cybersecurity threats can be managed by creating awareness and training programs to avoid human errors, which can lead to cybersecurity breaches (Al-Emran and Deveci, 2024; Chaudhary et al., 2023). The programs should target employees of agricultural companies and individual farmers with smart agricultural systems. Local or national government agencies can create training programs and make them available free of charge to all farmers to foster a culture of cybersecurity consciousness. The findings resonated with those of many researchers, who have pinpointed that training on cybersecurity enables safe browsing practices, improved password creating and account security, better data protection practices, and increased phishing awareness and avoidance (Majumdar et al., 2023; Manninen, 2018; Nikander et al., 2020; Riaz et al., 2022; Shafik et al., 2023). In agreement with the finding, other researchers have indicated that there is a need for companies to clarify personal liability principles where cyberattacks that occur due to employees' negligence and inappropriate handling of data leads to them being held accountable and penalized (Aliebrahimi and Miller, 2023; Carneiro et al., 2021; Kuzlu et al., 2021; Rudo and Zheng, 2020; Shaaban et al., 2022). The strategy can ensure that more employees understand the magnitude and seriousness of cybersecurity measures and take a proactive approach to learning about mitigation measures and response to any suspicious online activity. Therefore, one practical implication of the results is that training programs should target the different areas that align with standards, guidelines, and policies on cybersecurity management to ensure individuals involved are informed about the best practices in the industry.

The fourth result involved following regulatory standards and guidelines in cybersecurity to ensure effective monitoring and evaluation of risk and enable faster response and recovery in the case of a cybersecurity breach (Khan et al., 2022; Toussaint et al., 2024). The policy implication of the result is that governments should develop practical standards and guidelines that farmers and other agricultural stakeholders can use to enhance their cybersecurity practices and ensure uninterrupted smart farming systems. The result was consistent with those of many researchers who have noted that a lack of robust regulatory framework can affect compliance and response strategies to cybersecurity risk (Khan et al., 2024; Lone et al., 2023; Prasetio and Nurliyana, 2023; Tsao et al., 2022; Vatn, 2023). Of importance to note is that in creating laws and regulations, the emphasis should be on avoiding those that are costly, complicated, and difficult to implement, which discourage many people from following them (Chiara et al., 2024; Eashwar and Chawla, 2021; Furfaro et al., 2017; Mitra et al., 2022). Besides, since the use of cybersecurity varies based on the sector, there is no one-size-fits-all regulation, and efforts should be made to specify regulatory compliance based on the unique needs of companies in various industries. The view has been emphasized by other studies, which have shown that creating standards and regulations aligned with specific company operations as well as customizing cybersecurity software improves monitoring and engagement of employees in cybersecurity (Berguiga et al., 2023; Dayıoğlu and Turker, 2021; Demircioglu et al., 2023; Guruswamy et al., 2022; Hadi et al., 2024). The strategy can ensure that stakeholders in the agricultural sector obtain more benefits from the regulation in terms of ease of interpretation and implementation in their normal operations.

When implementing cybersecurity measures, it was noted that there are certain issues that need to be addressed to ensure effective outcomes, including technical challenges, legal challenges, and negative attitudes toward cybersecurity (Araújo et al., 2024; Raval et al., 202; Wurzenberger et al., 2024). The result implied that while implementing cybersecurity mitigation measures, companies should strive to reduce the vulnerability of their systems by checking potential weaknesses in the security framework and addressing them before they happen. The technical challenges, such as the inability of employees to identify configuration errors or scan for threats, have also been highlighted by other researchers who have emphasized employees training in cybersecurity-related areas such as network security control, coding, and encryption, understanding of operating systems, and cloud systems management (Lezoche et al., 2020; Maraveas et al., 2022; Roopak et al., 2019; Strecker et al., 2021; Tlili et al., 2024). In this regard, the policy implication of the finding is that regular training programs should be developed by agricultural firms to enhance the technical skills of their employees in cybersecurity management. Meanwhile, the result of legal challenges implied that companies should develop internal regulations and standards to ensure employees understand how to manage data and control access to smart systems, thereby complying with cybersecurity measures. The result resonates with those of other studies, which have revealed that although national and global standards may be developed on cybersecurity, it is only at the company management level that effective strategies can be developed to ensure appropriate organizational culture and employee behavior to ensure compliance with the cybersecurity regulations (Caviglia et al., 2024; Freyhof et al., 2022; Senturk et al., 2023; Vandezande, 2024). In this regard, the findings suggest the need for company managers to take initiatives to allocate adequate resources to train employees and acquire cybersecurity software to not only deal with potential threats but also vulnerabilities in smart systems.

5.3 Future Research Directions

One recommendation for future research is that more studies should be done on the financial impact of using IoT in smart farming. The analysis conducted showed that using cybersecurity technologies can enable improved efficiency and costs in agriculture as most systems, such as irrigation, weather, and logistics, are automated, secured, and integrated.

However, examining the extent of cost-benefit when using cybersecurity technology can be used as a basis to motivate more farmers to adopt AI/IoT systems in agriculture. The second recommendation for future research is that more studies should be done on policies that governments should create to promote cybersecurity and technology in agriculture. Although smart farming can improve the efficiency of resource use, such as water in irrigation, there are challenges linked to cybersecurity threats that should be addressed when adopting the system. Therefore, examining global and national policies on cybersecurity management can help to understand how farmers can be supported through private-public partnerships when engaging in smart agriculture. The third recommendation for future research is that more studies are needed on how to manage AI limitations, such as bias and discrimination of certain demographics, which hinder its widespread adoption in cybersecurity management. Conducting such a study can improve insights into the strategies to use to ethically use AI to promote cybersecurity. Moreover, future studies are needed on how to create global regulatory requirements and standards on cybersecurity to promote critical issues such as human rights and data privacy online. The fourth recommendation for future research is that more analysis is needed concerning AI consciousness, where AI algorithms develop self-awareness and can use the knowledge gained from training to solve problems in unrelated fields for which they are not trained. Although this feature of AI is useful in improving its detection and monitoring of potential online threats, it also poses the challenge of the unpredictable behavior of AI. In this respect, future analysis on the topic can improve insight into how agricultural companies can safely deploy AI in cybersecurity without compromising their systems.

5.4 Recommendations

One recommendation for practice based on the study is that cybersecurity training programs targeting farmers should be developed to improve their knowledge of data management and reduce the risk of cybersecurity breaches. In the training program, the main focus should be on unintentional threats such as data sharing and weak passwords, which can be easily found and used by other people to illegally access agricultural smart systems. The training of farmers should aim at positively shaping their behavior and attitudes towards cybersecurity management and ensure they take a proactive approach in monitoring, detecting, and responding to any suspicious malware. The second recommendation for practice is that farmers and agricultural companies implement a multi-layered security strategy where they use AI and IoT technologies to improve the integration of systems and quick detection of malicious attacks, as well as quantum cryptography technology to increase data encryption. The multilayered approach can enhance the protection of sensitive data and transactions while also ensuring better recovery of data in case of breach since data is stored on many devices. The underlying idea of a multilayered cybersecurity approach is recognizing that threats to digital systems emerge from various sources, and there is a need for diverse methods to tackle each potential threat. The third recommendation for practice in cybersecurity targeting farmers and the broader agricultural sector is that more support and digital infrastructure should be set up in rural areas to ensure that farmers who transition to digital systems can easily get help when faced with challenges of hacking and data breach. The strategy can be in the form of Starlink, which is the satellite internet provider that ensures even individuals in remote areas can enjoy high-speed internet connections and manage their digital systems. Providing more digital support to farmers can not only encourage them to digitize their agricultural systems but also implement cybersecurity measures to protect their smart systems. The fourth recommendation for practice is that agricultural companies should seek cyber insurance so that the liability associated with cyber-attacks, such as loss of customers and finances, can be managed by a secondary entity. The strategy is realized to be critical, especially in cases where employees have little cybersecurity education and show reluctance to take a proactive approach to learning about mitigation measures.

6.0 Conclusion

The main aim of this study was to examine the cybersecurity threats that affect Agriculture 4.0 and 5.0 and the potential strategies for mitigating the problems. The research methodology involved a secondary method in which a narrative review design was considered, where previous studies done on cybersecurity issues in agriculture were sampled and analyzed. Concerning cybersecurity threats, the review revealed that there are several risks that increase the risk of IoT device data breaches in agriculture. The main risks were identified to include obsolete unpatched software and wireless technologies, which can easily be hacked, and lack of strong authentication criteria to prevent illegal access to the technology systems. Moreover, the findings revealed that other cybersecurity risks included a lack of comprehensive policies on cybersecurity to guide farmers on the appropriate use of IoT devices to prevent data breaches and failure to update cybersecurity software. Meanwhile, the cybersecurity threats that were likely to affect smart systems in agriculture include attacks on data to steal customer data and sensitive company information, attacks on networks and equipment such as denial of service to disrupt the various agricultural operations, and attacks on software through malware injection or during software updates to change intended agricultural operations. Due to the many cybersecurity threats that affect agricultural technologies, it was noted that a diverse approach is required when mitigating the challenges.

The objective regarding strategies to mitigate cybersecurity risks in agriculture was also addressed. In particular, the findings revealed the strategies that can be employed to prevent or manage cybersecurity threats, including creating awareness and training programs that help farmers develop relevant skills to monitor, identify, and manage any cybersecurity threats. Secondly, the review showed that creating a robust policy framework on cybersecurity can help farmers understand the main issues to consider in implementing smart systems to enhance security in terms of detecting, responding, and recovering from any data breach. In addition, the result showed that utilizing AI algorithms in IoT devices can enhance security by enabling efficient and accurate analysis of large datasets to identify patterns of malware and phishing attacks. The findings also showed that using quantum computing techniques can improve the efficiency of identifying malware and responding to it since quantum computing presents a higher processing speed than conventional techniques.

The other crucial point from the analysis was that several challenges may be experienced when implementing cybersecurity mitigation measures. Firstly, a lack of technical expertise may hinder employees from taking a proactive approach to data security since they can fail to interpret warnings of suspicious cyber-attacks, which can lead to data breaches. Secondly, the review showed that work overload can cause stress on employees and hinder them from complying with cybersecurity standards when managing online data. Lastly, the findings showed that legal issues related to data privacy may restrict the adoption of AI technology, especially where its use in agricultural systems is unclear.

References

Abbasi, R., Martinez, P. and Ahmad, R., 2022. The digitization of agricultural industry–a systematic literature review on agriculture 4.0. *Smart Agricultural Technology*, **2**, 100042.

Abdelfatah, R. I., 2024. Robust biometric identity authentication scheme using quantum voice encryption and quantum secure direct communications for cybersecurity. *Journal of King Saud University-Computer and Information Sciences*, **36**(5), 102062.

Abdel-latif, A. A., Abd-El-Atty, B., Mehmood, I., Muhammad, K., Venegas-Andraca, S. E. and Peng, J., 2021. Quantum-inspired blockchain-based cybersecurity: securing smart edge utilities in IoT-based smart cities. *Information Processing & Management*, **58**(4), p.102549.

Adil, M., Song, H., Mastorakis, S., Abulkasim, H., Farouk, A. and Jin, Z., 2023. UAV-assisted IoT applications, cybersecurity threats, AI-enabled solutions, open challenges with future research directions. *IEEE Transactions on Intelligent Vehicles*, **9**(4), pp.1-21.

Ahmad, M. W., Akram, M. U., Mohsan, M. M., Saghar, K., Ahmad, R. and Butt, W. H., 2024. Transformer-based sensor failure prediction and classification framework for UAVs. *Expert Systems with Applications*, **248**, 123415.

Ahmadi, S., 2023. *A systematic literature review: security threats and countermeasure in smart farming*. University of Illinois at Chicago. doi:https://doi.org/10.36227/techrxiv.22029974.

Ahmed, I., Hossain, N. U. I., Fazio, S. A., Lezzi, M. and Islam, M. S., 2024. A decision support model for assessing and prioritization of industry 5.0 cybersecurity challenges. *Sustainable Manufacturing and Service Economics*, **3**, 100018.

Alahmadi, A. N., Rehman, S. U., Alhazmi, H. S., Glynn, D. G., Shoaib, H. and Solé, P., 2022. Cyber-security threats and side-channel attacks for digital agriculture. *Sensors*, **22**(9), pp.1-14.

Al Asif, M. R., Hasan, K. F., Islam, M. Z. and Khondoker, R., 2021. STRIDE-based cyber security threat modeling for IoT-enabled precision agriculture systems. In *2021 3rd International Conference on Sustainable Technologies for Industry 4.0 (STI)*. Piscataway: IEEE, pp.1-6.

AlDaajeh, S. and Alrabaee, S., 2024. Strategic cybersecurity. *Computers & Security*, **141**, 103845.

Al-Emran, M. and Deveci, M., 2024. Unlocking the potential of cybersecurity behavior in the metaverse: overview, opportunities, challenges, and future research agendas. *Technology in Society*, **77**, pp.102498–102498. doi:https://doi.org/10.1016/j.techsoc.2024.102498.

Ali, I.A., Bukhari, W.A., Adnan, M., Kashif, M.I., Danish, A. and Sikander, A., 2024. Security and privacy in IoT-based smart farming: a review. *Multimedia Tools and Applications*, pp.1-8. doi:https://doi.org/10.1007/s11042-024-19653-3.

Aliebrahimi, S. and Miller, E. E., 2023. Effects of cybersecurity knowledge and situation awareness during cyberattacks on autonomous vehicles. *Transportation Research Part F: Traffic Psychology and Behavior*, **96**, pp.82-91.

Alferidah, D. K. and Jhanjhi, N. Z., 2020. Cybersecurity impact over bigdata and IoT growth. In: *2020 International Conference on Computational Intelligence (ICCI)*. Piscataway: IEEE, pp.103-108

Alomari, A. and Kumar, S. A., 2024. Securing IoT systems in a post-quantum environment: vulnerabilities, attacks, and possible solutions. *Internet of Things*, **25**, 101132.

Aloqaily, M., Kanhere, S., Bellavista, P. and Nogueira, M., 2022. Special issue on cybersecurity management in the era of AI. *Journal of Network and Systems Management*, **30**(3), pp.1-7.

Alqudhaibi, A., Krishna, A., Jagtap, S., Williams, N., Afy-Shararah, M. and Salonitis, K., 2024. Cybersecurity 4.0: safeguarding trust and production in the digital food industry era. *Discover Food*, **4**(1), pp.1-18.

Alsamhi, S. H., Afghah, F., Sahal, R., Hawbani, A., Al-qaness, M. A., Lee, B. and Guizani, M., 2021. Green internet of things using UAVs in B5G networks: a review of applications and strategies. *Ad Hoc Networks*, **117**, 102505.

Alshaikh, O., Parkinson, S. and Khan, S., 2024. Exploring perceptions of decision-makers and specialists in defensive machine learning cybersecurity applications: the need for a standardised approach. *Computers & Security*, **139**, 103694.

Altulaihan, E., Almaiah, M. A. and Aljughaiman, A., 2022. Cybersecurity threats, countermeasures and mitigation techniques on the IoT: future research directions. *Electronics*, **11**(20), pp.1-41.

Amiri-Zarandi, M., Dara, R.A., Duncan, E. and Fraser, E.D.G., 2022. Big data privacy in smart farming: a review. *Sustainability*, **14**(15), pp.1-18. doi:https://doi.org/10.3390/su14159120.

Araújo, S. O., Peres, R. S., Barata, J., Lidon, F. and Ramalho, J. C., 2021. Characterising the agriculture 4.0 landscape—emerging trends, challenges and opportunities. *Agronomy*, **11**(4), pp.1-37.

Arce, D. G., 2020. Cybersecurity and platform competition in the cloud. *Computers & Security*, **93**, 101774.

Argillander, J., Alarcón, A., Bao, C., Kuang, C., Lima, G., Gao, F. and Xavier, G.B., 2023. Quantum random number generation based on a perovskite light emitting diode.

Communications Physics, [online] **6**(1), pp.1–7. doi:https://doi.org/10.1038/s42005-023-01280-3.

Aurangzeb, M., Wang, Y., Iqbal, S., Naveed, A., Ahmed, Z., Alenezi, M. and Shouran, M., 2024. Enhancing cybersecurity in smart grids: deep black box adversarial attacks and quantum voting ensemble models for blockchain privacy-preserving storage. *Energy Reports*, **11**, pp.2493-2515.

Awan, K.A., Ud Din, I., Almogren, A. and Almajed, H., 2020. AgriTrust—a trust management approach for smart agriculture in cloud-based internet of agriculture things. *Sensors*, **20**(21), pp.1-21. doi:https://doi.org/10.3390/s20216174.

Axelrod, C. W., 2017. Cybersecurity in the age of autonomous vehicles, intelligent traffic controls and pervasive transportation networks. In *2017 IEEE Long Island Systems, Applications and Technology Conference (LISAT)*. Piscataway: IEEE, pp.1-6.

Baethge, C., Goldbeck-Wood, S., & Mertens, S., 2019. SANRA—a scale for the quality assessment of narrative review articles. *Research Integrity and Peer Review*, **4**, pp.1-7.

Bahassi, H., Edddermoug, N., Mansour, A. and Mohamed, A., 2022. Toward an exhaustive review on machine learning for cybersecurity. *Procedia Computer Science*, **203**, pp.583-587.

Balaji, S. R. A., Rao, S. P. and Ranganathan, P., 2023. Cybersecurity challenges and solutions in IoT-based precision farming systems. In: *2023 IEEE 14th Annual Ubiquitous Computing, Electronics & Mobile Communication Conference (UEMCON)*. Piscataway: IEEE, pp.237-246.

Baltuttis, D., Teubner, T. and Adam, M. T., 2024. A typology of cybersecurity behavior among knowledge workers. *Computers & Security*, **140**, 103741.

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

Basheer, A., 2022. The art and science of writing narrative reviews. *International Journal of Advanced Medical and Health Research*, [online] **9**(2), pp.124-126.

Bashir, N., Boudjit, S., Dauphin, G. and Zeadally, S., 2023. An obstacle avoidance approach for UAV path planning. *Simulation Modelling Practice and Theory,* **129**, 102815.

Bell, E., Bryman, A. and Harley, B., 2022. *Business research methods*. Oxford: Oxford University Press.

Benmalek, M., 2024. Ransomware on cyber-physical systems: taxonomies, case studies, security gaps, and open challenges. *Internet of Things and Cyber-Physical Systems,* **4**, pp.186-202.

Berguiga, A., Harchay, A., Massaoudi, A., Ayed, M. B. and Belmabrouk, H., 2023. GMLP-IDS: a novel deep learning-based intrusion detection system for smart agriculture. *Computers, Materials & Continua*, **77**(1), pp.379-401.

Bissadu, K. D., Sonko, S. and Hossain, G., 2024. Society 5.0 enabled agriculture: drivers, enabling technologies, architectures, opportunities, and challenges. *Information Processing in Agriculture*, pp.1-13.

Bui, H. T., Aboutorab, H., Mahboubi, A., Gao, Y., Sultan, N. H., Chauhan, A. and Yan, S., 2024. Agriculture 4.0 and beyond: evaluating cyber threat intelligence sources and techniques in smart farming ecosystems. *Computers & Security*, **140**, 103754.

Boeckl, K., Boeckl, K., Fagan, M., Fisher, W., Lefkovitz, N., Megas, K. N. and Scarfone, K., 2019. *Considerations for managing Internet of Things (IoT) cybersecurity and privacy risks*. Gaithersburg: US Department of Commerce, National Institute of Standards and Technology.

Braun, V. and Clarke, V., 2023. Is thematic analysis used well in health psychology? A critical review of published research, with recommendations for quality practice and reporting. *Health Psychology Review*, **17**(4), pp.695-718.

Buchanan, K. and Murphy, T., 2022. *What the John Deere tractor hack reveals about cyber threats to food supply*. [online] 23 Aug. Available at: https://www.abc.net.au/news/rural/2022-08-24/tractor-hack-reveals-food-supply-vulnerable/101360062. (Accessed 15th July 2024)

Camacho, N. G., 2024. The role of AI in cybersecurity: addressing threats in the digital age. *Journal of Artificial Intelligence General science (JAIGS) ISSN: 3006-4023*, **3**(1), pp.143-154.

Campbell, K. A., Orr, E., Durepos, P., Nguyen, L., Li, L., Whitmore, C. and Jack, S. M., 2021. Reflexive thematic analysis for applied qualitative health research. *The Qualitative Report*, **26**(6), pp.2011-2028.

Carneiro, R., Duncan, S., Ramsey, F., Seyyedhasani, H. and Murch, R., 2021. *Cyber-attacks in agriculture: protecting your farm and small business with cyberbiosecurity.* Virginia: VCE Publications.

Caviglia, R., Gaggero, G., Portomauro, G., Patrone, F. and Marchese, M., 2023. An SDR-based cybersecurity verification framework for smart agricultural machines. *IEEE Access*, **11**, pp.54210-54220.

Caviglia, R., Davoli, F., Fausto, A., Gaggero, G., Marchese, M., Moheddine, A. and Portomauro, G., 2024. Vulnerability assessment of industrial and agricultural control systems within the IoT framework. In Obaidat, M., Nayak, P., and Ray, N. (Eds), *Intelligent computing on IoT 2.0, big data analytics, and block chain technology*. New York: Chapman and Hall/CRC, pp.350-371.

Chan, L., Morgan, I., Simon, H., Alshabanat, F., Ober, D., Gentry, J. and Cao, R., 2019. Survey of AI in cybersecurity for information technology management. In: *2019 IEEE Technology & Engineering Management Conference (TEMSCON)*. Piscataway: IEEE, pp.1-8.

Channon, M. and Marson, J., 2021. The liability for cybersecurity breaches of connected and autonomous vehicles. *Computer Law & Security Review*, **43**, p.105628.

Chatfield, A. T. and Reddick, C. G., 2019. A framework for Internet of Things-enabled smart government: a case of IoT cybersecurity policies and use cases in US federal government. *Government Information Quarterly*, **36**(2), pp.346-357.

Chaudhary, S., Gkioulos, V. and Katsikas, S., 2023. A quest for research and knowledge gaps in cybersecurity awareness for small and medium-sized enterprises. *Computer Science Review*, **50**, p.100592.

Chiara, P. G., 2024. Towards a right to cybersecurity in EU law? The challenges ahead. *Computer Law & Security Review*, **53**, p.105961.

Choo, K. K. R., Bishop, M., Glisson, W. and Nance, K., 2018. Internet-and cloud-of-things cybersecurity research challenges and advances. *Computers & Security*, **74**, pp.275-276.

Choo, K. K. R., Gai, K., Chiaraviglio, L. and Yang, Q., 2021. A multidisciplinary approach to Internet of Things (IoT) cybersecurity and risk management. *Computers & Security*, **102**, p.102136.

Chundhoo, V., Chattopadhyay, G., Karmakar, G. and Appuhamillage, G. K., 2021. Cybersecurity risks in meat processing plant and impacts on total productive maintenance. In: *2021 International Conference on Maintenance and Intelligent Asset Management (ICMIAM)*. Piscataway: IEEE, pp.1-5.

Condolo, C., Romero, S. and Ticona, W., 2024, January. Implementation of an Information Security Management System to Improve the IT Security of an Agricultural Tool Manufacturing Company. In *2024 14th International Conference on Cloud Computing, Data Science & Engineering (Confluence)* (pp. 177-183). IEEE.

Dahlman, E. and Lagrelius, K., 2019. *A game of drones: cyber security in UAVs*. Bachelor Thesis, KTH Royal Institute of Technology.

Daim, T., Lai, K. K., Yalcin, H., Alsoubie, F. and Kumar, V., 2020. Forecasting technological positioning through technology knowledge redundancy: patent citation analysis of IoT, cybersecurity, and Blockchain. *Technological Forecasting and Social Change*, **161**, p.120329.

Da Silveira, F., Lermen, F.H. and Amaral, F.G., 2021. An overview of agriculture 4.0 development: systematic review of descriptions, technologies, barriers, advantages, and disadvantages. *Computers and Electronics in Agriculture*, **189**, p.106405.

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

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

Demircioglu, P., Bogrekci, I., Durakbasa, M. N. and Bauer, J., 2023. Autonomation, automation, AI, and industry-agriculture 5.0 in sustainable agro-ecological food production. In: *The International Symposium for Production Research*. Cham: Springer Nature Switzerland, pp.545-556.

Demiris, G., Oliver, D.P. and Washington, K.T., 2019. Defining and analyzing the problem. In: Demiris, G., Oliver, D., and Washington, K. (Eds), *Behavioral intervention research in hospice and palliative care*. Amsterdam: Elsevier Science, pp.27–39.

Dhagarra, D., Goswami, M. and Kumar, G., 2020. Impact of trust and privacy concerns on technology acceptance in healthcare: an Indian perspective. *International Journal of Medical Informatics*, [online] **141**, p.104164. Available at: https://www.sciencedirect.com/science/article/pii/S1386505620302276#bib0390.

Drape, T., Magerkorth, N., Sen, A., Simpson, J., Seibel, M., Murch, R. S. and Duncan, S. E., 2021. Assessing the role of cyberbiosecurity in agriculture: a case study. *Frontiers in Bioengineering and Biotechnology*, **9**, p.737927.

Duncan, S. E., Reinhard, R., Williams, R. C., Ramsey, F., Thomason, W., Lee, K. and Murch, R., 2019. Cyberbiosecurity: a new perspective on protecting US food and agricultural system. *Frontiers in Bioengineering and Biotechnology*, **7**, p.63.

Eashwar, S. and Chawla, P., 2021. Evolution of Agritech business 4.0–architecture and future research directions. *IOP Conference Series: Earth and Environmental Science,* **775**(1), p. 012011.

El Alaoui, M., Amraoui, K. E., Masmoudi, L., Ettouhami, A. and Rouchdi, M., 2024. Unleashing the potential of IoT, artificial intelligence, and UAVs in contemporary agriculture: a comprehensive review. *Journal of Terramechanics*, **115**, p.100986.

Etemadi, N., Borbon, Y. G. and Strozzi, F., 2020. Blockchain technology for cybersecurity applications in the food supply chain: A systematic literature review. *Proceedings of the XXIV Summer School "Francesco Turco"—Industrial Systems Engineering, Bergamo, Italy*, pp.9-11.

Familoni, B. T., 2024. Cybersecurity challenges in the age of AI: theoretical approaches and practical solutions. *Computer Science & IT Research Journal*, **5**(3), pp.703-724.

Fatoki, J. G., Shen, Z. and Mora-Monge, C. A., 2024. Optimism amid risk: how non-IT employees' beliefs affect cybersecurity behavior. *Computers & Security*, **141**, p.103812.

Fernandez, C. M., Alves, J., Gaspar, P. D. and Lima, T. M., 2021. Fostering awareness on environmentally sustainable technological solutions for the post-harvest food supply chain. *Processes*, **9**(9), p.1611.

Ferrag, M. A., Shu, L., Djallel, H. and Choo, K. K. R., 2021. Deep learning-based intrusion detection for distributed denial of service attack in agriculture 4.0. *Electronics*, **10**(11), p.1257.

Fosch-Villaronga, E. and Mahler, T., 2021. Cybersecurity, safety and robots: strengthening the link between cybersecurity and safety in the context of care robots. *Computer Law & Security Review*, **41**, p.105528. doi:https://doi.org/10.1016/j.clsr.2021.105528.

Freyhof, M., Grispos, G., Pitla, S. and Stolle, C., 2022. Towards a cybersecurity testbed for agricultural vehicles and environments. In: *Proceedings of the 17th Midwest Association for Information Systems Conference, Omaha, Nebraska.* Omaha: MAIS.

Friha, O., Ferrag, M.A., Maglaras, L. and Shu, L., 2022. Digital agriculture security: aspects, threats, mitigation strategies, and future trends. *IEEE Internet of Things Magazine*, **5**(3), pp.82-90.

Furfaro, A., Argento, L., Parise, A. and Piccolo, A., 2017. Using virtual environments for the assessment of cybersecurity issues in IoT scenarios. *Simulation Modelling Practice and Theory*, **73**, pp.43-54.

Geil, A., Sagers, G., Spaulding, A. D. and Wolf, J. R., 2018. Cyber security on the farm: an assessment of cyber security practices in the United States agriculture industry. *International Food and Agribusiness Management Review*, **21**(3), pp.317-334.

Ghobadpour, A., Monsalve, G., Cardenas, A. and Mousazadeh, H., 2022. Off-road electric vehicles and autonomous robots in agricultural sector: trends, challenges, and opportunities. *Vehicles*, **4**(3), pp.843-864.

Gokool, S., Mahomed, M., Kunz, R., Clulow, A., Sibanda, M., Naiken, V., Chetty, K. and Mabhaudhi, T., 2023. Crop monitoring in smallholder farms using unmanned aerial vehicles to facilitate precision agriculture practices: A scoping review and bibliometric analysis. *Sustainability*, **15**(4), p.3557.

Gupta, M., Abdelsalam, M., Khorsandroo, S. and Mittal, S., 2020. Security and privacy in smart farming: challenges and opportunities. *IEEE Access*, **8**, pp.34564-34584.

Guruswamy, S., Pojić, M., Subramanian, J., Mastilović, J., Sarang, S., Subbanagounder, A. and Jeoti, V., 2022. Toward better food security using concepts from industry 5.0. *Sensors*, **22**(21), p.8377.

Hadi, H. J., Cao, Y., Li, S., Xu, L., Hu, Y. and Li, M., 2024. Real-time fusion multi-tier DNN-based collaborative IDPS with complementary features for secure UAV-enabled 6G networks. *Expert Systems with Applications*, **252**, p.124215.

Hafeez, G., Wadud, Z., Khan, I.U., Khan, I., Shafiq, Z., Usman, M. and Khan, M.U.A., 2020. Efficient energy management of IoT-enabled smart homes under price-based demand response program in smart grid. *Sensors*, **20**(11), p.3155.

Haloui, D., Oufaska, K., Oudani, M. and El Yassini, K., 2024. Bridging industry 5.0 and agriculture 5.0: historical perspectives, opportunities, and future perspectives. *Sustainability*, **16**(9), pp.3507–3507.

Hartanto, R., Arkeman, Y., Hermadi, I., Sjaf, S. and Kleinke, M., 2019. Intelligent unmanned aerial vehicle for agriculture and agroindustry. *IOP Conference Series: Earth and Environmental Science*, **335**(1), p.012001.

Hasan, M. K., Abdulkadir, R. A., Islam, S., Gadekallu, T. R. and Safie, N., 2024. A review on machine learning techniques for secured cyber-physical systems in smart grid networks. *Energy Reports*, **11**, pp.1268-1290.

Hofstetter, M., Riedl, R., Gees, T., Koumpis, A., & Schaberreiter, T., 2020. Applications of AI in cybersecurity. In *2020 Second International Conference on Transdisciplinary AI (TransAI)*. Piscataway: IEEE, pp.138-141.

Holzinger, A., Fister Jr, I., Fister, I., Kaul, H. P. and Asseng, S., 2024. Human-centered AI in smart farming: towards Agriculture 5.0. *IEEE Access*, **12**, pp.62199-62214.

Hung, P.C.K. and Cheng, V.S.Y., 2009. *Privacy*. London: Springer.

ISO, 2024. *ISO/IEC 27001:2022.* Available: https://www.iso.org/obp/ui/en/#iso:std:iso-iec:27001:ed-3:v1:en

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

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

Jin, T. and Han, X., 2024. Robotic arms in precision agriculture: a comprehensive review of the technologies, applications, challenges, and future prospects. *Computers and Electronics in Agriculture,* **221**, p.108938.

Kang, Y., 2023. Development of large-scale farming based on explainable machine learning for a sustainable rural economy: the case of cyber risk analysis to prevent costly data breaches. *Applied Artificial Intelligence*, **37**(1), p.2223862.

Kapoor, S. K., 2024. Addressing cybersecurity and privacy concerns in agricultural IoT systems and data-sharing practices for improved security. *African Journal of Biological Science,* **6**(9), pp.907-913.

Kaur, J., Hazrati Fard, S.M., Amiri-Zarandi, M. and Dara, R., 2022. Protecting farmers' data privacy and confidentiality: recommendations and considerations. *Frontiers in Sustainable Food Systems*, **6**, pp.1-9. doi:https://doi.org/10.3389/fsufs.2022.903230.

Kavallieratos, G. and Katsikas, S., 2023. An exploratory analysis of the last frontier: a systematic literature review of cybersecurity in space. *International Journal of Critical Infrastructure Protection*, **43**, p.100640.

Khan, R., Kumar, P., Jayakody, D. N. K. and Liyanage, M., 2019. A survey on security and privacy of 5G technologies: potential solutions, recent advancements, and future directions. *IEEE Communications Surveys & Tutorials*, **22**(1), pp.196-248.

Khan, S. K., Shiwakoti, N. and Stasinopoulos, P., 2022. A conceptual system dynamics model for cybersecurity assessment of connected and autonomous vehicles. *Accident Analysis & Prevention*, **165**, p.106515.

Khan, S. K., Shiwakoti, N., Stasinopoulos, P., Chen, Y. and Warren, M., 2024. Exploratory factor analysis for cybersecurity regulation and consumer data in autonomous vehicle acceptance: insights from four OECD countries. *Transportation Research Interdisciplinary Perspectives*, **25**, p.101084.

Kim, B. J. and Kim, M. J., 2024. The influence of work overload on cybersecurity behavior: a moderated mediation model of psychological contract breach, burnout, and self-efficacy in AI learning such as ChatGPT. *Technology in Society*, **77**, p.102543.

Kim, K., Kim, J. S., Jeong, S., Park, J. H. and Kim, H. K., 2021. Cybersecurity for autonomous vehicles: review of attacks and defense. *Computers & Security*, **103**, p.102150.

Klerkx, L., Jakku, E. and Labarthe, P., 2019. A review of social science on digital agriculture, smart farming and agriculture 4.0: new contributions and a future research agenda. *NJAS-Wageningen Journal of Life Sciences*, **90**, p.100315.

Koduru, T. and Koduru, N. P., 2022. An overview of vulnerabilities in smart farming systems. *Journal of Student Research*, **11**(1), pp.1-14.

Krishna, C. L. and Murphy, R. R., 2017. A review on cybersecurity vulnerabilities for unmanned aerial vehicles. In: *2017 IEEE International Symposium On Safety, Security and Rescue Robotics (SSRR)*. Piscataway: IEEE, pp.194-199.

Kshetri, N., 2017. Blockchain's roles in strengthening cybersecurity and protecting privacy. *Telecommunications Policy*, **41**(10), pp.1027-1038.

Kulkarni, A., Wang, Y., Gopinath, M., Sobien, D., Rahman, A. and Batarseh, F. A., 2024. A review of cybersecurity incidents in the food and agriculture sector. *arXiv preprint arXiv:2403.08036*.

Kusyk, J., Uyar, M. U., Ma, K., Plishka, J., Bertoli, G. and Boksiner, J., 2019. AI and game theory based autonomous UAV swarm for cybersecurity. In: *MILCOM 2019-2019 IEEE Military Communications Conference (MILCOM)*. Piscataway: IEEE, pp.1-6.

Kuzlu, M., Fair, C. and Guler, O., 2021. Role of artificial intelligence in the Internet of Things (IoT) cybersecurity. *Discover Internet of things*, **1**(1), p.7.

Lee, I., 2020. Internet of Things (IoT) cybersecurity: Literature review and IoT cyber risk management. *Future Internet*, **12**(9), p.157.

Lezoche, M., Hernandez, J. E., Díaz, M. D. M. E. A., Panetto, H. and Kacprzyk, J., 2020. Agri-food 4.0: a survey of the supply chains and technologies for the future agriculture. *Computers in Industry*, **117**, p.103187.

Li, X., Xiao, P., Tang, D., Li, X., Wang, Q. and Chen, D., 2024. UAVs-assisted QoS guarantee scheme of IoT applications for reliable mobile edge computing. *Computer Communications*, **223**, pp.55-67.

Li, J. H., 2018. Cyber security meets artificial intelligence: a survey. *Frontiers of Information Technology & Electronic Engineering*, **19**(12), pp.1462-1474.

Lima, G. C., Figueiredo, F. L., Barbieri, A. E. and Seki, J., 2021. Agro 4.0: enabling agriculture digital transformation through IoT. *Revista Ciência Agronômica*, **51**, p.e20207771.

Lin, X., Ghorbani, A., Ren, K., Zhu, S. and Zhang, A. eds., 2018. *Security and privacy in communication networks*. New York: Springer International Publishing.

Linkov, V., Zámečník, P., Havlíčková, D. and Pai, C. W., 2019. Human factors in the cybersecurity of autonomous vehicles: trends in current research. *Frontiers in Psychology*, **10**, p.995.

Liu, Y., Xia, Q., Li, X., Gao, J. and Zhang, X., 2023. An authentication and signature scheme for UAV-assisted vehicular ad hoc network providing anonymity. *Journal of Systems Architecture*, **142**, p.102935.

Liu, X. M. and Murphy, D., 2020. A multi-faceted approach for trustworthy ai in cybersecurity. *Journal of Strategic Innovation and Sustainability*, **15**(6), pp.68-78.

Lone, A. N., Mustajab, S. and Alam, M., 2023. A comprehensive study on cybersecurity challenges and opportunities in the IoT world. *Security and Privacy*, **6**(6), p.e318.

Lu, Y., Liu, M., Li, C., Liu, X., Cao, C., Li, X. and Kan, Z., 2022. Precision fertilization and irrigation: progress and applications. *AgriEngineering*, [online] **4**(3), pp.626–655.

Lundgren, B. and Möller, N., 2017. Defining Information Security. *Science and Engineering Ethics*, [online] **25**(2), pp.419–441.

Ly, B. and Ly, R., 2021. Cybersecurity in Unmanned Aerial Vehicles (UAVs). *Journal of Cyber Security Technology*, **5**(2), pp.120-137.

Macas, M., Wu, C. and Fuertes, W., 2023. Adversarial examples: ф survey of attacks and defenses in deep learning-enabled cybersecurity systems. *Expert Systems with Applications*, p.122223.

MacFarlane, A., Russell-Rose, T. and Shokraneh, F., 2022. Search strategy formulation for systematic reviews: issues, challenges and opportunities. *Intelligent Systems with Applications*, **15**(1), p.200091.

Maddikunta, P. K. R., Hakak, S., Alazab, M., Bhattacharya, S., Gadekallu, T. R., Khan, W. Z. and Pham, Q. V., 2021. Unmanned aerial vehicles in smart agriculture: Applications, requirements, and challenges. *IEEE Sensors Journal*, **21**(16), pp.17608-17619.

Majumdar, P., Bhattacharya, D., Mitra, S. and Bhushan, B., 2023. Application of green IoT in agriculture 4.0 and beyond: requirements, challenges and research trends in the era of 5G, LPWANs and Internet of UAV Things. *Wireless Personal Communications*, **131**(3), pp.1767-1816.

Malatji, M., 2023. Management of enterprise cyber security: A review of ISO/IEC 27001: 2022. In *2023 International conference on cyber management and engineering (CyMaEn)* (pp. 117-122). IEEE.

Manninen, O., 2018. *Cybersecurity in agricultural communication networks: Case dairy farms.* Master's Thesis, JAMK University of Applied Sciences.

Maraveas, C., Konar, D., Michopoulos, D. K., Arvanitis, K. G. and Peppas, K. P., 2024. Harnessing quantum computing for smart agriculture: empowering sustainable crop management and yield optimization. *Computers and Electronics in Agriculture*, **218**, p.108680.

Maraveas, C., Piromalis, D., Arvanitis, K. G., Bartzanas, T. and Loukatos, D., 2022. Applications of IoT for optimized greenhouse environment and resources management. *Computers and Electronics in Agriculture*, **198**, p.106993.

Meidan, Y., Sachidananda, V., Peng, H., Sagron, R., Elovici, Y. and Shabtai, A., 2020. A novel approach for detecting vulnerable IoT devices connected behind a home NAT. *Computers & Security*, **97**, p.101968.

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

Monteiro, A., Santos, S. and Gonçalves, P., 2021. Precision agriculture for crop and livestock farming—brief review. *Animals*, [online] **11**(8), p.2345.

Moravcsik, A., 2020. *Transparency in qualitative research*. London: SAGE Publications Limited.

Mourtzis, D., Angelopoulos, J. and Panopoulos, N., 2022. A literature review of the challenges and opportunities of the transition from industry 4.0 to society 5.0. *Energies*, **15**(17), p.6276.

Naeem, M., Ozuem, W., Howell, K., & Ranfagni, S., 2023. A step-by-step process of thematic analysis to develop a conceptual model in qualitative research. *International Journal of Qualitative Methods*, **22**, p.16094069231205789.

Nagaraju, R., Pentang, J. T., Abdufattokhov, S., CosioBorda, R. F., Mageswari, N. and Uganya, G., 2022. Attack prevention in IoT through hybrid optimization mechanism and deep learning framework. *Measurement: Sensors*, **24**, p.100431.

Nazir, A., He, J., Zhu, N., Qureshi, S. S., Qureshi, S. U., Ullah, F. and Pathan, M. S., 2024. A deep learning-based novel hybrid CNN-LSTM architecture for efficient detection of threats in the IoT ecosystem. *Ain Shams Engineering Journal*, **15**(7), p.102777.

Neilson, C.J. and Premji, Z., 2023. A study of search strategy availability statements and sharing practices for systematic reviews: ask and you might receive. *Research Synthesis Methods*, **15**(3), pp.41-449.

Nikander, J., Manninen, O. and Laajalahti, M., 2020. Requirements for cybersecurity in agricultural communication networks. *Computers and Electronics in Agriculture*, **179**, p.105776.

Okey, O. D., Udo, E. U., Rosa, R. L., Rodríguez, D. Z. and Kleinschmidt, J. H., 2023. Investigating ChatGPT and cybersecurity: A perspective on topic modeling and sentiment analysis. *Computers & Security*, **135**, p.103476.

Okupa, H., 2020. *Cybersecurity and the future of agri-food industries*. Doctoral dissertation, Kansas State University.

Oh, J., Yu, S., Lee, J., Son, S., Kim, M. and Park, Y., 2021. A secure and lightweight authentication protocol for IoT-based smart homes. *Sensors*, **21**(4), p.1488.

Onur, F., Gönen, S., Barışkan, M. A., Kubat, C., Tunay, M. and Yılmaz, E. N., 2024. Machine learning-based identification of cybersecurity threats affecting autonomous vehicle systems. *Computers & Industrial Engineering*, **190**, p.110088.

Oruc, A., 2022. Potential cyber threats, vulnerabilities, and protections of unmanned vehicles. *Drone Systems and Applications*, **10**(1), pp.51-58.

Padhy, S., Alowaidi, M., Dash, S., Alshehri, M., Malla, P. P., Routray, S., & Alhumyani, H., 2023. Agrisecure: a fog computing-based security framework for agriculture 4.0 via blockchain. *Processes*, **11**(3), p.757.

Pan, J. and Yang, Z., 2018. Cybersecurity challenges and opportunities in the new" edge computing+ IoT" world. In: *Proceedings of the 2018 ACM international workshop on security in software defined networks & network function virtualization*. New York: ACM, pp.29-32.

Pang, M. S. and Tanriverdi, H., 2022. Strategic roles of IT modernization and cloud migration in reducing cybersecurity risks of organizations: the case of US federal government. *The Journal of Strategic Information Systems*, **31**(1), p.101707.

Pärn, E., Ghadiminia, N., de Soto, B. G. and Oti-Sarpong, K., 2024. A perfect storm: digital twins, cybersecurity, and general contracting firms. *Developments in the Built Environment*, **18**, p.100466.

Pawlicki, M., Pawlicka, A., Kozik, R. and Choraś, M., 2024. Advanced insights through systematic analysis: mapping future research directions and opportunities for xAI in deep learning and artificial intelligence used in cybersecurity. *Neurocomputing*, **590,** p.127759.

Pechlivani, E. M., Gkogkos, G., Giakoumoglou, N., Hadjigeorgiou, I., & Tzovaras, D., 2023. Towards sustainable farming: a robust decision support system's architecture for agriculture 4.0. In: *2023 24th International Conference on Digital Signal Processing (DSP)*. Piscataway: IEEE, pp.1-5.

Pedchenko, Y., Ivanchenko, Y., Ivanchenko, I., Lozova, I., Jancarczyk, D. and Sawicki, P., 2022. Analysis of modern cloud services to ensure cybersecurity. *Procedia Computer Science*, **207**, pp.110-117.

Peppes, N., Daskalakis, E., Alexakis, T., Adamopoulou, E. and Demestichas, K., 2021. Performance of machine learning-based multi-model voting ensemble methods for network threat detection in agriculture 4.0. *Sensors*, **21**(22), p.7475.

Pirayesh, H. and Zeng, H., 2022. Jamming attacks and anti-jamming strategies in wireless networks: a comprehensive survey. *IEEE Communications Surveys & Tutorials*, **24**(2), pp.767-809.

Prasetio, E. A. and Nurliyana, C., 2023. Evaluating perceived safety of autonomous vehicle: the influence of privacy and cybersecurity to cognitive and emotional safety. *IATSS Research*, **47**(2), pp.160-170.

Prodanović, R., Rančić, D., Vulić, I., Zorić, N., Bogićević, D., Ostojić, G. and Stankovski, S., 2020. Wireless sensor network in agriculture: model of cyber security. *Sensors*, **20**(23), p.6747.

Pukrongta, N., Taparugssanagorn, A. and Sangpradit, K., 2024. Enhancing crop yield predictions with Pensemble 4: IoT and ML-driven for precision agriculture. *Applied Sciences*, [online] **14**(8), p.3313.

Pyzynski, M. and Balcerzak, T., 2021. Cybersecurity of the Unmanned Aircraft System (UAS). *Journal of Intelligent & Robotic Systems*, **102**(2), p.35.

Qadir, S. and Quadri, S.M.K., 2016. Information availability: an insight into the most important attribute of information security. *Journal of Information Security*, **7**(3), pp.185–194.

Rahaman, M., Lin, C.-Y., Pappachan, P., Gupta, B.B. and Hsu, C.-H., 2024. Privacy-centric AI and IoT solutions for smart rural farm monitoring and control. *Sensors*, [online] **24**(13), p.4157. doi:https://doi.org/10.3390/s24134157.

Raj, M., Harshini, N. B., Gupta, S., Atiquzzaman, M., Rawlley, O. and Goel, L., 2024. Leveraging precision agriculture techniques using UAVs and emerging disruptive technologies. *Energy Nexus*, **14**, p.100300.

Ram, S., Rao, S.P. and Ranganathan, P., 2023. Cybersecurity challenges and solutions in IoT-based precision farming systems. In: *2023 IEEE 14th Annual Ubiquitous Computing, Electronics & Mobile Communication Conference (UEMCON)*. Piscataway: IEEE. doi:https://doi.org/10.1109/uemcon59035.2023.10316154.

Ramos-Cruz, B. andreu-Perez, J. and Martínez, L., 2024. The cybersecurity mesh: a comprehensive survey of involved artificial intelligence methods, cryptographic protocols and challenges for future research. *Neurocomputing*, **581**, p.127427.

Rangan, K. K., Abou Halloun, J., Oyama, H., Cherney, S., Assoumani, I. A., Jairazbhoy, N. and Ng, S. K., 2022. Quantum computing and resilient design perspectives for cybersecurity of feedback systems. *IFAC-PapersOnLine*, **55**(7), pp.703-708.

Rao, A. R. and Elias-Medina, A., 2024. Designing an internet of things laboratory to improve student understanding of secure IoT systems. *Internet of Things and Cyber-Physical Systems*, **4**, pp.154-166.

Raval, K. J., Jadav, N. K., Rathod, T., Tanwar, S., Vimal, V. and Yamsani, N., 2023. A survey on safeguarding critical infrastructures: attacks, AI security, and future directions. *International Journal of Critical Infrastructure Protection*, **44**, p.100647.

Ray, A.K. and Bagwari, A., 2020, April. IoT based Smart home: Security Aspects and security architecture. In *2020 IEEE 9th international conference on communication systems and network technologies (CSNT)* (pp. 218-222). IEEE.

Riaz, A. R., Gilani, S. M. M., Naseer, S., Alshmrany, S., Shafiq, M. and Choi, J. G., 2022. Applying adaptive security techniques for risk analysis of internet of things (IoT)-based smart agriculture. *Sustainability*, **14**(17), p.10964.

Roopak, M., Tian, G. Y. and Chambers, J., 2019. Deep learning models for cyber security in IoT networks. In *2019 IEEE 9th annual computing and communication workshop and conference (CCWC)*. Piscatway: IEEE, pp.0452-0457.

Rose, D.C. and Chilvers, J., 2018. Agriculture 4.0: Broadening responsible innovation in an era of smart farming. *Frontiers in Sustainable Food Systems*, **2**, p.87

Rudo, D. and Zeng, D. K., 2020. Consumer UAV cybersecurity vulnerability assessment using fuzzing tests. *arXiv preprint arXiv:2008.03621*.

Rupnik, R., Kukar, M., Vračar, P., Košir, D., Pevec, D. and Bosnić, Z., 2019. AgroDSS: a decision support system for agriculture and farming. *Computers and Electronics in Agriculture*, [online] **161**, pp.260–271.

Salameh, H.A.B., Almajali, S., Ayyash, M. and Elgala, H., 2018. Spectrum assignment in cognitive radio networks for Internet-of-Things delay-sensitive applications under jamming attacks. *IEEE Internet of Things Journal*, **5**(3), pp.1904–1913.

Saleh, A. M. S., 2024. Blockchain for secure and decentralized artificial intelligence in cybersecurity: a comprehensive review. *Blockchain: Research and Applications*, **2024**, p.100193.

Sarker, I. H., Janicke, H., Ferrag, M. A. and Abuadbba, A., 2024a. Multi-aspect rule-based AI: methods, taxonomy, challenges and directions toward automation, intelligence and transparent cybersecurity modeling for critical infrastructures. *Internet of Things*, **25**, p.101110.

Sarker, I. H., Janicke, H., Mohsin, A., Gill, A. and Maglaras, L., 2024b. Explainable AI for cybersecurity automation, intelligence and trustworthiness in digital twin: methods, taxonomy, challenges and prospects. *ICT Express*, pp.1-24.

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

Senturk, S., Senturk, F. and Karaca, H., 2023. Industry 4.0 technologies in agri-food sector and their integration in the global value chain: a review. *Journal of Cleaner Production*, **408**, p.137096.

Shaaban, A. M., Chlup, S., El-Araby, N. and Schmittner, C., 2022. Towards optimized security attributes for IoT devices in smart agriculture based on the IEC 62443 security standard. *Applied Sciences*, **12**(11), p.5653.

Shafiq, M., Tian, Z., Bashir, A.K., Du, X. and Guizani, M., 2020. IoT malicious traffic identification using wrapper-based feature selection mechanisms. *Computers & Security*, **94**, p.101863.

Shah, Z., Ullah, I., Li, H., Levula, A. and Khurshid, K., 2022. Blockchain based solutions to mitigate Distributed Denial of Service (DDoS) attacks in the Internet of Things (IoT): a survey. *Sensors*, **22**(3), p.1094. doi:https://doi.org/10.3390/s22031094.

Shaik, K. S., Kumar Thumboor, N. S., Veluru, S. P., Bommagani, N. J., Sudarsa, D. and Muppagowni, G. K., 2023. Enhanced SVM model with orthogonal learning chaotic grey wolf optimization for cybersecurity intrusion detection in agriculture 4.0. *International Journal of Safety & Security Engineering*, **13**(3), pp.509-517

Sharma, P. and Gillanders, J., 2022. Cybersecurity and forensics in connected autonomous vehicles: a review of the state-of-the-art. *IEEE Access*, **10**, pp.108979-108996.

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

Singh, G., Kalra, N., Yadav, N., Sharma, A. and Saini, M., 2022. Smart agriculture: a review. *Siberian Journal of Life Sciences and Agriculture*, **14**(6), pp.423-454.

Sitnicki, M. W., Prykaziuk, N., Ludmila, H., Pimenowa, O., Imbrea, F., Șmuleac, L. and Pașcalău, R., 2024. Regional perspective of using cyber insurance as a tool for protection of agriculture 4.0. *Agriculture*, **14**(2), p.320.

Smith, K. J., Dhillon, G. and Carter, L., 2021. User values and the development of a cybersecurity public policy for the IoT. *International Journal of Information Management*, **56**, p.102123.

Sokullu, R., Akkaş, M.A. and Demir, E., 2020. IoT supported smart home for the elderly. *Internet of Things*, **11**, p.100239.

Sontowski, S., Gupta, M., Chukkapalli, S. S. L., Abdelsalam, M., Mittal, S., Joshi, A. and Sandhu, R., 2020. Cyber-attacks on smart farming infrastructure. In: *2020 IEEE 6th International Conference on Collaboration and Internet Computing (CIC)*. Piscataway: IEEE, pp.135-143.

Sott, M. K., da Silva Nascimento, L., Foguesatto, C. R., Furstenau, L. B., Faccin, K., Zawislak, P. A. and Bragazzi, N. L., 2021. Agriculture 4.0 and smart sensors. the scientific evolution of digital agriculture: Challenges and opportunities. *Sensors*, **21**, p.7889.

Soussi, A., Zero, E., Sacile, R., Trinchero, D. and Fossa, M., 2024. Smart sensors and smart data for precision agriculture: a review. *Sensors*, **24**(8), pp.2647–2647.

Stephen, S., Alexander, K., Potter, L. and Palmer, X. L., 2023. Implications of cyberbiosecurity in advanced agriculture. In: *Proceedings of the 18th International Conference on Cyber Warfare and Security*. N/a: Academic Conferences International Limited.

Stevens, T., 2020. Knowledge in the grey zone: AI and cybersecurity. *Digital War*, **1**(1), pp.164-170.

Strecker, S., Dave, R., Siddiqui, N. and Seliya, N., 2021. A modern analysis of aging machine learning based IOT cybersecurity methods. *arXiv preprint arXiv:2110.07832*.

Studiawan, H., Grispos, G. and Choo, K. K. R., 2023. Unmanned Aerial Vehicle (UAV) forensics: the good, the bad, and the unaddressed. *Computers & Security*, **132**, p.103340.

Sudharsanan, R., Rekha, M., Pritha, N., Ganapathy, G., Rasoni, G. A. N. and Uthayakumar, G. S., 2024. Intruder identification using feed forward encasement-based parameters for cybersecurity along with IoT devices. *Measurement: Sensors*, **32**, p.101035.

Sukhera, J., 2022. Narrative reviews in medical education: key steps for researchers. *Journal of Graduate Medical Education*, **14**(4), pp.418–419.

Suleiman, Z., Shaikholla, S., Dikhanbayeva, D., Shehab, E. and Turkyilmaz, A., 2022. Industry 4.0: clustering of concepts and characteristics. *Cogent Engineering*, [online] **9**(1), pp.1-26.

Sumathy, S., Revathy, M. and Manikandan, R., 2023. Improving the state of materials in cybersecurity attack detection in 5G wireless systems using machine learning. *Materials Today: Proceedings*, **81**, pp.700-707.

Sun, X., Yu, F. R. and Zhang, P., 2021. A survey on cyber-security of Connected and Autonomous Vehicles (CAVs). *IEEE Transactions on Intelligent Transportation Systems*, **23**(7), pp.6240-6259.

Taeihagh, A. and Lim, H. S. M., 2019. Governing autonomous vehicles: emerging responses for safety, liability, privacy, cybersecurity, and industry risks. *Transport Reviews*, **39**(1), pp.103-128.

Taji, K. and Ghanimi, F., 2024. Enhancing security and privacy in smart agriculture: a novel homomorphic signcryption system. *Results in Engineering*, pp.102310–102310. doi:https://doi.org/10.1016/j.rineng.2024.102310.

Tantalaki, N., Souravlas, S. and Roumeliotis, M., 2019. Data-driven decision making in precision agriculture: the rise of big data in agricultural systems. *Journal of Agricultural & Food Information*, **20**(4), pp.344–380.

Tlili, F., Ayed, S. and Fourati, L. C., 2024. Exhaustive distributed intrusion detection system for UAVs attacks detection and security enforcement (E-DIDS). *Computers & Security*, **142**, p.103878.

Tod, D., Booth, A. and Smith, B., 2022. Critical appraisal. *International Review of Sport and Exercise Psychology*, **15**(1), pp.52-72.

Torky, M. and Hassanein, A. E., 2020. Integrating blockchain and the internet of things in precision agriculture: analysis, opportunities, and challenges. *Computers and Electronics in Agriculture*, **178**, 105476.

Toussaint, M., Krima, S. and Panetto, H., 2024. Industry 4.0 data security: a cybersecurity frameworks review. *Journal of Industrial Information Integration,* **39**, p.100604. doi:https://doi.org/10.1016/j.jii.2024.100604.

Tsague, H.D. and Twala, B., 2017. Practical techniques for securing the Internet of Things (IoT) against side channel attacks. *Studies in Big Data*, **30**, pp.439–481.

Tsao, K. Y., Girdler, T. and Vassilakis, V. G., 2022. A survey of cyber security threats and solutions for UAV communications and flying ad-hoc networks. *Ad Hoc Networks*, **133**, p.102894.

Vandezande, N., 2024. Cybersecurity in the EU: How the NIS2-directive stacks up against its predecessor. *Computer Law & Security Review*, **52**, p.105890.

Vatn, K. J. D., 2023. *Cybersecurity in agriculture: a threat analysis of cyber-enabled dairy farm systems*. Master's thesis, NTNU.

Van Der Linden, D., Michalec, O. A. and Zamansky, A., 2020. Cybersecurity for smart farming: socio-cultural context matters. *IEEE Technology and Society Magazine*, **39**(4), pp.28-35.

Vangala, A., Das, A. K., Chamola, V., Korotaev, V. and Rodrigues, J. J., 2023. Security in IoT-enabled smart agriculture: architecture, security solutions and challenges. *Cluster Computing*, **26**(2), pp.879-902.

Van Hilten, M. and Wolfert, S., 2022. 5G in agri-food-A review on current status, opportunities and challenges. *Computers and Electronics in Agriculture*, **201**, p.107291.

Van Klompenburg, T., Kassahun, A. and Catal, C., 2020. Crop yield prediction using machine learning: a systematic literature review. *Computers and Electronics in Agriculture*, **177**, p.105709.

Venkatachary, S. K., Prasad, J., Alagappan, A. andrews, L. J. B., Raj, R. A. and Duraisamy, S., 2024. Cybersecurity and cyber-terrorism challenges to energy-related infrastructures-cybersecurity frameworks and economics–comprehensive review. *International Journal of Critical Infrastructure Protection*, **45**, p.100677.

Victor, N., Maddikunta, P. K. R., Mary, D. R. K., Murugan, R., Chengoden, R., Gadekallu, T. R. and Paek, J., 2024. 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*, **17**, pp.5920-5945.

Wang, Z., Li, Y., Wu, S., Zhou, Y., Yang, L., Xu, Y. and Pan, Q., 2023. A survey on cybersecurity attacks and defenses for unmanned aerial systems. *Journal of Systems Architecture*, **138**, p.102870.

Wheeler, E., 2011. Security controls and services. In: Wheeler, E. (Ed.), *Security Risk Management*. Oxford: Syngress, pp.127–146.

Wurzenberger, M., Höld, G., Landauer, M., and Skopik, F., 2024. Analysis of statistical properties of variables in log data for advanced anomaly detection in cyber security. *Computers & Security*, **137**, p.103631.

Yadav, S., 2024. *Cyber security market – Forecast (2024-2030)*. https://www.linkedin.com/pulse/cyber-security-market-forecast-2024-2030-sunitha-yadav-dgyxc/

Yang, R., He, H., Xu, Y., Xin, B., Wang, Y., Qu, Y. and Zhang, W., 2023. Efficient intrusion detection toward IoT networks using cloud–edge collaboration. *Computer Networks*, **228**, p.109724.

Yang, T., Qiao, Y. and Lee, B., 2024. Towards trustworthy cybersecurity operations using Bayesian deep learning to improve uncertainty quantification of anomaly detection. *Computers & Security*, **144**, p.103909.

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

Yee, C.K. and Zolkipli, M.F., 2021. Review on confidentiality, integrity and availability in information security. *Journal of ICT in Education*, [online] **8**(2), pp.34–42.

Yépez-Ponce, D.F., Salcedo, J.V., Rosero-Montalvo, P.D. and Sanchis, J., 2023. Mobile robotics in smart farming: current trends and applications. *Frontiers in Artificial Intelligence*, **6**, p.1213330.

Yu, Z., Wang, Z., Yu, J., Liu, D., Song, H. and Li, Z., 2023. Cybersecurity of unmanned aerial vehicles: a survey. *IEEE Aerospace and Electronic Systems Magazine*, **99**, pp.1-25.

Zanasi, C., Russo, S. and Colajanni, M., 2024. Flexible zero trust architecture for the cybersecurity of industrial IoT infrastructures. *Ad Hoc Networks*, **156**, p.103414.

Zanella, A.R. de A., da Silva, E. and Albini, L.C.P., 2020. Security challenges to smart agriculture: current state, key issues, and future directions. *Array*, **8**, p.100048. doi:https://doi.org/10.1016/j.array.2020.100048.

Zhao, W., Wang, M. and Pham, V.T., 2023. Unmanned aerial vehicle and geospatial analysis in smart irrigation and crop monitoring on IoT platform. *Mobile Information Systems*, [online] **2023**, p.e4213645.

Zhao, T., Gasiba, T., Lechner, U. and Pinto-Albuquerque, M., 2024a. Thriving in the era of hybrid work: raising cybersecurity awareness using serious games in industry trainings. *Journal of Systems and Software*, **210**, p.111946. doi:https://doi.org/10.1016/j.jss.2023.111946.

Zhao, X., Zhao, T., Wang, F., Wu, Y. and Li, M., 2024b. SAC-based UAV mobile edge computing for energy minimization and secure data transmission. *Ad Hoc Networks*, **157**, p.103435.

Zidi, K., Abdellafou, K. B., Aljuhani, A., Taouali, O. and Harkat, M. F., 2024. Novel intrusion detection system based on a downsized kernel method for cybersecurity in smart agriculture. *Engineering Applications of Artificial Intelligence*, **133**, p.108579.

Appendix

Appendix 1: Quality Assessment

SANRA checklist

SANRA Checklist
Q1: Justification of the article's importance for the readership – The importance is explicitly justified
Q2: Statement of concrete aims or formulation of questions – One or more concrete aims or questions are formulated.
Q3: Description of the literature search. – The literature search is described in detail, including search terms and inclusion criteria.

Q4: References – Key statements are supported by references.

Q5: Scientific reasoning – Appropriate evidence is generally present.

Q6: Appropriate presentation of data – Relevant outcome data are generally presented appropriately.

Scores: ✓ is 2 points; * is 1 point, x is 0 points;

Critical Appaisal using SANRA Checklist

No.	Authors and Year	Q1	Q2	Q3	Q4	Q5	Q6	Total (x/12)
1.	Abbasi et al. (2022)	✓	✓	✓	✓	✓	✓	12
2.	Abdelfatah (2024)	✓	✓	✓	✓	✓	x	10
3.	Abdel-latif et al. (2021)	✓	✓	✓	✓	✓	✓	12
4.	Adil et al. (2023)	✓	✓	✓	✓	✓	✓	12
5.	Aldhyani & Alkahtani (2023)	✓	✓	✓	✓	✓	✓	12
6.	Ahmad et al. (2024)	✓	✓	✓	✓	✓	✓	12
7.	Ahmadi (2023)	✓	✓	✓	✓	✓	✓	12
8.	Ahmed et al. (2024)	✓	✓	✓	✓	✓	✓	12
9.	Aithal & Aithal (2024)	✓	✓	✓	✓	✓	✓	12
10.	Alahmadi et al. (2022)	✓	✓	✓	✓	✓	✓	12
11.	Alam et al. (2023)	✓	✓	✓	✓	✓	✓	12
12.	Al Asif et al. (2021)	✓	✓	✓	✓	✓	✓	12
13.	AlDaajeh & Alrabaee (2024)	✓	✓	✓	✓	✓	✓	12

14.	Al-Emran & Deveci (2024)	✓	✓	✓	✓	✓	✓	12
15.	Ali et al. (2024)	✓	✓	✓	✓	✓	✓	12
16.	Aliebrahimi & Miller (2023)	✓	✓	✓	✓	✓	✓	12
17.	Alferidah & Jhanjhi (2020)	✓	✓	✓	✓	✓	✓	12
18.	Algarni & Thayananthan,(2022)	✓	✓	✓	✓	✓	✓	12
19.	Alomari & Kumar (2024)	✓	✓	✓	✓	✓	✓	12
20.	Aloqaily et al. (2022)	✓	✓	✓	✓	✓	✓	12
21.	Alqudhaibi et al. (2024)	✓	✓	✓	✓	✓	✓	12
22.	Alsamhi et al. (2021)	✓	✓	x	✓	✓	✓	10
23.	Alshaikh et al. (2024)	✓	✓	✓	✓	✓	✓	12
24.	Altulaihan et al. (2022)	✓	✓	✓	✓	✓	✓	12
25.	Amiri-Zarandi et al. (2022)	✓	✓	✓	✓	✓	✓	12
26.	Angyalos et al. (2021)	✓	✓	✓	✓	✓	✓	12
27.	Araújo et al. (2021)	✓	✓	✓	✓	✓	✓	12
28.	Arce (2020)	✓	✓	✓	✓	✓	✓	12
29.	Argillander et al. (2023)	✓	✓	✓	✓	✓	✓	12
30.	Arora et al. (2022)	✓	✓	✓	✓	✓	✓	12
31.	Arroyabe et al. (2024)	✓	✓	✓	✓	✓	✓	12
32.	Aurangzeb et al. (2024)	✓	✓	✓	✓	✓	✓	12
33.	Awan et al. (2020)	✓	✓	✓	✓	✓	✓	12
34.	Axelrod et al. (2017)	✓	✓	✓	✓	✓	✓	12

35.	Bahassi et al. (2022)	✓	✓	✓	✓	✓	✓	12
36.	Balaji et al. (2023)	✓	✓	✓	✓	✓	✓	12
37.	Baltuttis et al. (2024)	✓	✓	✓	✓	✓	✓	12
38.	Barreto & Amaral (2018)	✓	✓	✓	✓	✓	✓	12
39.	Bashir et al. (2023)	✓	✓	✓	✓	✓	✓	12
40.	Benmalek (2024)	✓	✓	✓	✓	✓	✓	12
41.	Berguiga et al. (2023)	✓	✓	✓	✓	✓	✓	12
42.	Bissadu et al. (2024)	✓	✓	✓	✓	✓	*	11
43.	Bui et al. (2024)	✓	✓	✓	✓	✓	✓	12
44.	Boeckl et al. (2019)	✓	✓	✓	✓	✓	✓	12
45.	Bozorgchenani et al. (2023)	✓	✓	✓	✓	✓	✓	12
46.	Burzio et al. (2018)	✓	✓	*	✓	✓	✓	11
47.	Camacho (2024)	✓	✓	✓	✓	✓	✓	12
48.	Carneiro et al. (2021)	✓	✓	✓	✓	✓	✓	12
49.	Caviglia et al. (2023)	✓	✓	✓	✓	✓	✓	12
50.	Caviglia et al. (2024)	✓	✓	✓	✓	✓	✓	12
51.	Chan et al. (2019)	✓	✓	✓	✓	✓	✓	12
52.	Channon & Marson (2021)	✓	✓	✓	✓	✓	✓	12
53.	Chatfield & Reddick (2019)	✓	✓	✓	✓	✓	✓	12
54.	Chaudhary et al. (2023)	✓	✓	✓	✓	✓	✓	12
55.	Chiara (2024)	✓	✓	✓	✓	✓	✓	12

56.	Choo et al. (2018)	✓	✓	*	✓	✓	*	10
57.	Choo et al. (2021)	✓	✓	✓	✓	✓	✓	12
58.	Chundhoo et al. (2021)	✓	✓	✓	✓	✓	✓	12
59.	Dahlman & Lagrelius (2019)	✓	✓	✓	✓	✓	✓	12
60.	Daim et al. (2020)	✓	✓	✓	✓	✓	✓	12
61.	Dayıoğlu & Turker (2021)	✓	✓	✓	✓	✓	✓	12
62.	Demestichas et al. (2020)	✓	✓	x	✓	✓	✓	10
63.	Demircioglu et al. (2023)	✓	✓	✓	✓	✓	✓	12
64.	Drape et al. (2021)	✓	✓	✓	✓	✓	✓	12
65.	Duncan et al. (2019)	✓	✓	✓	✓	✓	✓	12
66.	Eashwar & Chawla (2021)	✓	✓	✓	✓	✓	✓	12
67.	El Alaoui et al. (2024)	✓	✓	✓	✓	✓	✓	12
68.	Etemadi et al. (2020)	✓	✓	✓	✓	✓	✓	12
69.	Familoni (2024)	✓	✓	✓	✓	✓	✓	12
70.	Fatoki et al. (2024)	✓	✓	✓	✓	✓	✓	12
71.	Fernandez et al. (2021)	✓	✓	✓	✓	✓	✓	12
72.	Ferrag et al. (2021)	✓	✓	✓	✓	✓	✓	12
73.	Fosch-Villaronga & Mahler (2021)	✓	✓	✓	✓	✓	x	10
74.	Freyhof et al. (2022)	✓	✓	✓	✓	✓	✓	12
75.	Friha et al. (2022)	✓	✓	✓	✓	✓	✓	12
76.	Furfaro et al. (2017)	✓	✓	✓	✓	✓	✓	12

77.	Geil et al. (2018)	✓	✓	✓	✓	✓	✓	12
78.	Ghobadpour et al. (2022)	✓	✓	✓	✓	✓	✓	12
79.	Gupta, et al. (2020)	✓	✓	✓	✓	✓	✓	12
80.	Guruswamy et al. (2022)	✓	✓	✓	✓	✓	✓	12
81.	Gyamfi et al. (2024)	✓	✓	✓	✓	✓	✓	12
82.	Hadi et al. (2024)	✓	✓	✓	✓	✓	✓	12
83.	Hasan et al. (2024)	✓	✓	✓	✓	✓	✓	12
84.	Hofstetter et al. (2020)	✓	✓	✓	✓	✓	✓	12
85.	Holzinger et al. (2024)	✓	✓	✓	✓	✓	✓	12
86.	Javaid et al. (2022)	✓	✓	✓	✓	✓	*	11
87.	Jerhamre et al. (2022)	✓	✓	✓	✓	✓	✓	12
88.	Jin & Han (2024)	✓	✓	✓	✓	✓	✓	12
89.	Kang (2023)	✓	✓	✓	✓	✓	✓	12
90.	Kapoor (2024)	✓	✓	✓	✓	✓	✓	12
91.	Kaur et al. (2022)	✓	✓	✓	✓	✓	✓	12
92.	Kavallieratos & Katsikas (2023)	✓	✓	✓	✓	✓	✓	12
93.	Khan et al. (2019)	✓	✓	✓	✓	✓	✓	12
94.	Khan, et al. (2022)	✓	✓	✓	✓	✓	✓	12
95.	Khan, et al. (2024)	✓	✓	✓	✓	✓	✓	12
96.	Khan & Quadri (2020)	✓	✓	✓	✓	✓	✓	12
97.	Kim & Kim (2024)	✓	✓	✓	✓	✓	✓	12

98.	Kim et al. (2021)	✓	✓	✓	✓	✓	✓	12
99.	Kjønås & Wangen (2023)	✓	✓	✓	✓	✓	✓	12
100.	Klerkx et al. (2019)	✓	✓	✓	✓	✓	✓	12
101.	Koduru & Koduru (2022)	✓	✓	✓	✓	✓	✓	12
102.	Krishna & Murphy (2017)	✓	✓	✓	✓	✓	✓	12
103.	Kristen et al. (2021)	✓	✓	x	✓	✓	✓	10
104.	Kshetri (2017)	✓	✓	✓	✓	✓	✓	12
105.	Kukkala et al. (2022)	✓	✓	✓	✓	✓	✓	12
106.	Kulkarni et al. (2024)	✓	✓	✓	✓	✓	✓	12
107.	Kusyk et al. (2019)	✓	✓	✓	✓	✓	✓	12
108.	Kuzlu et al. (2021)	✓	✓	✓	✓	✓	✓	12
109.	Lee (2020)	✓	✓	✓	✓	✓	✓	12
110.	Lezoche et al. (2020)	✓	✓	✓	✓	✓	✓	12
111.	Li et al. (2024)	✓	✓	✓	✓	✓	✓	12
112.	Li (2018)	✓	✓	✓	✓	✓	✓	12
113.	Lim & Taeihagh (2018)	✓	✓	✓	✓	✓	✓	12
114.	Lima et al. (2021)	✓	✓	✓	✓	✓	✓	12
115.	Lin et al. (2018)	✓	✓	✓	✓	✓	✓	12
116.	Linkov et al. (2019)	✓	✓	✓	✓	✓	✓	12
117.	Liu et al. (2023)	✓	✓	✓	✓	✓	✓	12
118.	Liu & Murphy (2020)	✓	✓	✓	✓	✓	✓	12

119.	Lone et al. (2023)	✓	✓	✓	✓	✓	✓	12
120.	Lu & Da Xu (2018)	✓	✓	✓	✓	✓	✓	12
121.	Ly & Ly (2021)	✓	✓	✓	✓	✓	✓	12
122.	Macas et al. (2023)	✓	✓	✓	✓	✓	✓	12
123.	Maddikunta et al. (2021)	✓	✓	✓	✓	✓	*	11
124.	Majumdar et al. (2023)	✓	✓	✓	✓	✓	✓	12
125.	Manninen (2018)	✓	✓	✓	✓	✓	✓	12
126.	Maraveas et al. (2024)	✓	✓	✓	✓	✓	✓	12
127.	Maraveas et al. (2022)	✓	✓	*	✓	✓	✓	11
128.	Martínez-Rodríguez et al. (2021)	✓	✓	✓	✓	✓	✓	12
129.	Mesías-Ruiz et al. (2023)	✓	✓	✓	✓	✓	✓	12
130.	Mitra et al. (2022)	✓	✓	✓	✓	✓	✓	12
131.	Mourtzis et al. (2022)	✓	✓	✓	✓	✓	✓	12
132.	Nagaraju et al. (2022)	✓	✓	✓	✓	✓	✓	12
133.	Nazir et al. (2024)	✓	✓	✓	✓	✓	✓	12
134.	Nikander et al. (2020)	✓	✓	✓	✓	✓	✓	12
135.	Okey et al. (2023)	✓	✓	✓	✓	✓	✓	12
136.	Okupa (2020)	✓	✓	✓	✓	✓	✓	12
137.	Onur et al. (2024)	✓	✓	*	✓	✓	*	10
138.	Oruc (2022)	✓	✓	✓	✓	✓	✓	12
139.	Padhy et al. (2023)	✓	✓	✓	✓	✓	✓	12

140.	Pan & Yang (2018)	✓	✓	✓	✓	✓	✓	12
141.	Pang & Tanriverdi (2022)	✓	✓	✓	✓	✓	✓	12
142.	Pärn et al. (2024)	✓	✓	✓	✓	✓	✓	12
143.	Pawlicki et al. (2024)	✓	✓	x	✓	✓	✓	10
144.	Pechlivani et al. (2023)	✓	✓	✓	✓	✓	✓	12
145.	Pedchenko et al. (2022)	✓	✓	✓	✓	✓	✓	12
146.	Peppes et al. (2021)	✓	✓	✓	✓	✓	✓	12
147.	Polymeni et al. (2023)	✓	✓	✓	✓	✓	✓	12
148.	Prasetio & Nurliyana (2023)	✓	✓	✓	✓	✓	✓	12
149.	Prodanović et al. (2020)	✓	✓	✓	✓	✓	✓	12
150.	Prokofiev et al. (2017)	✓	✓	✓	✓	✓	✓	12
151.	Pyzynski & Balcerzak (2021)	✓	✓	✓	✓	✓	✓	12
152.	Rahaman et al. (2024)	✓	✓	✓	✓	✓	✓	12
153.	Raj et al. (2024)	✓	✓	✓	✓	✓	✓	12
154.	Ram et al. (2023)	✓	✓	✓	✓	✓	x	10
155.	Ramos-Cruz et al. (2024)	✓	✓	✓	✓	✓	✓	12
156.	Rangan et al. (2022)	✓	✓	✓	✓	✓	✓	12
157.	Rao & Elias-Medina (2024)	✓	✓	✓	✓	✓	✓	12
158.	Raval et al. (2023)	✓	✓	✓	✓	✓	✓	12
159.	Riaz et al. (2022)	✓	✓	✓	✓	✓	✓	12
160.	Roopak et al. (2019)	✓	✓	✓	✓	✓	✓	12

161.	Rudo & Zeng (2020)	✓	✓	✓	✓	✓	✓	12
162.	Rudrakar & Rughani (2023)	✓	✓	✓	✓	✓	✓	12
163.	Salam (2019)	✓	✓	✓	✓	✓	*	11
164.	Saleh (2024)	✓	✓	✓	✓	✓	✓	12
165.	Sari & Hindarto (2023).	✓	✓	✓	✓	✓	✓	12
166.	Sarker et al. (2024a)	✓	✓	✓	✓	✓	✓	12
167.	Sarker et al. (2024b)	✓	✓	x	✓	✓	✓	10
168.	Sarker et al. (2021)	✓	✓	✓	✓	✓	✓	12
169.	Senturk et al. (2023)	✓	✓	✓	✓	✓	✓	12
170.	Shaaban et al. (2022)	✓	✓	✓	✓	✓	✓	12
171.	Shafik et al. (2020)	✓	✓	✓	✓	✓	✓	12
172.	Shah et al. (2022)	✓	✓	✓	✓	✓	✓	12
173.	Shaik et al. (2023)	✓	✓	✓	✓	✓	✓	12
174.	Sharma & Gillanders (2022)	✓	✓	✓	✓	✓	✓	12
175.	Sharma et al. (2022)	✓	✓	✓	✓	✓	✓	12
176.	Singh et al. (2022)	✓	✓	✓	✓	✓	✓	12
177.	Sitnicki et al. (2024)	✓	✓	*	✓	✓	✓	11
178.	Smith et al. (2021)	✓	✓	✓	✓	✓	✓	12
179.	Sontowski et al. (2020)	✓	✓	✓	✓	✓	✓	12
180.	Sott et al. (2021)	✓	✓	✓	✓	✓	✓	12
181.	Stephen et al. (2023)	✓	✓	✓	✓	✓	✓	12

182.	Stevens (2020)	✓	✓	✓	✓	✓	✓	12
183.	Strecker et al. (2021)	✓	✓	✓	✓	✓	x	10
184.	Studiawan et al. (2023)	✓	✓	✓	✓	✓	✓	12
185.	Sudharsanan et al. (2024)	✓	✓	✓	✓	✓	✓	12
186.	Sumathy et al. (2023)	✓	✓	✓	✓	✓	✓	12
187.	Sun et al. (2021)	✓	✓	✓	✓	✓	✓	12
188.	Taeihagh & Lim (2019)	✓	✓	✓	✓	✓	✓	12
189.	Taji & Ghanimi (2024)	✓	✓	✓	✓	✓	✓	12
190.	Tankosić et al. (2024)	✓	✓	✓	✓	✓	✓	12
191.	Tlili et al. (2024)	✓	✓	✓	✓	✓	✓	12
192.	Torky & Hassanein (2020)	✓	✓	✓	✓	✓	✓	12
193.	Toussaint et al. (2024)	✓	✓	✓	✓	✓	✓	12
194.	Tsao et al. (2022)	✓	✓	✓	✓	✓	*	11
195.	Valkenburg & Bongiovanni (2024)	✓	✓	✓	✓	✓	✓	12
196.	Vandezande (2024)	✓	✓	✓	✓	✓	✓	12
197.	Vatn (2023)	✓	✓	✓	✓	✓	✓	12
198.	Van Der Linden et al. (2020)	✓	✓	✓	✓	✓	✓	12
199.	Vangala et al. (2023)	✓	✓	✓	✓	✓	✓	12
200.	Van Hilten & Wolfert (2022)	✓	✓	✓	✓	✓	✓	12
201.	Venkatachary et al. (2024)	✓	✓	✓	✓	✓	✓	12
202.	Victor et al. (2024)	✓	✓	✓	✓	✓	✓	12

203.	Wang et al. (2023)	√	√	√	√	√	√	12
204.	Wurzenberger et al. (2024)	√	√	√	√	√	√	12
205.	Yang et al. (2023)	√	√	√	√	√	√	12
206.	Yang et al. (2024)	√	√	√	√	√	√	12
207.	Yazdinejad et al. (2021)	√	√	√	√	√	√	10
208.	Yu et al. (2023)	√	√	√	√	√	√	12
209.	Zanasi et al. (2024)	√	√	√	√	√	√	12
210.	Zanella et al. (2020)	√	√	√	√	√	√	12
211.	Zhao et al. (2024a)	√	√	√	√	√	√	12
212.	Zhao et al. (2024b)	√	√	√	√	√	√	12
213.	Zidi et al. (2024)	√	√	√	√	√	√	12

2070

Appendix 2: Thematic Analysis Summary

Themes	**Subthemes**	**Codes**
Cybersecurity Technologies in Agriculture 4.0 and 5.0	Cybersecurity Framework	Identify threat, protection mechanism, monitor, respond, and recover
	Smart climate monitoring	Monitors and predicts weather conditions
	Smart livestock tracking and geofencing	Monitors livestock location on farm
	Smart crop monitoring	Monitors crop growth and development
	Smart equipment monitoring	Monitors irrigation systems, water flow, and water pressure
	Smart logistics and warehousing	Employ robotics to locate products around warehouse and track inventories or shipments.
	Importance of cybersecurity technologies in agriculture	Improved efficiency and cost savings in agricultural operations
Cybersecurity Threats in Agriculture 4.0 and 5.0	Factors affecting cybersecurity risks	Outdated applications, poor cybersecurity practices, and lack of proper security infrastructure
	Intentional cybersecurity threats	Malware, hacking, phising, ransomware

	Unintentional cybersecurity threat	Accidental data sharing, unauthorized access to computing infrastructure, improper encryption, and configuration error
	Impact of cybersecurity breach in agriculture	Affect irrigation systems, food supply chain, and food processing plants.
Cybersecurity Mitigation Measures in Agriculture 4.0 and 5.0	AI/IOT Tools	Enable integration of data across many devices; Convenient monitoring on mobile phone and faster response in case of breach
	Quantum safe cryptography technologies	Enable better encryption and protection of sensitive data, preserve integrity of digital transactions
	Human risk management	Creating awareness and training on data control and management
	Regulatory standards and compliance	Following best practices in cybersecurity reduce risk of attack and faster recovery in case it occurs