Computers & Security 162 (2026) 104790

Contents lists available at ScienceDirect

Computers & Security

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

Systematic mapping study to assess security landscape for IoT-based smart farming systems

Farzana Zahid [a,*], Xiao Chen [b], Shaleeza Sohail [b], Boyang Li [c], Melanie Po-Leen Ooi [d]

[a] School of Computing and Mathematical Sciences, University of Waikato, Hamilton, New Zealand
[b] School of Information and Physical Sciences, University of Newcastle, Sydney, NSW, Australia
[c] School of Engineering, University of Newcastle, Callaghan, NSW, Australia
[d] School of Engineering, University of Waikato, Hamilton, New Zealand

ARTICLE INFO

Keywords:
Cybersecurity
IoT
Smart farming
Machine learning
Systematic mapping study
Technology readiness level
ISO/IEC 25010

ABSTRACT

Smart farming systems sit at the intersection between three rapidly and independently advancing fields of IoT, Security, and Machine Learning. Its full realisation has tremendous positive impacts on food production; yet agricultural settings come with unique challenges that inhibit the rapid deployment of such state-of-the-art technologies. In this paper, we systematically study the current state of security for IoT-based smart farming research and development landscape and assess the proposed security solutions through the lens of technology readiness levels (TRL) and ISO/IEC 25010 security product evaluation framework. By analysing forty-eight primary studies, we identified the top security technologies under development, the critical security threats being addressed, and the most popularly used machine learning-based security solutions. Furthermore, we found that most of the ISO/IEC 25010 security characteristics considered by the security solutions are currently below TRL 6, indicating that they are well below the deployment readiness levels. Therefore, we recommend several supporting transitional technologies be developed to move the prototype development towards system validation and deployment to avoid the technology "valley of death", such as farming-specific intrusion detection public datasets and large-scale IoT agriculture testbeds to validate the interoperability and transparency of security solutions at different layers. This systematic mapping study, together with a TRL assessment and ISO 25010 standard mapping, is the first of its kind, intending to provide a standardised comparison of the current state of security technologies for IoT-based smart farms to define a clear roadmap for future research and development. It provides a common terminology for the multidisciplinary stakeholders of smart farming to distinguish between theoretical security concepts and ready-to-deploy solutions, facilitating crucial decisions for investment, deployment, and commercialisation.

1. Introduction

Agriculture or farming is the most fundamental business that greatly benefits humanity and boosts a country's economy. Recent advancements and trends in agriculture-related technology, specifically with the introduction of the Industrial Internet of Things (IIoT), autonomous systems such as drones, robotics, computer imaging, and predictive analysis by machine learning algorithms, have revolutionised farming productivity, efficiency, sustainability, and reduced operational cost (Carvalho et al., 2025; Sarowa et al., 2023; Vangala et al., 2023; Wolfert et al., 2017). Integrating these advanced technologies into agriculture and their use in various ways, from real-time monitoring of crop health and soil humidity to controlling operations like irrigation and fertigation, is the backbone of Smart Farming (SF) or Smart Agriculture (SA) (Ali et al., 2024; Boursianis et al., 2022; Shaikh et al., 2022).

Although a wider array of technologies employed has increased operational benefits, they have also extended the attack surfaces (immediate attack entry points such as connected devices or components) and threat landscape in SF. The vulnerabilities or weaknesses in a target SF system (device or component), such as a lack of appropriate or weak security measures, resource-constrained nature, and outdated technology stack, result in high-impact risks such as operational discontinuity, financial losses, or data breaches (Vangala et al., 2023; Carvalho et al., 2025). Real-world incidents like in New Zealand (2019), disabled pest control systems allowed fruit flies to enter the country undetected, and, in 2020, a data breach in Fonterra revealed information about several thousand personnel exemplifies these risks (Bui et al., 2024).

These incidents also illustrate the attack surfaces associated with the multi-layered architecture of SF (Gupta et al., 2020) as the attack on the component of one layer (e.g., an attack on the field sensor) could directly

* Corresponding author.

https://doi.org/10.1016/j.cose.2025.104790
Received 18 June 2025; Received in revised form 21 October 2025; Accepted 26 November 2025
Available online 3 December 2025

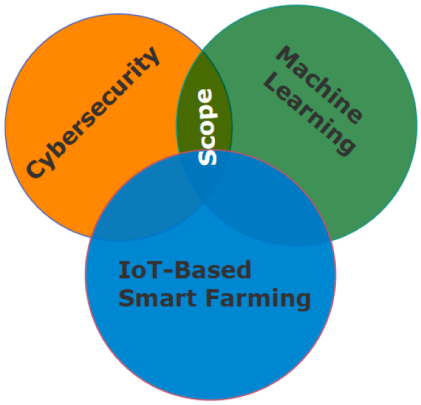

Fig. 1. Scope of Mapping Study.

or indirectly impact the cross-layer systems (such as cloud-based control platforms). These cross-layer cyberattacks present distinct security challenges for SF systems and are critical in addition to traditional cyberattacks. Moreover, SF systems are deployed in remote and sometimes harsh decentralised environments, where maintaining secure communications and data integrity is particularly challenging.

As SF systems become increasingly ubiquitous, the growing concerns surrounding the security vulnerabilities in the smart farming ecosystem, previously given less attention and under-explored, are now moving to the forefront. These concerns are further increasing due to the unique operational and environmental challenges these systems face, such as harsh rural environments, diverse farming conditions, unpredictable weather, low profit margins, resistance to technology adoption, and data overload (Demestichas et al., 2020). The time has come to critically evaluate the extent to which these cybersecurity issues have been addressed and to highlight areas that require further exploration within IoT-based SF. This evaluation must be based on a comprehensive and systematic approach to ensure that it is reproducible for fair future comparisons of security developments in Smart Farming.

This paper presents a Systematic Mapping Study (SMS) for identifying and analysing the body of literature on the security of SF with a particular focus on the intersection of cybersecurity, machine learning, and IoT-based smart farming (Fig. 1). **Please note, the terms SF systems and IoT-based SF systems are used interchangeably in this paper**. A total of 1903 papers were identified initially, of which 48 primary studies were selected and reviewed through the protocol described in Section 2. The major findings of the SMS are presented by highlighting key security technologies, contemporary evaluation of the selected primary studies, and their categorisation by potential security threats, ML-based security solutions, secure SF layers, publication years, utilised datasets, and proof of concepts. These findings help us to identify the research gaps and the most critical areas that require further investigation. Moreover, the results highlight the need for globally recognised frameworks, such as ISO/IEC 25010 and Technology Readiness Level (TRL), to provide both operational and strategic perspectives, which are especially useful to advance technology from research towards commercialisation and real-world adoption.

The ISO/IEC 25010 is a global standard for evaluating a system's quality based on the interested stakeholders' needs (International Organization for Standardization, 2023). One of the significant characteristics of this standard is *security*, which includes sub-characteristics such as confidentiality, integrity, non-repudiation, accountability, authenticity, and resistance (Fig. 2).

While ISO/IEC 25010 evaluates the system quality, it is significant to understand how ready these systems are for deployment. Technology readiness level (TRL) is a global technology maturity framework to evaluate and communicate the levels of development of technology from TRL 1 (basic research) to TRL 9 (system proven and ready for full

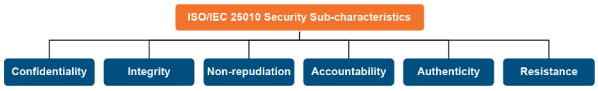

Fig. 2. ISO/IEC Security Sub-Characteristics.

Fig. 3. Technology Readiness Levels (TRL) (Bruno et al., 2020).

commercial deployment), shown in Fig. 3 (Mankins et al., 1995). TRL assesses the maturity of a technology using nine measurement scales, which provide a common understanding of a particular technology for academic and industrial practitioners.

Therefore, another significant contribution of this study is to map the security aspects mentioned in the primary studies against the security characteristics in the ISO/IEC 25010 standard and to assess the maturity of the proposed solutions using TRL. To the best of our knowledge (evidenced by an analysis of published secondary works in Table 2), this specific combination of security evaluation and TRL assessment in SF has not been covered by any existing secondary studies. A few studies (Vardhani et al., 2023; Balafoutis et al., 2020; Appolloni et al., 2024; Sadeghizadeh et al., 2025) have used TRL levels in agriculture or farming perspective; however, their scope differs from ours (Fig. 1). For example, unlike our study, the authors in Vardhani et al. (2023), Balafoutis et al. (2020) briefly discuss TRL levels in the context of smart farming workers, the environment, and agricultural economics. The authors in Sadeghizadeh et al. (2025) conducted a qualitative study to develop a framework for assessing smartphone-based applications in agricultural extension and education, based on TRL and other criteria, i.e., market readiness level (MRL). Similarly, TRL, along with other criteria, was used to assess the frontier agricultural technologies (hydroponics, aquaponics, rooftop agriculture, vermiculture, insect farming, and saline agriculture) to be practiced in Mediterranean countries in Appolloni et al. (2024). Regarding ISO/IEC 25010 mapping, the authors in Esteban and Santos (2025), Esteban (2019) developed an online platform for crop production with a Decision Support System to assist young generation of farmers in the Philippines. ISO/IEC 25010 was used as an evaluation tool to determine the reliability of their platform. Likewise, the study (Gerance et al., 2025) focused solely on the usability and reliability characteristics to identify banana pests and diseases in the Philippines. In Peng and Jinli (2023), Binayao et al. (2024), researchers also used ISO/IEC 25010 standard to evaluate their proposed works; however, both studies relied on verbal interpretation to assess the standard.

Thus, to achieve the goal of SMS, this study leads to the following research questions:

Table 1
Abbreviations and Full Forms.

Abbreviation	Full Name	Abbreviation	Full Name
AE	Autoencoder	ML	Machine Learning
AI	Artificial Intelligence	MLP	Multilayer Perceptron
ANN	Artificial Neural Network	NA	Not Available
CNN	Convolutional Neural Network	NC	Not Considered
DDOS	Distributed Denial-of-Service	NG	Not Given
DNN	Deep Neural Network	NIDS	Network Intrusion Detection System
EC	Exclusion Criteria	R2L	Remote-to-LocaL
GAN	Generative Adversarial Network	RF	Random Forest
GMM	Gaussian Mixture Model	RNN	Recurrent Neural Network
GRU	Gated Recurrent Unit	RQ	Research Question
HIDS	Host-based Intrusion Detection System	SA	Smart Agriculture
IC	Inclusion Criteria	SF	Smart Farming
IEC	International Electrotechnical Commission	SMS	Systematic Mapping Study
IIOT	Industrial Internet of Things	SVM	Support Vector Machine
IoT	Internet of Things	TRL	Technology Readiness Level
ISO	International Organisation for Standardisation	U2R	User-to-Root
KNN	K-Nearest Neighbour	UAV	Unmanned Aerial Vehicle
LSTM	Long Short-Term Memory	MitM	Man-in-the-Middle

- RQ1. What are the main research directions explored in the literature for securing smart farming?
- RQ2. Referring to RQ1, what security aspects have been considered in selected primary studies in the context of SF?
  - RQ2.1 Which potential security threats have been identified by the existing primary studies?
  - RQ2.2 What ML-based security solutions have been devised in the primary studies to deal with the threats identified in RQ2.1.?
  - RQ2.3 Which (smart farming architecture) layers have been secured in the identified primary studies?
- RQ3. With Reference to RQ1 and RQ2, what are the observed state-of-the-art contributions of the selected primary studies?
  - RQ3.1 Which methods have been used to assess the applicability of primary studies?
  - RQ3.2: How can the identified primary studies be categorised in terms of publication years?
- RQ4. To what extent do the identified cybersecurity solutions in RQ1 and RQ2 address key security requirements and demonstrate readiness for real-world deployment?
- RQ4.1 How are the identified security aspects aligned with the ISO/IEC 25010 security characteristics?
- RQ4.2: What is the technology maturity of the identified primary studies?

The major contributions of this paper are:

1. Conducting a SMS to identify and categorise the current security research in the IoT-based SF environment (Section 3).
2. Contemporary evaluation of the state-of-the-art technologies found in the primary studies (Section 3).
3. Assessment of the technology readiness levels of the existing ML-based cybersecurity solutions in SF environment (Sec. 4).
4. Mapping of existing ML-based cybersecurity solutions against security characteristics of ISO/IEC 25010 (Section 4).
5. Identification of underexplored areas relevant for further study in SF cybersecurity (Section 4).

A comprehensive list of all abbreviations used throughout this paper is provided in Table 1 for ease of reference.

2. Systematic mapping study

SMS is a multi-phase research methodology that provides a broader overview of a specific research area by systematically performing planning, searching, and reporting the existing literature (BA and Charters, 2007). This section provides the details of the protocol for conducting the SMS.

2.1. Planning the review

2.1.1. Scope definition and formulation of research questions

Based on the previously discussed scope (Fig. 1) and formulated RQs (mentioned in Section 1), in this study, the SMS is conducted to identify and explore existing research directions and works within an area of securing IoT-based SF systems using ML algorithms. The identified scope is confined to the recent research studies published in the time period from 2021 to the present (May 2025). Our SMS also identifies several secondary studies in this area, but the focus and methodology of these studies differ significantly from our SMS, as shown in Table 2.

2.1.2. Keywords identification and search string

Following several methods reported in Petersen et al. (2015), we identified relevant keywords from the domains we included in our mapping study (Fig. 1). As shown below, these keywords were joined with `OR` and `AND` operators to form a search string.

```
("smart agriculture" OR "precision farming"
OR "precision agriculture" OR "smart
farming") AND ("secur*" OR "privacy") AND
("iot" OR "smart technologies" OR
"internet of things") AND ("ai" OR
"artificial intelligence" OR
"ml" OR machine learning")
```

It is important to note that the terms smart farming, precision agriculture and precision farming are used interchangeably in literature.

2.1.3. Database selection

In (Franceschini et al., 2016), authors recommend choosing four or five robust databases relevant to the research area to perform high-quality research. This study used Scopus, IEEE Xplore, ACM Digital Library, and Web of Sciences. Scopus is considered one of the largest commercially available databases of peer-reviewed articles and includes indexing for IEEE Xplore, ACM Digital Library, and SpringerLink. However, we performed individual searches in these databases to identify any articles Scopus may not have indexed. The devised search string was formatted for Scopus but was adapted as necessary for other databases.

2.1.4. Inclusion and exclusion criteria

To select the most relevant studies from all the search results, the following inclusion criteria (IC) and exclusion criteria (EC) are used:

- IC1: Studies that investigate security and privacy issues.
- IC2: Studies that analyze techniques in the domain of smart agriculture.

Table 2
Comparison of our Work with Existing Secondary Studies.

References	Type of Research	ISO25010 Mapping	TRL Mapping	SF Layers	Detailed Evaluation of Studies	Identified Utilised Dataset	Considering Technology	Categorise Research
(Alahe et al., 2024)	Survey	No	No	Yes	No	No	IoT, Cryptography	No
(Ali et al., 2024)	Survey	No	No	Yes	No	No	IoT	No
(Ahmadi, 2023)	Survey	No	No	Yes	No	No	IoT, ICT, FL	No
(Rouzbahani et al., 2022)	Survey	No	No	Communication layer	No	No	IoT, AI	No
(Koduru and Koduru, 2022)	Survey	No	No	No	No	No	IoT	No
(Yazdinejad et al., 2021)	Survey	No	No	Yes	No	No	-	No
(Demestichas et al., 2020)	Survey	No	No	Yes	No	No	IoT, AI/ML	No
(Gupta et al., 2020)	Survey	No	No	Yes	No	No	-	No
(Ferrag et al., 2020)	Survey	No	No	Yes	Yes	No	IoT, Blockchain, ML	No
Our	*SMS*	*Yes*	*Yes*	*Yes*	*Yes*	*Yes*	*IoT, AI/ML, ID, BlockChain, Anomaly-based, Cryptography*	*Yes*

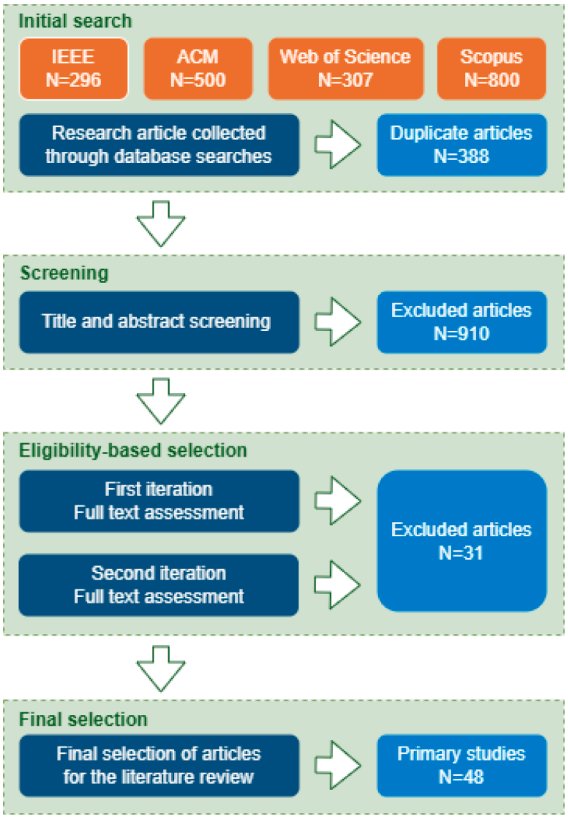

Fig. 4. Workflow of Systematic Mapping Study.

- IC3: Studies that apply machine learning techniques.
- IC4: Studies that are applicable to Internet of Things.
- IC5: Studies that are published in conferences, journals, workshops and symposiums.
- EC1: Studies that do not include smart farming applications.
- EC2: Studies that do not use a machine learning approach, or are Generative AI-based or federated-learning based approaches
- EC3: Systematic reviews, other mapping studies, opinion papers, books, and magazines.

2.2. Conducting the review

We have conducted the review following the search execution chronology shown in Fig. 4. Using the search string, we found 966 research papers after removing duplicates. 889 studies were excluded while reading the title and abstract and considering all inclusion and exclusion criteria. After a careful full-text examination, 31 studies were removed further, and 48 primary studies were left for final analysis.

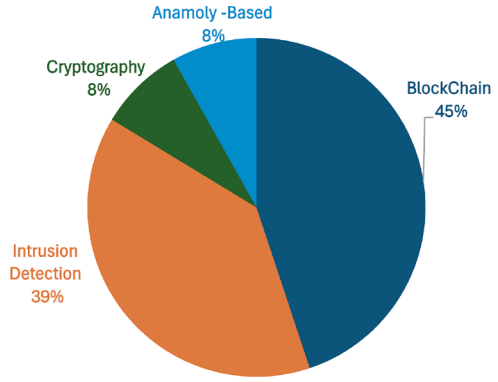

Fig. 5. Classification of Primary Studies w.r.t Innovative Technologies.

2.3. Threats to validity

Because different research domains are involved in this mapping study, there is always a threat of missing important, relevant studies that may result in incomplete coverage of all relevant existing literature. The search string is devised to mitigate this threat as it returns a maximum number of studies from all the database searches. In addition to the title and abstract, the full text was read to identify any relevant information.

Another factor that may affect the validity is researcher bias, which was mitigated by ensuring that at least two co-authors made inclusion and exclusion decisions at every study stage. In case of a conflict, a other co-authors were called to make the decision.

3. Results of the SMS on key security technologies

In this section, we will summarise the major findings and results of the SMS.

3.1. Insight into the main research directions

This subsection addresses the following research question:

RQ1. What are the main research directions identified in the literature for securing smart farming?

The SMS identified key technologies contributing to the security of IoT-based SF systems. These technologies are categorised into

Table 3
Analysis of IDS-Based Primary Studies.

References	Type of IDS	Model	Layer	Datasets	Proof of Concept	Trans-parency	Types of Attacks	Metrics
Thilakarathne et al. (2025)	NIDS	CNN	Network	NSL-KDD, KDD99Cup,UNSW-NB15, NGIDS-DS	Experimental Results	NC	Reconnaissance, DDoS, Malware	NG
Saadouni et al. (2025)	NIDS	RF, BGGO	Fog	CICIoT2023	Lab Simulation	NC	DDoS,Web-based,Re-con,Brute-force,Spoofing	Acc = 99 %, 99.83 %
Addanki et al. (2025)	NIDS	XGBoost,RF, DT	Network	NSL-KDD	Experimental Results	NC	DDoS,Reconnaiss-ance,Backdoor, Worms	Acc = 99 %, 98 %
Zidi et al. (2024)	NIDS	DKPLS, KELM	Network	X-IIoTID	Experimental Results	NC	DDoS	Acc = 98.81 %, 99 %
Kethineni and Pradeepini (2024)	NIDS	CNN, BiGRU	Network	ToN-IoT,APA-DDoS	Lab Simulation	NC	DDoS	Acc = 98.81 %, 99 %
Aburasain (2024)	HIDS	BiGRU-CNN	Edge	ToN-IoT,Edge-IIoT	Experimental Results	NC	Back-doors,Ranso-mware,DDoS	Acc = 99.2 %, 96.9 %
Mohy-eddine et al. (2024)	HIDS	ANN	Fog	NF-Bot-IoT, NF-ToN-IoT	Lab Simulation	NC	Reconnaissance, DDoS,Brute-force	Acc = 95 %
Vatambeti et al. (2023)	NIDS	IDSNet, PDO	Network	TON IoT	Lab Simulation	NC	DDoS	Acc = 97 %
El-Ghamry et al. (2023)	NIDS	CNN	Network	NSL-KDD dataset	Experimental Results	NC	Probe,DDoS	Acc = 99.9 %
Berguiga et al. (2023)	HIDS	GMM, MLP	Fog, Network	CIC-DDoS2019	Experimental Evaluations	NC	DDoS	Acc = 98.81 %, 99 %
Javeed et al. (2023)	NIDS	CNN, BiGRU	Network	CICIDS2018	Lab Simulation	NC	DDoS	Acc = 99.2 %, 96.9 %
Fu et al. (2023)	NIDS	CNN-LSTM, XGBoost	Physical	KDD-CUP99, HIKARI-2021	Lab Simulation	NC	DDoS,Probe,R2L, U2R	Acc = 93.5 %, 94.4 %
Sajid et al. (2023)	NIDS	CNN-LSTM, XGBoost	Edge, Fog	HIKARI-2021	Lab Simulation	NC	DDoS,Probe,U2R	Acc = 92 %, 78 %
Raghuvanshi et al. (2022)	NIDS	SVM, LR, RF	Network	NSL-KDD	Experimental Results	NC	DDoS	Acc = 99.8 %, 99.5 %, 98.3 %
Smmarwar et al. (2022)	HIDS	DWT,GAN, CNN	Network	IoT Malware, Malimg	Experimental Results	NC	Brute-force,Malware	Acc = 98 %, 97 %, 98 %
Rajak et al. (2022)	NIDS	CNN-LSTM	Network	HIKARI-2021	Lab Simulation	NC	Probing, Brute-force,,Malware	Acc = 97.4 %
Zrelli et al. (2022)	NIDS	ANN	Network	Own	Prototype	NC	DDoS,MitM	Acc = 99 %
Kumar et al. (2021a)	HIDS	LSTM, GRU	Edge	ToN-IoT	Experimental Results	NC	Inference attack	Acc = 97.5 %, 96 %
Ferrag et al. (2021)	NIDS	CNN,DNN, RNN	Networks	CIC-DDoS2019, TON-IoT	Theoretical	NC	DDoS	Acc = 93.2 %, 95 %, 99.7 %

Blockchain-based techniques (45 %), Intrusion detection (39 %), Cryptography, and Anomaly detection (8 %), as illustrated in Fig. 5. Intrusion detection is a way or mechanism used to monitor activities within a network or on a host device for the identification of any abnormal or malicious behavior that compromises the security or standard policies. (Zarpelão et al., 2017). Intrusion is a subset of anomalous behaviour, therefore in this paper, we keep anomaly detection-only as a separate category to make a clear distinction between the literature focused on anomaly detection-only and intrusion detection in smart farming systems. Similarly, while many primary studies include cryptography, some are cryptography-only, and these are discussed as a separate category. The following subsections provide an in-depth discussion of each category.

3.1.1. Machine learning-Based intrusion detection primary studies

Intrusion detection techniques are critical for ensuring the security of IoT-based SF systems by identifying and mitigating unauthorized activities. While widely applied in domains such as healthcare and industrial IoT, their adaptation to smart agriculture introduces unique challenges due to decentralized IoT devices, resource-constrained environments, and the need for real-time decision-making. Table 3 shows that several studies have proposed network (NIDS) or host-based (HIDS) intrusion detection systems by integrating ML algorithms, specifically for smart farming.

The recent study (Saadouni et al., 2025) have proposed IDS based on Random Forest and Binary Greylag Goose (BGGO) for the detection of attacks (DDoS, DoS, Reconnaissance, Web-based, brute force, ARS and DNS spoofing) from image network traffic using CICIoT2023 dataset. DDoS, and reconnaissance are also the focus of the ML-based IDS proposed in (Thilakarathne et al., 2025). Several techniques combining Convolutional Neural Networks (CNN) and recurrent neural network (RNN) models, such as bidirectional gated recurrent unit (Bi-GRU) and long short-term memory (LSTM), have been extensively explored to detect DDoS attacks. For example, frameworks integrating CNN with Bi-GRU demonstrated high accuracy in detecting DDoS attacks using datasets like ToN-IoT, APA-DDoS, and CICIDS2018 (Kethineni and Pradeepini, 2024; Javeed et al., 2023). Similarly, an Enhanced Black Widow Optimization approach coupled with BiGRU-CNN effectively classified attacks such as backdoors, ransomware, and DDoS in smart farming environments (Aburasain, 2024). For the security of UAVs and IoT networks, intrusion detection models using CNN-LSTM and XGBoost have been proposed. These frameworks effectively detect attacks like DoS, Probe, and Remote-to-Local (R2L) using datasets such as KDD-CUP99 and HIKARI-2021 (Fu et al., 2023; Sajid et al., 2023). Additionally, models integrating CNN, RNN, and radial basis function neural

Table 4
Analysis of Anomaly Detection-Only Primary Studies.

References	Model	Statistical Technique	Layer	Datasets	Transparency	Type of Attacks	Proof of Concept	Metric
Eleftheriadis et al. (2024)	RF, XGBoost, CATBoost	Entropy	Application	NG	NC	DDoS, Replay, Trojan horse	Prototype	NG
Kethineni and Gera (2023)	AGRU, SCAE	Mutual Information	Network	ToN-IoT, IoT-Botnet	NC	Backdoor, MitM, DDoS, Injection, Brute-force, Ransomware	Simulation	Acc = 99.9 %
Catalano et al. (2022)	MLR, LSTM	Dissimilarity metric	Physical	Agri dataset	NC	Insider threat	Prototype	Acc = 87 %, 90 %
Adkisson et al. (2021)	Autoencoder	-	Physical	NG	NC	Zero-day attack	Prototype	Acc = 98.9 %

networks (RBFNN) have been used to secure IoT-based agricultural environments against DDoS attacks (Berguiga et al., 2023; Vatambeti et al., 2023; Zidi et al., 2024; Ferrag et al., 2021).

Advanced intrusion detection frameworks have also utilised hybrid Machine Learning (ML) approaches. For instance, (Addanki et al., 2025) uses DT, RF, XGBoost, and stacking models to detect DoS, reconnaissance, backdoor, and worms. Similarly, a three-phase Deep Malware Detection (DMD) framework fused Discrete Wavelet Transform (DWT), Generative Adversarial Networks (GAN), and a lightweight CNN to analyze malware families using benchmark datasets (Smmarwar et al., 2022). Lightweight intrusion detection systems, such as those based on Kernel Extreme Learning Machine (KELM) and Random Forest, have also been developed for resource-constrained IoT environments, demonstrating their efficacy on datasets like NSL-KDD and X-IIoTID (Mohy-eddine et al., 2024; Raghuvanshi et al., 2022; El-Ghamry et al., 2023).

In addition, specific frameworks have been designed to address a range of transport-layer attacks, including brute-force, probing, and cryptomining. For example, a CNN-LSTM-based intrusion detection system evaluated using the HIKARI-2021 dataset effectively identified and mitigated such attacks (Rajak et al., 2022).

A few studies (Kumar et al., 2021a) protect against inference attacks by combining perturbation-based encoding and deep learning-based LSTM for reshaping data to be used by GRU neural networks to perform intrusion detection using the ToN-IoT dataset.

3.1.2. Anomaly-Based intrusion detection primary studies

Various innovative approaches have been explored in the context of SF to address specific challenges (such as zero-day attacks, insider threats, etc), using anomaly-based detection systems, arising from the deviation from normal behavior. Note: Anomaly-based systems can also be classified under the IDS category (Section 3). In (Eleftheriadis et al., 2024), an anomaly-based system is proposed to detect cyberattacks using RF, XGBoost, and CATBoost along with an entropy-based method. Similarly, the AGRU neural network model detects anomalies by selecting the features through a mutual information theory-based process in privacy-preserved data Kethineni and Gera (2023). Zero-day attack detection at the sensor level is considered using dissimilarity metric, dynamic threshold, and hybrid ML models in (Catalano et al., 2022). Autoencoder has been used in (Adkisson et al., 2021) for the detection of anomalous behaviour in various sensors deployed in a SF environment.

3.1.3. Blockchain-based primary studies

Blockchain, as a distributed ledger technology, offers secure, decentralized, and immutable transaction management, making it highly relevant for addressing key challenges in smart agriculture, such as data security, transparency, and traceability. Its integration with IoT and machine learning has been explored in diverse ways to enhance agricultural operations. Table 5 shows a summary of blockchain-based primary studies.

Recent studies emphasise using blockchain to secure IoT-enabled smart farming systems by ensuring decentralized authentication, secure communication, and data transparency. Approaches include trust models leveraging Ethereum blockchain (Mohanta et al., 2021), and frameworks integrating blockchain with IoT and machine learning for secure data transmission and privacy (Singh and Musale, 2024; Maurya et al., 2023). Similarly, blockchain has been combined with edge computing and machine learning for secure data storage and crop yield prediction, showcasing the effectiveness of platforms like Ethereum and Hyperledger Fabric (Sakthi et al., 2023; Zhang et al., 2022). Multiple studies proposed blockchain frameworks for enhancing system security in specific domains. For instance, smart irrigation systems have been enhanced using blockchain-based architectures for water quality monitoring (Drăgulinescu et al., 2021). Hydroponics frameworks integrate IoT, fog, and cloud layers to ensure secure communication and plant monitoring (Mehare and Bartere, 2021; Mehare and Gaikwad, 2023). Additionally, privacy-preserving frameworks for UAV-based precision agriculture combine blockchain with smart contracts and deep learning to tackle inference attacks (Kumar et al., 2021b, 2022; Guven and Parlak, 2022). Blockchain's role extends to resource management, optimizing water usage, and real-time monitoring through secure data storage (Zeng et al., 2023). Integrated systems combining blockchain and machine learning have improved data reliability, reduced network overhead, and enhanced energy efficiency (Saba et al., 2023). Blockchain-enabled systems also demonstrate improved supply chain security, crop prediction accuracy, and temper-proof communication among stakeholders (Shreya et al., 2023; Sumathi et al., 2022; Biswas et al., 2021). Broader applications explore blockchain's potential in creating transparent and fraud-resistant systems for crop monitoring, billing, and supply chain management (Mukherjee et al., 2020; Harini et al., 2023). Cloud-enabled frameworks further address privacy concerns by securely monitoring device status and detecting anomalies in real-time (Chaganti et al., 2022). Additional studies highlight blockchain's integration with AI, IoT, and cloud computing to ensure data integrity and prevent manipulation in applications such as real-time irrigation systems (Sumarudin et al., 2022).

3.1.4. Cryptography-only primary studies

Cryptography is the cornerstone of secure communication in interconnected systems, providing mechanisms to ensure the confidentiality, integrity, and authenticity of transmitted data. In IoT communication, cryptographic protocols are widely employed to protect data exchanged between devices, prevent unauthorized access, and guard against tampering. Techniques such as symmetric encryption, asymmetric encryption, and hashing algorithms are commonly used to encrypt data, authenticate devices, and verify the integrity of messages. By safeguarding data during transmission, cryptography enhances the trustworthiness and reliability of IoT ecosystems.

Several studies have focused on applying cryptographic solutions to smart farming environments. For instance, fog nodes have been utilised as intermediaries between IoT sensors and cloud servers, encrypting and forwarding only relevant data. These nodes also identify and drop compromised data, making smart agriculture systems resilient to DoS and

Table 5
Analysis of Blockchain-Based Primary Studies.

References	Technique	Layer	Datasets	Proof of Concept	Type of Threats	Scenario	Metric
Shen et al. (2025)	Blockchain-based SVM	Cloud, Edge	Own	Experimental Results	Data loss, privacy leakage	Protection of agricultural data	NG
Singh and Musale (2024)	Blockchain-secured cloud	Cloud, Network	Own	Lab simulation	Data breaches, privacy leakage	Crop monitoring and protection	NG
Subramani et al. (2024)	Blockchain-based authentication protocol	Physical, Edge, Network	NA	Theoretical	Spoofing, unauthorised access	Smart agriculture authentication	Communication overhead(160 bytes)
Zeng et al. (2023)	Smart contracts	Edge, Cloud	Own	Prototype	Data tampering, unauthorised access	Smart irrigation	Response time(20 sec)
Saba et al. (2023)	Blockchain, Linear Regression Model	Edge, Network	NA	Theoretical	Trust-related manipulation	Agricultural trust management	Latency(0.15sec)
Shreya et al. (2023)	Blockchain-secured IoT	Edge, Cloud	Own	Experimental results	Data falsification, unauthorised access	General Smart farming	Latency(0.003sec), Throughput(75Kbps)
Sakthi et al. (2023)	Blockchain with edge computing	Edge, Network	Own	Lab simulation	Data tampering, sensor spoofing	Precision agriculture	Latency(90sec), Throughput(8Kbps)
Maurya et al. (2023)	General blockchain	Network, Cloud	NA	Theoretical	Data falsification	Food supply chain	NG
Harini et al. (2023)	Blockchain, ANN	Network, Cloud	Own	Lab simulation	Data manipulation, traceability issues	Supply chain	NG
Mehare and Gaikwad (2023)	Blockchain, SVM, MLP, SGD	Fog, Cloud	Own	Lab simulation	Communication interception	Plant monitoring	Energy consumption(20 %)
Guven and Parlak (2022)	Blockchain-secured drone network	Edge, Network	Own	Prototype	Communication spoofing, data manipulation (Inference attack)	Drone-based precision agriculture	NG
Kumar et al. (2022)	Smart contracts	Cloud, Network	Own	Experimental results	Unauthorised access (Inference attack)	Data sharing	NG
Sumarudin et al. (2022)	General blockchain	Edge, Cloud	Own	Lab simulation	Data tampering	Irrigation system	NG
Zhang et al. (2022)	Blockchain, CP-ABE	Edge, Network	Own	Experimental results	Unauthorized access, privacy leakage	Agricultural IoT	NG
Chaganti et al. (2022)	Blockchain, Cloud-based IoT security	Network, Cloud	NA	Theoretical	Data tampering, unauthorized access	Security monitoring	Latency(0.11sec)
Sumathi et al. (2022)	Blockchain, ANN	Network, Cloud	Own	Lab simulation	Data manipulation	Crop yield prediction	Latency(3sec)
Mohanta et al. (2021)	Trust model on blockchain	Edge, Network	Own	Experimental results	Trust-based manipulation	General smart farming	NG
Mehare and Bartere (2021)	Lightweight blockchain with off-chain logic	Edge, Network	Own	Experimental results	Data falsification, intrusion	General smart farming	Energy consumption (25 %)
Drăgulinescu et al. (2021)	Blockchain-secured IoT system	Edge, Cloud	NA	Lab simulation	Tampering, unauthorized control	Smart irrigation	NG
Biswas et al. (2021)	Blockchain-integrated IoT	Network, Cloud	NA	Theoretical	Data tampering	Smart agriculture monitoring	NG

Table 6
Analysis of Cryptography-Only Primary Studies.

References	Technique	Protocol	Layer	Datasets	Proof of Concept	Focused Technology	Metric
Kaushal et al. (2024)	AES, CBC, HMAC	NG	Edge	DeepWeed	Lab Simulation	Robots	Latency(0.5–0.53 %)
Fathy and Ali (2023)	Expeditious Cipher (X-cipher)	MQTT	Physical, Cloud	NG	Lab Simulation	WiFi, GSM, ThingsSpeak	Throughput(140kbps)
Abunadi et al. (2022)	Symmetric Key Encryption	NG	Fog	NG	Prototype	GPS	Energy efficiency (85 %)
Morel et al. (2021)	ChaCha20-Poly1305	MAVLink	Edge	BOUN DDoS	Lab Simulation, Emulation	UAV	Memory usage (0.12 %)

replay attacks while ensuring user authentication and data integrity (Abunadi et al., 2022). Cryptographic methods like ChaCha20-Poly1305 have been implemented to secure messages between UAVs and edge devices to address the security challenges of UAV communication in zero-trust architectures. These methods enable data access control and help detect and mitigate potential attacks before launching security responses (Morel et al., 2021).

In addition to traditional data encryption, cryptographic techniques have been integrated with optimization strategies for specific agricultural applications. For example, encrypted channels have been employed to secure data transmission in crop management systems that use image analysis for disease detection. These systems leverage the multilayer perceptron (MLP) algorithm to accurately identify plant diseases from leaf images processed on cloud servers (Jeyabalu et al., 2024).

3.2. Security landscape in selected primary studies

The security landscape could be determined by the following research questions.

RQ2.1 What potential cyber-security threats have been identified by the existing primary studies?

RQ2.2 What ML-based security solutions have been devised in the primary studies to deal with the threats identified in RQ2.1.?

RQ2.3 Which layers have been secured in identified primary studies?

3.2.1. Classification of primary studies w.r.t potential security threats

Due to the technological advancement and usage of interconnected heterogeneous devices, smart farming infrastructure is vulnerable to various cyber-attacks, as shown in Fig. 6. Among them, Distributed

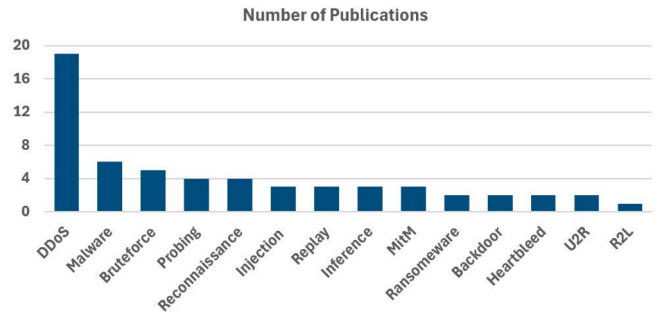

Fig. 6. Classification of Primary Studies w.r.t Attack types.

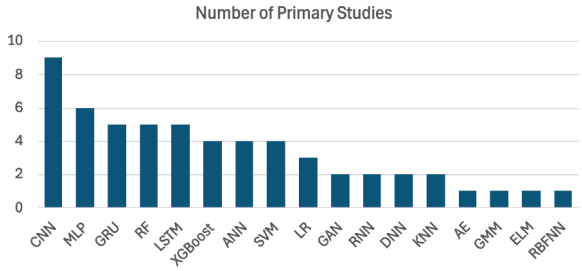

Fig. 7. Classification of Primary Studies Based on ML/DL Models.

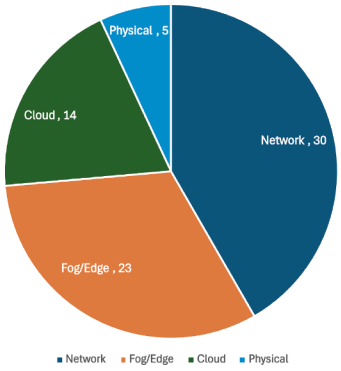

Fig. 8. Classification of Primary Studies w.r.t Multi-Layers in Smart Farming Infrastructure.

denial-of-service (DDoS) attacks are the most prevalent, i.e., more than half (19) of the primary studies focus on that attack, followed by malware (6 primary studies). DDoS attacks are considered to be very critical issues because these attacks disrupt and degrade the devices' availability by overwhelming the victim's network connection with flood or preventing the autonomous devices (drones) or sensor data from being sent to the other layers in the smart farming architecture. The unavailability of these devices results in an unsafe environment, the destruction of crops, flooding of farmlands, over-spraying of pesticides, or impacts on harvesting and financial losses. Similarly, using malware, depending on the motives of attackers, attackers can get unauthorized access to interconnected devices or networks. The entire farming network is exposed to the attackers once access is gained. As a result, attackers could tamper with the critical data (crop, soil, or temperature readings), which may result in inaccurate irrigation, pest control, or fertilization schedules. It has also been observed that only one study (Adkisson et al., 2021) and (Fu et al., 2023) focuses on zero-day and Remote-to-Local (R2L) attacks, respectively, which are also critical attacks to be detected to avoid the risks of information disclosure and operational discontinuity.

We also analysed the temporal trends of attack types reported in the reviewed studies. The results show that DDoS attacks dominate recent research, which consistently high frequency since 2022 and peaks in 2023–2025. Reconnaissance attacks have recently gained traction, growing from a single instance in 2024 to three in 2025, reflecting a shift towards the study of adversarial information-gathering behavior. Other attack types such as malware, brute-force, and probing remain present but with lower and fluctuating mentions, while sporadic attacks (e.g., injection, replay, ransomware, backdoor) appear occasionally, suggesting they are less prominent but still present in current discourse. By contrast, legacy attack categories (e.g., U2R, R2L, Heartbleed) show minimal or no recent presence, suggesting reduced emphasis in contemporary security discourse. Overall, the trends indicate a clear research focus on large-scale availability threats and reconnaissance activities in recent years.

3.2.2. *Classification of primary studies w.r.t security solutions*

Implementing effective and efficient security solutions to protect data integrity, confidentiality, availability, and privacy as SF expands is crucial for maintaining a reliable and resilient agricultural environment.

Fig. 7 shows the categorisation of primary studies based on the proposed security solutions. It has been found that eleven studies use Convolutional Neural Networks (CNN), followed by GRU, which was used in eight studies for securing smart farming environments. CNN is a deep learning model that can be trained to identify intrusions or malicious activities by analyzing sensor, tractor, or drone data and alerting farm operators to security threats (Kethineni and Pradeepini, 2024). In addition, Multilayer Perceptron (MLP) is a sub-type of a feedforward neural network (FNN) and is significant for effectively analysing intricate patterns within the data (Berguiga et al., 2023). MLP is valuable in smart farming for monitoring and detecting security threats to the environmental data, such as temperature readings, humidity levels, and soil moisture, generated from sensors.

None of the primary studies explicitly discussed interpretability, but the machine learning methods they used have clear implications for stakeholder trust. Simple models such as Logistic Regression, K-Nearest Neighbors, and Random Forests are highly interpretable, as their decision-making processes can be easily explained, making them more suitable for building trust with farmers and agricultural professionals who may not have technical expertise. More complex models, like XGBoost, Support Vector Machines, and Artificial Neural Networks, can offer partial explanations using tools such as feature importance plots, but these can still be difficult for non-technical users to understand. Deep learning models such as CNNs, RNNs, LSTMs, and GRUs are low in interpretability, which can make it harder to establish confidence and trust among agricultural stakeholders.

3.2.3. *Primary studies w.r.t securing the layers*

Fig. 8 shows the breakdown of the primary studies according to the various layers of smart farming infrastructure, including the physical layer, network layer, cloud layer, and edge/fog layer. The physical layer comprises sensors, gateway devices, drones, and autonomous tractors. These devices sense the data and actuate other devices based on the decisions made according to the use cases of agricultural farms. Similarly, the network layer facilitates physical and edge/fog layer connectivity and provides a medium for interacting with the cloud layer. The edge/Fog layer is near the devices (in the control of end-users) for local real-time computations, communication, and decisions. The application layer is used for data storage, real-time monitoring, and managing field conditions remotely, and for parameters such as soil moisture, temperature, and weather conditions. Securing all these layers is critical in the smart farming ecosystem, as each layer has its own security challenges. It has been observed from Fig. 8 that most of the work has been done to secure the communication among the devices, while one study (Eleftheriadis et al., 2024) focuses on securing the application layer.

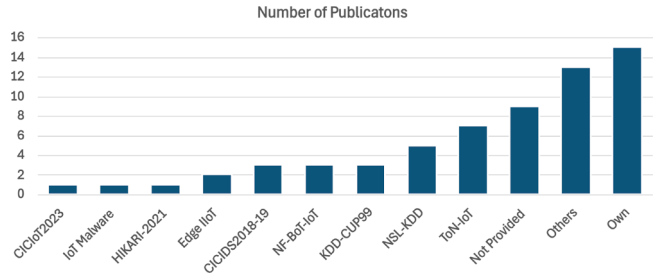

Fig. 9. Classification of Primary Studies w.r.t Datasets.

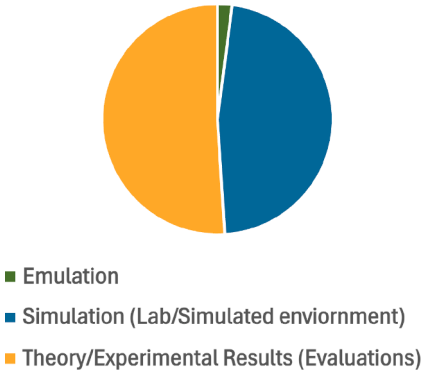

Fig. 10. Categorisation of Primary Studies Based on Proof of Concepts.

3.3. Contributions

This subsection presents the findings related to the following research questions.

RQ3.1 What methods have been used to assess the applicability of primary studies?

RQ3.2: How can the identified primary studies be categorised in terms of publication years?

3.3.1. Findings on the basis of applicability of primary studies

Datasets Utilised in the Primary Studies: We have classified the primary studies based on various publicly available intrusion detection datasets. The purpose of mapping primary studies with the datasets is helpful in several ways. For example, different datasets contain different types of attacks, configurations, and detection goals. This mapping would help the researchers select the datasets according to their detection goals. Also, this mapping can help identify the research gaps in the existing datasets from a security perspective in smart farming. It has been represented in Fig. 9 that the existing studies used traditional intrusion detection datasets to detect specific attacks in a smart farming environment. For securing smart farming in particular, there is no widely adopted public dataset available; therefore, most of the researchers create their own attack scenarios to demonstrate the feasibility of their work, and only one primary study utilized the dataset CICIoT2023. In contrast, many studies (9) did not evaluate the effectiveness of their proposed models on any datasets.

Proof of Concepts adopted in Primary Studies: The proof of concepts adopted in selected primary studies to evaluate the effectiveness of the proposed works, shown in Fig. 10, have been divided into simulation (lab simulation or prototype in a simulated controlled environment), emulation, and theoretical concepts, or experimental results (evaluations). In about 25 (51 %) selected primary studies, theoretical and experimental results are mentioned, 47 % works are based on lab simulations, and the only study (Morel et al., 2021) focuses on emulation.

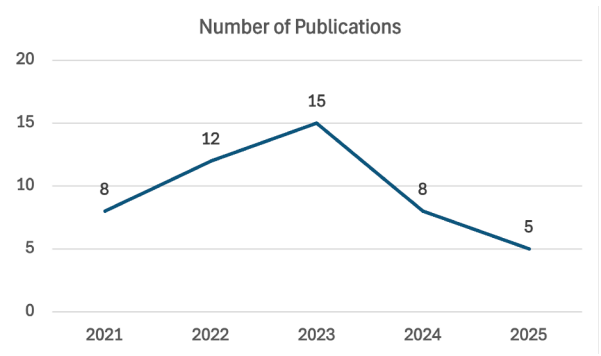

Fig. 11. Classification of Primary Studies w.r.t Publication Years.

3.3.2. Categorisation of the primary studies by publication years

The categorisation of the primary studies w.r.t published years is depicted in Fig. 11. Overall, there is an increasing trend over the given period, except in 2024 where only eight research studies were found. However, five studies by May 2025 indicate a growing volume of research interested in securing IoT-based smart farming environments.

4. Principal findings or observations

This section elaborates on the observations determined by the research questions below.

RQ4.1: What is the technology maturity of the identified primary studies?

RQ4.2 How are the identified security aspects aligned with the ISO/IEC 25010 security characteristics?

4.1. TRL-based observations

In this section, the maturity level (technology readiness level) of the proposed solutions identified in each primary study (discussed in Sect. 3) is presented. We have adopted the definition of TRL (Fig. 3) and tailored each TRL level in the context of securing SF, as shown in Table 7. To facilitate the reproducibility of these mappings, we have provided the algorithmic mapping for the TRLs discussed in this section in Appendix 1. These tailored definitions provide a roadmap for evaluating security solutions' development and deployment levels. The evaluation results in Table 8 offer insight into the overall technology readiness of the proposed solutions.

Contextualised TRL Definitions for SF Security:

TRL 1: Basic security attributes in SF systems are observed and reported: The primary studies are at the level 1 if the cybersecurity objectives or characteristics (Fig. 2), security weaknesses, vulnerabilities, threat, and their impact within farming environments are only being identified and reported in the studies.

TRL 2: Basic technological (analytical) aspects to secure smart farming systems are identified. At this level, only the initial conceptualisation of the proposed security solutions identified in primary studies is presented to address the security attributes identified in TRL1. The activities, such as threat modeling approaches, risk assessment, and existing technology stack review, etc, can be performed at this level to identify attack surfaces or potential attack vectors.

TRL 3: Active research and development initiated/proof of concept to validate the analytical aspects. The primary studies are at level 3 if they have demonstrated the proposed security solutions' feasibility through the research and experimental developments (results or evaluation) to validate the initial concepts identified in TRL 2. The incident and disaster recovery plans, business continuity planning, and playbooks can be drafted at this level based on the information from the previous level.

Table 7
Adopted TRL Levels with Tailored Definitions.

TRL Level	Definition
TRL 1	Basic security attributes in smart farming systems are observed and reported.
TRL 2	Basic technological (analytical) aspects to secure farming environments are identified
TRL 3	Active research and development initiated/proof of concept to validate the analytical aspects.
TRL 4	A prototype implementation and validation in a lab environment.
TRL 5	A prototype implementation and validation in a simulated environment.
TRL 6	A prototype demonstration in a relevant field environment (closely resembles real-world scenarios and technology), but under controlled test conditions.
TRL 7	A fully functional prototype serves as a foundation for beta testing on a farm
TRL 8	A complete, secure system is ready to be integrated with mass production
TRL 9	Secure farming system is deployed in an operational farming environment with continuous monitoring and updates

TRL 4: A prototype implementation and validation in a lab environment. The proposed solutions and their performance are validated in a laboratory environment to demonstrate the integration of the proposed approach (solution) with other relevant components of SF systems.

TRL 5: A prototype implementation and validation in a simulated environment. The proposed solution's prototype is tested in a simulated environment that closely mimics the attacks on real-world farming and validates that the solution can meet the system's security objectives. Threat models and risk assessments are validated against prototypes.

TRL 6: A prototype demonstration in a relevant field environment (closely resembles real-world scenarios and technology), but under controlled test conditions. The prototype is demonstrated in the real-world farming conditions, but under controlled settings. The incident and disaster recovery plans, business continuity planning, and playbooks become more specific and tested in field environments.

TRL 7: A fully functional prototype serves as a foundation for beta testing on a farm. A mature and fully functional prototype is developed, ready to be deployed and tested by end-users (farmers or agricultural professionals) in an actual farm setting, and the real-world feedback should be adopted at this level.

TRL 8: A complete, secure system is ready to be integrated with mass production. The secure farming system or component is refined, completed, and ready to be integrate into widespread deployment.

TRL 9: A secure farming system is deployed in an operational farming environment with continuous monitoring, feeback loop, and updates. The secure farming system or component is completely deployable and operational in a real-world farming environment. This level also focuses on continuous monitoring of the deployed secure systems, maintenance, and updates, not at the technology level, but also based on the feedback received from farmers to ensure ongoing security and effectiveness.

Key Observations: Our analysis in Table 8 shows that vast majority of the proposed solutions to secure the smart farming systems have not progressed beyond technology validation and prototype development stages (TRL 4 to TRL 6), with only a few moving beyond system validation and prototype development.

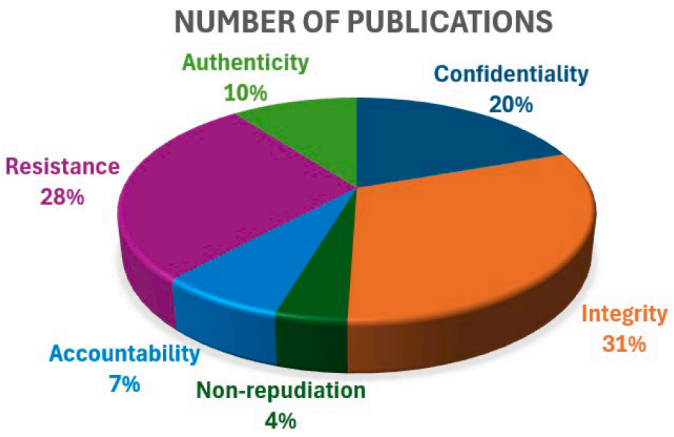

Fig. 12. ISO/IEC Security Sub-Characteristics Considered in Primary Studies.

Only a few primary studies progress towards the system validation and deployment (TRL 7–9). Most of the existing literature is heavily focused on conceptual discussion, which is on the lowest technology readiness levels. There are few examples of actual implementation of specific frameworks or methods and even fewer with practical applications or system-level experiments. There is a lack of standardization in security protocols, which is a prohibitive factor when comparing or benchmarking security solutions for smart agriculture systems.

The adapted TRL framework provides a structured and standardized method for assessing the maturity of various cybersecurity solutions. The assessment has introduced a development trajectory that can help connect academic innovation and industrial deployment and support the creation of a future work roadmap. However, the assignment of TRL levels is based on subjective observations by security, educational, and farming technology experts, particularly when primary studies do not document implementation details and would vary when assessed by other experts. Moreover, TRL is the backbone for the evaluation of deployment readiness; it does not consider user-centric factors such as transparency, usability, or trust for various farming environments unless they are manually embedded into the analysis. Lastly, TRL focuses primarily on technology maturity, i.e., how much the solution has advanced from conceptualisation to real-world deployment; nevertheless, it does not inherently assess the effectiveness of security of the solution. Thus, as discussed in the next section. we map the existing proposed security solutions to the security sub-characteristics (one of the key quality characteristics) defined in the ISO/IEC 25010 standard to determine the effectiveness or quality of secure software and systems.

4.2. ISO/IEC 25010-based observations

Quality is a subjective matter, yet, product quality is a crucial aspect of security solutions in smart farming. In this paper, the definition of quality is standardised to the key security characteristics in ISO/IEC in order to perform fair comparisons across different aspects of quality across the body of literature (Fig. 12). Since none of the existing studies (Table 2) directly utilised the ISO/IEC 25010, the authors reviewed and mapped them against the standard to identify the overlooked critical security aspects.

Confidentiality: Confidentiality is the basic pillar of cybersecurity, and it is the degree to which a product or system ensures that data is accessible to authorised persons only.

The motives of the attacks, such as probing (Tchakoucht and Ezziyyani, 2018), and inference (Wu et al., 2024; Kumar et al., 2021a),

Table 8
Key Technologies, ISO 25010 Security Sub-Characteristics and TRL.

References	Cybersecurity Technology	ISO/IEC 25010 Security Attributes						TRL Level
		Confidentiality	Integrity	Non-Repudiation	Accountability	Resistance	Authenticity	
Shen et al. (2025)	Blockchain	✓					✓	TRL 2
Subramani et al. (2024)		✓					✓	TRL 2
Zeng et al. (2023)		✓	✓					TRL 5
Saba et al. (2023)			✓					TRL 2
Shreya et al. (2023)		✓	✓			✓		TRL 3
Sakthi et al. (2023)			✓			✓		TRL 4
Maurya et al. (2023)			✓			✓		TRL 2
Mehare and Gaikwad (2023)			✓			✓		TRL 4
Biswas et al. (2021)			✓					TRL 2
Guven and Parlak (2022)		✓	✓				✓	TRL 4
Singh and Musale (2024)		✓					✓	TRL 4
Harini et al. (2023)		✓	✓	✓				TRL 3
Mehare and Bartere (2021)			✓			✓		TRL 3
Chaganti et al. (2022)		✓	✓					TRL 2
Sumathi et al. (2022)			✓			✓		TRL 4
Mohanta et al. (2021)			✓	✓				TRL 3
Drăgulinescu et al. (2021)			✓			✓		TRL 4
Kumar et al. (2022)		✓						TRL 3
Sumarudin et al. (2022)			✓					TRL 4
Kumar et al. (2021b)		✓			✓			TRL 3
Zhang et al. (2022)		✓					✓	TRL 3
El-Ghamry et al. (2023)	IDS	✓				✓		TRL 3
Thilakarathne et al. (2025)			✓			✓		TRL 3
Addanki et al. (2025)			✓		✓	✓		TRL 3
Saadouni et al. (2025)			✓		✓	✓		TRL 4
Zidi et al. (2024)						✓		TRL 3
Raghuvanshi et al. (2022)						✓		TRL 3
Smmarwar et al. (2022)		✓	✓					TRL 3
Rajak et al. (2022)			✓	✓			✓	TRL 4
Zrelli et al. (2022)			✓			✓		TRL 5
Aburasain (2024)					✓	✓		TRL 3
Fu et al. (2023)		✓				✓	✓	TRL 4
Javeed et al. (2023)						✓		TRL 4
Ferrag et al. (2021)					✓	✓		TRL 2
Kumar et al. (2021a)			✓			✓	✓	TRL 3
Sajid et al. (2023)			✓			✓	✓	TRL 4
Kethineni and Pradeepini (2024)						✓		TRL 4
Mohy-eddine et al. (2024)					✓	✓	✓	TRL 4
Vatambeti et al. (2023)						✓		TRL 4
Berguiga et al. (2023)			✓			✓		TRL 3
Catalano et al. (2022)	Anomaly Detection		✓			✓		TRL 4
Adkisson et al. (2021)			✓					TRL 4
Kethineni and Gera (2023)		✓	✓					TRL 4
Eleftheriadis et al. (2024)			✓		✓	✓		TRL 3
Kaushal et al. (2024)	Cryptography	✓	✓			✓		TRL 4
Morel et al. (2021)		✓		✓				TRL 6
Abunadi et al. (2022)		✓						TRL 5
Fathy and Ali (2023)		✓	✓					TRL 4

are to gain unauthorised access to sensitive data. It has been found from the results of our study (Table 8) that some of the studies (19 out of 48) have discussed the proposed solutions to deal with the attacks in smart farming, which compromise the confidentiality objective of cybersecurity.

Integrity: Integrity is another important objective of cybersecurity, ensuring that the state of the system, product, component, or data is protected from unauthorised tampering or alteration intentionally (with malicious intent) or unintentionally.

The man-in-the-middle (MITM) (Conti et al., 2016), injection attacks (Ferrag et al., 2021) (such as cross-site scripting attack) and malware like worms, and trojan horse exploit the integrity and a few studies (8) deal with these attacks. Please note that we can categorize malware into the confidentiality category as well.

Non-repudiation: Non-repudiation guarantees that the actions or events performed within a system cannot be denied by the entity that executed them. This validation is particularly critical for data exchanges over the Internet, where ensuring accountability and traceability is important.

The replay attacks (Syverson, 1994) affect non-repudiation using valid credentials and messages. These attacks undermine the authenticity of transactions and could also be classified under confidentiality breaches due to their overlapping implications. Our study identified a limited number of proposed solutions addressing non-repudiation in smart farming systems.

Accountability: Accountability is the principle of ensuring that the actions or activities of a particular individual on a system or component/data can be traced uniquely to that person.

The attacks, like a backdoor attack and reconnaissance attack (Ferrag et al., 2021; Sanghvi and Dahiya, 2013), which evade their detections, lie under the category that compromises the accountability characteristics of the system. Note that the reconnaissance attack could also be categorised under attacks that compromise confidentially, but to be more specific, we categorise it under accountability. Only four studies focus on protecting smart farming against backdoor and reconnaissance attacks.

Resistance: Resistance is the ability of the product or system to maintain operational continuity during a cyber-attack. All the security sub-characterstics mentioned above collectively contribute to a system's attack resistance. However, attacks like DDoS (Tchakoucht and Ezziyyani, 2018) and ransomware (CERT, 2024) make the system or product unavailable, and they cannot sustain operations under these attacks. Most of the primary studies (15 studies) proposed solutions to detect or mitigate DDoS attacks, and only three studies focus on ransomware attacks (Fig. 6).

Authenticity: Authenticity validates the data's subject, resource, or origin through identity proof. This security attribute is significant because it ensures that the transmitted data is not corrupted or eavesdropped.

The attacks that compromise authenticity are brute force attacks, user-to-root (U2R), and remote-to-local (R2L). Table 8 shows that only 4 studies address the challenges caused by these attacks.

Key Observations: Overall, *availability is the most important security pillar for smart farming (Yazdinejad et al., 2021).* Generally, confidentiality, integrity, and availability are three basic pillars of security. However, ISO/IEC 25010 mentioned the first two as security sub-characteristics, while availability is categorised as a sub-characteristic of reliability feature. In addition, the standard includes non-repudiation, authenticity, accountability, and resistance features. As already mentioned, resistance to the attacks is provided by all the security features. Nevertheless, the attacks mentioned in this category result in operational discontinuity. The authors have proposed various intrusion detection systems to detect DDoS; however, none of the studies has focused on the stealthy variant of DDoS attacks known as slow-rate attacks. Slow-rate attacks resemble legitimate traffic as they use slow connection and low bandwidth. Detecting these attacks are critical in smart farming due to the involvement of resource-constrained IoT devices because these attacks slowly degrade the available resources and impact system performance, resulting in operational discontinuity (Zahid et al., 2025). Moreover, the high degree of distribution creates the large attack surfaces, making these attacks hard to detect. There is also a need to develop secure solutions for smart farming with a special emphasis on non-repudiation to ensure accountability and trust in SF environment. Similarly, ML-specific attacks like poisoning attacks, prompt injection attacks, and evasion attacks are also overlooked (Shaihn, Singh, 2023). Compromised ML-models could results in malfunctioning outputs, leading to significant economic and operational losses. This gap highlights the need for robustness of ML-based solutions against sophisticated and evolving attacks to ensure the security of SF technologies.

4.3. Wider observations

The analysis of 48 primary studies using a systematic mapping study (Sect. 2) results in some interesting general observations that highlight current trends and areas requiring additional research.

Observation 1. *None of the existing studies considered TRL to determine the maturity of the proposed solutions in smart farming.*

Meta-analysis: While various emerging approaches for securing smart farming environments have been proposed, many lack real-world deployment and validation. Practical implementation and validation of IoT security solutions are essential for developing reliable and secure systems in smart farming. Theoretical solutions without real-world testing undermine their applicability, as actual farming environments introduce complexities like decentralized networks, unreliable connectivity, and hardware limitations that cannot be fully replicated in controlled settings. Comprehensive risk assessments and consequence analysis of potential cyberattacks are also necessary to guide the development of security standards. Without practical deployment, it doesn't remain easy to assess the true effectiveness of these systems, making them less attractive for large-scale adoption.

Observation 2. *Industrial technology should comply with the ISO/IEC 25010 standard for product quality.*

Meta-analysis: The biggest hurdle in adapting smart agriculture technology is the farmers' lack of trust in the black box machine learning approaches. Using interpretable ML approaches like decision trees provides an ability to understand the decisions of the machine learning algorithms, which may be shared with the stakeholders to build trust in decisions made by the system. Accountability can be ensured by following ethical practices in the design of smart agriculture systems, responsibly handling data, prioritising sustainability, providing long-term reliability, and upholding environment-friendly practices.

Observation 3. *There is a lack of publicly available intrusion detection datasets within the domain of smart farming.*

Meta-analysis: In the smart farming context, the Farm-Flow dataset (Ferreira et al., 2025) represents an important first step toward domain-specific benchmarking. It includes traffic and event data from a precision agriculture testbed, consisting of domain-specific devices such as soil and climate sensors and irrigation actuators. This makes it more representative of the cyber-physical threats that occur in smart farming. However, its major focus is on flooding attacks only and this indicates a lack of consideration for other critical cyber attacks in SF. Currently, Farm flow is the only publicly available dataset tailored for smart farming, demonstrating a clear gap in the literature. The lack of diverse and publicly available datasets significantly hinders reproducibility and benchmarking, as existing intrusion detection datasets fail to capture the operational characteristics and threat landscape of smart farming environments. Therefore, we emphasise that further efforts are required to develop diverse public datasets that reflects the heterogeneity of farming systems worldwide. Such resources will be critical to ensure reproducibility and to mitigate the current over-reliance on generic IoT security datasets.

Observation 4. *Overlooking the performance of security solutions w.r.t resource-constrained farming IoT devices.*

Meta-analysis: IoT devices are inherently resource-constrained, having limited processing speed and memory. Existing security solutions for securing smart farming devices are highly accurate but have limited real-world implementation. There is a need to focus on lightweight security solutions (minimizing the proposed solution's memory and space footprint) to meet the computational requirements of resource-constrained IoT devices. For example, our survey found that most of the studies use CNN for securing IoT-based SF devices and described its

Table 9
Comparative Analysis of Key Security Technologies.

Criteria	IDS	BlockChain	Cryptography	Anomaly Based
Performance Evaluation	Reported accuracy range (78–99 %)	Latency 0.003-90sec% (5 papers); Throughput 8-75Kbps (2 papers); Energy efficiency 20-25s% (2 paper); Communication overhead 160bytes (1 paper); Response time 20sec (1 paper)	No consensus: Latency 0.5-0.53 % (1 paper); Throughput 140Kbps (1 paper); Energy efficiency 85 % (1 paper); Memory Usage 0.12 % (1 paper)	Reported accuracy range (88–99 %)
Advantages	Improved detection rates and accuracy with training data, adaptable to new and evolving threats, helpful for real-time analysis of traffic and system logs	Improved security and efficiency, greater data ownership and control tamper-proof records, decentralized trust, high data integrity, decentralized trust, tamper resistance, lower operational costs	Proven mathematical secure communication, well-established standards, strong confidentiality, authentication and integrity, availability of mature techniques	Detects unknown attacks, less dependent on signatures, able to handle large and complex data stream, capable of customising the normal activity profiles for every system, application and network.
Disadvantages	Resource intensive with high computational cost, high false rates, need large and high-quality training data, lack of transparency, vulnerable to adversarial attack, sometimes need manual setting of thresholds and parameters	Immutability challenge as it is difficult to alter the data in blockchain, high computational overhead, latency and scalability issues	Key management complexity that may impact performance on constrained devices, complex mathematical internal working, regulatory compliance, rigid against dynamic threats, lacks adaptability, system require comprehensive planning and maintenance	Complex, need light-weight solutions for resource-constrained devices as requires large datasets for pattern identification, susceptible to subtle attacks, high false alarms, and difficult in determining the false alarm events, needs continuous retraining

general functionality in detecting security threats. It has been demonstrated by our survey that in smart farms, CNN has achieved higher accuracy scoring, however the researchers have mentioned that these models are typically resource intensive (Mankins et al., 1995; Altalak et al., 2022; El Sakka et al., 2025; Alzubaidi et al., 2021). CNN involves a large number of parameters, complex convolutional operations, retraining, forward and backward propagation, and require large amount of data for training, all of which demand higher computational power, memory, and energy. These requirements can pose challenges for deployment of CNN-based models on low-power or resource-constrained IoT devices. This is further underscored with our TRL mapping in Table 8, which shows that most of these studies correspond to TRL 2–4, indicating that CNN-based approaches are largely at the concept or lab-validation stage. This shows a gap between the high-accuracy models developed in controlled simulations and real-world deployment on low-resource hardware. Future research must consider the tradeoff between "accuracy-first" and "efficiency-first" architectures. There is an urgent need to explore lightweight security solutions, such as model quantisation, pruning, or TinyML frameworks, which minimise the memory and energy footprint to meet the strict computational requirements of real-world farming infrastructure.

Observation 5. *The weakest link in the security chain could compromise the entire smart agriculture system.*

Meta-analysis: The reviewed literature proposed security enhancements for smart agriculture systems while focusing on a particular layer in system architecture as summarised in Fig. 8. For a full stack secure system, interoperability of those security measures and their impact on system performance needs to be evaluated. A layered-security approach requires evaluating solutions proposed at different layers, including overhead and performance impact due to the different complexities involved at the device level, network, and computing. Also, the multi-layer smart farming infrastructure introduces cross-layer attacks, which need to be addressed by extending existing foundational research.

Observation 6. *High computational and communication overheads impact real-time monitoring and decision-making in blockchain-enabled smart farming systems.*

Meta-analysis: One of the critical challenges in utilizing blockchain for smart agriculture is the high computational and communication overhead, particularly for real-time monitoring and decision-making. Blockchain inherently requires significant resources to process and validate transactions, leading to latency and inefficiencies when applied in real-time agricultural operations. The integration of edge computing has been proposed as a solution to reduce the load on centralized cloud servers, but further optimization is required. The high resource demands of blockchain can weaken the usability of these systems, especially in resource-constrained agricultural settings where real-time responses are crucial. To address this issue, future research should focus on optimizing blockchain protocols to minimize computational overhead and network latency while ensuring data security and integrity in smart farming systems.

Observation 7. *Cross-layer security validation is underexplored.*

Meta-analysis: Although existing studies have investigated security at specific layers such as the network, fog/edge, or cloud, a few have explicitly addressed cross-layer security validation. This is a critical gap, as attacks often traverse multiple layers, and validating each layer in isolation may overlook vulnerabilities that arise from their interactions. For instance, a compromised sensor node (physical layer) can inject false data into the communication channels (network layer) and ultimately manipulate cloud or AI-driven decision-making. To ensure holistic protection, cross-layer validation mechanisms such as coordinated penetration testing across layers, anomaly detection spanning device-to-cloud pathways, and unified access control enforcement are needed. The limited attention to such approaches in current literature highlights an important avenue for future research.

Observation 8. *A Comparative analysis of key Security Technologies.*

Meta-analysis: Table 9 provides a high-level comparative analysis of ML-based IDS, blockchain, cryptography and anomaly-based approaches, benchmarked by three criteria: performance evaluation, advantages and disadvantages. Note that a direct one-to-one comparison is not feasible because of significant variations across the reviewed studies in terms of experimental setups, models, datasets, configurations, security aspects, and performance metrics. For example, the literature on ML-based IDS typically focused on detection accuracy whereas papers on blockchain emphasized integrity and decentralization. Despite these differences, the analysis in Table 9 discusses the operational tradeoff between these technologies, emphasizes that each approach perform well in their intended application environment and none of the single approach is universally optimal. As detailed earlier in

Table 3 and Table 4, it has been found that ML-based IDS and anomaly-based research works demonstrate accuracy in the range of 78–99 % and 87–99 %, depending on the algorithms, feature selection, and dataset, respectively. Meanwhile, blockchain and cryptographic solutions do not have consensus in the literature regarding performance metrics. For example, there were 4 cryptography-only solutions (Table 6) reporting different assessments (throughput, latency, energy and CPU consumptions), for which accuracy was not a reported measure. This finding highlights the importance of context-aware evaluation criteria. To secure IoT-based smart farming systems against the sophisticated cyber-attacks effectively and efficiently, the combination of one or more approaches can provide a multi-level and better resilience for the environment. This analysis will also help the researchers and industrial experts to design hybrid frameworks based on their objectives.

Observation 9. *A lack of ambition for Industry 5.0 readiness*

Meta-analysis: Industry 5.0 is a fast-approaching reality (Maddikunta et al., 2022). A notable finding from our systematic mapping study is the scarcity of discussion around future-proofing the solutions by discussing them in relation to Industry 5.0. The analysis results of our SMS, and TRL mapping of recent studies reveal that most solutions are at early stages of development, implying that the deployment timeline could be years away. Despite this, we found a lack of discussion or even awareness in the primary studies of the real-world factors that will be critical in that future state of farming. This oversight is a significant risk, as any security product currently under development will likely be deployed into an Industry 5.0 ecosystem. We identify a crucial need for cybersecurity approaches to explicitly discuss and evaluate their strengths and weaknesses within this future context of Industry 5.0, especially since their deployment timelines could be closer to Industry 5.0 than 4.0.

5. Conclusions and future work

In this systematic mapping study, we reviewed published work from 2021 to May 2025 on the security aspects of IoT-based smart agriculture systems. The mapping results indicate that the major technologies in the current literature are blockchain, and intrusion detection, which comprised almost 85 % of the primary studies. The contemporary evaluation of the primary studies found in each technology is performed, which is not done by any existing surveys. The analysis results show that primary studies addressed the top three security threats: distributed denial-of-service, brute-force attacks, and malware. Furthermore, the most popular security solutions were based on convolutional neural networks, with feedforward neural networks as a distant second. Over 50 % of the primary studies aimed at securing the network and fog/edge layers. One recent publicly available intrusion detection dataset meets the specific requirements of a farming environment but deals with only flooding attacks.

We also assessed the technology readiness levels of studies against the six characteristics of a reliable security product listed by ISO/IEC 25010: confidentiality, integrity, non-repudiation, accountability, resistance, and authenticity. Of these, the most mature security technology has undergone a simulated controlled environment (TRL 5). Six studies are the least mature (TRL 2), indicating that they are still at a theoretical phase. Mostly, confidentiality, accountability, resistance, and authenticity are at the technology validation and prototype development phases (TRL 4–5). This study reveals our current security research landscape's strengths, weaknesses, and maturity levels in smart farming and IoT. Smart agriculture systems rely on machine learning, which introduces additional data security and privacy challenges. To avoid the technology and commercialization "valley of deaths", we must focus on increasing the scope and scale of public datasets for testing and benchmarking diverse security solutions, especially because there are no farming intrusion detection datasets. Moreover, more techniques are required to secure the cloud and physical layers, which currently receive less attention than the network layer, and to expand on the types of attacks each layer may encounter. Crucially, standardised, large-scale IoT-based smart farming testbeds may be useful to validate the interoperability of the security at different layers in order to rapidly transition the current security solutions from TRL 4–6 to TRL 7–9.

Furthermore, there is a considerable lack of light-weight security solutions for resource-constrained IoT devices, which could become vulnerable endpoints in a security network. In our ongoing research, we are developing a smart farming intrusion detection dataset and conduct comprehensive threat modeling to identify critical attack surfaces and attack vectors that could make smart farming systems vulnerable. In future, we will also evaluate the computational complexity of CNN-based models to identify solutions that are more suitable for real-world IoT smart farming environment. Finally, we call for developers of cybersecurity solutions for smart farming to strongly consider critically evaluating their solutions against the TRLs, and also to assess the quality of their solution against a well-established quality standard such as the ISO/IEC 25010. Both of these frameworks are useful to identify their possible deployment timelines. This is crucial, because their practical deployment may require strategic planning to facilitate acceptance and integration with potential early-stage Industry 5.0 frameworks that are already at conceptual stages of research.

CRediT authorship contribution statement

Farzana Zahid: Writing - review & editing, Writing - original draft, Visualization, Validation, Methodology, Investigation, Formal analysis, Data curation, Conceptualization; **Xiao Chen:** Writing - review & editing, Writing - original draft, Visualization; **Shaleeza Sohail:** Writing - review & editing, Writing - original draft, Investigation, Conceptualization; **Boyang Li:** Visualization, Investigation; **Melanie Po-Leen Ooi:** Writing - review & editing.

Data availability

No data was used for the research described in the article.

Ethical approval

This article does not report any research with human participants or animals.

Informed consent

This article does not report any studies with human participants.

Financial interests

The authors do not have any financial interests in this research.

Funding

University of Waikato - University of Newcastle Seed Funding 2024 received for conducting this study.

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.

Acknowledgements

Not applicable.

Appendix A. Appendix

Listing 1
Algorithm mapping TRL to ISO/IEC 25010

```
def map_trl_iso25010(study: Dict[str, bool]) -> Tuple[int, Set[str]]:
    """
    Input keys expected in 'study':
      # TRL signals
      identifies_threats, conceptualises_solution, proof_of_concept,
      lab_prototype, sim_validation, field_demo, beta_farm_test,
      production_ready, operational_deployed

      # ISO/IEC 25,010 sub-characteristics (evidence flags)
      confidentiality, integrity, authenticity,
      accountability, non_repudiation, resistance
    """
    # Step 1: TRL assignment
    trl = 0
    if study.get("identifies_threats"): trl = 1
    if trl >= 1 and study.get("conceptualises_solution"): trl = 2
    if trl >= 2 and study.get("proof_of_concept"): trl = 3
    if trl >= 3 and study.get("lab_prototype"): trl = 4
    if trl >= 4 and study.get("sim_validation"): trl = 5
    if trl >= 5 and study.get("field_demo"): trl = 6
    if trl >= 6 and study.get("beta_farm_test"): trl = 7
    if trl >= 7 and study.get("production_ready"): trl = 8
    if trl >= 8 and study.get("operational_deployed"): trl = 9

    # Step 2: ISO/IEC 25,010 mapping
    iso = set()
    if study.get("confidentiality"): iso.add("Confidentiality")
    if study.get("integrity"): iso.add("Integrity")
    if study.get("authenticity"): iso.add("Authenticity")
    if study.get("accountability"): iso.add("Accountability")
    if study.get("non_repudiation"): iso.add("Non-repudiation")
    if study.get("resistance"): iso.add("Resistance")

    return trl, iso
```

References

Abunadi, I., Rehman, A., Haseeb, K., Parra, L., Lloret, J., 2022. Traffic-aware secured cooperative framework for iot-based smart monitoring in precision agriculture. Sensors 22 (17), 6676.

Aburasain, R.Y., 2024. Enhanced black widow optimization with hybrid deep learning enabled intrusion detection in internet of things-based smart farming. IEEE Access.

Addanki, U.K., Devareddi, R.B., Kamarajugadda, K.K., Pavani, M., Gera, P., 2025. Machine learning-powered intrusion detection system for agriculture 4.0: securing the next generation of farming. Int. J. Innov. Res. Sci. Stud. 8 (1), 1964–1978.

Adkisson, M., Kimmell, J.C., Gupta, M., Abdelsalam, M., 2021. Autoencoder-based anomaly detection in smart farming ecosystem. In: 2021 IEEE International Conference on Big Data (Big Data). IEEE, pp. 3390–3399.

Ahmadi, S., 2023. A systematic literature review: security threats and countermeasure in smart farming. Authorea Preprints.

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, 109401.

Ali, I.A., Bukhari, W.A., Adnan, M., Kashif, M.I., Danish, A., Sikander, A., 2024. Security and privacy in iot-based smart farming: a review. Multimed. Tools Appl., 1–61.

Altalak, M., Ammad uddin, M., Alajmi, A., Rizg, A., 2022. Smart agriculture applications using deep learning technologies: a survey. Appl. Sci. 12 (12), 5919.

Alzubaidi, L., Zhang, J., Humaidi, A.J., Al-Dujaili, A., Duan, Y., Al-Shamma, O., Santamaría, J., Fadhel, M.A., Al-Amidie, M., Farhan, L., 2021. Review of deep learning: concepts, CNN architectures, challenges, applications, future directions. J. Big Data 8 (1), 53.

Appolloni, E., Pennisi, G., Cerasola, V.A., Biru, W., Buchenrieder, G., Uyar, T.S., Yavuz, Y., Orsini, F., 2024. Frontier agriculture systems in the mediterranean region: current status and future opportunities. In: V All Africa Horticultural Congress-AAHC2024 1422, pp. 69–78.

BA, K., Charters, S., 2007. Guidelines for performing systematic literature reviews in software engineering. Technical Report. Keele University and Durham University Joint Report. The Pennsylvania State University.

Balafoutis, A.T., Evert, F. K.V., Fountas, S., 2020. Smart farming technology trends: economic and environmental effects, labor impact, and adoption readiness. Agronomy 10 (5), 743.

Berguiga, A., Harchay, A., Massaoudi, A., Ayed, M.B., Belmabrouk, H., 2023. Gmlp-ids: a novel deep learning-based intrusion detection system for smart agriculture. Comput., Mater. Continua 77 (1).

Binayao, R.P., Mantua, P. V.L., Namocatcat, H. R. M.P., Seroy, J. K. K.B., Sudaria, P. R. A.B., Gumonan, K. M. V.C., Orozco, S. M.M., 2024. Smart water irrigation for rice farming through the internet of things. arXiv:2402.07917.

Biswas, M., Akhund, T. M. N.U., Ferdous, M.J., Kar, S., Anis, A., Shanto, S.A., 2021. Biot: blockchain based smart agriculture with internet of thing. In: 2021 Fifth World Conference on Smart Trends in Systems Security and Sustainability (WorldS4). IEEE, pp. 75–80.

Boursianis, A.D., Papadopoulou, M.S., Diamantoulakis, P., Liopa-Tsakalidi, A., Barouchas, P., Salahas, G., Karagiannidis, G., Wan, S., Goudos, S.K., 2022. Internet of things (iot) and agricultural unmanned aerial vehicles (UAVs) in smart farming: a comprehensive review. Internet Things 18, 100187.

Bruno, I., Lobo, G., Covino, B.V., Donarelli, A., Marchetti, V., Panni, A.S., Molinari, F., 2020. Technology readiness revisited: a proposal for extending the scope of impact assessment of european public services. In: Proceedings of the 13th International Conference on Theory and Practice of Electronic Governance, pp. 369–380.

Bui, H.T., Aboutorab, H., Mahboubi, A., Gao, Y., Sultan, N.H., Chauhan, A., Parvez, M.Z., Bewong, M., Islam, R., Islam, Z., et al., 2024. Agriculture 4.0 and beyond: evaluating cyber threat intelligence sources and techniques in smart farming ecosystems. Comput. Security, 103754.

Carvalho, N., Adão, T., Morais, R., Costa, A.R., Peres, E., 2025. Cybersecurity in precision agriculture: a short review and a practical status assessment over mysense iot-based platform. Procedia Comput. Sci. 256, 255–266.

Catalano, C., Paiano, L., Calabrese, F., Cataldo, M., Mancarella, L., Tommasi, F., 2022. Anomaly detection in smart agriculture systems. Comput. Ind. 143, 103750.

CERT, N.Z., 2024. How ransomware happens and how to stop it. https://www.cert.govt.nz/information-and-advice/guides/how-ransomware-happens-and-how-to-stop-it/. [Online; accessed 20-Novemember-2024].

Chaganti, R., Varadarajan, V., Gorantla, V.S., Gadekallu, T.R., Ravi, V., 2022. Blockchain-based cloud-enabled security monitoring using internet of things in smart agriculture. Future Internet 14 (9), 250.

Conti, M., Dragoni, N., Lesyk, V., 2016. A survey of man in the middle attacks. IEEE Commun. Surv. Tutor. 18 (3), 2027–2051.

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

Drăgulinescu, A.-M., Constantin, F., Orza, O., Bosoc, S., Streche, R., Negoita, A., Osiac, F., Balaceanu, C., Suciu, G., 2021. Smart watering system security technologies using blockchain. In: 2021 13th International Conference on Electronics, Computers and Artificial Intelligence (ECAI). IEEE, pp. 1–4.

El-Ghamry, A., Darwish, A., Hassanien, A.E., 2023. An optimized CNN-based intrusion detection system for reducing risks in smart farming. Internet Things 22, 100709.

El Sakka, M., Ivanovici, M., Chaari, L., Mothe, J., 2025. A review of CNN applications in smart agriculture using multimodal data. Sensors 25 (2), 472.

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

Esteban, A.P., 2019. Algri: a programming model and algorithm for building a smart agricultural production system. Agric. Res. Technol.: Open Access J. 22 (5), 195–208.

Esteban, A. P.L., Santos, R. A.G., 2025. Development and assessment of online platform for crop production with decision support system. J. Multidiscip. Res. Dev.) 4 (1).

Fathy, C., Ali, H.M., 2023. A secure iot-based irrigation system for precision agriculture using the expeditious cipher. Sensors 23 (4), 2091.

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

Ferrag, M.A., Shu, L., Yang, X., Derhab, A., Maglaras, L., 2020. Security and privacy for green iot-based agriculture: review, blockchain solutions, and challenges. IEEE Access 8, 32031–32053. https://doi.org/10.1109/ACCESS.2020.2973178

Ferreira, R., Bispo, I., Rabadão, C., Santos, L., de C. Costa, R.L., 2025. Farm-flow dataset: intrusion detection in smart agriculture based on network flows. Comput. Electr. Eng. 121, 109892.

Franceschini, F., Maisano, D., Mastrogiacomo, L., 2016. Empirical analysis and classification of database errors in scopus and web of science. J. Informetr. 10 (4), 933–953. https://doi.org/10.1016/j.joi.2016.07.003

Fu, R., Ren, X., Li, Y., Wu, Y., Sun, H., Al-Absi, M.A., 2023. Machine-learning-based uav-assisted agricultural information security architecture and intrusion detection. IEEE Internet Things J. 10 (21), 18589–18598.

Gerance, M.D., Rufina, K.S., Fabito, J., Magnaye, N., 2025. Sabatech: a banana fruit pest and disease detection web application. Am. J. Data Sci. Artif. Intell. (AJDSAI) 1 (1).

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

Guven, I., Parlak, M., 2022. Blockchain, ai and iot empowered swarm drones for precision agriculture applications. In: 2022 IEEE 1st Global Emerging Technology Blockchain Forum: Blockchain & beyond (iGETblockchain). IEEE, pp. 1–6.

Harini, M., Dhinakaran, D., Prabhu, D., Sankar, S.M.U., Pooja, V., Sruthi, P.K., 2023. Levarging blockchain for transparency in agriculture supply chain management using iot and machine learning. In: 2023 World Conference on Communication & Computing (WCONF). IEEE, pp. 1–6.

International Organization for Standardization, 2023. Systems and software engineering - Systems and software Quality Requirements and Evaluation (SQuaRE) - Product quality model. Available at: https://www.iso.org/standard/ [Accessed: 20-Novemeber 2024].

Javeed, D., Gao, T., Saeed, M.S., Kumar, P., 2023. An intrusion detection system for edge-envisioned smart agriculture in extreme environment. IEEE Internet Things J..

Jeyabalu, M., Ghodi, A.S., Balasubramanian, S., Chinnayan, B., Jayapal, J., 2024. Internet of things-based smart agriculture advisory system. In: Intelligent Robots and Drones for Precision Agriculture. Springer, pp. 159–177.

Kaushal, A., Almurshed, O., Almoghamis, O., Alabbas, A., Auluck, N., Veeravalli, B., Rana, O., 2024. Shield: a secure heuristic integrated environment for load distribution in rural-ai. Future Gen. Comput. Syst. 161, 286–301.

Kethineni, K., Gera, P., 2023. Iot-based privacy-preserving anomaly detection model for smart agriculture. Systems 11 (6), 304.

Kethineni, K., Pradeepini, G., 2024. Intrusion detection in internet of things-based smart farming using hybrid deep learning framework. Cluster Comput. 27 (2), 1719–1732.

Koduru, T., Koduru, N.P., 2022. An overview of vulnerabilities in smart farming systems. J. Stud. Res. 11 (1), 1–14.

Kumar, P., Gupta, G.P., Tripathi, R., 2021a. Pefl: deep privacy-encoding-based federated learning framework for smart agriculture. IEEE Micro 42 (1), 33–40.

Kumar, R., Kumar, P., Aljuhani, A., Islam, A.N., Jolfaei, A., Garg, S., 2022. Deep learning and smart contract-assisted secure data sharing for iot-based intelligent agriculture. IEEE Intell. Syst. 38 (4), 42–51.

Kumar, R., Kumar, P., Tripathi, R., Gupta, G.P., Gadekallu, T.R., Srivastava, G., 2021b. Sp2f: a secured privacy-preserving framework for smart agricultural unmanned aerial vehicles. Comput. Networks 187, 107819.

Maddikunta, P. K.R., Pham, Q.-V., Prabadevi, B., Deepa, N., Dev, K., Gadekallu, T.R., Ruby, R., Liyanage, M., 2022. Industry 5.0: a survey on enabling technologies and potential applications. J. Ind. Inf. Integr. 26, 100257.

Mankins, J.C., et al., 1995. Technology readiness levels. White Paper, April 6, 1995.

Maurya, V.K., Rathore, N.S., Khan, L., Sachdev, P., 2023. Adopting blockchain technology for smart farming and food security. In: International Conference on Data Science and Applications. Springer, pp. 583–594.

Mehare, J., Gaikwad, A., 2023. Secured framework for smart farming in hydroponics with intelligent and precise management for iot with blockchain technology. J. Data Acquisition Process. 38 (2), 127.

Mehare, J.P., Bartere, M.M., 2021. Lightweight blockchain secured framework for smart precise farming system. In: 2021 International Conference on Computational Intelligence and Computing Applications (ICCICA). IEEE, pp. 1–6.

Mohanta, B.K., Chedup, S., Dehury, M.K., 2021. Secure trust model based on blockchain for internet of things enable smart agriculture. In: 2021 19th OITS International Conference on Information Technology (OCIT). IEEE, pp. 410–415.

Mohy-eddine, M., Guezzaz, A., Benkirane, S., Azrour, M., 2024. Malicious detection model with artificial neural network in iot-based smart farming security. Cluster Comput., 1–16.

Morel, A.E., Ufuktepe, D.K., Ignatowicz, R., Riddle, A., Qu, C., Calyam, P., Palaniappan, K., 2021. Enhancing network-edge connectivity and computation security in drone video analytics. In: 2020 IEEE Applied Imagery Pattern Recognition Workshop (AIPR). IEEE, pp. 1–12.

Mukherjee, P., Barik, R.K., Pradhan, C., 2020. Agrochain: ascending blockchain technology towards smart agriculture. In: International Conference on Emerging Trends and Advances in Electrical Engineering and Renewable Energy. Springer, pp. 53–60.

Peng, L., Jinli, L., 2023. Research on agricultural products recommendation system using spark technology. In: 2023 IEEE 11th Joint International Information Technology and Artificial Intelligence Conference (ITAIC). Vol. 11. IEEE, pp. 331–334.

Petersen, K., Vakkalanka, S., Kuzniarz, L., 2015. Guidelines for conducting systematic mapping studies in software engineering: an update. Inf. Softw. Technol. 64, 1–18. https://doi.org/10.1016/j.infsof.2015.03.007

Raghuvanshi, A., Singh, U.K., Sajja, G.S., Pallathadka, H., Asenso, E., Kamal, M., Singh, A., Phasinam, K., 2022. Intrusion detection using machine learning for risk mitigation in iot-enabled smart irrigation in smart farming. J. Food Qual. 2022 (1), 3955514.

Rajak, P., Lachure, J., Doriya, R., 2022. Cnn-lstm-based ids on precision farming for iiot data. In: 2022 IEEE 4th International Conference on Cybernetics, Cognition and Machine Learning Applications (ICCCMLA). IEEE, pp. 99–103.

Rouzbahani, H.M., Karimipour, H., Fraser, E., Dehghantanha, A., Duncan, E., Green, A., Russell, C., 2022. Communication layer security in smart farming: A survey on wireless technologies. arXiv:2203.06013.

Saadouni, R., Gherbi, C., Aliouat, Z., Harbi, Y., Khacha, A., Mabed, H., 2025. Securing smart agriculture networks using bio-inspired feature selection and transfer learning for effective image-based intrusion detection. Internet Things 29, 101422.

Saba, T., Rehman, A., Haseeb, K., Bahaj, S.A., Lloret, J., 2023. Trust-based decentralized blockchain system with machine learning using internet of agriculture things. Comput. Electr. Eng. 108, 108674.

Sadeghizadeh, E., Sobhani, S. M.J., Forouzani, M., 2025. Alignment of the TRL-MRL for selected smartphone-based applications in agricultural extension and education. Agric. Educ. Administration Res. 16 (71), 98–109.

Sajid, J., Hayawi, K., Malik, A.W., Anwar, Z., Trabelsi, Z., 2023. A fog computing framework for intrusion detection of energy-based attacks on UAV-assisted smart farming. Appl. Sci. 13 (6), 3857.

Sakthi, U., Thangaraj, K., Anuradha, M., Kirubakaran, M.K., 2023. Blockchain-enabled precision agricultural system using iot and edge computing. In: International Conference on Smart Trends in Computing and Communications. Springer, pp. 397–405.

Sanghvi, H.P., Dahiya, M.S., 2013. Cyber reconnaissance: an alarm before cyber attack. Int. J. Comput. Appl. 63 (6).

Sarowa, S., Kumar, V., Bhanot, B., Kumar, M., 2023. Enhancement of security posture in smart farming: challenges and proposed solution. In: 2023 International Conference on Device Intelligence, Computing and Communication Technologies,(DICCT). IEEE, pp. 1–5.

Shaihn, Singh, 2023. Owasp machine learning security top ten. Available online at: https://owasp.org/www-project-machine-learning-security-top-10/.

Shaikh, T.A., Rasool, T., Lone, F.R., 2022. Towards leveraging the role of machine learning and artificial intelligence in precision agriculture and smart farming. Comput. Electron. Agric. 198, 107119.

Shen, R., Zhang, H., Chai, B., Wang, W., Wang, G., Yan, B., Yu, J., 2025. Bafl-svm: a blockchain-assisted federated learning-driven svm framework for smart agriculture. High-Confidence Comput. 5 (1), 100243.

Shreya, S., Chatterjee, K., Singh, A., 2023. Bfsf: a secure iot based framework for smart farming using blockchain. Sustain. Comput.: Inform. Syst. 40, 100917.

Singh, A., Musale, V., 2024. Crop prevention through machine learning and IOT with cloud security using blockchain. In: AIP Conference Proceedings. Vol. 3028. AIP Publishing, pp. 020–086.

Smmarwar, S.K., Gupta, G.P., Kumar, S., 2022. Deep malware detection framework for iot-based smart agriculture. Comput. Electr. Eng. 104, 108410.

Subramani, J., Maria, A., Rajasekaran, A.S., Lloret, J., 2024. Physically secure and privacy-preserving blockchain enabled authentication scheme for internet of drones. Security Privacy 7 (3), e364.

Sumarudin, A., Putra, W.P., Puspaningrum, A., Suheryadi, A., Anam, I.S., Yani, M., Hanif, I., 2022. Implementation of iot sensored data integrity for irrigation in precision agriculture using blockchain ethereum. In: 2022 5th International Seminar on Research of Information Technology and Intelligent Systems (ISRITI). IEEE, pp. 29–33.

Sumathi, M., Rajkamal, M., Raja, S.P., Venkatachalapathy, M., Vijayaraj, N., 2022. A crop yield prediction model based on an improved artificial neural network and yield monitoring using a blockchain technique. Int. J. Wavelets Multiresolut. Inf. Process. 20 (06), 2250030.

Syverson, P., 1994. A taxonomy of replay attacks [cryptographic protocols]. In: Proceedings the Computer Security Foundations Workshop VII. IEEE, pp. 187–191.

Tchakoucht, T.A., Ezziyyani, M., 2018. Building a fast intrusion detection system for high-speed-networks: probe and dos attacks detection. Procedia Comput. Sci. 127, 521–530.

Thilakarathne, N.N., Bakar, M. S.A., Abas, P.E., Yassin, H., 2025. A novel cyber threat intelligence platform for evaluating the risk associated with smart agriculture. Sci. Rep. 15 (1), 3904.

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

Vardhani, V., Vasunthara, K., Vaishnavi, V., Saravanan, T.P., Krishnamoorthy, V., 2023. Revolutionizing agriculture: smart farming with autonomous robots and AI. In: International Conference on Innovations in Bio-Inspired Computing and Applications. Springer, pp. 160–167.

Vatambeti, R., Venkatesh, D., Mamidisetti, G., Damera, V.K., Manohar, M., Yadav, N.S., 2023. Prediction of DDos attacks in agriculture 4.0 with the help of prairie dog optimization algorithm with IDSNet. Sci. Rep. 13 (1), 15371.

Wolfert, S., Ge, L., Verdouw, C., Bogaardt, M.-J., 2017. Big data in smart farming–a review. Agric. Syst. 153, 69–80.

Wu, F., Cui, L., Yao, S., Yu, S., 2024. Inference attacks in machine learning as a service: A taxonomy, review, and promising directions. arXiv:2406.02027.

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), 7518.

Zahid, F., Kuo, M. M.Y., Sinha, R., 2025. Light-weight slow-rate attack detection framework for resource-constrained industrial cyber-physical systems. Comput. Security, 104508.

Zarpelão, B.B., Miani, R.S., Kawakani, C.T., De Alvarenga, S.C., 2017. A survey of intrusion detection in internet of things. J. Network Comput. Appl. 84, 25–37.

Zeng, H., Dhiman, G., Sharma, A., Sharma, A., Tselykh, A., 2023. An iot and blockchain-based approach for the smart water management system in agriculture. Expert Syst. 40 (4), e12892.

Zhang, G., Chen, X., Zhang, L., Feng, B., Guo, X., Ling, J., Zhang, Y., 2022. Staibt: blockchain and cp-abe empowered secure and trusted agricultural iot blockchain terminal. IJIMAI 7 (5), 66–75.

Zidi, K., Abdellafou, K.B., 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, 108579.

Zrelli, A., Nakkach, C., Ezzedine, T., 2022. Cyber-security for iot applications based on ANN algorithm. In: 2022 International Symposium on Networks, Computers and Communications (ISNCC). IEEE, pp. 1–5.