Computers & Security 150 (2025) 104284

Contents lists available at ScienceDirect

Computers & Security

journal homepage: www.elsevier.com/locate/cose

Cybersecurity in smart agriculture: A systematic literature review

Milton Campoverde-Molina [a,*,1], Sergio Luján-Mora [b,*,2]

[a] Universidad Católica de Cuenca, Cuenca, 010107, Azuay, Ecuador
[b] Universidad de Alicante, San Vicente del Raspeig, 03690, Alicante, Spain

ARTICLE INFO

Dataset link: https://doi.org/10.17632/5ddfvwfj9p.1

Keywords:
Agriculture
Cybersecurity
Frameworks
Models
Smart agriculture
Systematic literature review
Threats

ABSTRACT

Agriculture is essential because of the current and future challenges related to food that our society must face. Agriculture is a precious resource (asset), and problems with agriculture can lead to famine and migration crises that destabilize a society. Smart agriculture can increase productivity and crop yield with new operating and business models. Smart agriculture relies on information and communication technology (ICT). However, a cyberattack on a country's agricultural ICT can jeopardize an entire nation. In light of the aforementioned challenges and threats, this research presents a systematic literature review (SLR) to address the lack of a comprehensive review of the literature on cybersecurity in smart agriculture. This SLR analyzes 58 documents extracted from Scopus, Web of Science, and IEEE Xplore. The main findings on cybersecurity in smart agriculture encompass the challenges of cybersecurity in agriculture, the detection of attacks and intrusions, the evaluation of case studies, the assessment of frameworks, and the analysis of applied models. Organizations should also train their employees to recognize and respond to cyber threats. In addition, organizations should invest in cybersecurity processes, equipment, and training. The main contribution of this SLR is the consolidation of results to identify research findings, research gaps, and trends in cybersecurity in smart agriculture. The intended audience for this article includes researchers, farmers, and agribusinesses who may utilize frameworks, models, case studies, or emerging technologies in smart agriculture with the objective of mitigating or preventing cybersecurity threats.

Contents

* Corresponding authors.
E-mail addresses: mcampoverde@ucacue.edu.ec (M. Campoverde-Molina), sergio.lujan@ua.es (S. Luján-Mora).
[1] Unidad Académica de Informática, Ciencias de la Computación, e Innovación Tecnológica, Grupo de Investigación Simulación, Modelado, Análisis y Accesibilidad (SMA^2).
[2] Departamento de Lenguajes y Sistemas Informáticos.

https://doi.org/10.1016/j.cose.2024.104284
Received 8 July 2024; Received in revised form 28 October 2024; Accepted 12 December 2024
Available online 18 December 2024

1. Introduction

Agriculture is composed of crop and livestock production. Agricultural production is a set of activities and knowledge created by humans to cultivate the land and obtain plant products (such as vegetables, fruits, cereals, and herbs) as food for people and animals. Therefore, it is the source of life for the beings that inhabit the present and future world. As the population grows, the demand for agricultural products also grows (Debdas et al., 2021). It is estimated that by 2050 there will be 9.6 billion people, so agriculture must grow faster to meet their rising food demands (Pyingkodi et al., 2022).

On the other hand, agriculture is the world's largest industry and is fundamental to social stability and economic development (Blandford, 2011; Ma et al., 2019; Meijerink and Roza, 2007). Like many industries, agriculture is undergoing a digital transformation driven by information and communication technology (ICT) (Hentea, 2008; Slobodan, 2018). Implementing ICT in agricultural management and production activities has changed the business culture toward smart agriculture. Smart agriculture increases agricultural productivity with new operating and business models. For this, it is necessary the incorporation of current and emerging computational paradigms such as artificial intelligence (AI), big data, cloud computing, robotics, the internet, and the internet of things (IoT) (Pivoto et al., 2018; Said Mohamed et al., 2021; Santiteerakul et al., 2020).

Smart agriculture systems rely heavily on digital technologies such as sensors, automated data collection and analysis, machine learning, and AI. As such, these systems are vulnerable to cyberattacks that could compromise the data, potentially leading to crop damage, financial losses, etc. Cybersecurity is a critical component of smart agriculture, as it helps protect these assets by providing solutions that prevent, detect, and respond to malicious activity. Smart agriculture also requires a comprehensive approach that includes training and awareness, secure system design and development, risk assessment, and ongoing monitoring. With the proper measures, smart agriculture systems can be better protected, allowing farmers to focus on producing safe and healthy food.

However, the current state of cybersecurity in agriculture is still being determined, as well as what kind of technological resources, limitations, protections against cybercrime, cyberattacks, cybersecurity impacts, and countermeasures exist. For these reasons, a systematic literature review (SLR) was conducted to systematically analyze the research conducted on cybersecurity in smart agriculture and identify existing knowledge gaps (Piškur et al., 2012). Furthermore, it should be noted that cybersecurity in smart agriculture employs emerging technologies and a SLR represents a framework that enables the synthesis of literature in disciplines where developments occur on a continuous basis (Tricco et al., 2018). Our research adopts Kitchenham's guidelines (Kitchenham et al., 2011) in SLR methodology to guide the research process. Our SLR analyzes and interprets the results published in 58 selected documents.

This SLR includes the following sections. Section 2, we provide an overview of the fundamental concepts that are essential for an understanding of our research. Section 3, we present the details of the methods applied to achieve the SLR objective. In Section 4, we analyze, synthesize, and interpret the results of the research questions. In Section 5, we highlight the most important findings of this SLR in an orderly and logical manner and identify challenges and opportunities for future avenues of research. In Section 6, we present the bias of this SLR. Finally, in Section 7, we present conclusions, and future work is presented.

2. Background

This section is necessary to interpret the results obtained from the SLR. It describes the concepts of agriculture 4.0, IoT, AI, and cloud computing in agriculture.

2.1. Agriculture 4.0

The term "Industry 4.0" became widely known at the Hannover Fair, an initiative of the German Federal Government in 2011 (Müller et al., 2017). The introduction of ICT in agriculture and the Fourth Industrial Revolution (Industry 4.0) (Gagliardi et al., 2022) have enabled new approaches in agriculture to optimize crop production, giving rise to the so-called agriculture 4.0. This approach combines traditional agriculture with today's most popular computational paradigms such as IoT, big data analytics, robotics, systems, and AI, among others. These computational paradigms allow collecting data through systems (flow, humidity, and pressure) that would enable determining the state of the soil; sensors can capture weather information and send it in real-time so that farmers know at all times what is the state of their fields. In addition, data analytics and artificial intelligence can estimate different scenarios, and the most appropriate response measures can be adopted (Cooke et al., 2019). Therefore, smart agriculture, also called precision agriculture or agriculture 4.0, significantly improves crops' economic, environmental and social impact (Gagliardi et al., 2021). Also, modern ICT has driven smart agriculture (characterized by uncrewed operations) toward intelligent technician processes.

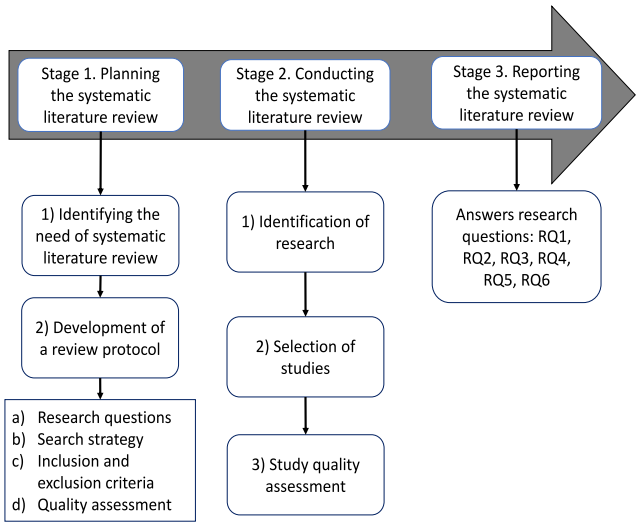

Fig. 1. Flowchart of the steps of the SLR methodology.

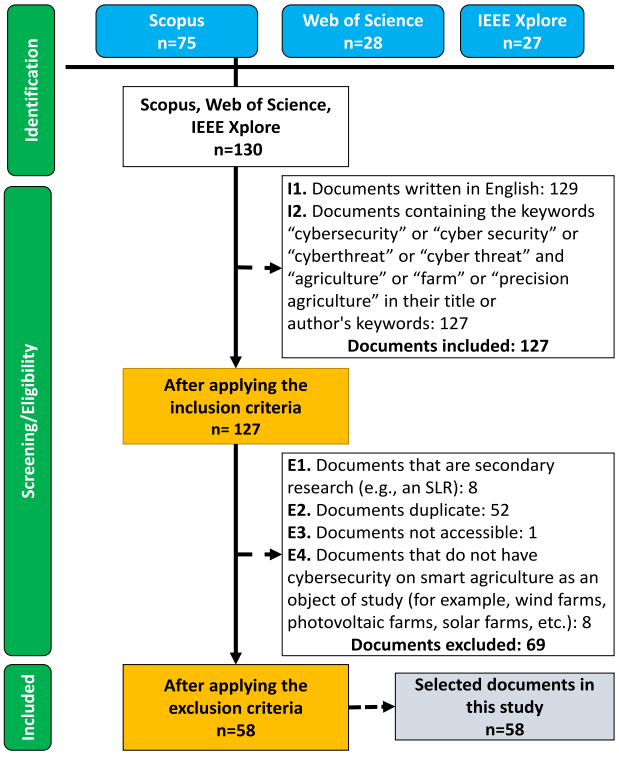

Fig. 2. PRISMA flowchart of the document selection process.

2.2. Internet of things

Ashton (Srivastava et al., 2021) first used the term IoT in 1999. The Internet Society (Rose et al., 2015) defines IoT as "scenarios where network connectivity and computing capability extends to objects, sensors and everyday items not normally considered computers, allowing these devices to generate, exchange and consume data with minimal human intervention". Therefore, the IoT integrates operational technology (OT) and ICT devices (Chen and Yang, 2019). The IoT is used to implement, monitor, and industrial control systems from manufacturing to energy, transportation, logistics, and utilities, such as programmable logic controllers (PLCs) (Thong-un and Wongsaroj, 2022), remote terminals units (RTUs), intelligent electronic devices (IEDs), embedded systems (Adami et al., 2021), systems on a chip (SoC), among others. As more devices can be connected to the IoT, end-to-end security becomes more essential and necessary (Shahbazi and Ko, 2021).

2.3. Artificial intelligence

AI simulates the intelligence capabilities of the human brain. AI is part of computer science that designs intelligent systems, i.e., systems that exhibit the characteristics we associate with intelligence in human behavior (Boucher, 2020; Silva Megeto et al., 2020). These computer systems handle a range of different algorithms and decision-making capabilities, as well as large amounts of data, to a solution or answer to a request (Berryhill et al., 2019; De Kleijn et al., 2019; Goertzel, 2014; Samoili et al., 2020).

Today, the agricultural sector also uses AI to improve important tasks: crop quality, crop control, pest control, soil control, seed propagation, human labor reduction, resource optimization, and water management, among others. Therefore, AI can transform conventional farming techniques into smart farming (Rehman et al., 2022; Talaviya et al., 2020).

2.4. Cloud computing

Cloud computing is a model that provides on-demand network access to a variety of configurable computing services, such as infrastructure, applications, and storage. In recent years, this model has enabled businesses to stay on the web and acquire ICT services at an affordable price without investing in purchasing hardware and software (Catteddu and Hogben, 2009). These services offer a wide range of solutions (data storage, computational hardware, and data analysis tools) with high scalability and flexibility, allowing the extraction of meaningful insights from the collected data, facilitating informed decision-making (Khan et al., 2017b; Soni et al., 2016; Zanoon et al., 2017). Therefore, connectivity and cloud computing through ICT optimize production processes in agriculture, using AI, IoT, and data analytics. These technologies have been successfully deployed in other areas. However, the agricultural sector is only now beginning to adopt these technologies, which facilitate innovation and the formation of businesses with a future orientation (Costa et al., 2022; Maiti and Ghosh, 2021).

3. Methodology

This SLR applied the Kitchenham's methodology, with the following stages: planning, conducting, and reporting the SLR (Kitchenham, 2004; Kitchenham et al., 2009). In Fig. 1, the flowchart of the steps of the SLR methodology can be seen, and in Fig. 2, we present an overview of the PRISMA (Page et al., 2021) flowchart for the document selection process.

3.1. Stage 1. Planning the systematic literature review

This subsection outlines the rationale for conducting an SLR, which will entail a preliminary investigation into existing SLRs in scientific databases, followed by the formulation of a review protocol.

3.1.1. Identifying the need for a systematic literature review

The need for an SLR was determined by searching for similar SLRs in Scopus and Web of Science scientific databases. Custom search strings were created for the query using the keywords cybersecurity, cyberthreat, agriculture, and SLR, with some of their synonyms and replacement terms to enhance search results. The search strings used in each scientific database can be seen below:

- **Scopus:** TITLE ((cybersecurit* OR "cyber security" OR cyber threat* OR "cyber threat") AND (agriculture* OR farm* OR "precision agriculture")) OR AUTHKEY ((cybersecurit* OR "cyber security" OR cyberthreat* OR "cyber threat") AND (agriculture* OR farm* OR "precision agriculture")) AND (LIMIT-TO (DOCTYPE, "re"))
- **Web of Science:** (((TI=cybersecurit* OR TI="cyber security" OR TI=cyberthreat* OR TI="cyber threat") AND (TI=agriculture* OR TI=farm* OR TI="precision agriculture")) OR ((AK= cybersecurit* OR AK="cyber security" OR AK=cyberthreat* OR AK="cyber threat") AND (AK=agriculture* OR AK=farm* OR AK= "precision agriculture"))) AND (DT==("REVIEW"))

Scopus (LIMIT-TO (DOCTYPE, "re")) refers to publications that are classified "Review". Likewise, Web of Science (DT==("REVIEW")) refers to publications that are classified "Review Article".

After applying the previously defined search strings to identify the need for an SLR in the scientific databases Scopus and Web of Science, four articles were found in each one. Three of the eight articles were duplicates, and one was discarded because it was not an actual SLR. It should be emphasized that one conference article from a literature review was added to the four articles found. This article was found by applying the search strings to select the articles for the analysis in Section 3.2. Stage 2. Conducting systematic literature review. Table 1 shows a synthesis of the five SLRs and their differences with our SLR.

In summary, the first literature review (Demestichas et al., 2020) identified the rise of ICTs in the agricultural sector and its effects when new methods or systems are used. The second literature review (Zhu et al., 2023) identified deep learning models and methods and their applications in sensor systems. The third literature review (Kjonas and Wangen, 2023) determined cybersecurity threats and attacks in agricultural technology. The fourth literature review (Bui et al., 2024) evaluated existing cyber threat intelligence (CTI) techniques on smart farm infrastructures (SFIs). The fifth literature review (Alahe et al., 2024) presented an overview of security issues and threats in the different layers of smart farming systems. Unlike these five SLRs, our SLR is focused on cybersecurity in smart agriculture. Our SLR begins with a bibliometric analysis of the main information about the data, author's keyword cloud, scientific production by year, sources of publication, scientific production of the countries over time, and a thematic map. The second part answers six research questions (RQ) analyzing cybersecurity challenges in agriculture, attacks and intrusion detection, evaluating case studies, frameworks, models, and threats.

3.1.2. Development of a review protocol

Scopus includes more journals than Web of Science (Mongeon and Paul-Hus, 2016; Singh et al., 2021), but there are journals that Web of Science includes that are not in Scopus. Therefore, if comprehensive results on a topic are desired, a single database is not sufficient in most cases; several relevant or even partially relevant databases must be consulted (Bar-Ilan, 2018). Therefore, IEEE Xplore, a database specializing in scientific articles on engineering and ICT, was also considered as a source of potential relevant articles for this SLR.

This research contemplates the documents published on cybersecurity in agriculture in the scientific databases Scopus, Web of Science, and IEEE Xplore until October 2024. The review protocol determines the RQs, the search strategies for the extraction of publications, the inclusion and exclusion criteria, and the evaluation of the quality of the selected documents.

Research questions. In this SLR, six RQs were defined. The RQs are related to cybersecurity in smart agriculture. In Table 2, we present the RQs and the expected results.

After defining the RQs that are multiple related questions, these questions will allow for reviewing different types of studies related to cybersecurity in smart agriculture. Therefore, the PICOC method (Population, Intervention, Comparison, Outcomes, Context) proposed by Petticrew and Roberts (2008) is used, which helps the researcher to define the review scope:

- **Population (P):** Cybersecurity.
- **Intervention (I):** Computational paradigms used in smart agriculture.
- **Comparison (C):** Computational paradigms and major cyberattacks and cybersecurity countermeasures applied in smart agriculture.
- **Outcomes (O):** Cybersecurity awareness in the implementation of smart agriculture.
- **Context (C):** Agriculture related environments.

The RQs defined in Table 2 are answered in the results of this SLR. The RQs are responded to by analyzing, interpreting, and synthesizing the results found in the selected documents.

Search strategy. The keywords and their synonyms and replacement terms are:

- Cybersecurity: (cybersecurit* OR "cyber security" OR cyberthreat* OR "cyber threat")
- Agriculture: (agriculture* OR farm* OR "precision agriculture")

Search strings were customized using keywords, synonyms, Boolean operators (AND, OR), double quotation marks (""), and the asterisk (*) as a wildcard symbol. Boolean operators allowed to join and combine keywords and synonyms. The double quotation marks allowed for searching for specific phrases. The asterisk allowed searching for the singular and plural of keywords or synonyms.

Considering none of the scientific databases contains 100 % of the scientific production of a specific area of knowledge, it is necessary to use several databases to extract a more significant number of documents (Gusenbauer and Haddaway, 2020; Pastor-Ramón et al., 2022). Therefore, the publications were extracted from Scopus, Web of Science, and IEEE Xplore. For this purpose, we created a specific search string for each scientific database. The search strings used are presented below:

- Scopus: TITLE ((cybersecurit* OR "cyber security" OR cyberthreat* OR "cyber threat") AND (agriculture* OR farm* OR "precision agriculture")) OR AUTHKEY ((cybersecurit* OR "cyber security" OR cyberthreat* OR "cyber threat") AND (agriculture* OR farm* OR "precision agriculture"))
- Web of Science: ((TI=cybersecurit* OR TI="cyber security" OR TI=cyberthreat* OR TI="cyber threat") AND (TI=agriculture* OR TI=farm* OR TI="precision agriculture")) OR ((AK=cybersecurit* OR AK="cyber security" OR AK=cyberthreat* OR AK="cyber threat") AND (AK=agriculture* OR AK=farm* OR AK= "precision agriculture"))
- IEEE Xplore: (("Document Title":cybersecurit* OR "Document Title":"cyber security" OR "Document Title":cyberthreat* OR "Document Title":"cyber threat") AND ("Document Title":agriculture* OR "Document Title":farm* OR "Document Title":"precision agriculture")) OR (("Author Keywords":cybersecurit* OR "Author Keywords":"cyber security" OR "Author Keywords":cyberthreat* OR "Author Keywords":"cyber threat") AND ("Author Keywords": agriculture* OR "Author Keywords":farm* OR "Author Key words": "precision agriculture"))

Inclusion and exclusion criteria. The inclusion and exclusion criteria are intended to help select documents analyzed in an SLR. To this end, documents that do not meet all the inclusion criteria are excluded from the SLR. Similarly, documents that meet at least one exclusion criterion are excluded from the SLR. The inclusion criteria defined for the selection of documents in this SLR are as follows:

- I1. Documents written in English AND,
- I2. Documents containing the keywords "cybersecurity" or "cyber security" or "cyberthreat" or "cyber threat" and "agriculture" or "farm" or "precision agriculture" in their title or author's keywords.

Table 1
SLR overtime on smart agriculture.

References	SLR synthesis	What makes our SLR different?
Demestichas et al. (2020)	In 2020, an exhaustive literature research was conducted on the existing and potential threats when incorporating ICTs in agriculture. The results revealed that the agricultural sector tends to be more vulnerable than other sectors using digital tools. The new era of agriculture emerged with smart agriculture or agriculture 4.0. Smart agriculture faces significant security challenges in growing and producing agricultural products using ICTs. In addition, innovations, techniques, advantages, threats, and measures regarding the impact of using ICTs in agriculture were highlighted. Finally, the authors concluded that for a new method or system to be successful, it must be able to (i) reduce costs, (ii) save time, (iii) increase confidence, and (iv) reduce risks. In addition, stakeholders in the agricultural sector must adopt new ways of working with methods or systems that are safe, reliable, usable, increase productivity, and add value to the business.	This literature review research identified the rise of ICT in the agricultural sector and its effects when new methods or systems are used. It is important to note that their literature review was performed in 2020, while our SLR is up to date as of October 2024.
Kjonas and Wangen (2023)	In 2023, a literature review researched cybersecurity in agricultural technology. This review included 19 documents published since 2017. The findings presented in the results determined that the majority of studies conducted are on the topics of threats and potential attacks.	This literature review determined the potential threat and attack issues on cybersecurity in agricultural technology. The main difference of our study is that we evaluated 58 selected documents published in journals, conferences, book chapters, and one book.
Zhu et al. (2023)	In 2023, a systematic investigation of deep learning models and methods and their applications in sensor systems was carried out. In addition, it presents a summary of implementation tips, links to tutorials, models, and open access codes. Also, it provides an overview of deep learning sensor systems, highlighting future challenges and opportunities.	This literature review identified deep learning models and methods and their applications in sensor systems. Furthermore, our study covers specific criteria that were not taken into account such as challenges in agriculture, attacks and intrusion detection, case study evaluation, frameworks, models and threats.
Alahe et al. (2024)	In 2024, a literature review on cybersecurity in smart agriculture was conducted by answering two research questions, "RQ1: What are the current advancements, challenges, and potential future research scopes in the implementation of data security within smart agriculture?" and "RQ2: How can the integration of cryptographic solutions and edge computing devices in smart agriculture be optimized to maximize their impact?". The results identified security threats in smart agriculture systems, advances and highlighted the need to improve data security. The authors concluded that there are barriers in sustainable agriculture on cybersecurity that need to be addressed to protect data manipulated by technological resources.	This literature review provided an overview of security issues and threats in the different layers of smart agriculture systems. In addition, a synthesis of advances and future lines of research in cybersecurity in smart agriculture was presented. However, no details are provided for the digital twins, the STRIDE and PASTA models.
Bui et al. (2024)	In 2024, a systematic literature review was conducted to evaluate existing CTI techniques in SFIs. In addition, a taxonomy of CTI tailored to SFIs was developed. One potential finding highlights the need for a virtual Chief Information Security Officer (vCISO) in smart agriculture. The authors concluded that a vCISO framework needs to be integrated into smart farming practices to strengthen cybersecurity.	This systematic literature review evaluated existing CTI techniques on SFIs. In contrast, our work provides a comprehensive SLR, contributing valuable insights to new proposals in the field as the Cybersecurity Framework 2.0.

Table 2
Research questions.

No.	Research question	Expected results
RQ1	What are the cybersecurity challenges in agriculture?	IoT, smart agricultural machines, economy, ontology, and supply chain.
RQ2	What are the cybersecurity attacks and intrusion detection applied in agriculture?	Intrusion detection systems, cyber-attacks, and Cyber–physical attack graphs (CPAGs).
RQ3	What are the assessed case studies of cybersecurity in agriculture?	Assessed, application of surveyed, workshop, comparative study, and test applied.
RQ4	What are the cybersecurity frameworks applied in agriculture?	Frameworks.
RQ5	What are the cybersecurity models applied in agriculture?	Models.
RQ6	What are the cybersecurity threats in agriculture?	Threats.

Table 3
Quality assessment checklist.

No.	Quality assessment question
QA1	Are the articles, books, book chapters, conferences a full or short document (not just an abstract)?
QA2	Are the empirical results related to challenges, or attacks and intrusion detection, or assessed case studies, or frameworks, or models, or threats?
QA3	Are the research goals related to cybersecurity in smart agriculture?
QA4	Are the search keywords in the title, or abstract or author keywords of the extracted documents?

The exclusion criteria defined in this SLR are as follows:

- E1. Documents that are secondary research (e.g., an SLR) OR,
- E2. Documents duplicate OR,
- E3. Documents not accessible (documents that cannot be downloaded) OR,
- E4. Documents that do not have cybersecurity on smart agriculture as an object of study (for example, wind farms, photovoltaic farms, solar farms, etc.).

Quality assessment. Quality assessment (QA) allows the inclusion or exclusion of documents through a set of questions. Four evaluation questions have been defined to measure the quality of each document. Each question has a value of 1 giving a total score of 4. The minimum score that documents must meet to be included in the SLR is 3. The QA questions are presented in Table 3.

QA1: Yes (value = 1.00) if the selected documents for SLR are articles, books, book chapters, or conferences; No (value = 0.00) if the selected documents are abstracts, reports, letters to the editor, etc.

QA2: Yes (value = 1.00) if the selected documents on cybersecurity in smart agriculture in the empirical results contribute to one or more of the following categories: challenges, or attacks and intrusion detection, or assessed case studies, or frameworks, or models, or threats; No (value = 0.00) if the selected documents do not contribute to any category.

QA3: Yes (value = 1.00) if the two keywords defined in the "search strategy" (cybersecurity and agriculture) or replacement terms are included in the goal of the selected documents; Partially (value = 0.50), if only one of the keywords or replacement terms is included in the goal of the selected documents; No (value = 0.00), if none of the keywords or replacement terms is included in the goal of the selected documents.

QA4: Yes (value = 1.00) if the two keywords defined in the "search strategy" (cybersecurity and agriculture) or substitution terms are included in the title, abstract, and authors' keywords in the extracted documents; Partially (value = 0.50) if the search keywords or substitution terms are included in two of the three cases (title, abstract or authors' keywords) in the extracted documents; No (value = 0.00), if none of the search keywords or substitution terms are included in the title, abstract and authors' keywords in the extracted documents.

3.2. Stage 2. Conducting the systematic literature review

3.2.1. Identification of research

The scientific databases used to select documents are Scopus, Web of Science, and IEEE Xplore because these databases index documents from different high-impact indexed journals. In addition, they meet the following requirements:

- Peer reviewers evaluate the documents.
- These databases index articles, books, chapters of books, conferences, etc.
- These databases allow the use of customized search strings.

3.2.2. Selection of studies

After applying search strings in the scientific databases Scopus, Web of Science, and IEEE Xplore, 130 documents were found. Then, applying the inclusion and exclusion criteria, 58 documents were selected for the analysis in this SLR. The details of the document selection process are presented in Fig. 2 following the PRISMA flowchart.

The researchers carried out the study selection procedure in three phases. In the identification phase, the researcher retrieved the documents from the Scopus, Web of Science, and IEEE Xplore databases through search strings defined in the search strategy. In the screening/eligibility phase, documents written in English and documents containing the keywords "cybersecurity" or "cyber security" or "cyberthreat" or "cyber threat" and "agriculture" or "farm" or "precision agriculture" in their title or author's keywords were included. In addition, the researchers excluded duplicate documents, documents not accessible, documents that are secondary research (e.g., an SLR), and documents that do not have cybersecurity in agriculture as a subject of study (e.g., wind farms, photovoltaic farms, solar farms, etc.); this was done by the researchers. In the study selection and data extraction phase, disagreements were resolved by consensus and discussion among the researchers.

3.2.3. Study quality assessment

The documents extracted considering the inclusion and exclusion criteria were also evaluated with the QA questions presented in Table 3. Table 4 presents the results of the QA of the selected documents. All the documents in the selection process obtained a minimum score of 3 and were therefore used in the subsequent analysis.

3.3. Stage 3. Reporting the systematic literature review

In this stage of the study, the RQs are addressed through a systematic analysis of the selected documents, with the findings serving as the basis for the responses. The results highlight the most important aspects found in the documents. The report is presented in the following section.

4. Results

In this section, the results are divided into two parts. A bibliometric analysis of the extracted documents is performed in the first part, and then, the RQs are answered in the second part.

4.1. Bibliometric analysis of selected documents

In this research, the bibliometric analysis was carried out using the bibliometrix package in R (Büyükkı dık, 2022). The bibliometric analysis contains a cloud with authors' keywords and three-field plot, the most relevant sources, the scientific production by year, the scientific production of countries over time, and a thematic map of the keywords plus, considering that keywords plus are as effective as author keywords for the bibliometric analysis of the knowledge structure of scientific fields (Moawia Mohammed et al., 2024; Zhang et al., 2016).

4.1.1. Main information and word cloud of authors' keywords

The main information presents an overview of the data (main information about data, document types, authors and document content) of the 58 documents selected for analysis. The 58 selected documents were published from 2017 to 2024 in 52 sources. The results can be seen in Fig. 3.

Of the 58 documents selected, a word cloud of 100 authors' keywords was made. In Fig. 4, we can see the authors' keywords, with the largest font size representing each word's frequency of repetition.

Table 4
Selected documents and quality assessment results, sorted by the reference and publication year.

References	Document type	Country	Category	Quality assessment				
				QA1	QA2	QA3	QA4	Score
Chi et al. (2017)	Conference	United States	Frameworks	1.00	1.00	1.00	1.00	4.00
Barreto and Amaral (2018)	Conference	Portugal	Challenges	1.00	1.00	1.00	1.00	4.00
Geil et al. (2018)	Article	United States	Assessed case studies	1.00	1.00	0.50	0.50	3.00
Straub (2018)	Conference	United States	Challenges	1.00	1.00	0.50	0.50	3.00
Duncan et al. (2019)	Article	United States	Challenges	1.00	1.00	1.00	1.00	4.00
Patel and Doshi (2019)	Book chapter	India	Challenges	1.00	1.00	0.50	0.50	3.00
Chukkapalli et al. (2020)	Conference	United States	Assessed case studies	1.00	1.00	0.50	0.50	3.00
Kristen et al. (2020)	Article	Austria	Challenges	1.00	1.00	1.00	0.50	3.50
Nikander et al. (2020)	Article	Finland	Challenges	1.00	1.00	1.00	1.00	4.00
Prodanović et al. (2020)	Article	Serbia	Models	1.00	1.00	1.00	1.00	4.00
Van der Linden et al. (2020)	Article	Israel	Challenges	1.00	1.00	1.00	0.50	3.50
Asif et al. (2021)	Conference	Bangladesh	Models	1.00	1.00	1.00	1.00	4.00
Bathalapalli et al. (2021)	Conference	United States	Challenges	1.00	1.00	1.00	1.00	4.00
Despoudi et al. (2021)	Book	United Kingdom	Challenges	1.00	1.00	0.50	0.50	3.00
Drape et al. (2021)	Article	United States	Assessed case studies	1.00	1.00	1.00	1.00	4.00
Dutta et al. (2021)	Article	United States	Challenges	1.00	1.00	1.00	0.50	3.50
Kristen et al. (2021)	Article	Austria	Assessed case studies	1.00	1.00	1.00	1.00	4.00
Peppes et al. (2021)	Article	Greece	Models	1.00	1.00	1.00	1.00	4.00
Tariq et al. (2021)	Conference	Pakistan	Challenges	1.00	1.00	0.50	0.50	3.00
Yazdinejad et al. (2021)	Article	Canada	Threats	1.00	1.00	1.00	1.00	4.00
Agarwal et al. (2022)	Conference	United Kingdom	Assessed case studies	1.00	1.00	0.50	1.00	3.50
Alahmadi et al. (2022)	Article	Saudi Arabia	Models	1.00	1.00	1.00	0.50	3.50
Erdei-Gally and Vágány (2022)	Article	Hungary	Assessed case studies	1.00	1.00	0.50	0.50	3.00
Ferrag et al. (2022)	Article	Algeria	Attacks and intrusion detection	1.00	1.00	1.00	1.00	4.00
Gaggero Battista et al. (2022)	Conference	Italy	Frameworks	1.00	1.00	1.00	1.00	4.00
Heikkilä et al. (2022)	Article	Finland	Challenges	1.00	1.00	1.00	1.00	4.00
Hoffmann et al. (2022)	Conference	Germany	Attacks and intrusion detection	1.00	1.00	1.00	1.00	4.00
Priyadharshini and Balamurugan (2022)	Conference	India	Challenges	1.00	1.00	1.00	1.00	4.00
Aldhyani and Alkahtani (2023)	Article	Saudi Arabia	Models	1.00	1.00	1.00	1.00	4.00
Arya et al. (2023)	Conference	India	Challenges	1.00	1.00	1.00	1.00	4.00
Balaji et al. (2023)	Conference	United States	Challenges	1.00	1.00	1.00	1.00	4.00
Barrère et al. (2023)	Article	United Kingdom	Attacks and intrusion detection	1.00	1.00	1.00	0.50	3.50
Caviglia et al. (2023)	Article	Italy	Frameworks	1.00	1.00	1.00	1.00	4.00
El-Ghamry et al. (2023)	Article	Egypt	Attacks and intrusion detection	1.00	1.00	1.00	1.00	4.00
Oussous et al. (2023)	Conference	Morocco	Challenges	1.00	1.00	0.50	0.50	3.00
Padhy et al. (2023)	Article	India	Frameworks	1.00	1.00	1.00	1.00	4.00
Shaik et al. (2023)	Article	India	Models	1.00	1.00	1.00	1.00	4.00
Taji et al. (2023)	Article	Morocco	Models	1.00	1.00	1.00	1.00	4.00
Usmani et al. (2023)	Book Chapter	India	Threats	1.00	1.00	0.50	0.50	3.00
Vangipuram et al. (2023)	Conference	United States	Challenges	1.00	1.00	1.00	0.50	3.50
Valenza et al. (2023)	Article	Italy	Models	1.00	1.00	0.50	0.50	3.00
Verma et al. (2023)	Book Chapter	India	Threats	1.00	1.00	1.00	0.50	3.50
Bissadu et al. (2024a)	Conference	United States	Frameworks	1.00	1.00	1.00	1.00	4.00
Bissadu et al. (2024b)	Conference	United States	Assessed case studies	1.00	1.00	1.00	1.00	4.00
Bissadu et al. (2024c)	Conference	United States	Assessed case studies	1.00	1.00	1.00	1.00	4.00
Eleftheriadis et al. (2024)	Conference	Cyprus	Frameworks	1.00	1.00	1.00	0.50	3.50
Kaushik (2024)	Book chapter	India	Challenges	1.00	1.00	1.00	0.50	3.50
Kataev et al. (2024)	Article	Russian Federation	Challenges	1.00	1.00	1.00	0.50	3.50
Kuppusamy and Khang (2024)	Book chapter	India	Models	1.00	1.00	1.00	0.50	3.50
Leligou et al. (2024)	Article	Greece	Challenges	1.00	1.00	0.50	0.50	3.00
Morchid et al. (2024)	Article	Morocco	Challenges	1.00	1.00	1.00	0.50	3.50
Quadri et al. (2024)	Article	India	Attacks and intrusion detection	1.00	1.00	1.00	0.50	3.50
Sharma and Garg (2024)	Book chapter	India	Challenges	1.00	1.00	1.00	1.00	4.00
Sitnicki et al. (2024)	Article	Ukraine	Challenges	1.00	1.00	1.00	1.00	4.00
Vangipuram et al. (2024)	Conference	United States	Challenges	1.00	1.00	1.00	1.00	4.00
Vardhan et al. (2024)	Conference	India	Frameworks	1.00	1.00	1.00	0.50	3.50
Zelisko et al. (2024)	Article	Ukraine	Challenges	1.00	1.00	0.50	0.50	3.00
Zidi et al. (2024)	Article	Saudi Arabia	Attacks and intrusion detection	1.00	1.00	1.00	1.00	4.00

*__Country__. Countries were obtained from the affiliation of the first author of each document. *__Conference__. Conference paper.

4.1.2. Most relevant sources

The 58 selected documents were published in 30 journals, 21 conferences, 6 book chapters, and 1 book. Sensors journal published three articles (Alahmadi et al., 2022; Peppes et al., 2021; Prodanović et al., 2020), Frontiers in Bioengineering and Biotechnology journal two articles (Drape et al., 2021; Duncan et al., 2019), IEEE Access journal two articles (Caviglia et al., 2023; Dutta et al., 2021), Applied Sciences journal two articles (Kristen et al., 2021; Yazdinejad et al., 2021), and one document in each of the remaining 21 journals. In Table 5, we show the sources with the number of documents published.

4.1.3. Scientific production per year

The 58 documents selected for analysis in this SLR were published between 2017 and 2024. The most publications occurred in 2024, with 16 documents; in 2023, with 14 documents; in 2021, with 9 documents; in 2022, with 8 documents; in 2020, with 5 documents. In 2018, there were 3 documents; in 2019, there were 2 documents, and in 2017, there was only 1 document. The results show an overall increase in the number of documents published over the years, indicating a growing interest and work in cybersecurity in smart agriculture due to the incorporation of new computational paradigms. In Fig. 5, we show

Table 5
Most relevant sources sorted by the number of references and the source.

Sources	Source type	References
Sensors	Journal	Alahmadi et al. (2022), Peppes et al. (2021), Prodanović et al. (2020)
IEEE Access	Journal	Caviglia et al. (2023), Dutta et al. (2021)
Frontiers in Bioengineering and Biotechnology	Journal	Drape et al. (2021), Duncan et al. (2019)
Applied Sciences	Journal	Kristen et al. (2021), Yazdinejad et al. (2021)
Advances in Cyberology and the Advent of the Next-Gen Information Revolution	Book Chapter	Usmani et al. (2023), Verma et al. (2023)
12th International Conference on Cyber Warfare and Security, ICCWS 2017	Conference	Chi et al. (2017)
9th International Conference on Intelligent Systems 2018: Theory, Research and Innovation in Applications, IS 2018	Conference	Barreto and Amaral (2018)
International Food and Agribusiness Management Review	Journal	Geil et al. (2018)
Proceedings - Applied Imagery Pattern Recognition Workshop	Conference	Straub (2018)
Lecture Notes in Intelligent Transportation and Infrastructure	Book chapter	Patel and Doshi (2019)
IEEE 6th Intl Conference on Big Data Security on Cloud, Big Data Security 2020, IEEE Intl Conference on High Performance and Smart Computing, HPSC 2020 and IEEE Intl Conference on Intelligent Data and Security, IDS 2020	Conference	Chukkapalli et al. (2020)
Ercim News	Journal	Kristen et al. (2020)
Computers and Electronics in Agriculture	Journal	Nikander et al. (2020)
IEEE Technology and Society Magazine	Journal	Van der Linden et al. (2020)
3rd International Conference on Sustainable Technologies for Industry 4.0, STI 2021	Conference	Asif et al. (2021)
19th OITS International Conference on Information Technology, OCIT 2021	Conference	Bathalapalli et al. (2021)
Agricultural Supply Chains and Industry 4.0: Technological Advance for Sustainability	Book	Despoudi et al. (2021)
Procedia Computer Science	Conference	Tariq et al. (2021)
ACM International Conference Proceeding Series	Conference	Agarwal et al. (2022)
Ukrainian Food Journal	Journal	Erdei-Gally and Vágány (2022)
IEEE/CAA Journal of Automatica Sinica	Journal	Ferrag et al. (2022)
26th International Conference Electronics, Electronics 2022	Conference	Gaggero Battista et al. (2022)
Network	Journal	Heikkilä et al. (2022)
Lecture Notes in Informatics (LNI), Proceedings - Series of the Gesellschaft fur Informatik (GI)	Conference	Hoffmann et al. (2022)
International Conference on Innovative Computing, Intelligent Communication and Smart Electrical Systems, ICSES 2022	Conference	Priyadharshini and Balamurugan (2022)
Mathematics	Journal	Aldhyani and Alkahtani (2023)
International Conference on Contemporary Computing and Informatics, IC3I 2023	Conference	Arya et al. (2023)
Computers and Security	Journal	Barrère et al. (2023)
IEEE 14th Annual Ubiquitous Computing, Electronics and Mobile Communication Conference, UEMCON 2023	Conference	Balaji et al. (2023)
Internet of Things (Netherlands)	Journal	El-Ghamry et al. (2023)
9th International Conference on Optimization and Applications, ICOA 2023	Conference	Oussous et al. (2023)
Processes	Journal	Padhy et al. (2023)
International Journal of Safety and Security Engineering	Journal	Shaik et al. (2023)
Data and Metadata	Journal	Taji et al. (2023)
IEEE Transactions on Dependable and Secure Computing	Journal	Valenza et al. (2023)
21st International Conference on Information Technology, OCIT 2023	Conference	Vangipuram et al. (2023)
IEEE 5th World AI IoT Congress, AIIoT 2024	Conference	Bissadu et al. (2024a)
12th International Symposium on Digital Forensics and Security, ISDFS 2024	Conference	Bissadu et al. (2024c)
IEEE International Conference on Consumer Electronics, ICCE 2024	Conference	Bissadu et al. (2024b)
28th International Conference on Information Technology, IT 2024	Conference	Eleftheriadis et al. (2024)
Systems Research and Behavioral Science	Journal	Kataev et al. (2024)

(*continued on next page*)

Table 5 (*continued*).

Sources	Source type	References
Convergence of Cloud with AI for Big Data Analytics: Foundations and Innovation	Book chapter	Kaushik (2024)
Agriculture and Aquaculture Applications of Biosensors and Bioelectronics	Book chapter	Kuppusamy and Khang (2024)
Electronics (Switzerland)	Journal	Leligou et al. (2024)
Results in Engineering	Journal	Morchid et al. (2024)
Journal of Theoretical and Applied Information Technology	Journal	Quadri et al. (2024)
Intelligent Security Solutions for Cyber–Physical Systems	Book chapter	Sharma and Garg (2024)
Agriculture (Switzerland)	Journal	Sitnicki et al. (2024)
IFIP Advances in Information and Communication Technology	Conference	Vangipuram et al. (2024)
2nd IEEE International Conference on Networking and Communications 2024, ICNWC 2024	Conference	Vardhan et al. (2024)
Ekonomika APK	Journal	Zelisko et al. (2024)
Engineering Applications of Artificial Intelligence	Journal	Zidi et al. (2024)

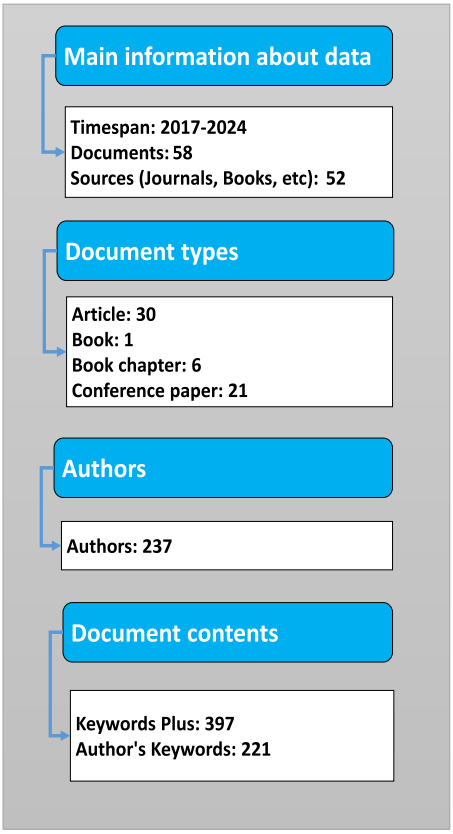

Fig. 3. Overview of the main information about the data.

Fig. 4. Word cloud of authors' keywords.

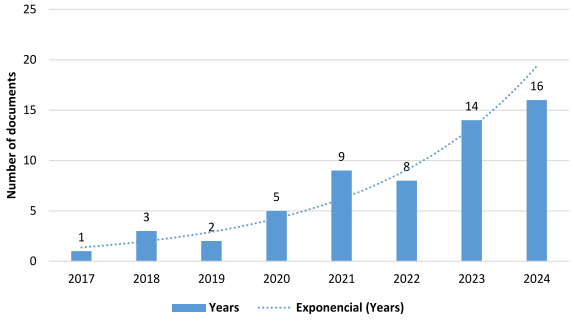

Fig. 5. Scientific production per year.

the trend in agricultural cybersecurity publications over time and their growth. The exponential approximation of the number of publications per year is also shown.

4.1.4. Scientific production of countries over time

The geographical analysis of the countries in which were published was linked to the country of affiliation of the first author of each selected document. The results show that the documents come from 21 countries: United States, the India, United Kingdom, Saudi Arabia, Morocco, Italy, Ukraine, Greece, Finland, and Austria are the countries with the highest number of documents in this SLR. In Fig. 6, we present the countries of affiliation of authors and co-authors and their publication trends from 2017 to October 2024.

4.1.5. Thematic map

The thematic map is composed of groups of keywords and their interconnections. These groups are called themes and are classified into four categories (López-Robles et al., 2019): "Motor Themes", "Niche Themes", "Emerging or Declining Themes", and "Basic Themes". The thematic map was elaborated with the "keywords plus" of the 58 selected documents. Fig. 7 shows nine clusters of occurrence networks obtained from the keywords plus (Moawia Mohammed et al., 2024). Three of the nine clusters are in the "Motor Themes" quadrant, meaning these themes are well developed in the research in the selected documents. Likewise, in the "Emerging or Declining Themes" quadrant,

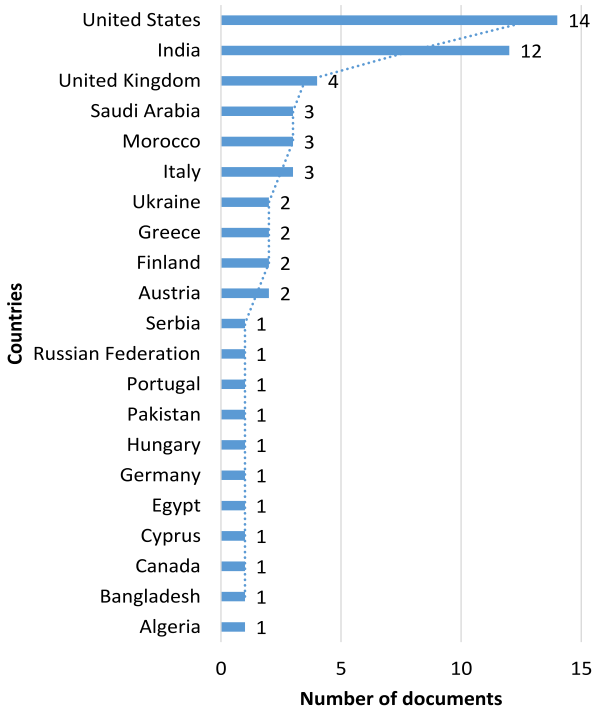

Fig. 6. Scientific production of countries over time.

there are three clusters of occurrence networks, which are basic or cross-cutting themes in the research. In the "Basic Themes" quadrant, we have a cluster of occurrence network with themes not yet well developed in the research.

4.2. Answering the research questions with the selected documents

In this subsection, the RQs are answered according to the findings found in the selected documents. The results highlight the most important aspects found in the documents.

4.2.1. RQ1: What are the cybersecurity challenges in agriculture?

The selected documents have identified that the challenges focus on IoT, smart agricultural machines, challenges and trends, the role and reflections of smart agriculture in the economy, supply chain, and cyber insurance. Immersed in these challenges is the use and application of emerging technologies and new computational paradigms. The cybersecurity challenges in agriculture are presented below:

1. **Challenges and trends.** Some reflections and challenges on smart agriculture's security (Barreto and Amaral, 2018) threats and how to overcome them were addressed. In addition, security means financial investment and smart agriculture has even more cybersecurity impacts. Threats of cyber-attacks when adopting technologies to optimize food production processes were highlighted. In addition, it was discussed how farmers' culture and attitudes can influence cybersecurity. It was also expressed that cybersecurity threats from one country to another may differ according to different social environments in the agricultural sector. Similarly, it examined cybersecurity challenges in the increasing reliance on technology in smart agriculture (Sharma and Garg, 2024), such as AI and the IoT, which are generating new vulnerabilities. In addition, cybersecurity trends and challenges in cyber attacks and the need to develop more robust security solutions were discussed. Future directions of cybersecurity research to protect smart agricultural systems were also explored.
2. **Internet of things.** As more and more things become connected to the Internet (Patel and Doshi, 2019), from portable devices to industrial sensors, more security threats emerge as personal and sensitive data becomes exposed to ransomware attacks that can wreak havoc. Therefore, key challenges to keep the IoT ecosystem safe from cyber threats were examined by analyzing application and component vulnerabilities and exploring lightweight cryptographic solutions. In addition, IoT helps farmers monitor field conditions through connected edge devices for real-time analytics (Bathalapalli et al., 2021). However, the duplicity of an IoT device, system security vulnerabilities, and data integrity put all processes in the agricultural sector at risk. Therefore, a hardware security primitive based on a physical unclonable function (PUF) was presented to authenticate Internet of Agro-Things (IoAT) devices. Also, the AFarCloud project (Kristen et al., 2020), which implemented the Agriculture IoT (AIoT) to ensure secure communication between agricultural sensors and the cloud, addressing cybersecurity risks, was successfully developed. The project seeks to establish standards and guidelines for cybersecurity in Agriculture 4.0 in the European Union.
   On the other hand, the authors examined the main security challenges in smart IoT applications such as smart agriculture, e-health, and energy (Tariq et al., 2021). It also highlighted the importance of understanding and addressing vulnerabilities to ensure the security of a growing IoT environment. The findings underscored the need for proactive and technologically advanced security solutions to mitigate emerging cyber threats. Also, IoT and cloud computing improve production in the agricultural sector through cost control, performance monitoring, and maintenance (Kaushik, 2024). For this reason, an intelligent drone has been implemented to manage real-time data using IoT and cloud computing to build sustainable smart agriculture.
   Finally, in the results of the selected documents, it has been found that an IoT architecture has been developed that integrates blockchain (Kataev et al., 2024) to improve data security in agricultural systems to ensure greater security in data transmission over networks. Also, a real-time fire detection system adapted to smart agriculture has been developed (Morchid et al., 2024) using the IoT, integrated systems, and Flask-based web software that considers cybersecurity measures such as login authentication and secure HTTP protocols.
3. **Smart agricultural machines.** IoT-based greenhouse agriculture faces the challenge of ensuring the confidentiality and integrity of data transmitted over protocols such as MQTT and I2C (Oussous et al., 2023). To this end, the authors focused on visual optimization tools, elliptic curve cryptography in PAYLOAD security, and data analytics in prediction. In addition, the choice of fixed and mobile nodes and how these influence energy efficiency, environmental preservation, and overall system performance was addressed. Adopting IoT, Unmanned Aerial Vehicles (UAV), and blockchain in agriculture has revolutionized farming activities and introduced cybersecurity challenges (Balaji et al., 2023). Hence, the current status of IoT-based precision farming systems was reviewed, including their technological applications, cybersecurity challenges, and mitigation measures. Also, CroPAiD (Vangipuram et al., 2024) is a system that uses storage-IPFS and IOTA Tangle to improve agricultural sensor data's security and privacy, bypassing centralized systems' limitations through an edge node that generates secure and distributed hashes. Current challenges in information gathering in multi-robot precision agriculture were explored (Dutta et al., 2021), highlighting the importance of trajectory planning, data security, and energy efficiency as significant hurdles. The interdependence of these challenges determined that there

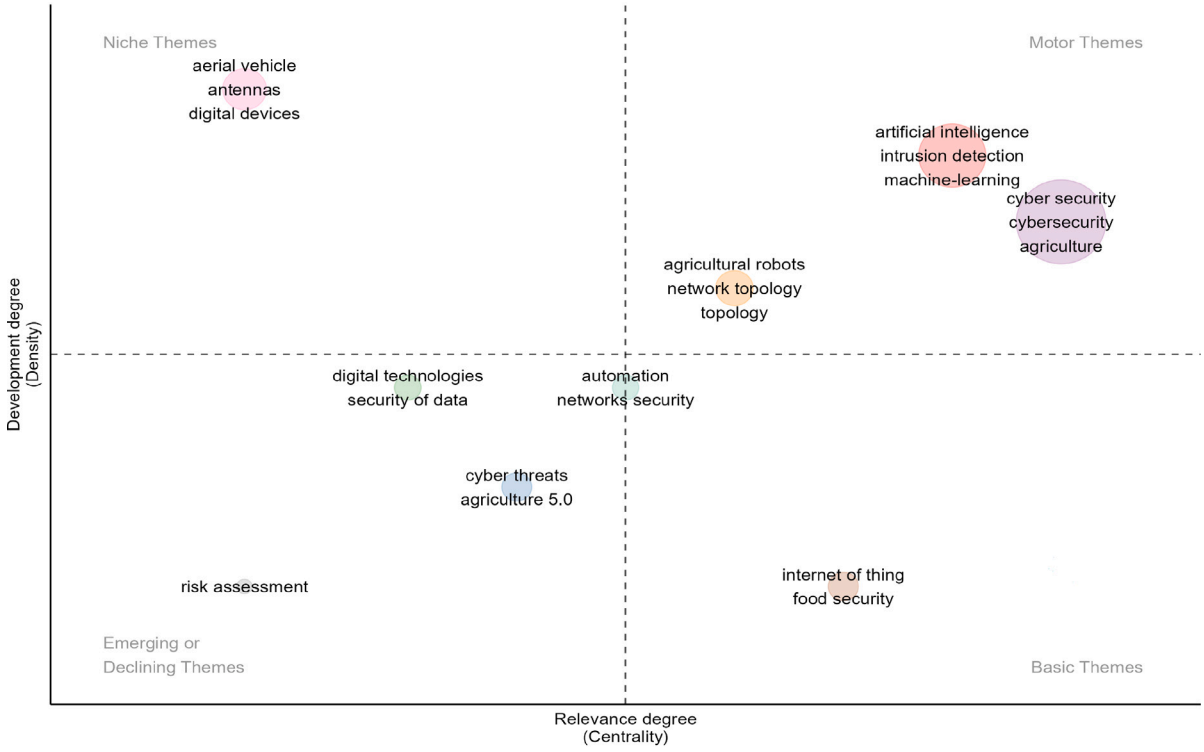

Fig. 7. Thematic map of keywords plus.

must be a balance between theoretical optimization, data integrity, and energy consumption, for which specialized research must be conducted to address the unique needs of precision agriculture. Challenges and case studies were presented in implementing uncrewed agricultural tractors in private mobile networks (Heikkilä et al., 2022). In addition, connectivity solutions, including technologies such as 4G and 5G, satellites, and tactical networks, were discussed for remote control of agricultural machinery. Also, the results of a comparative technology analysis and field test were discussed, highlighting cybersecurity requirements and opportunities for future research in smart agriculture.

4. **Role and reflections of the smart agriculture in economic.** The role of smart agriculture in economic growth was examined (Priyadharshini and Balamurugan, 2022), highlighting emerging technologies such as uncrewed aerial vehicles in agricultural environments. Cybersecurity threats and challenges in implementing security in smart agriculture were discussed, highlighting the importance of addressing these issues to ensure the security of agricultural supply chains. The cyberbiosecurity of U.S. food and agricultural systems (Duncan et al., 2019) determined that providing adequate protection from cyber criminals is crucial. A multidisciplinary approach is needed to integrate agriculture, food, engineering, and ICT. Also, it was critical to develop risk assessment and mitigation strategies, train workers, and apply policies and regulations to improve communication across sectors. Likewise, it was articulated and delved into the security issues of the main technologies of Agriculture 4.0 (Arya et al., 2023), emphasizing security measures since the devices produce a large amount of data that must be safeguarded from initial detection to final decision-making and storage at each stage of the agroecosystem.
   On the other hand, economic security in agricultural enterprises was analyzed (Zelisko et al., 2024), demonstrating that smart agriculture increases agribusiness efficiency. An analysis of successful examples of digital technologies, such as John Deere, increased by 56 % from 2019 to 2023, reaching $61.3 billion, and the Agricultural Bank of China increased its revenue by 60 % from 2019 to 2023, reaching 39.9 billion yuan. The analysis also covered the state of the Ukrainian agricultural sector and identified the potential operations of Myronivsky Hliboproduct and the issues and challenges facing this company in the context of innovation. It concluded that the new computational paradigms such as Big Data, blockchain technologies, drones, satellite technologies, and AI improve agribusiness management and help predict yields and optimize agricultural processes.
5. **Supply chain.** Agriculture 4.0 (Despoudi et al., 2021) leverages disruptive technologies such as AI and the IoT to optimize food production and address security challenges. However, more research is still needed on the new operating and business models driven by these technologies and their impact on the sustainability, circular economy, and resilience of agricultural supply chains. An application was designed with the IoT-Edge device Raspberry Pi to detect the data from the DHT11 sensor (Vangipuram et al., 2023). In addition, temperature and humidity data were collected from the IoT-Edge device. It sent the statistics directly to the Distributed Ledger with a Masked Authenticated Message (MaM) and called it agroString 2.0. agroString 2.0, with the help of a distributed ledger, contributed aspects of data security in the supply chain domain with zero cost and faster transaction times. The system increased sensor data security and provided integrity by delivering quality food data to end consumers. The FISHY platform (Leligou et al., 2024) was unveiled to protect ICT systems from multiple attacks and increase the confidence of supply chain actors. It used machine learning and blockchain to detect and mitigate threats. It was adaptable and could be applied in other systems, such as healthcare.
6. **Cyber insurance.** Smart agriculture through IoT and cloud computing was analyzed, considering cybersecurity is crucial to protecting agricultural information systems. Automation in agriculture reduces labor and improves information processing, yet

cyber risks can significantly disrupt farming operations. For this, an algorithm was developed (Sitnicki et al., 2024) that makes it possible to conclude a cyber threats insurance contract focused on customer requirements in cooperation between an agricultural company and an insurance company, considering that the need for cyber insurance differs from region to region. In addition, cyber insurance can minimize the likelihood of cyber incidents with the support of cybersecurity specialists.

4.2.2. RQ2: What are the cybersecurity attacks and intrusion detection applied in agriculture?

The selected documents examined intrusion detection systems (IDS) for Agriculture 4.0, the increase of cyber-attacks in the agricultural sector due to the adoption of emerging technologies, the proposal of an IDS based on Deep Learning, the rule-based approach to design more complex CPAGs, criteria for evaluating, classifying, and assessing IDS in cybersecurity in Agriculture 4.0, and An IDS is proposed to identify cyber-attacks in IoAT. Cybersecurity attacks and intrusion detection applied in agriculture are presented below:

1. **Intrusion detection systems.** IDS for Agriculture 4.0 were examined (Ferrag et al., 2022), evaluating their performance against cyber threats in emerging technologies such as cloud computing, Fog/Edge computing, autonomous tractors, network virtualization, drones, IoT, smart grids, and industrial agriculture. IDS were classified according to machine learning techniques and identified challenges and future directions in cybersecurity for Agriculture 4.0.
   A Deep Learning-based IDS was proposed to detect intruders in agricultural IoT networks (El-Ghamry et al., 2023). The NSL-KDD dataset allowed the evaluation of the proposed method by feature selection and image conversion. Then, these images were learned for intrusion detection using different CNN architectures, such as the VGG16, Inception, and Xception models. In addition, their performance was compared with traditional machine learning algorithms.
   The document (Quadri et al., 2024) described the criteria for evaluating, classifying, and assessing IDS in cybersecurity in Agriculture 4.0 using ABCIS techniques (AI, Blockchain Technology, Cloud computing, IoT, and software-defined networking (SDN)). In addition, obstacles and potential gaps to be investigated for cybersecurity IDSs in Agriculture 4.0 were outlined.
   An IDS is proposed (Zidi et al., 2024) to identify cyber-attacks in IoAT using the Downsized Kernel Partial Least Square (DKPLS) method, which extracts and reduces the dimension of data features to improve detection performance. The proposed IDS is evaluated on a new industrial IoT dataset, X-IIoTID. The results achieved an accuracy rate of 99.92% for binary classification and 99.99% for multi-class classification.
2. **Cyber-attacks.** The increase in cyber-attacks, especially ransomware, in the agricultural sector was discussed, highlighting the growing vulnerability due to the adoption of precision technologies in smart agriculture (Hoffmann et al., 2022). The need to research and address vulnerabilities specific to smart agriculture was raised. In addition, cybersecurity management systems should be implemented to reduce future attacks and the cost of protecting them.
   A scalable rule-based methodology for building complex CPAGs was proposed (Barrère et al., 2023), and risk analysis techniques using Bayesian CPAGs were analyzed. In addition, its application in smart agriculture was demonstrated with the open-source tool T-CITY for CPAG design and analysis. The CPAG integrated aspects of cyber and physical security, which made it possible to analyze sophisticated cyber–physical attacks.

4.2.3. RQ3: What are the assessed case studies of cybersecurity in agriculture?

The selected documents conducted the evaluation of dairy farms, application of a survey to measure perceptions, application of a survey to farmers in Hungary to find out their opinion on precision farming, virtual workshop to determine challenges, solutions, and gaps, comparative study using machine learning in network traffic, smart agricultural ontology, evaluation process with the IEC 62443 standard for agricultural systems, a test applied to the MacDonald dairy industry, a methodology of fuzzy cognitive mapping, and cyber threats and human factors in Agriculture 5.0. The evaluated cases of cybersecurity in agriculture are presented below:

1. **Survey.** Eighteen hundred farmers and agribusiness owners were surveyed (Geil et al., 2018) about their perceptions of cybersecurity, and how age, gender and education might affect those perceptions. The results showed that more than half of the respondents had been victims of cyber attacks. It concludes that technology can improve productivity in agriculture, but it must be protected and secure.
   An 18-question questionnaire was developed and administered to 110 farmers in Hungary in September 2022 to determine their thoughts about precision farming (Erdei-Gally and Vágány, 2022). According to the respondents' results, 81 % of the farmers use some support system, 70 % believe that precision technology systems are too expensive, and 31 % would like to have more knowledge about precision technologies (productivity, planting, input distribution).
2. **Network.** The research described findings found on six Finnish dairy farms (Nikander et al., 2020), assessing the state of cybersecurity on their local networks and connected devices. They analyzed real farm case studies, identifying challenges such as farmers' need for knowledge about network topologies, malware protection, backups, etc. In addition, they concluded that there is a low preparedness for cybersecurity in primary agricultural production; considering the small sample size, this study is preliminary, so the results cannot be generalized.
   Another study (Peppes et al., 2021) compared the performance of five machine learning classifiers in network traffic classification, individually and with hard and soft voting methods. The NSL-KDD dataset was used in three variants, and it was found that the ensemble voting models achieved higher accuracy in most cases. These solutions had potential applications in network traffic classification in Agriculture 4.0, thus contributing to a more secure and robust network infrastructure.
3. **Supply chains.** A 2-day multi-sector virtual workshop (Drape et al., 2021) identified challenges, solutions, and gaps in agricultural cyberbiosecurity. Participants needed cybersecurity training and resources, evidencing the need for educational programs. Greater interdisciplinary collaboration and government involvement are required to implement cybersecurity best practices in agricultural supply chains and protect the economy.
4. **Systems.** An ontology for smart farms has been developed (Chukkapalli et al., 2020), and an "attribute-based access control (ABAC) system" has been implemented using this ontology. This access control ontology addresses cyber-attack vulnerabilities in smart farm systems and classifies farm equipment and interactions for better management. In addition, digital twins optimize resource usage and improve security, and the representation graph tracks interactions between farm entities. The ontology encodes farm-specific sensors and interactions and implements an attribute-based access control (ABAC) system. It is intended to help farmers create and apply access control rules for their smart farms. In addition, various usage scenarios for access control are discussed.
   An evaluation process based on the IEC 62443 cybersecurity standard (Kristen et al., 2021) adapted to agricultural systems

was presented, identifying specific security gaps. After two years of research, the need for cybersecurity standards for Agriculture 4.0 is highlighted, and initial recommendations are provided. In agriculture, existing standards must be reviewed and expanded to mitigate cybersecurity gaps.

5. **Testbed.** The need for more research in smart farming safety and the scarcity of realistic test environments was addressed (Agarwal et al., 2022). The design of a test environment focused on MacDonald's dairy industry was discussed, providing an overview and analyzing challenges and lessons learned in the design process. In addition, preliminary results of the devices and software analysis were presented, along with future research directions.
6. **Methodology.** A methodology of fuzzy cognitive mapping and asset-centric assessments was proposed (Bissadu et al., 2024b) to quantify cybersecurity risks inherent to the farming practices of low-income farmers. The methodology was applied to a real case study: the "Ferme-Ecole of Tsevie, Togo" project to validate its effectiveness. The proposed methodology highlights support policies and streamlines agricultural system risk assessment and training programs.
7. **Human factors.** Insider cyber threats and human factors in Agriculture 5.0 were analyzed (Bissadu et al., 2024c), with emphasis on threats affecting agricultural cybersecurity. In addition, preventive strategies based on human factors analysis were proposed to improve security measures and safeguard critical and sensitive agricultural information. Use case diagrams were created using UML notation for insider threat analysis and defense strategies.

4.2.4. RQ4: What are the cybersecurity frameworks applied in agriculture?

In the selected documents, we found a framework for a security approach to data flow in precision agriculture, a framework to evaluate the network security of agricultural vehicles, a framework for agriculture 4.0 that integrates blockchain, fog computing, and software-defined networking, a framework to verify the cybersecurity of smart agricultural machines, a framework that use IPSec/VPN and the SiVi platform, and a cyber threat monitoring framework. The frameworks found are presented below:

1. **Security approach to data.** The authors laid a foundation focused on solutions to current and emerging challenges of wireless sensor networks (WSN) (Chi et al., 2017) in digital farms. The study highlights cybersecurity challenges in smart agriculture, considering that interdisciplinary collaboration is crucial for effective cybersecurity solutions. It also stated that implementing government standards can accelerate the adoption of cybersecurity in agriculture. In addition, a framework for a data flow security approach in precision agriculture was discussed, considering that cyber-attacks in agriculture are inevitable; proactive measures are needed.
2. **Network security.** In the agricultural sector, automated vehicles are increasingly used for data collection. These vehicles use wireless networks for data exchange. Therefore, a framework was proposed to evaluate (Gaggero Battista et al., 2022) the "network security of agricultural vehicles based on four main dimensions: CANbus security and network segmentation, remote control based on radio links, wireless gateways, and GPS security". In addition, they tested and discussed procedures and methods related to a testbed.
3. **IoT.** A security framework for agriculture 4.0 (Padhy et al., 2023) that integrates blockchain, fog computing, and SDN was proposed. In addition, SDN controllers were linked with block chain for secure IoT communications and distributed trust verification. Likewise, the performance against distributed denial of service (DDoS) attacks was evaluated using three cases demonstrating its good performance. Also, a framework for securing agricultural data generated from internet-connected IoT devices was proposed (Vardhan et al., 2024) that combines three components: honeycomb architecture, intrusion detection and prevention systems (IDPS), and AI and machine learning principles. The honeycomb architecture deters potential attackers with a layer of defense while protection and intrusion prevention methods monitor in real-time, enabling rapid response to possible threats and preserving the integrity of agricultural data.
4. **Smart agricultural machines.** A framework was proposed to verify the cybersecurity of smart agricultural machines (SAMs) (Caviglia et al., 2023), particularly wireless communications, using software-defined radio (SDR) technology capabilities. In addition, testing was conducted to corroborate SAMs' vulnerability detection effectiveness and security assessment.
5. **Machine learning.** The proposed framework used IPSec/VPN and the SiVi platform (Eleftheriadis et al., 2024). IPSec/VPN addressed confidentiality and identity authentication concerns through a robust and encrypted communication channel. The SiVi platform visually identifies, detects, and analyzes appli cation-layer cyber-attacks. The novel anomaly and intrusion detection system uses two supervised and unsupervised machine learning algorithms.
6. **Digital twins.** A cyber threat monitoring framework was designed to mitigate and manage cyber threats in the food chain and smart agriculture based on digital twins (Bissadu et al., 2024a). The framework enabled cyber threats to be identified, categorized, and mitigated using various countermeasures. Cyber threats can manifest as phishing attacks, sensor attacks, hardware/device tampering attacks, DDoS attacks, sniffing, tolerance failures, and sensitive data leakage.

4.2.5. RQ5: What are the cybersecurity models applied in agriculture?

This question is answered based on the results of the documents that have proposed a model, considering that a model is the explanation of a specific process seen from an author's point of view to provide a solution to a problem. The models found are the following:

1. **Image pattern recognition system.** A model of an image pattern recognition system (Straub, 2018) has been developed by identifying multiple points of vulnerability and analyzing the attacks to which each point of vulnerability is exposed. Finally, these types of attacks and the applicable countermeasures have been analyzed. They are considering patterns and image analysis as also being applied in agriculture.
2. **Sensor network.** A data security model for wireless sensor networks in agricultural monitoring was proposed (Prodanović et al., 2020), considering node architecture, energy saving, and optimization. The model meets the security requirements of distributed systems through authentication, and digital signatures and certificates are achieved. Message integrity is confirmed by public key verification. Non-repudiation prevents the sender from revoking sent messages. Trust is established through a trusted certificate authority. Encryption algorithms ensure data confidentiality. The proposed model improves energy efficiency in data transmission. Simulations showed good security with a slight increase in energy consumption of up to 7 % due to authentication overhead.
3. **Security threats and vulnerabilities.** Cybersecurity in precision agriculture was examined (Asif et al., 2021), identifying 58 potential threats using the Microsoft STRIDE model. In addition, mitigation suggestions were proposed to strengthen security in precision agriculture, laying the groundwork for future research in this field.

Security threats and vulnerabilities in digital agriculture were addressed (Alahmadi et al., 2022), focusing on specific side-channel attacks with a generic threat analysis through the proposed four-layer Digital agriculture (DigAg) model. Open research challenges and future directions were also discussed, highlighting the importance of addressing these issues from the early stages of developing and deploying digital technologies in agriculture.

4. **Cyber–physical systems.** A new threat model for cyber–physical systems (Valenza et al., 2023) has been presented that considers cyber, physical, and human aspects. In addition, a threat analysis method, implemented in the automatic tool TAMELESS, allowed to know the system components' security status and generate prevention/mitigation solutions. In addition, three case studies from different sectors corroborated the use of the model.
5. **DDoS.** A deep learning method was used to build the Convolutional Neural Network and Long Short-Term Memory (CNN-LSTM) model (Aldhyani and Alkahtani, 2023). The model achieved 100 % accuracy in detecting DDoS attacks in IoT-based Agriculture 4.0 networks using the CIC-DDDoS2019 dataset.
   The Enhanced Multiclass Support Vector Machine (EMSVM) model for DDoS attack detection in Agriculture 4.0 (Shaik et al., 2023) used Orthogonal Learning Chaotic Grey Wolf Optimization (OLCGWO) to improve attack detection on real data. In addition, it highlighted the importance of raising awareness of cyber threats among farmers and addressing the lack of resources in agricultural cybersecurity.
6. **IoT.** It explored security in smart farming systems and identified vulnerabilities and risks of cyber-attacks in IoT agriculture. For this, a security meta-model for IoT-based smart agriculture (Taji et al., 2023) with two certificate schemes (CBHA and SCKA) is proposed. The CBHA and SCKA schemes improved the security against various attacks. Security testing of the schemes confirmed the robustness of the proposed meta-model. In addition, continuous improvement of security in IoT systems was suggested.
7. **Cloud.** Rapid population growth increases the demand for agricultural products. Data-driven technologies can improve the quality and quantity of agricultural products. Hence, cybersecurity threats increase in smart farming environments, and cyber-attacks can compromise consumer safety and economic stability by remotely manipulating installed sensors and self-driving vehicles in crops. Hence, a real-time cybersecurity model has been proposed (Kuppusamy and Khang, 2024) for a high-tech, multi-cloud-based agricultural system to implement cybersecurity measures in all agricultural solutions.

4.2.6. *RQ6: What are the cybersecurity threats in smart agriculture?*

In the selected documents, we found cyber threats to smart agriculture and precision agriculture, a retro perspective study of cyber threats in India's agriculture, cyber threats in the agricultural, healthcare, and food sectors. The cyber threats found are presented below:

1. **Cyber threats.** The document (Yazdinejad et al., 2021) analyzed the security of smart agriculture and precision agriculture, highlighting the critical security aspects and studying the attacks that violate each of these security aspects. In addition, they presented cyber threats to smart agriculture and precision agriculture, resulting in a systematic taxonomy of these threats based on the cyber-attack chain.
   A retro perspective study of cyber threats in India's agriculture and food industry was conducted (Verma et al., 2023), considering that it contributes to its economy with food production, employment, and raw materials for industry, among other things. It was identified that most farmers need high-speed internet access and regular data backup. In addition, farmers needed to improve their farms' cybersecurity and understand its importance. Farmers generally give very little importance to the Internet and cybersecurity in India.
2. **Strategies.** The increase in cyber threats in the agricultural, healthcare, and food sectors was analyzed due to globalization, industrialization, and technologies (Usmani et al., 2023), which have made these sectors valuable targets for cybercriminals, considering the large amount of sensitive data. In addition, cyber threats, such as service interruption, reputational damage, and identity theft, were reviewed, taking into account their consequences. A number of strategies were also developed to help mitigate cyber threats, such as investment and training your employees in cybersecurity.

5. Discussion

This section is divided into two parts. In the first part, the bibliometric analysis of the selected documents is carried out. In the second part, the results of the selected documents are analyzed.

The bibliometric analysis determines the trend of agricultural cybersecurity research results in recent years. A significant increase in agricultural cybersecurity research is observed from 2020 to 2024. The documents analyzed in this SLR have been published in 30 journals, 21 conferences, 6 book chapters, and 1 book. The analysis yielded the following findings:

- **Author keyword cloud.** The four most prominent words in the author's keyword cloud are cybersecurity, agriculture, IoT, and network security.
- **Scientific production by year.** Of the 58 documents selected, it has been seen that the trend of publications has increased in the last two years: 16 documents published in 2024, and 14 documents in 2023.
- **Scientific production of the countries over time.** The authors have developed the documents from 21 countries. The three countries with the highest number of publications over time are the United States, the India, and United Kingdom.
- **Sources of publication.** The journals with the highest number of publications are Sensors (3 documents), Frontiers in Bioengineering and Biotechnology (2 documents), IEEE Access (2 documents), and Applied Sciences (2 documents).
- **Thematic map.** In the thematic map, we can see in the "Motor Themes" quadrant that the topics most developed in the selected documents are agricultural robots, network topology, AI, intrusion detection, machine-learning, cybersecurity, and agriculture.

The second part of the SLR answers the RQs. The first research question analyzes the challenges facing smart agriculture. The challenges have been classified into seven categories: challenges and trends, role and reflections of smart agriculture in economics, the IoT, smart agricultural machines, smart farm ontology, supply chain, and cyber insurance (see Appendix, Table A.1, for complete classification data). Fig. 8 shows the findings and gaps found.

The second research question analyzes the attacks and intrusion detection faced by smart agriculture. The attacks and intrusion detection have been classified into two categories: intrusion detection systems, and cyber-attacks (see Appendix, Table A.2, for complete classification data). Fig. 9 shows the findings and gaps found.

The third research question analyzes case studies applied to smart farming. The case studies have been classified into six categories: survey, network, supply chains, systems, testbed and methodology (see Appendix, Table A.3, for complete classification data). Fig. 10 shows the findings and gaps found.

The fourth research question looks at frameworks applied to smart agriculture. The frameworks have been classified into six categories: security approach to data flow, network security, IoT, smart agricultural

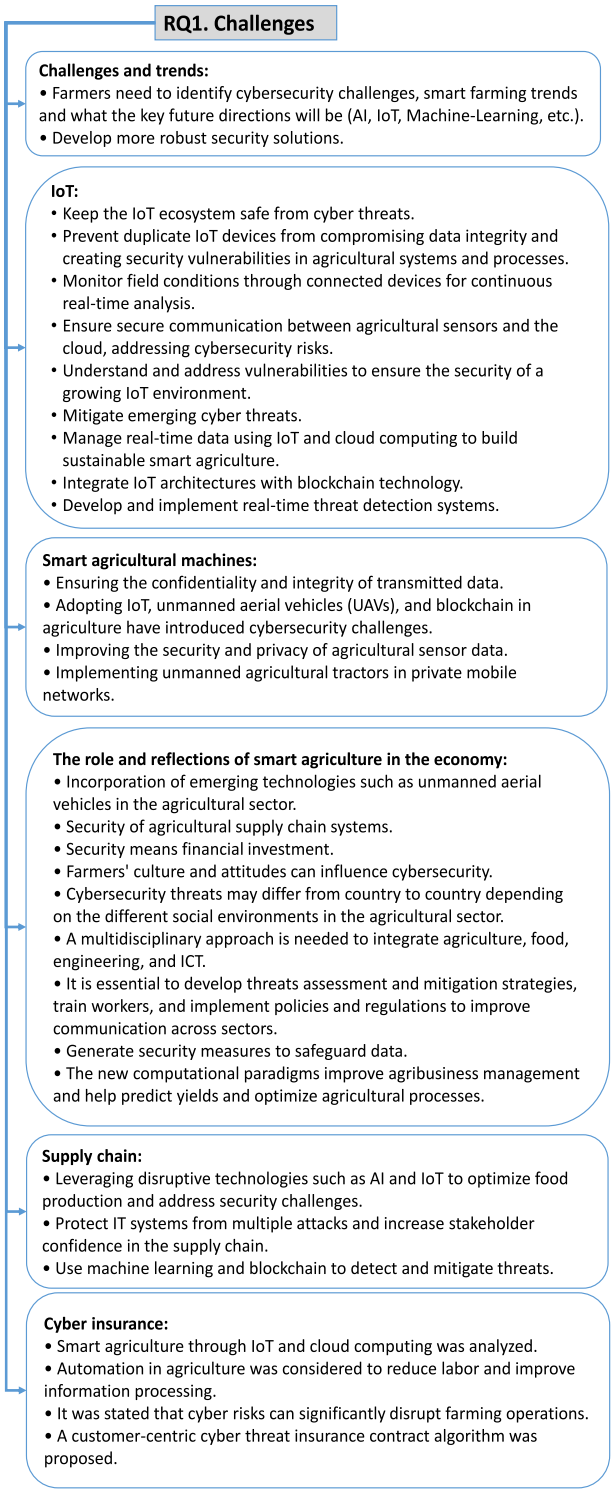

Fig. 8. Findings and gaps in cybersecurity challenges in smart agriculture.

machines, machine learning, and digital twin (see Appendix, Table A.4, for complete classification data). Fig. 11 shows the findings and gaps found.

Frameworks can help smart agriculture manage and reduce its cybersecurity risks. A research (Bissadu et al., 2024c) analyzed internal cyber threats and human factors with the National Institute of Standards and Technology (NIST) cybersecurity framework as a

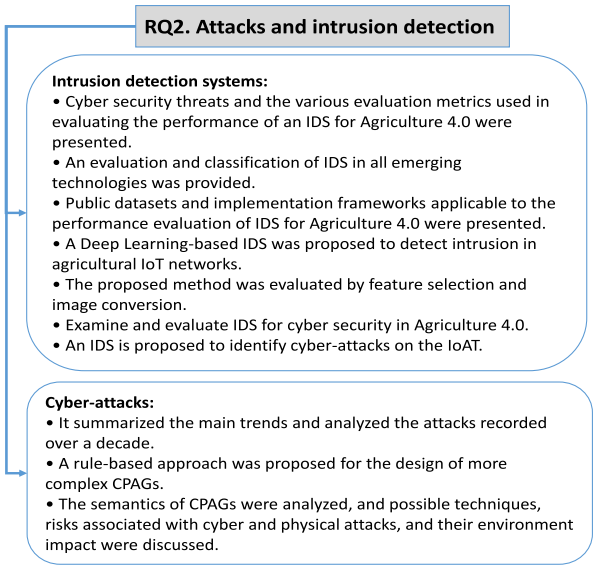

Fig. 9. Findings and gaps of attacks and intrusion detection systems on cybersecurity in smart agriculture.

recommended best practice in Agriculture 5.0. The recognized framework for managing and reducing cybersecurity risks (NIST, 2024; McIntosh et al., 2024) from NIST is the "Cybersecurity Framework (CSF)" (NIST Special Publication, 2024). NIST introduced CSF 2.0 in April 2022 (Rababah et al., 2024) based on years of industry feedback. The CSF 2.0 provides guidelines and best practices for managing and mitigating cybersecurity risks across all industries and organizational sizes. CSF 2.0 is organized into six Functions (Govern, Identify, Protect, Detect, Respond and Recover) and is composed of Core, Organizational Profiles and Tiers. Fig. 12 shows the structure of the CSF 2.0 and Fig. 13 shows its functions.

Another important aspect found is that no specific standards have been defined for the security areas of Information Technology/Operational Technology in agriculture (Kristen et al., 2021). For this reason, the currently well-established security standards for industrial control are also perfectly valid sources for agricultural applications. A recognized standard (Malatji, 2023) for information security management systems is ISO/IEC 27001:2022 "Information security, cybersecurity and privacy protection — Information security management systems — Requirements" (ISO, 2022). This standard could also be used in smart agriculture to protect the confidentiality, integrity and availability of information.

The fifth research question analyzes models applied to smart agriculture. The models have been classified into seven categories: image pattern recognition system, sensor network, security threats and vulnerabilities, cyber–physical systems (CPS), DDoS, IoT, and Cloud (see Appendix, Table A.5, for complete classification data). Fig. 14 shows the findings and gaps found.

An important finding is the STRIDE model (Asif et al., 2021). The STRIDE model acronym covers six threat categories, namely "Spoofing, Tampering, Repudiation, Information Disclosure, Denial of Service, and Elevation of Privilege". STRIDE is a systematic approach that analyzes cyber threats and vulnerabilities at the component level to ensure system-wide security (Khan et al., 2017a). Fig. 15 shows the STRIDE-based threat modeling methodology.

The document (Asif et al., 2021) also states that multiple models are available to perform cyber security threats assessment. Some existing models (Shevchenko et al., 2018) are listed below.

- Process for Attack Simulation and Threat Analysis (PASTA).
- Common Vulnerability Scoring System (CVSS).

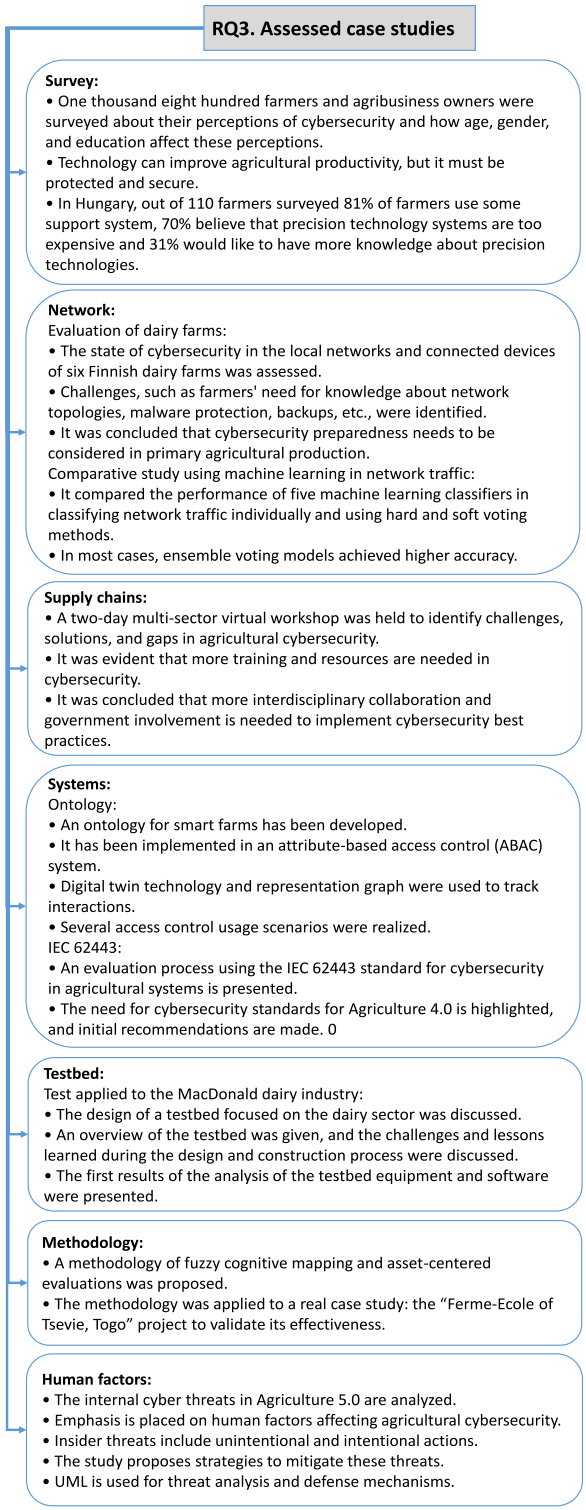

Fig. 10. Findings and gaps of case studies on cybersecurity in smart agriculture.

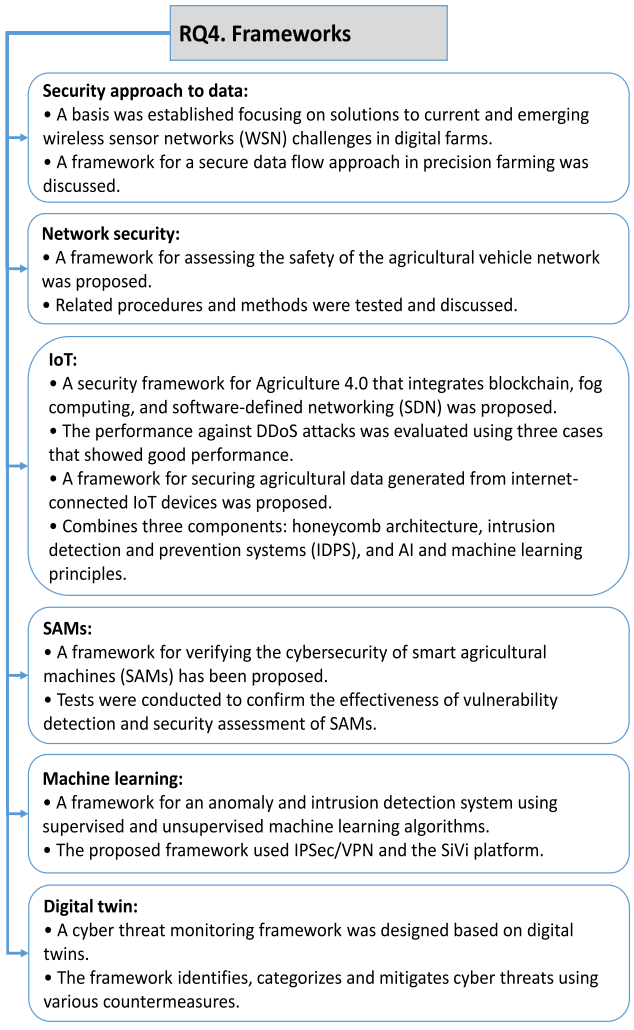

Fig. 11. Findings and gaps of frameworks on cybersecurity in smart agriculture.

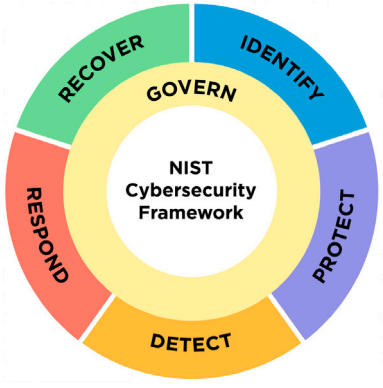

Fig. 12. Structure of the CSF 2.0 (NIST, 2024).

- Attack trees.
- Security Cards.
- Hybrid Threat Modeling Method (hTMM).
- Trike.
- Persona non Grata (PnG).
- LINDDUN (linkability, identifiability, nonrepudiation, detectability, disclosure of information, unawareness, noncompliance).
- Operationally Critical Threat, Asset, and Vulnerability Evaluation (OCTAVE).
- Quantitative Threat Modeling Method (Quantitative TMM).
- Visual, Agile, and Simple Threat (VAST) Modeling.

PASTA is an asset-centric approach (Badawy et al., 2024; Uceda Vélez and M. Morana, 2015) and a comprehensive threat modeling

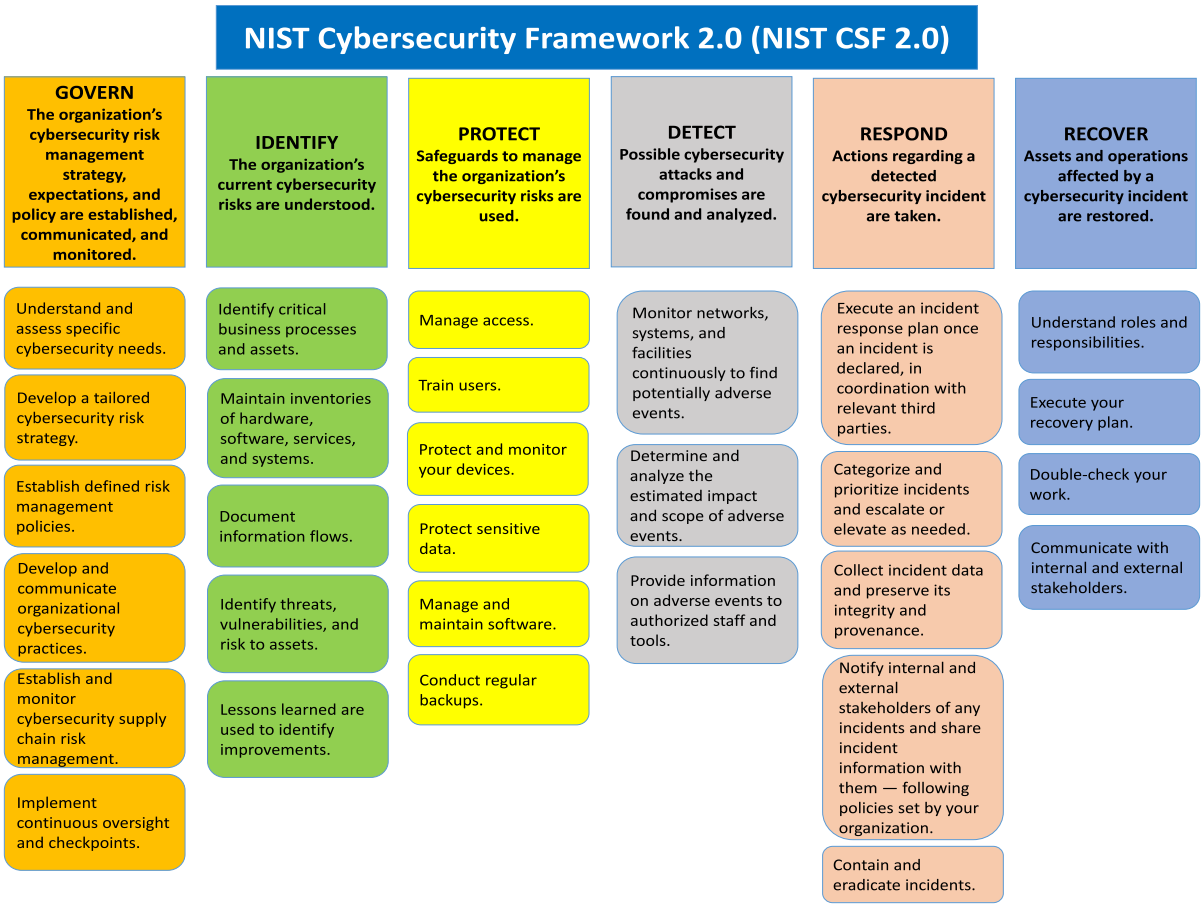

Fig. 13. Functions of the CSF 2.0 (NIST, 2024).

framework best suited for large, complex enterprises. In addition, PASTA is highly customizable, allowing agricultural organizations to tailor their threat modeling process to their needs. It also allows security specialists to collaborate with operational stakeholders to prioritize threats in the enterprise based on their impact. Fig. 16 shows the stages of the PASTA hazard modeling methodology.

The sixth research question analyzes the threats facing smart agriculture. The threats have been classified into one category: cyber threats, and human factors (see Appendix, Table A.6, for complete classification data). Fig. 17 shows the findings and gaps found.

Various cyberattacks or cyber threats applicable to the agricultural sector have been compiled. The five cyber attacks that stand out are malware, ransomware, Man-in-the-Middle, phishing, and spoofing. Table 6 presents the list of various cyberattacks or cyber threats applicable to agriculture.

The documents analyzed apply technological resources to cybersecurity in agriculture (AI, cloud computing, big data, IoT, AIoT, ICT, wireless networks, sensors, cyber–physical systems, digital twins, and digital platforms). The most used technological resource is IoT, which provides greater efficiency in production through smart agriculture. It consists of deploying high-tech systems that allow remote management through crop data networks thanks to the help of sensors that measure environmental and soil conditions (temperature, humidity, luminosity, and radiation, among others) (Ndjuluwa et al., 2023).

The evolution of agriculture has allowed the incorporation of software and hardware in its activities and processes to improve the efficiency of its production. The main findings found in the results of the analyzed documents when applying cybersecurity in agriculture are the need for more knowledge and resources (money, time). Nevertheless, it is of paramount importance to foster a culture of cybersecurity within the agricultural sector. This will enable avoiding various attacks, fraud, extortion, and other problems. For this purpose, personnel training through cybersecurity experts and allocating economic resources for its implementation are necessary. In addition, awareness helps protect the information systems, as a large part of the responsibility for defense lies with the end user. Also, the end-user must be sufficiently armed through cybersecurity education and training. Mitigation of cybersecurity issues in smart agriculture should focus on the protection of critical infrastructure (irrigation systems, pest control, intelligent environmental monitoring, etc.), security of sensitive data (financial information, production data, intellectual property records, unauthorized access, information leakage or alteration), supply chain threats (logistics, distribution and marketing), IoT device vulnerabilities (sensors, drones, robots, networks, etc.), awareness and training (phishing, social engineering and other common tactics) and regulatory frameworks (cybersecurity framework).

According to the United Nations (United Nations, 2022), "the world's population is expected to increase by 2 billion persons in the next 30 years, from 7.7 billion currently to 9.7 billion in 2050 and could peak at nearly 11 billion around 2100". Therefore, the challenge of adding agricultural production is becoming increasingly crucial for feeding the population. With the implementation of new computational paradigms, it will be possible to improve the profitability and effectiveness of agricultural production. However, agricultural companies must look for alternatives to automate their processes using appropriate cybersecurity measures to protect their hardware, software, and data that may compromise or risk their business.

6. Limitations of the study

An SLR can be affected by some limitations. One of them is bias in data collection by the authors. For this reason, this SLR starts by

Table 6
List of various cyber attacks or cyber threats applicable to the agriculture domain.

References	Cyber attack terminologies or cyber threats
Patel and Doshi (2019)	Attack vectors, viruses, malware, worms, trojans, ransomware, adware, zero-day vulnerabilities, stuxnet, exploit toolkit, botnet, Man-in-the-Middle (MITM), phishing and spoofing, side-channel, Denial of Service (DoS), Distributed Denial of Service (DDoS), RFID based.
Nikander et al. (2020)	Ransomware, viruses, worms, malware, botnets, keyloggers, rootkits, ARP spoofing, MITM attack, spyware, cache poisoning, DNS-redirecting, RIP attacks, SYN flooding, IP smurfing, address spoofing.
Kristen et al. (2021)	Unauthorized data access, data leakage, loss of know-how (IP) and production data, phishing, trojans, IP theft, spyware, causing physical damage to farming equipment, deterioration of product quality, ransomware, data manipulation, data destruction, loss of farming equipment availability, loss of production, deterioration of product quality, botnets, DDoS attacks, MITM attacks.
Peppes et al. (2021)	Neptune, satan, ipsweep, portsweep, smurf, nmap, back, teardrop, warezclient, pod, guess_passwd, buffer_overflow, warezmaster, land, imap, rootkit, loadmodule, ftp_write, multihop, phf, perl, spy.
Tariq et al. (2021)	Analysis of network traffic, routing attacks, spoofing of RFID/sensors, unauthorized access, selective forwarding attacks, internal attacks (e.g., blackhole, greyhole, Sybil), external attacks, MITM attack, DoS attacks, malware attacks (e.g., worms, adware, virus, spyware, trojan horses).
Yazdinejad et al. (2021)	Side-channel attack, RF jamming, DoS, MITM attacks, botnets, cloud computing attacks, data leakage, ransomware, cloud data leakage, false data injection, misconfiguration, software update attacks, malware injection, buffer overflow, indirect attacks (SQL injection), third party attacks, data fabrication, cyber-terrorism, invalidation and /compliance.
Agarwal et al. (2022)	DoS attack
Alahmadi et al. (2022)	Firmware alteration, side-channel attacks, eavesdropping, booting, physical damage, malicious code, forgery, sleep deprivation attacks, authentication, MITM, interference, firmware, routing, jamming, DoS/DDoS, sniffing attacks, SQL injection, data privacy, IP theft, encryption, cloud malware injection, misconfiguration, flooding attacks in the cloud, social engineering, phishing, access control, service interruption, insider attacks.
Ferrag et al. (2022)	DDoS+PortScan, botnet attacks, web attacks, DoS attacks, bruteforce attacks, data exfiltration attacks, keylogging, data theft, false control injection.
Hoffmann et al. (2022)	SQL injection, phishing (email containing malware), ransomware.
Priyadharshini and Balamurugan (2022)	Misinformation attack, false data injection attack, data leakage, malware injection attack, DoS attack, botnet attack, side-channel attack, service authentication, data fabrication attack, third party attack, supply chains attack, cloud attacks, private leakage, resource and service unavailability.
Arya et al. (2023)	Ransomware, DoS.
Balaji et al. (2023)	Reverse engineering, MITM attack, spoofing attack, DoS attack, physical tampering, false data injection (FDI), RF jamming, evil twin, password cracking, key reinstallation attack, side-channel attack, cloud computing attack.
Shaik et al. (2023)	DDoS attacks
Taji et al. (2023)	DoS attack, access attack, MITM attack, data theft attack, access control attack, sniffing attack, service interruption attack, false data injection attack, side channel attack, sleep deprivation attack, node capture attack, data transit attack, eavesdropping and interference.
Usmani et al. (2023)	Ransomware, phishing, malware, DoS attack, identity theft.
Verma et al. (2023)	Malware (ransomware, trojans, spyware, viruses, worms, keyloggers, bots), DoS attacks, phishing, spoofing, identity-based attacks, code injection attacks, supply chain attacks.
Bissadu et al. (2024a)	Sniffing attacks, spoof attacks, hardware/device manipulation attacks, DDoS attacks, sensitive data leakage, faults intolerance.
Eleftheriadis et al. (2024)	DoS attacks, replay attacks, trojan horse attacks.
Kaushik (2024)	RFID or sensors spoofing attacks, MITM attacks, routing protocols attacks, malware attacks, DoS attacks.
Quadri et al. (2024)	Bruteforce, web attack, DoS attack, DDoS attack, botnet, infiltration, benign, information gathering, information theft.
Vangipuram et al. (2024)	Data loss or theft, insecure interfaces, DoS attack, data Leakage, malware attacks, phishing attacks, ransomware attacks, internet anonymity, attack on middleware.
Zidi et al. (2024)	Bruteforce, command control, crypto ransomware, dictionary, xxfiltration, generic scanning, scanning Vul, RDoS, false data injection, discovering resources, reverse shell, MITM, TCP relay, fake notification, fuzzing, inside malicious, modbus register read, MQTT cloud sub.

creating customized search strings with keywords and replacement terms determined in the scope of the research. We customized the search strings and performed several preliminary searches of scientific databases to assess whether the retrieved data were relevant and refine the search string. In addition, exclusion and inclusion criteria were applied when selecting documents. Also, this SLR does not include discussions, prefaces, commentaries, panels, tutorial summaries, or workshop summaries.

Both authors participated in planning the SLR to identify the need for it and develop a review protocol. The first author applied the search

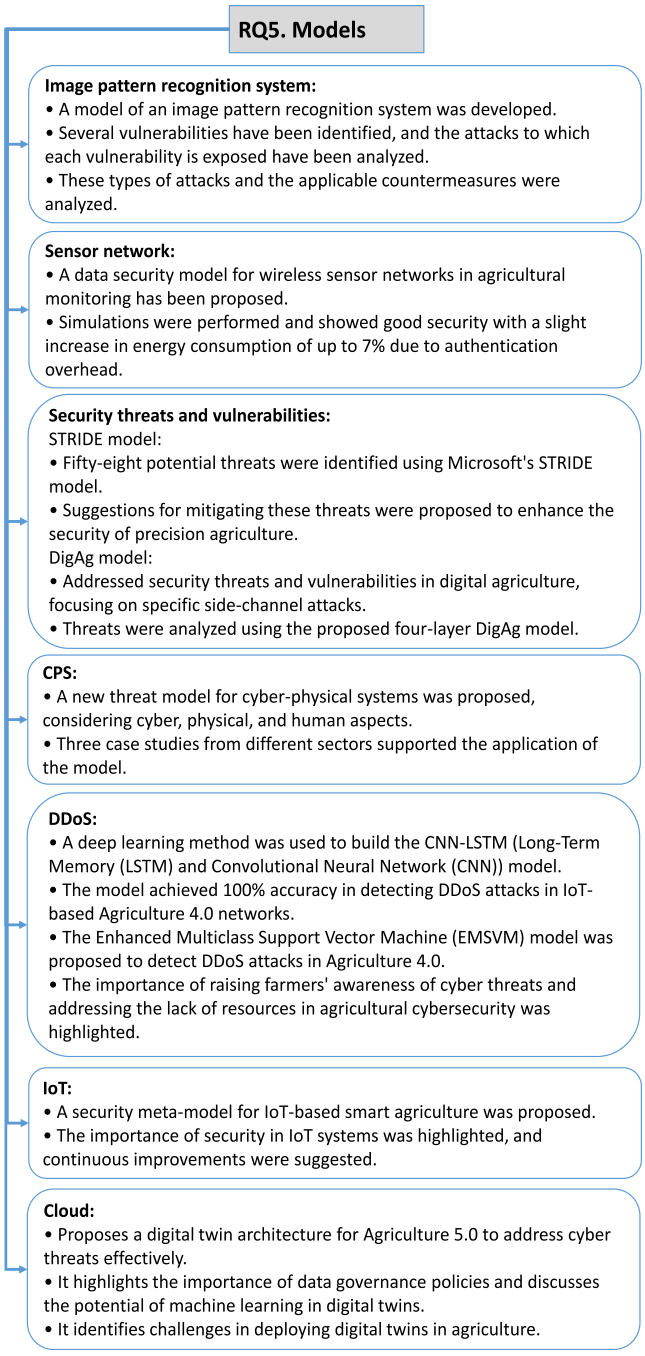

Fig. 14. Findings and gaps of models on cybersecurity in smart agriculture.

strings in the scientific databases and performed the data extraction, while the second author performed a second validation of the final results.

However, one limitation is that the query string created in the search process excludes some relevant documents. Although a well-structured and well-defined protocol is followed, there is no guarantee that all documents pertinent to this SLR will be retrieved.

Another significant limitation is that our SLR does not consider the Multivocal Literature Review (MLR) approach (Garousi et al., 2019). MLRs include gray literature such as blog posts, videos, white papers, etc., in their analysis. They summarize the state of the art and practice in a given area and are helpful for both researchers and practitioners.

Fig. 15. STRIDE-based threat modeling methodology (Khan et al., 2017a).

7. Conclusions and future work

The objective of this research was to conduct an SLR to identify, analyze, and consolidate existing findings on cybersecurity in smart agriculture. This study aimed to explore the challenges, attacks, detection methods, frameworks, and models associated with cybersecurity in smart agricultural systems. The research also sought to identify gaps in current knowledge, provide insights into emerging trends, and offer practical recommendations for enhancing cybersecurity practices in the agricultural sector, with the ultimate goal of aiding researchers, farmers, and agribusinesses in mitigating or preventing cyber threats. Of the 58 documents selected for analysis in this SLR, 23 documents contributed to RQ1 (Challenges), 6 documents contributed to RQ2 (Attacks and intrusion detection), 10 documents contributed to RQ3 (Assessed case studies), 7 documents contributed to RQ4 (Frameworks), 9 documents contributed to RQ5 (Models), and 3 documents contributed to RQ6 (Threats). The analyzed documents evaluate the authors' research across 21 countries. In summary, the results obtained are as follows:

- It provided an overview of digitization and bio/natural algorithms used in various areas of agricultural engineering to improve efficiency, reduce input costs, increase yields and improve environmental sustainability. These technologies have enabled better access to agricultural markets and products and improved agricultural products' management, safety, and quality. Challenges such as security and privacy remain in implementing these technologies, and further research, policy, and governance are needed to ensure their successful implementation.
- It provided an overview of the emerging field of cybersecurity, which combines cybersecurity and biosecurity to address the growing threats posed by malicious actors. They discussed the use of wireless sensor networks in agriculture, the requirements for cybersecurity in agricultural communication networks, the security architecture for swarms of autonomous vehicles, the role of cyberbiosecurity in agriculture, and the security measures for distributed control systems. In addition, machine learning-based solutions for intrusion detection, the cybersecurity threats and side-channel attacks targeting digital agriculture systems, and the need for cybersecurity in optimized and smart irrigation systems. It also discusses the need for secure protocols, access control, and further research into the security of these systems.
- An overview of IoT development and its security challenges was presented. They cover IoT's evolution, security technologies used to protect IoT devices, potential threats, mitigation strategies, and a host-based anomaly detection framework. These also present

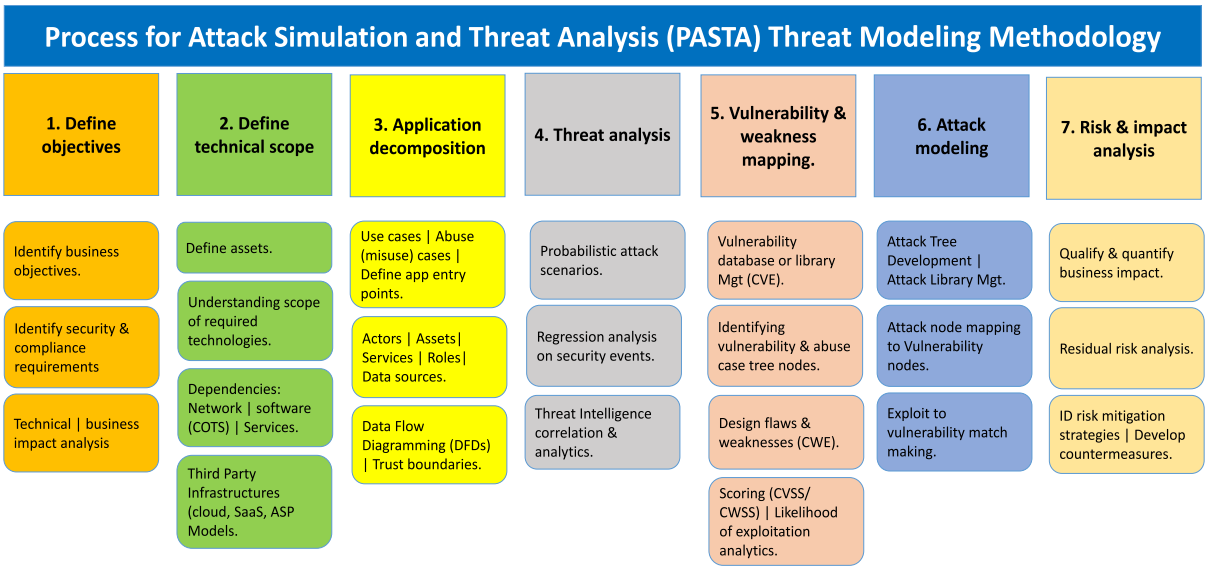

Fig. 16. Stages of the PASTA threat modeling methodology (Uceda Vélez and M. Morana, 2015).

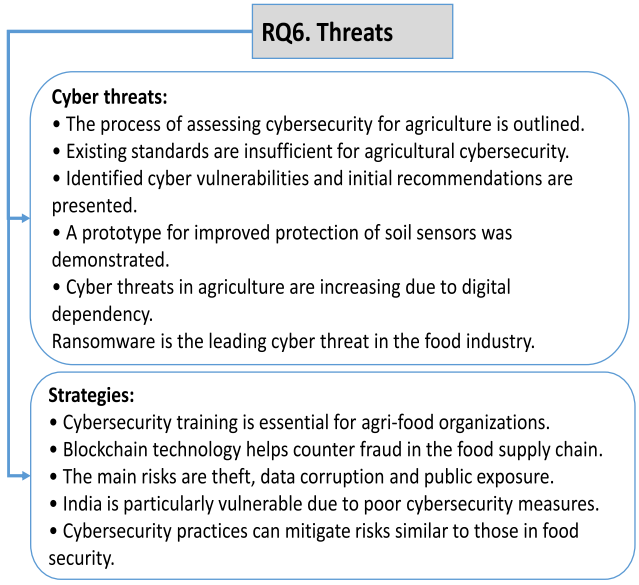

Fig. 17. Findings and gaps of threats on cybersecurity in smart agriculture.

a distributed misbehavior detection system, a lightweight random neural network-based attack detection scheme, an adaptive protection system, and an authentication scheme for IoT devices. Additionally, these cover the security issues associated with Agriculture IoT (AIoT) applications, an adaptive security technique for risk analysis, and the security considerations of an IoT-powered agricultural cyber–physical system. Finally, an overlook of the current status of crop robots in Europe and the challenges associated with their deployment is provided.

- The potential of big data analytics to provide valuable business insights was examined. They look at the various aspects of the field, including data mining, predictive analytics, and machine learning, and how these can be used to create value. This research also analyzes the challenges and opportunities of current methodologies, data integration issues, lack of standardization, privacy and security issues. This research conducts a case study in a large organization to illustrate how they successfully integrated big data analytics into their operations.
- Blockchain technology in food safety, traceability and sustainability was analyzed. These documents identify the potential benefits of blockchain technology, such as transparent and secure recording of transactions and more efficient and secure data management. The authors also examine the potential of combining blockchain technology with e-agricultural supply chain management, decentralized autonomous organizations (DAOs), and smart contracts to improve sustainability and food safety. In addition, they discussed the risks associated with blockchain technology, such as the potential for fraud, inequality in the food system, and the secure data transfer between drones, operators, and other stakeholders.
- It addressed the evolution of IoT technologies, their advantages and challenges, and proposed several security measures to protect them. An anomaly detection framework and a robust authentication scheme for IoT devices in the context of smart agriculture are proposed. Security issues associated with UAVs and a hybrid protocol for smart containers are also discussed. Finally, an overview of the security challenges associated with smart irrigation systems is provided.
- In the transition from Agriculture 4.0 to 5.0, digital twins play a very important role, encouraging the integration of current technologies and computational paradigms to improve productivity. However, as technology evolves, new cybersecurity challenges appear. For this reason, it is necessary to establish governmental norms, standards, frameworks, ontologies and models that facilitate the implementation of measures to mitigate cybersecurity threats and risks. These countermeasures must evolve along with the technology.

The results show that incorporating new computational paradigms and emerging technologies in agriculture provides farmers with data for decision-making on their land to make production more sustainable. However, new cyber risks emerge as technology gains a foothold in agricultural processes. Consequently, it is crucial for agricultural organizations to undertake periodic cybersecurity risk assessments in order to gain insight into their vulnerabilities and develop robust strategies to safeguard against cyber threats. Properly configured technology tools provide vital cybersecurity countermeasures to safeguard information in smart agriculture (Qadir and Quadri, 2016).

Smart agriculture, driven by IoT, big data, AI, and cloud computing technologies, is revolutionizing the agricultural industry. However, this transformation also brings new cybersecurity challenges that require immediate attention. Key research challenges include:

Table A.1
Data extraction for RQ1 sorted by year of publication and classification column.

References	RQ1 Challenges	Classification
Barreto and Amaral (2018)	The security challenges that Smart Farming systems face.	Challenges and trends
Sharma and Garg (2024)	Challenges, trends and future directions in cybersecurity.	
Duncan et al. (2019)	Assessment of critical cyber control points to strengthen cyberbiosecurity in U.S. food systems.	Smart agriculture in economic
Van der Linden et al. (2020)	The socio-cultural context in relation to food security and the use of digital technologies to optimize food production processes.	
Priyadharshini and Balamurugan (2022)	Unmanned Aerial Vehicle in the Smart Farming Systems.	
Arya et al. (2023)	Cybersecurity of key agriculture 4.0 technologies.	
Zelisko et al. (2024)	Impact of the digitization of the agricultural sector.	
Patel and Doshi (2019)	Cybersecurity challenges in the Internet of Things ecosystem.	IoT
Kristen et al. (2020)	"AFarCloud" project, which implements the AIoT concept.	
Bathalapalli et al. (2021)	Use of Physical Unclonable Functions (PUFs) to enhance cybersecurity in the agricultural sector, focusing on smart agriculture practices.	
Tariq et al. (2021)	Security Challenges in IoT Smart Applications.	
Kataev et al. (2024)	IoT architecture integrated with blockchain to improve data security in agricultural applications.	
Kaushik (2024)	Smart drone for real-time crop data management coupled with IoT and Cloud Computing.	
Morchid et al. (2024)	Real-time fire detection system adapted to smart agriculture uses IoT, integrated systems, a web application in Flask, and cybersecurity measures.	
Dutta et al. (2021)	Challenges in Precision Farming with Multiple Robots.	Smart agricultural machines
Heikkilä et al. (2022)	Implementation of Unmanned Farm Tractors in Private Mobile Networks.	
Balaji et al. (2023)	Cybersecurity Challenges and Solutions in IoT.	
Oussous et al. (2023)	Agricultural IoT based on greenhouse cybersecurity.	
Vangipuram et al. (2024)	CroPAiD that combines IPFS distributed storage and IOTA Tangle distributed ledger technology.	
Despoudi et al. (2021)	Agriculture 4.0 leverages disruptive technologies.	Supply chains
Vangipuram et al. (2023)	agroString 2.0.	
Leligou et al. (2024)	FISHY platform.	
Sitnicki et al. (2024)	Algorithm of cooperation between agricultural and insurance companies.	Cyber insurance

Table A.2
Data extraction for RQ2 sorted by year of publication and classification column.

References	RQ2 Attacks and intrusion detection	Classification
Ferrag et al. (2022)	Analysis of intrusion detection systems for Agriculture 4.0 cybersecurity.	Intrusion detection systems
El-Ghamry et al. (2023)	Deep Learning-based IDS for intrusion detection in agricultural IoT networks.	
Quadri et al. (2024)	Criteria for evaluating, classifying, and assessing IDS in cybersecurity in Agriculture 4.0 using ABCIS techniques.	
Zidi et al. (2024)	Intelligent IDS to identify cyber-attacks in the IoAT.	
Hoffmann et al. (2022)	Analysis of cyber-attacks and their main trends in agribusiness.	Cyber-attacks
Barrère et al. (2023)	Cyber–physical attack graphs.	

- Developing robust security technologies specifically for the agricultural context, including device authentication, real-time intrusion detection, and cyber-attack-resistant cryptography.
- Provide cybersecurity education and training to farmers and agricultural staff to increase their awareness of risks and best practices for protecting their systems and data.
- Foster collaboration between academia, industry, and government to establish standards and regulatory frameworks that clearly define cybersecurity responsibilities in smart agriculture.
- Create scalable, affordable, easy-to-deploy security solutions for small and medium-sized farmer businesses.
- Implement globally recognized frameworks (CSF 2.0, ISO/IEC 27001:2022, etc.) or models (STRIDE, PASTA, etc.) to manage, reduce, and mitigate cybersecurity attacks and threats in smart agriculture.

Introducing Digital Twin (DT) technology (Haloui et al., 2024) and new computational paradigms in farming practices has enabled the transition from Agriculture 4.0 to 5.0. DT technology aims to make farming practices more efficient and sustainable through intelligent, real-time data analysis. Agriculture 5.0 emphasizes precision, the introduction of new computational paradigms (advanced and emerging technologies), and sustainability to improve resource management and productivity in the agricultural sector (Symeonaki et al., 2024). To this end, the DTs contribute to remote monitoring, simulation, analysis, and optimization of processes, among other things (Escribà-Gelonch et al., 2024), through virtual replicas of physical agricultural systems. The application of DT technology in smart agriculture is multifaceted as it can be used for various purposes such as irrigation management, fertilization, pest control, crop growth modeling, simulation, and prediction through multiple scenarios (Kalyani et al., 2024) with

Table A.3
Data extraction for RQ3 sorted by year of publication and classification column.

References	RQ3 Assessed case studies	Classification
Geil et al. (2018)	Survey of farmers and farm business owners on their perception of cybersecurity.	Survey
Erdei-Gally and Vágány (2022)	Overview of the role and challenges of precision agriculture in Hungary.	
Nikander et al. (2020)	Evaluation of case studies on cybersecurity in agricultural communication networks on Finnish dairy farms.	Network
Peppes et al. (2021)	Security in Agriculture 4.0 with Network Traffic Classification through Machine Learning.	
Drape et al. (2021)	Assessing the role of cyberbiosecurity in agricultural supply chains.	Supply chains
Chukkapalli et al. (2020)	Creation of an smart farm ontology and implement Attribute Based Access Control (ABAC) system.	Systems
Kristen et al. (2021)	Evaluation with the IEC 62443 cybersecurity standard adapted to agricultural systems.	
Agarwal et al. (2022)	Testbed cybersecurity in smart dairy farming.	Testbed
Bissadu et al. (2024b)	Methodology of fuzzy cognitive mapping.	Methodology
Bissadu et al. (2024c)	Insider cyber threats and human factors in Agriculture 5.0.	Human factors

Table A.4
Data extraction for RQ4 sorted by year of publication and classification column.

References	RQ4 Frameworks	Classification
Chi et al. (2017)	Framework for a security approach to data flow in precision agriculture.	Security approach to data
Gaggero Battista et al. (2022)	Framework to evaluate the network security of automated agricultural vehicles.	Network security
Padhy et al. (2023)	Security framework for agriculture 4.0 that integrates blockchain, fog computing, and software-defined networking (SDN).	IoT
Vardhan et al. (2024)	Framework for securing agricultural data generated from Internet-connected IoT devices.	
Caviglia et al. (2023)	Framework for verifying the cybersecurity of smart agricultural machines (SAMs) using software defined radio (SDR).	SAMs
Eleftheriadis et al. (2024)	A novel framework for improving the security of smart agriculture using machine learning.	Machine learning
Bissadu et al. (2024a)	Digital twin framework for monitoring cyber threats in Agriculture 5.0.	Digital twin

Table A.5
Data extraction for RQ5 sorted by year of publication and classification column.

References	RQ5 Models	Classification
Straub (2018)	Model for a image pattern recognition system.	Image pattern recognition system
Prodanović et al. (2020)	Data security model for wireless sensor network in agricultural monitoring.	Sensor network
Asif et al. (2021)	Microsoft STRIDE model.	Security threats and vulnerabilities
Alahmadi et al. (2022)	Digital agriculture (DigAg) model.	
Valenza et al. (2023)	Threat model for cyber–physical systems.	CPS
Aldhyani and Alkahtani (2023)	CNN-LSTM (Long Short-Term Memory (LSTM) and Convolutional Neural Network (CNN)) model.	DDoS
Shaik et al. (2023)	EMSVM (Enhanced Multiclass Support Vector Machine) model for DDoS attack detection in Agriculture 4.0.	
Taji et al. (2023)	Meta-model for smart agriculture based on the IoT.	IoT
Kuppusamy and Khang (2024)	Real-time cybersecurity model for a multi cloud-based hi-tech farming system.	Cloud

Table A.6
Data extraction for RQ6 sorted by year of publication and classification column.

References	RQ6 Threats	Classification
Yazdinejad et al. (2021)	Cyber threats, attacks and countermeasures	Cyber threats
Verma et al. (2023)	Cyber threats in agriculture and food industry in India.	
Usmani et al. (2023)	Cyber threats in the health, agriculture and food sectors.	Strategies

different inputs. Advances in cloud computing and data analysis favor the implementation of DTs. However, it is challenging to implement them in rural areas that need a stable internet connection to integrate innovative technologies and its high costs (Rogachev et al., 2022). In conclusion, Agriculture 5.0, which integrates the DT technology, has a promising future in the agricultural sector (Warren and Thomas, 2023) through technologies such as IoT, machine learning, cyber–physical systems, AI, big data, robotics, and cloud computing.

It is crucial to acknowledge that the advent of novel computational paradigms, which facilitate the transition from Agriculture 4.0 to 5.0, also introduces a new set of cybersecurity challenges. Therefore, the use of cybersecurity in agriculture has become increasingly important in recent years as threats to the agricultural industry have grown. Cybersecurity measures help protect farmers and ranchers from cyberattacks, data breaches, and other malicious activities. This includes protecting against unauthorized access to farm operations, protecting data stored in the cloud, and ensuring secure communications between farmers and suppliers. Additionally, it is important to ensure the security of the IoT devices used on farms, as these can be vulnerable to cyberattacks. Cybersecurity measures also help protect against insider threats and ensure that critical agricultural systems are secure. Therefore, as future work, this SLR proposes to conduct real case studies using digital twin technology to analyze data from industrial IoT sensors in the cloud, cybersecurity risks, and cost. Another important factor of analysis is cybersecurity at the junction between society and the new human-centered computing paradigms, called Agriculture 6.0 (Catala-Roman et al., 2024). Also, future work should conduct a gray literature analysis, i.e., a MLR (Garousi et al., 2019) of the ethical use of new computational paradigms.

CRediT authorship contribution statement

Milton Campoverde-Molina: Writing – review & editing, Writing – original draft, Validation, Project administration, Methodology, Investigation, Formal analysis, Conceptualization. **Sergio Luján-Mora:** Writing – review & editing, Validation, Project administration, Methodology, Investigation.

Declaration of competing interest

The authors declare that they have no known competing financial interests or personal relationships that could have appeared to influence the work reported in this paper.

Appendix

Data collected. See Tables A.1, A.2, A.3, A.4, A.5, and A.6. The information in these tables will allow the reader to understand the results of the SLR. In addition, it details the challenges, attacks, and intrusion detection and evaluates case studies, frameworks, models, and threats applied to cybersecurity in smart agriculture.

Data availability

The manuscript contains a link to a repository in Mendeley (DOI: https://doi.org/10.17632/5ddfvwfj9p.1).

References

Adami, D., Ojo, M.O., Giordano, S., 2021. Design, development and evaluation of an intelligent animal repelling system for crop protection based on embedded edge-AI. IEEE Access 9, 132125–132139.

Agarwal, S., Rashid, A., Gardiner, J., 2022. Old MacDonald had a smart farm: Building a testbed to study cybersecurity in smart dairy farming. In: Proceedings of the 15th Workshop on Cyber Security Experimentation and Test. New York, USA, pp. 1–9.

Alahe, M.A., Wei, L., Chang, Y., Gummi, S.R., Kemeshi, J., Yang, X., Won, K., Sher, M., 2024. Cyber security in smart agriculture: Threat types, current status, and future trends. Comput. Electron. Agric. 226, 1–15.

Alahmadi, A.N., Rehman, S.U., Alhazmi, H.S., Glynn, D.G., Shoaib, H., Solé, P., 2022. Cyber-security threats and side-channel attacks for digital agriculture. Sensors 22 (9), Article 3520.

Aldhyani, T.H., Alkahtani, H., 2023. Cyber security for detecting distributed denial of service attacks in agriculture 4.0: deep learning model. Mathematics 11 (1), Article 233.

Arya, S., Tripathi, S., Srivastava, A., Aggarwal, S., Soni, N., Ansar, S.A., 2023. Double-edged agriculture 4.0: hodiernal expedient technologies and cyber-security challenges. In: Proceedings of International Conference on Contemporary Computing and Informatics. IC3I 2023, Gautam Buddha Nagar, India, pp. 313–320.

Asif, R.A., Hasan, K.F., Islam, Z., 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, Dhaka, Bangladesh, pp. 1–6.

Badawy, M., Sherief, N.H., Abdel-Hamid, A.A., 2024. Legacy ICS cybersecurity assessment using hybrid threat modeling—An oil and gas sector case study. Appl. Sci. 14 (18).

Balaji, S.R.A., Rao, S.P., 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, New York, USA, pp. 237–246.

Bar-Ilan, J., 2018. Tale of three databases: the implication of coverage demonstrated for a sample query. Front. Res. Metrics Anal. 3 (6).

Barrère, M., Hankin, C., O'Reilly, D., 2023. Cyber-physical attack graphs (CPAGs): Composable and scalable attack graphs for cyber-physical systems. Comput. Secur. 132 (103348).

Barreto, L., Amaral, A., 2018. Smart farming: cyber security challenges. In: 2018 International Conference on Intelligent Systems. IS, Funchal, Portugal, pp. 870–876.

Bathalapalli, V.K.V.V., Mohanty, S.P., Kougianos, E., Yanambaka, V.P., Baniya, B.K., Rout, B., 2021. A PUF-based approach for sustainable cybersecurity in smart agriculture. In: Proceedings - 2021 19th OITS International Conference on Information Technology. OCIT 2021, Bhubaneswar, India, pp. 375–380.

Berryhill, J., Heang, K.K., Clogher, R., McBride, K., 2019. Hello, World: Artificial intelligence and its use in the public sector. pp. 1–184, OECD Working Papers on Public Governance, No. 36.

Bissadu, K., Hossain, G., Vajpayee, P., 2024a. Agriculture 5.0 cybersecurity: monitoring agricultural cyber threats with digital twin technology. In: 2024 IEEE 5th World AI IoT Congress. AIIoT 2024, Seattle, WA, USA, pp. 252–258.

Bissadu, K., Hossain, G., Velagala, L.P., 2024b. A enhancing cybersecurity resilience for low-income farmers in developing nations: a fuzzy cognitive mapping approach. In: IEEE International Conference on Consumer Electronics. ICCE 2024, Las Vegas, NV, USA, pp. 1–6.

Bissadu, K., Hossain, G., Velagala, L.P., Sonko, S., 2024c. Analyzing insider cyber threats and human factors within the framework of agriculture 5.0. In: 12th International Symposium on Digital Forensics and Security. ISDFS 2024, San Antonio, TX, USA, pp. 1–5.

Blandford, D., 2011. The contribution of agriculture to green growth. Report OECD 1–36.

Boucher, P., 2020. Artificial Intelligence: How Does it Work, Why Does it Matter, and What We Can Do About it?. European Parliamentary Research Service, p. 64.

Bui, H.T., Aboutorab, H., Mahboubi, A., Gao, Y., Sultan, N.H., Chauhan, A., Parvez, M.Z., Bewong, M., Islam, R., Islam, Z., Camtepe, S.A., Gauravaram, P., Singh, D., Ali Babar, M., Yan, S., 2024. Agriculture 4.0 and beyond: Evaluating cyber threat intelligence sources and techniques in smart farming ecosystems. Comput. Secur. 140, 1–32.

Catala-Roman, P., Navarro, E.A., Segura-Garcia, J., Garcia-Pineda, M., 2024. Harnessing digital twins for agriculture 5.0: a comparative analysis of 3D point cloud tools. Appl. Sci. 14 (5).

Catteddu, D., Hogben, G., 2009. Cloud computing security risk assessment. Enisa (December), 1–125.

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

Chen, J., Yang, A., 2019. Intelligent agriculture and its key technologies based on internet of things architecture. IEEE Access 7, 77134–77141.

Chi, H., Welch, S., Vasserman, E., Kalaimannan, E., 2017. A framework of cybersecurity approaches in precision agriculture. In: Proceedings of the 12th International Conference on Cyber Warfare and Security. ICCWS 2017, Dayton, Ohio, USA, pp. 90–95.

Chukkapalli, S.S.L., Piplai, A., Mittal, S., Gupta, M., Joshi, A., 2020. A smart-farming ontology for attribute based access control. In: Proceedings - 2020 IEEE 6th Intl Conference on Big Data Security on Cloud, Big Data Security 2020, 2020 IEEE Intl Conference on High Performance and Smart Computing, HPSC 2020 and 2020 IEEE Intl Conference on Intelligent Data and Security, IDS 2020. Baltimore, MD, USA, pp. 29–34.

Cooke, P., Zhao, X., Yun, J.J., Kim, Y., 2019. The digital, quaternary or 4.0 web economy: aspects, effects and implications. Int. J. Knowl.-Based Dev. 10 (3), 193–212.

Costa, I., Riccotta, R., Montini, P., Stefani, E., de Souza Goes, R., Gaspar, M.A., Martins, F.S., Fernandes, A.A., Machado, C., Loçano, R., Larieira, C.L.C., 2022. The degree of contribution of digital transformation technology on company sustainability areas. Sustainability 14 (1), 1–27.

De Kleijn, M., Siebert, M., Huggett, S., 2019. Artificial Intelligence: How knowledge is created, transferred and used. In: Proceedings of the IFLA WLIC 2019. Athens, Greece, pp. 1–17.

Debdas, S., Chakraborty, S., Biswas, B., Mohapatra, S., Gupta, Y., Dutta, T., 2021. Smart farming using IoT and LoRaWAN. In: 2021 IEEE 2nd International Conference on Applied Electromagnetics, Signal Processing, & Communication. AESPC, Bhubaneswar, India, pp. 1–5.

Demestichas, K., Peppes, N., Alexakis, T., 2020. Survey on security threats in agricultural iot and smart farming. Sensors (Switzerland) 20 (22), 1–17.

Despoudi, S., Spanaki, K., Rodriguez-Espindola, O., Zamani, E.D., 2021. Agricultural Supply Chains and Industry 4.0: Technological Advance for Sustainability. Palgrave Macmillan Cham, pp. 1–101.

Drape, T., Magerkorth, N., Sen, A., Simpson, J., Seibel, M., Murch, R.S., Duncan, S.E., 2021. Assessing the role of cyberbiosecurity in agriculture: a case study. Front. Bioeng. Biotechnol. 9, Article 737927.

Duncan, S.E., Reinhard, R., Williams, R.C., Ramsey, F., Thomason, W., Lee, K., Dudek, N., Mostaghimi, S., Colbert, E., Murch, R., 2019. Cyberbiosecurity: a new perspective on protecting U.S. food and agricultural system. Front. Bioeng. Biotechnol. 7 (63), 1–7.

Dutta, A., Roy, S., Kreidl, O.P., Bölöni, L., 2021. Multi-robot information gathering for precision agriculture: current state, scope, and challenges. IEEE Access 9, 161416–161430.

El-Ghamry, A., Darwish, A., Hassanien, A.E., 2023. An optimized CNN-based intrusion detection system for reducing risks in smart farming. Internet Things (Netherlands) 22.

Eleftheriadis, C., Andronikidis, G., Kyranou, K., Pechlivani, E.M., Hadjigeorgiou, I., Batzos, Z., 2024. Machine learning for cybersecurity frameworks in smart farming. In: 28th International Conference on Information Technology. IT 2024, Zabljak, Montenegro, pp. 1–5.

Erdei-Gally, S., Vágány, J., 2022. Role of precision agriculture in food supply. Ukrainian Food J. 11 (3), 458–473.

Escribà-Gelonch, M., Liang, S., van Schalkwyk, P., Fisk, I., Long, N.V.D., Hessel, V., 2024. Digital twins in agriculture: orchestration and applications. J. Agric. Food Chem. 72 (19), 10737–10752.

Ferrag, M.A., Shu, L., Friha, O., Yang, X., 2022. Cyber security intrusion detection for agriculture 4.0: machine learning-based solutions, datasets, and future directions. IEEE/CAA J. Autom. Sin. 9 (3), 407–436.

Gaggero Battista, G., Fausto, A., Patrone, F., Marchese, M., 2022. A framework for network security verification of automated vehicles in the agricultural domain. In: 2022 26th International Conference Electronics. Palanga, Lithuania, pp. 1–5.

Gagliardi, G., Cosma, A.I.M., Marasco, F., 2022. A decision support system for sustainable agriculture: the case study of coconut oil extraction process. Agronomy 12 (1), Article 177.

Gagliardi, G., Lupia, M., Cario, G., Cicchello Gaccio, F., D'Angelo, V., Cosma, A.I.M., Casavola, A., 2021. An internet of things solution for smart agriculture. Agronomy 11 (11), Article 2140.

Garousi, V., Felderer, M., Mäntylä, M.V., 2019. Guidelines for including grey literature and conducting multivocal literature reviews in software engineering. Inf. Softw. Technol. 106, 101–121.

Geil, A., Sagers, G., Spaulding, A.D., Wolf, J.R., 2018. Cyber security on the farm: an assessment of cyber security practices in the United States agriculture industry. Int. Food Agribus. Manag. Rev. 21 (3), 317–334.

Goertzel, B., 2014. Artificial general intelligence: concept, state of the art, and future prospects. J. Artif. General Intell. 5 (1), 1–48.

Gusenbauer, M., Haddaway, N.R., 2020. Which academic search systems are suitable for systematic reviews or meta-analyses? Evaluating retrieval qualities of Google Scholar, PubMed, and 26 other resources. Res. Synth. Methods 11 (2), 181–217.

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

Heikkilä, M., Suomalainen, J., Saukko, O., Kippola, T., Lähetkangas, K., Koskela, P., Kalliovaara, J., Haapala, H., Pirttiniemi, J., Yastrebova, A., Posti, H., 2022. Unmanned agricultural tractors in private mobile networks. Network 2 (1), 1–20.

Hentea, M., 2008. Improving security for SCADA control systems. Interdiscip. J. Inf. Knowl. Manag. 3, 73–86.

Hoffmann, C., Haas, R., Bhimrajka, N., Penjarla, N.S., 2022. Cyberattacks in agribusiness. In: 42. GIL-Jahrestagung, Künstliche Intelligenz in der Agrar- und Ernährungswirtschaft. Gesellschaft für Informatik e.V., Bonn, pp. 117–122.

ISO, 2022. ISO/IEC 27001:2022 Information security, cybersecurity and privacy protection — Information security management systems — Requirements. [Online]. Available: https://www.iso.org/es/contents/data/standard/08/28/82875.html.

Büyükkı dık, S., 2022. A bibliometric analysis: a tutorial for the bibliometrix package in R using IRT literature. Eğitimde ve Psikolojide Ölçme ve değerlendirme Derg. 13, 164–193.

Kalyani, Y., Vorster, L., Whetton, R., Collier, R., 2024. Application scenarios of digital twins for smart crop farming through cloud–fog–edge infrastructure. Future Internet 16 (3).

Kataev, M., Bulysheva, L., Krupskiy, A., 2024. Blockchain-driven IoT solutions in agriculture. Syst. Res. Behav. Sci. 1–13.

Kaushik, K., 2024. Smart agriculture applications using cloud and IoT. In: Convergence of Cloud with AI for Big Data Analytics. John Wiley & Sons, Ltd, pp. 89–105, (Chapter 5).

Khan, R., McLaughlin, K., Laverty, D., Sezer, S., 2017a. STRIDE-based threat modeling for cyber-physical systems. In: 2017 IEEE PES Innovative Smart Grid Technologies Conference Europe, ISGT-Europe 2017 - Proceedings, vol. 2018-January, Turin, Italy, pp. 1–6.

Khan, S., Shakil, K.A., Alam, M., 2017b. Big data computing using cloud-based technologies, challenges and future perspectives. ArXiv, abs/1712.05233.

Kitchenham, B., 2004. Procedures for performing systematic reviews. Keele UK Keele Univ. 33, 1–33.

Kitchenham, B., Budgen, D., Pearl Brereton, O., 2011. Using mapping studies as the basis for further research – A participant-observer case study. Inf. Softw. Technol. 53 (6), 638–651.

Kitchenham, B., Pearl Brereton, O., Budgen, D., Turner, M., Bailey, J., Linkman, S., 2009. Systematic literature reviews in software engineering – A systematic literature review. Inf. Softw. Technol. 51 (1), 7–15.

Kjonas, K., Wangen, G., 2023. A survey on cyber security research in the field of agriculture technology. In: 2023 IEEE International Symposium on Technology and Society. ISTAS, Swansea, United Kingdom, pp. 1–8.

Kristen, E., Kloibhofer, R., Díaz, V.H., Castillejo, P., 2021. Security assessment of agriculture IoT (AIoT) applications. Appl. Sci. 11 (13), Article 5841.

Kristen, E., Kloibhofer, R., Hernández, V., 2020. Future cyber-security demands in modern agriculture. Ercim News (123), 37–38.

Kuppusamy, P., Khang, A., 2024. An advanced cybersecurity model for high-tech farming using machine learning approach. In: Agriculture and Aquaculture Applications of Biosensors and Bioelectronics. IGI Global, pp. 461–495, (Chapter 26).

Leligou, H.C., Lakka, A., Karkazis, P.A., Costa, J.P., Tordera, E.M., Santos, H.M.D., Romero, A.A., 2024. Cybersecurity in supply chain systems: the farm-to-fork use case. Electronics (Switzerland) 13 (1).

Van der Linden, D., Michalec, O.A., Zamansky, A., 2020. Cybersecurity for smart farming: socio-cultural context matters. IEEE Technol. Soc. Mag. 39 (4), 28–35.

López-Robles, J.-R., Guallar, J., Otegi-Olaso, J.-R., Gamboa-Rosales, N.-K., 2019. El profesional de la información (EPI): Bibliometric and thematic analysis (2006–2017). Profesional de la inf.Inf. Prof. 28 (4), 1–23.

Ma, L., Long, H., Zhang, Y., Tu, S., Ge, D., Tu, X., 2019. Agricultural labor changes and agricultural economic development in China and their implications for rural vitalization. J. Geograph. Sci. 29 (2), 163–179.

Maiti, M., Ghosh, U., 2021. Next generation internet of things in fintech ecosystem. IEEE Internet Things J.

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, Bangkok, Thailand, pp. 117–122.

McIntosh, T.R., Susnjak, T., Liu, T., Watters, P., Xu, D., Liu, D., Nowrozy, R., Halgamuge, M.N., 2024. From COBIT to ISO 42001: Evaluating cybersecurity frameworks for opportunities, risks, and regulatory compliance in commercializing large language models. Comput. Secur. 144, 103964.

Meijerink, G.W., Roza, P., 2007. The Role of Agriculture in Economic Development. (Markets, Chains and Sustainable Development; No. 4). Wageningen UR, [Online]. Available: https://edepot.wur.nl/690.

Moawia Mohammed, A.E., Ibrahim, M., Ibrahim, Q., Verna, V., Jeannette, P., Yuh-Shan, H., 2024. Pediatric cancer research trends and performance in Africa: A bibliometric analysis from 1991 to 2022. Pediatr. Hematol. Oncol. J. 9 (4), 211–218.

Mongeon, P., Paul-Hus, A., 2016. The journal coverage of Web of Science and Scopus: a comparative analysis. Scientometrics 106 (1), 213–228.

Morchid, A., Jebabra, R., Ismail, A., Khalid, H.M., El Alami, R., Qjidaa, H., Ouazzani Jamil, M., 2024. IoT-enabled fire detection for sustainable agriculture: A real-time system using flask and embedded technologies. Results Eng. 23, 1–14.

Müller, J., Dotzauer, V., Voigt, K.-I., 2017. Industry 4.0 and its impact on reshoring decisions of german manufacturing enterprises. In: Bode, C., Bogaschewsky, R., Eß ig, M., Lasch, R., Stölzle, W. (Eds.), Supply Management Research. Advanced Studies in Supply Management. Springer Gabler, Wiesbaden, pp. 165–179.

Ndjuluwa, L.N.P., Adebisi, J.A., Dayoub, M., 2023. Internet of things for crop farming: a review of technologies and applications. Commodities 2 (4), 367–381.

Nikander, J., Manninen, O., Laajalahti, M., 2020. Requirements for cybersecurity in agricultural communication networks. Comput. Electron. Agric. 179, 105776.

NIST, 2024. The NIST Cybersecurity Framework (CSF) 2.0. National Institute of Standards and Technology, [Online]. Available: https://doi.org/10.6028/NIST.CSWP.29.

NIST Special Publication, 2024. NIST Cybersecurity Framework 2.0: Resorce & Overview Guide. National Institute of Standards and Technology, [Online]. Available: https://doi.org/10.6028/NIST.SP.1299.

Oussous, S.A., Bajit, A., Achour, Y., Morino, I., Zejli, D., Elbouayadi, R., 2023. Applying computational intelligence, visual optimization tools, and synchronized PAYLOAD's handshaking to enhance greenhouses ECC cyber security-based agriculture IoT's properties. In: 2023 9th International Conference on Optimization and Applications. ICOA, AbuDhabi, United Arab Emirates, pp. 1–8.

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), 1–27.

Page, M.J., McKenzie, J.E., Bossuyt, P.M., Boutron, I., Hoffmann, T.C., Mulrow, C.D., Shamseer, L., Tetzlaff, J.M., Akl, E.A., Brennan, S.E., Chou, R., Glanville, J., Grimshaw, J.M., rn Hróbjartsson, A., Lalu, M.M., Li, T., Loder, E.W., Mayo-Wilson, E., McDonald, S., McGuinness, L.A., Stewart, L.A., Thomas, J., Tricco, A.C., Welch, V.A., Whiting, P., Moher, D., 2021. The PRISMA 2020 statement: An updated guideline for reporting systematic reviews. Int. J. Surg. 88 (105906), 1–9.

Pastor-Ramón, E., Herrera-Peco, I., Agirre, O., García-Puente, M., Morán, J.M., 2022. Improving the reliability of literature reviews: detection of retracted articles through academic search engines. Eur. J. Invest. Health Psychol. Educ. 12 (5), 458–464.

Patel, C., Doshi, N., 2019. Security challenges in IoT cyber world. In: Security in Smart Cities: Models, Applications, and Challenges. Springer International Publishing, Cham, pp. 171–191, (Chapter 8).

Peppes, N., Daskalakis, E., Alexakis, T., Adamopoulou, E., Demestichas, K., 2021. Performance of machine learning-based multi-model voting ensemble methods for network threat detection in agriculture 4.0. Sensors 21 (22), 1–17.

Petticrew, M., Roberts, H., 2008. Systematic Reviews in the Social Sciences: A Practical Guide. Wiley.

Piškur, B., Beurskens, A.J., Jongmans, M.J., Ketelaar, M., Norton, M., Frings, C.A., Hemmingsson, H., Smeets, R.J., 2012. Parents' actions, challenges, and needs while enabling participation of children with a physical disability: a scoping review. BMC Pediatr. 12 (1), 1–13.

Pivoto, D., Waquil, P.D., Talamini, E., Finocchio, C.P.S., Dalla Corte, V.F., de Vargas Mores, G., 2018. Scientific development of smart farming technologies and their application in Brazil. Inf. Process. Agric. 5 (1), 21–32.

Priyadharshini, S., Balamurugan, P., 2022. Unmanned aerial vehicle in the smart farming systems: types, applications and cyber-security threats. In: 2022 International Conference on Innovative Computing, Intelligent Communication and Smart Electrical Systems. ICSES, Chennai, India, pp. 1–9.

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

Pyingkodi, M., Thenmozhi, K., Nanthini, K., Karthikeyan, M., Palarimath, S., Erajavignesh, V., Bala Ajith Kumar, G., 2022. Sensor based smart agriculture with IoT technologies: a review. In: 2022 International Conference on Computer Communication and Informatics. ICCCI, Coimbatore, India, pp. 1–7.

Qadir, S., Quadri, S., 2016. Information availability: an insight into the most important attribute of information security. J. Inf. Secur. 7, 185–194.

Quadri, N.S., Durga Charan, Y.K., Babu, K.S., Tanveer, S., Reddy, K.S.S., Kumar, M.K., 2024. Intrusion detection system for cyber security in smart agriculture with ABCIS techniques. J. Theoret. Appl. Inf. Technol. 102 (10), 5301–5315.

Rababah, A.A.A., Dash, B.B., Syed, A.H., Barik, L., Rout, S., Tembo, S., Lubobya, C., Patra, S.S., 2024. NIST CSF-2.0 compliant GPU shader execution. Eng. Technol. Appl. Sci. Res. 14 (4), 15187–15193.

Rehman, A., Saba, T., Kashif, M., Fati, S.M., Bahaj, S.A., Chaudhry, H., 2022. A revisit of internet of things technologies for monitoring and control strategies in smart agriculture. Agronomy 12 (1), Article 127.

Rogachev, A.F., Skiter, N.N., Ketko, N.V., Simonov, A.B., Makarevich, I.V., 2022. Digital twins as a tool for systemic integration of innovative digital technologies in agriculture. IOP Conf. Ser.: Earth Environ. Sci. 1069 (1), 012042.

Rose, K., Eldridge, S., Chapin, L., 2015. The Internet of Things (IoT): An Overview. Internet Society, [Online]. Available: https://n9.cl/3ip04.

Said Mohamed, E., Belal, A., Kotb Abd-Elmabod, S., El-Shirbeny, M.A., Gad, A., Zahran, M.B., 2021. Smart farming for improving agricultural management. Egypt. J. Remote Sens. Space Sci. 24 (3, Part 2), 971–981.

Samoili, S., Lopez Cobo, M., Gomez Gutierrez, E., De Prato, G., Martinez-Plumed, F., Delipetrev, B., 2020. AI WATCH. Defining Artificial Intelligence. EUR 30117 EN, Publications Office of the European Union, Luxembourg.

Santiteerakul, S., Sopadang, A., Yaibuathet Tippayawong, K., Tamvimol, K., 2020. The role of smart technology in sustainable agriculture: a case study of wangree plant factory. Sustainability 12 (11), Article 4640.

Shahbazi, K., Ko, S.-B., 2021. Area-efficient nano-AES implementation for internet-of-things devices. IEEE Trans. Very Large Scale Integr. (VLSI) Syst. 29 (1), 136–148.

Shaik, K.S., Thumboor, N.S.K., Veluru, S.P., Bommagani, N.J., Sudarsa, D., Muppagowni, G.K., 2023. Enhanced SVM model with orthogonal learning chaotic grey wolf optimization for cybersecurity intrusion detection in agriculture 4.0. Int. J. Saf. Secur. Eng. 13 (3), 509–517.

Sharma, A., Garg, K.D., 2024. Cybersecurity challenges, trends, and future directions for smart agriculture. In: Intelligent Security Solutions for Cyber-Physical Systems. CRC Press, pp. 246–265.

Shevchenko, N., Chick, T.A., O'Riordan, P., Scanlon, T.P., Woody, C., 2018. Threat modeling: a summary of available methods. Softw. Eng. Inst.| Carnegie Mellon Univ. 1–24.

Silva Megeto, G.A., Da Silva, A.G., Fernandes Bulgarelli, R., Fabiel Bublitz, C., Cavalcante Valente, A., Guerra da Costa, D.A., 2020. Artificial intelligence applications in the agriculture 4.0. Rev. Ciencia Agron. 51, 1–8.

Singh, V.K., Singh, P., Karmakar, M., Leta, J., Mayr, P., 2021. The journal coverage of Web of Science, Scopus and Dimensions: A comparative analysis. Scientometrics 126 (6), 5113–5142.

Sitnicki, M.W., Prykaziuk, N., Ludmila, H., Pimenowa, O., Imbrea, F., Şmuleac, L., Paşcalău, R., 2024. Regional perspective of using cyber insurance as a tool for protection of agriculture 4.0. Agriculture (Switzerland) 14 (2), 1–17.

Slobodan, A., 2018. Digitalization in agriculture: digital revolution in agriculture – industry 4.0. In: XII. International Conference on Logistics in Agriculture 2018: Conference Proceedings. Novo mesto, Slovenia, pp. 53–68.

Soni, R., Ambalkar, S., Bansal, P., 2016. Security and privacy in cloud computing. In: 2016 Symposium on Colossal Data Analysis and Networking. CDAN, Indore, India, pp. 1–6.

Srivastava, V., Debnath, S.K., Stănică, P., Pal, S.K., 2021. A multivariate identity-based broadcast encryption with applications to the internet of things. Adv. Math. Commun. Advance online publication.

Straub, J., 2018. Cybersecurity considerations for image pattern recognition applications. AIPR, In: 2018 IEEE Applied Imagery Pattern Recognition Workshop, vol. 2018-October, Washington, USA, pp. 1–6.

Symeonaki, E., Maraveas, C., Arvanitis, K.G., 2024. Recent advances in digital twins for agriculture 5.0: applications and open issues in livestock production systems. Appl. Sci. 14 (2).

Taji, K., Elkhalyly, B., Taleb Ahmad, Y., Ghanimi, I., Ghanimi, F., 2023. Securing smart agriculture: proposed hybrid meta-model and certificate-based cyber security approaches. Data Metadata 2.

Talaviya, T., Shah, D., Patel, N., Yagnik, H., Shah, M., 2020. Implementation of artificial intelligence in agriculture for optimisation of irrigation and application of pesticides and herbicides. Artif. Intell. Agric. 4, 58–73.

Tariq, N., Khan, F.A., Asim, M., 2021. Security challenges and requirements for smart internet of things applications: a comprehensive analysis. Procedia Comput. Sci. 191, 425–430, The 18th International Conference on Mobile Systems and Pervasive Computing (MobiSPC), The 16th International Conference on Future Networks and Communications (FNC), The 11th International Conference on Sustainable Energy Information Technology.

Thong-un, N., Wongsaroj, W., 2022. Productivity enhancement using low-cost smart wireless programmable logic controllers: A case study of an oyster mushroom farm. Comput. Electron. Agric. 195, Article 106798.

Tricco, A., Lillie, E., Zarin, W., O'Brien, K., Colquhoun, H., Levac, D., Moher, D., Peters, M., Horsley, T., Weeks, L., Hempel, S., Akl, E., Chang, C., McGowan, J., Stewart, L., Hartling, L., Aldcroft, A., Wilson, M., Garritty, C., Lewin, S., Godfrey, C., Macdonald, M., Langlois, E., Soares-Weiser, K., Moriarty, J., Clifford, T., Tunçalp, Ö., Straus, S., 2018. PRISMA extension for scoping reviews (PRISMA-scr): checklist and explanation. Ann. Internal Med. 169 (7), 467–473.

Uceda Vélez, T., M. Morana, M., 2015. Risk centric threat modeling: process for attack simulation and threat analysis. John Wiley & Sons, Hoboken, New Jersey, USA, pp. 1–693.

United Nations, 2022. Population. United Nations, [Online]. Available: https://www.un.org/en/global-issues/population.

Usmani, M.A., Usmani, K.A., Kaleem, A., Samiuddin, M., 2023. Cyber threat migration: perpetuating in the healthcare sector and agriculture and food industries. In: Advances in Cyberology and the Advent of the Next-Gen Information Revolution. IGI Global, pp. 62–85.

Valenza, F., Karafili, E., Steiner, R.V., Lupu, E.C., 2023. A hybrid threat model for smart systems. IEEE Trans. Dependable Secur. Comput. 20 (5), 4403–4417.

Vangipuram, S.L.T., Mohanty, S.P., Kougianos, E., 2023. agroString 2.0: A distributed-ledger based smart agriculture framework to ensure transparency in food delivery. In: 21st International Conference on Information Technology, Proceedings. OCIT 2023, Raipur, India, pp. 444–449.
Vangipuram, S.L.T., Mohanty, S.P., Kougianos, E., 2024. CroPAiD: protection of information in agriculture cyber-physical systems using distributed storage and ledger. In: Internet of Things. Advances in Information and Communication Technology. Springer, Cham, pp. 375–394.
Vardhan, R., Kumar, R., Supraja, P., 2024. Intelligent fortification of agricultural data integrity. In: Proceedings of the 2nd IEEE International Conference on Networking and Communications 2024. ICNWC 2024, Chennai, India, pp. 1–8.
Verma, H.C., Srivastava, S., Ahmed, T., Usmani, N.A., 2023. Cyber threats in agriculture and the food industry: an indian perspective. In: Advances in Cyberology and the Advent of the Next-Gen Information Revolution. IGI Global, pp. 109–122.
Warren, P., Thomas, N., 2023. Digital twins in agriculture: a state-of-the-art review. Smart Agric. Technol. 3, 100094.
Yazdinejad, A., Zolfaghari, B., Azmoodeh, A., Dehghantanha, A., Karimipour, H., Fraser, E., Green, A.G., Russell, C., Duncan, E., 2021. A review on security of smart farming and precision agriculture: security aspects, attacks, threats and countermeasures. Appl. Sci. 11 (16).
Zanoon, N., Al-Haj, A., Khwaldeh, S.M., 2017. Cloud computing and big data is there a relation between the two: a study. Int. J. Appl. Eng. Res. 12 (17), 6970–6982.
Zelisko, N., Raiter, N., Markovych, N., Matskiv, H., Vasylyna, O., 2024. Improving business processes in the agricultural sector considering economic security, digitalization, risks, and artificial intelligence. Ekonomika APK 31 (3), 10–21.
Zhang, J., Yu, Q., Zheng, F., Azad, C.L., Lu, Z., Duan, Z., 2016. Comparing keywords plus of WOS and author keywords: A case study of patient adherence research. J. Assoc. Inf. Sci. Technol. 67 (4), 967–972.
Zhu, Y., Wang, M., Yin, X., Zhang, J., Meijering, E., Hu, J., 2023. Deep learning in diverse intelligent sensor based systems. Sensors 23 (1), 1–86.
Zidi, K., Ben Abdellafou, K., Aljuhani, A., Taouali, O., Harkat, M.F., 2024. Novel intrusion detection system based on a downsized kernel method for cybersecurity in smart agriculture. Eng. Appl. Artif. Intell. 133, 1–12.

Milton Campoverde-Molina received a Ph.D. degree in Information and Communication Technologies from the Department of Mathematics and Computer Science, University of the Balearic Islands, in Spain, in 2022, the Master's degree in Evaluation and Audit of Technological Systems from the University of the Armed Forces - ESPE (Ecuador), in 2015, the Master's degree in University Teaching from the University of the Armed Forces - ESPE (Ecuador), in 2014, the title of Systems Engineering from the Catholic University of Cuenca (Ecuador), in 2009. He is a tenured professor of the Academic Unit of Informatics, Computer Science, and Technological Innovation at the Catholic University of Cuenca (Ecuador). In recent years, he has been involved in web accessibility research. He authorizes chapters of books and articles published in several conferences and journals. His main research topics include Web Accessibility, Education, and Software Engineering.

Sergio Luján-Mora received a Ph.D. degree in computer engineering from the Department of Software and Computing Systems, University of Alicante, in Spain, in 2005 and a Computer Science and Engineering degree from the University of Alicante, in 1998. He is currently a Senior Lecturer with the Department of Software and Computing Systems, University of Alicante. In recent years, he has focused on elearning, massive open online courses (MOOCs), open educational resources (OERs), and the accessibility of video games. He is the author of several books, and many published articles in various conferences, including ER, UML, and DOLAP, and high-impact journals, including DKE, JCIS, JDBM, JECR, JIS, JWE, IJEE, and UAIS. His main research interests include web applications and web development, and web accessibility and usability.