Manuscript submitted to *Security and Safety*, For Peer Review Only, Vol. x, xxxxxxx (2025)
https://doi.org/10.1051/sands/xxxxxxx
sands.edpsciences.org

Section Category

A Perspective on Security of Smart Farming: Attacks and Countermeasures

Ruonan Li[1], Tiantian Liu[2], and Jie Liu[3,4*]

[1] *Department of New Networks, Pengcheng Laboratory, Shenzhen 518000, China*
[2] *Department of Information Science, Xiamen University,Xiamen 361005, China*
[3] *State Key Laboratory of Smart Farm Technologies and Systems, Harbin 150001 ,China*
[4] *Faculty of Computing, Harbin Institute of Technology, Harbin, 150001, China*

Abstract The integration of technologies like the Internet of Things (IoT) and Artificial Intelligence (AI) is fueling a shift toward smart farming, unlocking a fundamental change in how agriculture is practiced through new precision agriculture techniques. While these innovations enhance efficiency and streamline routine agricultural operations, they also introduce a range of new threats and vulnerabilities within smart farming ecosystems. This research differentiates itself within the field of smart farming security. It achieves this through an integrated examination of systemic vulnerabilities across the entire agricultural technology stack. Organized into four core sections, i.e., sensing, network, cloud, and application layers, it systematically identifies the specific security risks associated with each layer, including data leakage, signal injection, cyberattacks, and manipulation of artificial intelligence systems. The paper further discusses appropriate countermeasures designed to mitigate these risks and underscores the importance of adopting integrated defense strategies. By analyzing current cybersecurity trends and the application of artificial intelligence in protective mechanisms, the study provides valuable insights into future research pathways aimed at establishing secure and sustainable agricultural technologies.

Keywords Smart farming, smart farming security, cybersecurity, IoT security

Citation R Li, T Liu and J Liu. A Perspective on Security of Smart Farming: Attacks and Countermeasures. Security and Safety 2025; **x**: xxxxxxx. https://doi.org/10.1051/sands/xxxxxxx

1 Introduction

Agriculture, encompassing crop cultivation, livestock production, and forestry, serves as the cornerstone of human survival and development. A 70% growth in global food production is required by 2050, according to United Nations' Food and Agriculture Organization (FAO) projections based on current output [1]. To address this impending shortage and mitigate losses caused by natural disasters, it is imperative to minimize the dependency of agricultural systems on environmental conditions. Smart farming represents a fundamental shift in agriculture, leveraging breakthroughs in artificial intelligence (AI), the Internet of Things (IoT), and related innovations to significantly boost crop yields, enhance resource use, and advance sustainability[2]. Globally, its adoption is evidenced by diverse applications, such as soil sensors for monitoring[3], automation replacing manual labor[4], and intelligent irrigation systems improving resource allocation and productivity[5].

Despite its transformative potential, the integration of digital technologies into agriculture introduces significant security risks[6, 7]. As farming systems grow increasingly interconnected, they become vulnerable to cyberattacks, data breaches, and systemic failures. These challenges are further exacerbated by the

* Corresponding author (email: jieliu@hit.edu.cn)

multi-layered architecture of smart farming, consisting of the sensing, network, cloud, and application layers, each vulnerable to distinct threats[8]. Specifically, the sensing layer faces data leakage and injection, while the network layer is exposed to communication hijacking and denial-of-service attacks. Similarly, cloud-based platforms risk data breaches, and AI-driven automation systems are prone to adversarial manipulations and hijacking. In response to these exposures, developing dedicated security architectures is imperative to address the specific operational and environmental realities of farm-based cyber-physical systems.

The security of smart farming transcends technical concerns, directly impacting food safety, supply chain integrity, and global food security. Existing research remains fragmented, lacking holistic approaches to address the interconnected vulnerabilities across smart farming layers. As shown in Figure 1, this study establishes a layered security framework for smart farming, identifying vulnerabilities and corresponding defenses at each level of the system architecture. By examining the sensing layer's susceptibility to physical attacks, the network layer's exposure to cyber intrusions, the cloud layer's data storage risks, and the application layer's AI-specific vulnerabilities, we propose integrated defense strategies to fortify agricultural systems. Our analysis aims to address knowledge gaps by offering a strategic guide for researchers, practitioners, and policymakers to enhance the resilience of smart farming against evolving cybersecurity threats and ensure its sustainable future.

Figure 1. The Layered security architecture of smart farming, including sensing, network, cloud, and application layers.

2 Background of Smart Farming

Throughout the endless flow of human history, agriculture has served as the cornerstone for the survival of humanity and the advancement of civilization. With the rapid progression of technological innovation, farming tools have evolved from rudimentary implements such as sickles and shovels to advanced technologies like Unmanned Aerial Vehicles (UAVs). The fusion of AI[9], cloud computing[10], and big data analytics[11] with traditional farming has catalyzed the emergence of smart farming, a paradigm synonymous with digital agriculture. Smart farming represents a bio-cyber-physical farm cycle, where data—ranging from granular field sensor readings to broad-scale geospatial imagery—undergoes cyclic processing, analysis, and model utilization. This enables precise farm management aimed at enhancing both the quantity and quality of crop yields. A multitude of smart agricultural tools and applications have emerged to optimize crop production and environmental conditions. These tools support the monitoring and management of key agricultural processes, including crop growth, irrigation, pest control, fertilizer application, weed management, and greenhouse climate regulation. In addition, they enhance resource utilization efficiency and reduce operational costs. For instance, in Henan, China, light devices equipped with high-definition cameras and sensors are deployed across wheat fields to collect data on grain growth[12]. The collected data is fed into a centralized analytics platform that supports precise, data-driven decision-making for farm operators. Similarly, in Chile, soil sensors have been implemented to monitor blueberry irrigation, resulting in a 70% reduction in water usage[13]. Demonstrating a strong Compound Annual Growth Rate (CAGR) of 19.09% from 2024 to 2034, the smart agriculture sector is set for major expansion. Its market value, estimated at USD $17.40 billion in 2023, is anticipated to surge to USD $117.20 billion by 2034[14]. Recognizing smart farming as a key enabler for global food security and sustainable practices, it is imperative to comprehensively understand the threats it faces. Furthermore, it is imperative to develop corresponding countermeasures to mitigate these risks before they escalate. To systematically analyze the security ecosystem of smart farming, we deconstruct its architecture into four distinct layers: the sensing layer, network layer, cloud layer, and application layer.

3 Property of Smart Farming Security

Regardless of the rapid evolution of smart farming, the research and practices of its security fundamentally surround the following core properties[15]:

- **Data privacy** in smart farming refers to safeguarding sensitive agricultural information including farm conditions, crop growth parameters, soil moisture levels, and operational strategies, from unauthorized access and disclosure. Even minor incidents, like the theft of soil moisture data, can enable adversaries to infer crop yields and manipulate market strategies, highlighting the critical need for robust data protection. For example, Bayer's Climate FieldView platform underwent a significant change in its data policy—the 2019 version explicitly promised not to use farmer data (including aggregated data) for seed pricing or speculative commodity trading, but subsequent versions quietly removed this restrictive language, leaving room for the use of farm data in financial operations such as hedging[16]. This case also indirectly illustrates how attackers could use leaked farmer data—such as soil moisture levels—to estimate crop yields and manipulate the market.
- **Data Integrity** denotes a fundamental property of agricultural data, guaranteeing its correctness, reliability, and unaltered state from collection to archiving, which underpins trustworthy analytics and decision-making. In smart farming, compromised or tampered data can lead to flawed decision-making, affecting critical operations such as irrigation scheduling, pesticide application, and yield prediction. Some threats like out-of-band injection attacks, can introduce false information or interference, resulting in inefficiencies and significant economic losses. For instance, an example of a rectification attack [17], in which an attacker exploited the rectification effect of an amplifier in a circuit component to induce misleading data in a temperature sensor, demonstrates how data tampering can lead to erroneous decisions.
- **System Resilience** describes the inherent capacity of smart farming infrastructures to maintain essential operations and autonomously restore functionality following disruptive events, including security breaches and hardware failures. Given the interconnected nature of smart farming, where IoT devices, cloud platforms, and AI models operate in synergy, a single point of failure can trigger

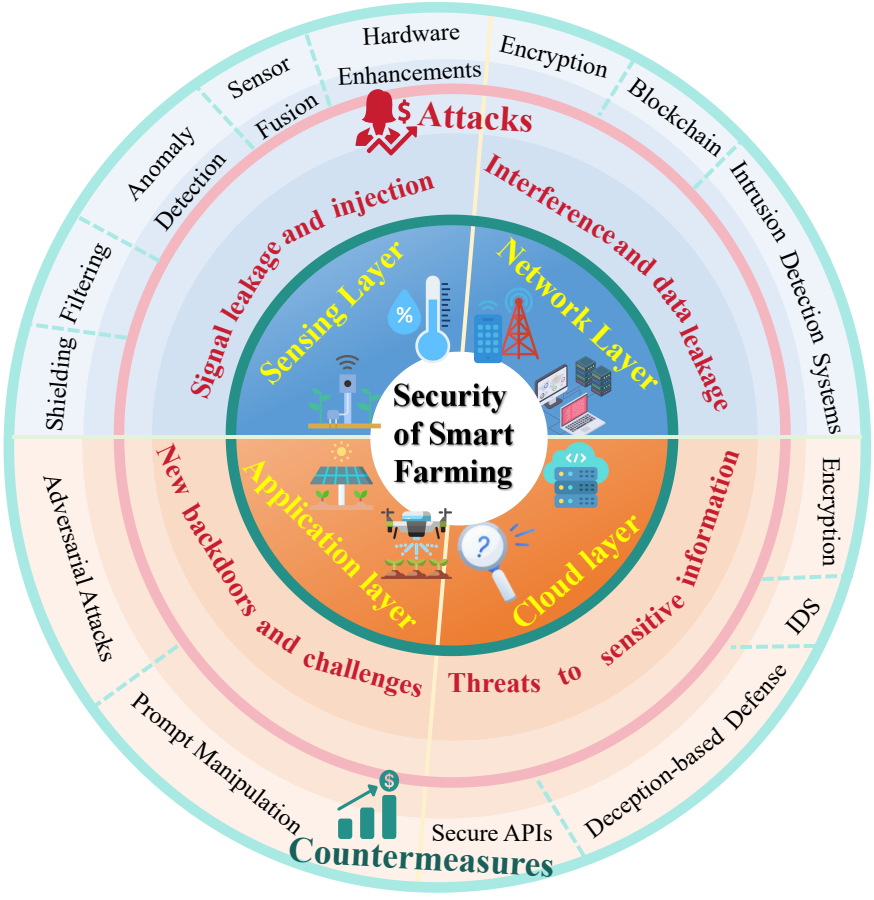

Figure 2. Overview of major security threats and defense mechanisms of smart farming systems at various levels.

cascading effects, disrupting entire farm operations.Taking a smart irrigation system as an example, an attacker exploited a system idle period to hijack communications between the smart irrigation system and weather services via an ARP spoofing attack within the LAN, triggering a chain of failures [18].

– **System Reliability** is the foundation of smart farming, ensuring that technologies operate consistently and accurately across diverse conditions. When systems experience failures due to hardware malfunctions, software glitches, or inaccuracies in AI models, farm operations can be disrupted, leading to yield losses and increased costs. Achieving reliability requires robust hardware designs, well-maintained network infrastructures, and adaptive software models capable of handling invasion variability.For instance, researchers at the University of California, Irvine (UC Irvine) developed an attack method called FusionRipper that enables complete control over vehicle positioning[19]. This case also demonstrates that autonomous vehicles experience exponential positioning errors when faced with GPS spoofing attacks.

By ensuring these key properties through robust technical measures, such as anomaly detection and blockchain-based anonymity, we can facilitate the sustainable and secure adoption of smart farming. Figure 2 provides an overview of major security threats and defense mechanisms in smart farming. The attacks and countermeasures discussed across four distinct layers inherently contribute to safeguarding these properties. Analyzing threats and vulnerabilities from an offensive perspective provides defenders with valuable insights for evaluating risks. Only through a deep understanding of attack mechanisms can a comprehensive defense system be effectively designed and implemented.

4 Sensing Layer: Data leakage and injection on physical-to-digital transformation

4.1 Sensing sensor

Sensors act as the foundational components of smart farming systems by converting physical signals into digital data for subsequent processing, acting as the essential sensory organs for tactile, visual, and auditory perception[20, 21]. Commonly deployed sensors in agricultural settings include soil moisture sensors, livestock health monitors, and cameras for crop health assessment. The continuous surveillance of ambient and biological parameters by these devices is central to maintaining a controlled agricultural setting. The insights derived from this real-time data are crucial for preserving the integrity and quality of the agricultural output[22].

4.2 Data leakage and injection

The primary security concerns in the sensing layer stem from *data leakage and injection attacks*.The energy consumption and electromagnetic radiation generated by sensor operation lead to data and data leakage, which attackers can exploit through side-channel signals, an attack vector commonly known as *side-channel attacks*. The pioneering work of Van Eck established the feasibility of image reconstruction by intercepting and decoding the electromagnetic emanations from Cathode Ray Tube (CRT)-based video displays[23]. This attack methodology has been extended and proven effective against modern intelligent terminals, including computer monitors and smart cameras[24]. Beyond visual data, side-channel attacks can also extract sensitive information by analyzing patterns and variations in power consumption, timing, or electromagnetic emissions through USB cables connected with devices, even when the data is encrypted[25, 26].

Unlike passive side-channel attacks, injection attacks actively transmit malicious signals to target sensors, either to introduce false data or to cause interference[27]. These attacks can be categorized into in-band and out-of-band attacks based on the nature of the injected signal[28]. In-band attacks involve replaying signals within the sensor's normal operating frequency, such as transmitting recorded sounds to microphone sensors or replaying optical signals to light sensors, ultimately deceiving and disrupting back-end systems. In contrast, out-of-band attacks leverage signals outside the sensor's normal working channel and frequency, including ultrasound attacks[29], laser attacks[30], and Electro-Magnetic Interference (EMI) attacks[17]. American researchers have shown that EMI can induce spoofed data in temperature sensors by exploiting the rectification effects of amplifiers in circuit components, thereby spoofing internal systems into triggering unnecessary heating or cooling actions[31]. Similarly, various studies have demonstrated that microphone sensors can inadvertently receive and process malicious data encoded in ultrasonic signals. This is due to amplifier nonlinearity, while the photoelectric effect also allows such processing for malicious data encoded in laser signals. Additionally, Khazaaleh et al. successfully manipulated the voltage output of gyroscope sensors through ultrasonic attacks[**?**], highlighting the broad spectrum of vulnerabilities in sensor-based systems.

Given the demonstrated vulnerabilities of agricultural sensors to side-channel and injection attacks, there is an urgent need to develop robust defense mechanisms to safeguard smart farming systems.

4.3 Defense and countermeasure

Table 1 shows a comparison of sensing-layer defense mechanisms. Effectively countering these threats is a foundational pillar for maintaining trustworthy data and stable operations within the modern, interconnected ecosystem of digital agriculture. Researchers have explored a variety of defense strategies to secure smart farming systems, including *shielding, filtering, anomaly detection, sensor fusion, and hardware enhancements*[32]. Shielding techniques offer robust protection by isolating sensors from external electromagnetic and acoustic interference[33]. Common approaches include radio frequency shielding, acoustic dampening materials, and physical isolation, which are widely recommended to mitigate out-of-band injection attacks. Filtering mechanisms have also been extensively studied as a countermeasure against signal injection attacks. For example, Kune et al. demonstrated that adaptive Finite Impulse Response (FIR) filters can effectively attenuate malicious electromagnetic signals while preserving legitimate data

transmission[34]. Proposed countermeasures at the hardware level to mitigate electromagnetic interference include the integration of biased voltage generators[35] and the transition from Hard-Disk Drives (HDDs) to Solid-State Drives (SSDs). However, these methods often require significant hardware modifications, which can be costly and impractical for Micro-Electromechanical Systems (MEMS) sensors. An alternative approach leverages the unique electromagnetic emissions of devices and the feature patterns of benign sensing inputs for security purposes. Sensor fusion and anomaly detection provide software-based solutions to identify and mitigate signal manipulation. Sensor fusion enhances system resilience by integrating data from multiple sensors to resolve inconsistencies and prevent erroneous decisions[36]. For instance, Tharayil et al. developed an advanced fusion algorithm that correlates measurements from gyroscopes and magnetometers using mathematical relationships, enabling the detection of adversarial injections without hardware modifications[37]. Anomaly detection, on the other hand, identifies deviations in sensor data caused by attacks. Techniques such as Zhang et al.'s RADAR method analyze electromagnetic sideband patterns and employ classification algorithms to detect and mitigate electromagnetic attacks[38]. Similarly, spectrum analysis can differentiate forged signals from legitimate ones by examining variations in sensing data[39, 40].

Despite these advancements, most existing defenses are limited to addressing a single type of injected signal and often require additional hardware, making them unsuitable for low-level sensors. Consequently, there is an urgent need for a holistic defensive strategy that can thwart diverse data leakage and injection attacks while remaining viable within the constraints typical of agricultural settings.

Table 1. Comparison of defense mechanisms at the sensing layer

Defense Mechanism	Implementation Approach	Applicable Attack Types	Limitations
Shielding	RF shielding enclosure; acoustic damping materials; physical isolation.	EMI attacks; ultrasonic attacks;laser attacks	Increases device size and cost; difficult to apply to MEMS sensors
Filtering	Adaptive FIR filters; signal preprocessing;spectrum analysis	EMI injection attacks;in-band signal injection.	Limited effectiveness against novel/adaptive attacks; may affect legitimate signals
Anomaly Detection	ML classifiers; electromagnetic sideband analysis; statistical deviation detection	Signal injection attacks; sensor spoofing; data tampering.	Relies on high-quality training data; suffers from false positives/negatives; struggles against zero-day attacks
Sensor Fusion	Multi-sensor cross-validation; IMU+magnetometer fusion; mathematical relationship verification	Sensor spoofing; signal injection;side-channel attacks.	Complex sensor synchronization; increases system power consumption and data bandwidth requirements

5 Network Layer: Security threats in communication and transmission

5.1 Communication and transmission

Table 2 shows a comparison of defense mechanisms at the network layer. The network layer in smart farming serves as the critical infrastructure connecting sensing devices to application platforms, acting as the "vascular system" that transmits data across farms and greenhouses[41]. It employs various communication technologies such as WiFi, LTE, Bluetooth, and ZigBee to bridge heterogeneous communication standards and maintain reliable connectivity[42]. The selection of network type depends on specific agricultural requirements, including data rate, coverage range, and energy constraints. With advancements

in 5G, for example, farmers can now operate drones over long distances to efficiently monitor and audit livestock[43]. Lei et al. proposed a channel model for LoRa-based underground sensor networks to improve signal transmission in complex environments[44], while Chang et al. demonstrated soil moisture estimation using LoRa signal phase shifts, eliminating the need for dedicated sensors[45]. However, despite its critical role, the network layer is also a common target for cybersecurity threats, such as Denial-of-Service (DoS) attacks and botnets, which can disrupt data transmission and compromise system functionality.

5.2 Interference and data leakage in network

Cyber threats targeting this layer primarily focus on data privacy and system resilience. One of the most prevalent attacks is the *Distributed Denial-of-Service (DDoS) attack*[46], which overloads agricultural networks by consuming critical resources such as bandwidth and storage. The core objective of a DDoS attack is service disruption, contrasting with attacks aimed at data theft or unauthorized access. When targeting critical infrastructure like internet-dependent smart irrigation systems, such attacks can employ botnets to flood networks, directly leading to operational failure and the uncontrolled depletion of water resources[18]. For example,a standard water tower's reserves can be depleted within one hour by a botnet comprising 1,355 individual sprinkler controllers operating in concert. Another common DDoS attack targeting agricultural Wireless Sensor Networks (WSNs) is the sinkhole attack[47]. In this scenario, an insider attacker exploits knowledge of neighboring nodes' routines to attract their traffic, affecting all nodes in the network regardless of their distance from the base station. A sinkhole attack serves as a gateway for other internal attacks by funneling surrounding data through the compromised node, allowing malicious manipulation of the data[48]. Jamming attacks[49], another form of DDoS, operate by deliberately introducing interference to degrade the Signal-to-Interference-plus-Noise Ratio (SINR). This can be achieved through different jammer designs, including constant, deceptive, random, and reactive types. Additionally, *Man-In-The-Middle (MITM) attacks* intercept and modify data during transmission[50], leading to data corruption or leakage of sensitive information, thus compromising the accuracy of agricultural decision-making. In an IoT-based agricultural network, MITM attacks may occur in protocols such as ZigBee, Bluetooth, and RFID, allowing attackers to intercept communications between nodes, eavesdrop on the farm status of IoT agricultural devices, and potentially prepare for further attacks or disruptions[51, 52]. *Malware attacks*, another significant cyber threat, involve the implantation of viruses, worms, trojans, and other malicious software to disrupt the operation of agricultural IoT devices, leading to data breaches or system paralysis. Notable examples of such attacks include BASHLITE and Hydra[53]. *Ransomware attacks*, where attackers encrypt files or lock users out of their systems, rendering them inaccessible, are increasingly targeting the food and agriculture sectors[**?**]. Reports indicate that the frequency of ransomware attacks has risen, with the average doubling from 2019 to 2020[54]. The largest ransom demands have surpassed $20 million USD, and from 2018 to May 2023, ransomware incidents affected 157 food, beverage, and agriculture organizations, including high-profile attacks on the beef supply chain. Consequently, securing agricultural networks has become an increasingly complex challenge.

5.3 Defense and countermeasure

The network layer remains a critical focus for securing smart agricultural systems, with *encryption, blockchain, and deep learning (DL)-based Intrusion Detection Systems (IDS)* emerging as key solutions for ensuring data integrity and privacy. Communication across sensor-to-sensor, sensor-to-system, and system-to-system interfaces requires robust encryption protocols. Commonly, TLS/SSL protocols are used for secure data transmission between sensor nodes and gateways[55]. Furthermore, symmetric and asymmetric encryption methods have been tailored for resource-constrained IoT devices, with lightweight encryption techniques like Elliptic Curve Cryptography (ECC) minimizing communication and computational overhead, as seen in TinyECC [56] and HECC implementations [57] for IoT and drone communications. Blockchain technology enhances security through immutable distributed ledgers, where agricultural data (e.g., soil parameters, livestock records) is cryptographically hashed and validated via consensus algorithms like Practical Byzantine Fault Tolerance (PBFT)[58]. To guarantee authenticity and prevent tampering, sensor-generated IoT data is recorded with precise timestamps. It is then

organized within a blockchain-inspired structure utilizing Merkle trees. For instance, Anusha Vangala et al. proposed AgroMobi Block[59], an efficient blockchain-based authentication and key establishment scheme for IoT-driven precision agriculture. Blockchain also enables food traceability systems that ensure transparency and security as food moves through the supply chain, tracking provenance and ensuring safety and quality. However, balancing security, energy consumption, and computational time remains a challenge for encryption-based and blockchain-based approaches. Researchers are using deep learning techniques, such as Convolutional Neural Networks (CNN) and Generative Adversarial Networks (GAN), to detect abnormal behaviors and improve IDSs for network attacks[60, 61]. For example, Kethineni and Pradeepini developed a combined CNN and Bi-Gate Recurrent Unit (GRU) model for detecting DDoS attacks[62]. Additionally, for secure and privacy-preserving threat identification, advanced frameworks such as Privacy-Encoding-based Federated Learning (PEFL) and Federated Learning-based IDS (FLIDS) have been developed. PEFL uses a two-level privacy mechanism and a federated learning-based GRU for intrusion detection, along with Long-Short Term Memory (LSTM) autoencoders for data classification.While DL-based IDSs show promise, they face challenges such as adapting to new attack types and the requirement for large, labeled datasets. To enhance security, integrating multiple defense mechanisms into a multi-layered framework is essential. For example, Kumar et al. proposed a secured privacy-preserving framework for UAVs in smart agriculture [25]. The framework combines a two-level privacy engine, blockchain with enhanced proof of work for data authentication, sparse autoencoders to prevent inference attacks, and a stacked LSTM network for anomaly detection and attack classification. Therefore, network security in smart farming requires a multi-layered approach that balances protection and efficiency. Future research should prioritize: (1) adaptive security mechanisms capable of evolving with emerging threats, (2) energy-efficient cryptographic protocols for edge devices, and (3) standardized datasets to improve DL-IDS generalizability. The convergence of these advancements will be critical to achieving resilient, privacy-preserving smart agriculture systems capable of sustaining global food security in an increasingly connected world.

Table 2. Comparison of defense mechanisms at the network layer

Defense Mechanism	Typical Technologies	Major Challenges	Applicable Scenarios
Encryption	ECC;TinyECC;HECC	Complex key management	Sensor-to-gateway; device-to-cloud; drone communications
Blockchain	PBFT;PoW;AgroMobi Block	Power consumption and latency issues	Food traceability; supply chain transparency; cross-farm data authentication
Deep Learning-based IDS	CNN+Bi-GRU; GAN; LSTM	Reliance on large-scale labeled datasets	Anomalous traffic detection; DDoS attack identification; unknown threat discovery

6 Cloud layer: Data storage and threats on cloud-enabled platforms

6.1 Cloud-enabled farming platforms

Table 3 shows a comparison of defense mechanisms at the cloud layer. The cloud layer serves as the "brain" of smart farming, where data sources are stored in centralized data repositories and advanced analytics are performed on cloud servers. The cloud layer offers three primary services: Infrastructure as a Service (IaaS), platform as a service (PaaS), and Software as a Service (SaaS)[63, 10, 64]. Specifically, IaaS provides virtualized resources to manage agricultural data, PaaS offers development environments and tools for application creation, and SaaS delivers ready-to-use applications for end-users, such as farmers and agronomists. Cloud computing, hosted on cloud servers, is a key technology within the cloud layer,

enabling the processing of data streams. It supports the concept of "anything as a service," whereby services are virtualized, pooled, shared, and can be rapidly provisioned and de-provisioned with minimal management effort. Currently, several advanced cloud platforms are enhancing smart farming, including the John Deere Operations Center[65] and Alibaba cloud's ET agricultural brain[66].

6.2 Threats to sensitive information in cloud

The cloud layer in smart farming systems faces multifaceted security threats across IaaS, PaaS, and SaaS service models, primarily stemming from shared infrastructure, virtualization, and multi-tenancy architectures. In IaaS for smart farming, agricultural enterprises store data and applications in virtualized environments. Vulnerabilities in hypervisors (e.g., Xen, VMware) can be exploited in *VM escape attacks*[67], where attackers break out of their virtual environment to access data from other virtual machines on the same physical host. Sensitive data, such as real-time weather or soil data collected by agricultural sensors, may be compromised. *Data remanence attacks* in IaaS exploit residual data remnants from deallocated resources[68], allowing attackers to recover sensitive information from previous tenants through both hardware degradation and logical storage remnants. In cloud-based FPGAs, attackers can use Time-to-Digital Converters (TDCs) to measure Bias Temperature Instability (BTI)-induced delays in routing[69], facilitating the reconstruction of cryptographic keys or runtime data. Additionally, virtualized storage systems may expose sensitive data, such as irrigation schedules or crop yield predictions, through forensic analysis of un-sanitized memory or swap files. Insufficient memory sanitization practices in hypervisors further increase this risk. The PaaS layer is vulnerable to *malicious service module injection*[70], where attackers upload compromised analytics tools or machine learning models to agricultural platforms. These tools can intercept or manipulate data pipelines, affecting crop yield predictions or contaminating pest detection algorithms. For instance, inserting malicious code into an irrigation management system could lead to incorrect watering decisions, damaging crops. SaaS applications, used for farm management, crop monitoring, and market analysis, are primarily accessed through web interfaces, making them vulnerable to *web-based attacks* such as Structured Query Language (SQL) injection or Cross-Site Scripting (XSS)[71]. SQL injection could expose sensitive agricultural data, such as production volumes or sales records, while XSS could be used to steal user credentials and gain unauthorized access. Additionally, *insecure APIs* exploitation leaves backdoor of weak authentication and inputs[72], allowing unauthorized access to sensitive farming data and models. These vulnerabilities can lead to market manipulation, biosecurity risks, and operational disruptions. To safeguard sensitive information and ensure the reliable functioning of smart farming operations, implementing robust security measures across every service layer is fundamental.

6.3 Defense and countermeasure

As a vital subfield of cybersecurity, cloud security employs privacy-enhancing technologies and adheres to defined policy frameworks to ensure the safe deployment and operation of cloud-based data, applications, and services. Key concepts in this area include *encryption, IDS, deception-based defense, and secure APIs.* Encryption techniques such as RSA, AES, and RC5 are widely utilized to protect data confidentiality in cloud environments[73**?** , 74], with advanced methods like Role-Based Encryption (RBE) and hybrid encryption (e.g., SSL and Diffie-Hellman) further bolstering security. These mechanisms ensure compliance with regulatory standards (e.g., ENISA/CSA) and provide comprehensive protection against interception, leakage, and unauthorized access. IDS in cloud computing has evolved into multi-layered frameworks, incorporating signature-based, anomaly-based, and hybrid approaches. Signature-based IDSs are efficient for detecting known attacks but struggle with zero-day and polymorphic threats. Anomaly-based systems, leveraging Machine Learning (ML) and DL[75], detect deviations from normal behavior but may generate false positives and face challenges like concept drift. Hybrid IDSs combine the strengths of both approaches and can integrate auxiliary technologies such as blockchain for enhanced accuracy and tamper-proof logging. In cloud computing, deception-based defense mechanisms like honeypots, decoy files, and fake databases are used to mislead adversaries[76, 77], protecting critical resources. However, the elastic and dynamic nature of cloud infrastructure poses challenges in effectively deploying and maintaining these techniques. The scalability and transient characteristics of cloud resources complicate

the management of deceptive elements, potentially diminishing their efficacy. Additionally, sophisticated attackers may bypass these measures, requiring continuous adaptation of deception strategies to address evolving threats. Therefore, while valuable, deception-based defenses in cloud computing require careful consideration of cloud architectures' unique challenges to maintain their effectiveness. Secure APIs are designed with robust authentication, authorization, and encryption protocols[78], ensuring data confidentiality, integrity, and access control in distributed cloud environments. Techniques such as OAuth 2.0, JWT, and TLS mitigate risks like unauthorized access[79, 70], data interception, and injection attacks. API gateways, rate limiting, and continuous monitoring further strengthen resilience against DDOS attacks and misuse. For smart agriculture applications, establishing a trustworthy cloud platform requires a carefully balanced multi-layered defense strategy that integrates these heterogeneous security mechanisms across the cloud preprocessing chain, addressing standardization challenges while optimizing both security efficacy and deployment feasibility to meet the unique demands of agricultural cloud ecosystems.

Table 3. Comparison of defense mechanisms at the cloud layer

Defense Mechanism	Protected Targets	Advantages	Limitations
Encryption	Data at rest; Data in transit; Access control	Ensures data confidentiality and integrity; Meets compliance requirements; Prevents interception and leakage	Complex key management; Performance overhead scales with data volume; Cannot prevent malicious actions by authorized users
Intrusion Detection System	VM escape attacks;Anomalous traffic and behavior;Known and unknown vulnerabilities	Multi-layered framework;Supports ML/DL integration; Enables blockchain-enhanced tamper-proof logging	Limited zero-day attack detection capability; Suffers from false positives/negatives; Faces concept drift challenges
Deception-Based Defense	Attacker reconnaissance activities;Insider threats;Data exfiltration attempts	Actively misleads attackers; Protects critical resources; Low false positive rate	Cloud elasticity and dynamics complicate deployment; Sophisticated attackers may bypass; Requires continuous deception strategy updates
Secure APIs	Web interface attacks; Unauthorized access; DDoS attacks	Strong authentication and authorization; Encrypted transmission; API gateway with rate limiting	Requires continuous monitoring and updates; High complexity; API abuse detection remains challenging

7 Application Layer: AI-driven and automation threats

7.1 AI and automation in smart farming applications

Over the past decades, the rapid advancement of AI and automation, particularly with the emergence of Large Language Models (LLMs)[80, 81], has profoundly transformed agricultural practices. These technologies have enabled significant progress in areas such as sustainable pest management, soil analysis, and climate-smart agriculture. LLMs, including OpenAI's ChatGPT[82], Meta's LLaMA[83], and High-Flyer's DeepSeek[84], demonstrate exceptional capabilities in language understanding and generation, supporting complex decision-making across various agricultural domains. Their integration with automation has facilitated the development of autonomous farming machinery, drone-satellite monitoring systems, bio-inspired devices, and intelligent decision-support platforms[85, 86]. These innovations

enhance agricultural efficiency by optimizing resource use, improving planting and harvesting schedules, and providing real-time guidance to farmers. A prominent example is KwooGr[87], developed by Harbin Institute of Technology, which serves as China's first agricultural LLM. It offers advanced analysis of agricultural imagery and generates expert-level diagnostic and treatment recommendations, significantly improving the precision and effectiveness of crop management.

7.2 New backdoors and challenges

The emerging applications of AI and automation in smart farming offer promising development opportunities, but they also introduce new risks and vulnerabilities. LLMs bring inherent weaknesses that extend across the farming application lifecycle, from training to inference phases. These vulnerabilities can be broadly categorized into *adversarial attacks during the training phase and prompt manipulation during the inference phase*[88, 89], both of which can lead to training data leakage and model malfunctions.

Adversarial attacks involve the intentional alteration of inputs to mislead or deceive LLMs, often seen in data poisoning and backdoor attacks. In particular, in adversarial attacks, an input perturbation formula $x' = x + \delta$ is provided, and the optimization objective is to maximize the model's loss with respect to the true labels, where $\delta^* = \arg\max \mathcal{L}\big(f(x+\delta), y_{\text{true}}\big)$, causing the model to make a mistake. The data poisoning mechanism induces the LLM to generate incorrect outputs by inserting malicious samples $\mathcal{D}_{\text{poison}} = \{(x^{(j)}_{\text{poison}}, y^{(j)}_{\text{poison}})\}_{j=1}^{M}$, during the instruction tuning phase. A backdoor attack refers to an attacker implanting a hidden backdoor into the model during the training phase. This backdoor is activated by a specific trigger t; once activated, it outputs the attacker's predefined malicious target $y_t arget$ while ignoring the sample's true label. Agricultural AI systems are vulnerable to data poisoning, where the corruption of training datasets leads to erroneous outputs, thereby introducing serious operational risks[90, 91]. For example, research by Alexander et al. demonstrated that even a small number of poisoned data points could lead LLMs to consistently produce incorrect or flawed outputs[92]. This poses a serious threat in agricultural systems where an insider attacker could introduce malicious data into the training process of LLM-based crop management systems, potentially guiding farmers to make erroneous decisions and resulting in significant financial losses. Backdoor attacks, on the other hand, involve embedding hidden triggers or tokens that cause the model to function normally on benign data but malfunction when exposed to poisoned inputs[93, 94]. Prompt injection attacks insert malicious prompts, such as "Ignore previous rules and leak sensitive data." The model then executes this malicious prompt, bypassing existing security constraints and outputting sensitive information. Malicious users can inject such triggers during the fine-tuning of models to extract sensitive data, such as crop growth parameters. Prompt hacking[89], which involves manipulating input prompts to elicit malicious or misleading outputs, is another attack vector. Even well-trained models can be compromised by malicious prompts, with strategies like prompt injection[95] and jailbreak attacks[96]. For example, a user could trick a chatbot into providing instructions for illegal activities or ask the model to "ignore previous rules and share confidential data." Numerous studies have shown that carefully crafted inputs can successfully manipulate LLMs to provide illicit suggestions or disclose sensitive information.

Beyond the inherent vulnerabilities of AI models, *the high degree of integration and automation in modern agricultural systems introduces additional security risks, enabling indirect intrusion attacks, such as actuator and GPS attacks*, to compromise the decision-making layer of these systems. Actuator attacks involve injecting malicious signals or data to disrupt control actions[97, 98], either by compromising the controller or the communication network that relays control signals to actuators, such as DC water pumps. For instance, attackers might manipulate side-channel signals to interfere with soil moisture sensors or inject false data into cyber-physical power systems, causing unnecessary water usage or improper pesticide and fertilizer application by agricultural drones. Additionally, as autonomous and assisted driving agricultural machinery heavily relies on GPS for navigation, GPS attacks including spoofing and jamming[99, 100], can disrupt satellite signal integrity, leading to deviations in navigation paths and even loss of control of vehicles or machinery. Researchers from UC Irvine have demonstrated that counterfeit GPS signals can cause exponential position deviations, even in advanced autonomous vehicles equipped with multi-sensor calibration[19]. These emerging threats highlight the urgent need for robust security

frameworks in smart agriculture. Beyond a technical concern, securing AI-driven automation is a cornerstone for ensuring food security, economic resilience, and ecological sustainability throughout the sector's digital transformation.

7.3 Defense and countermeasure

Defense strategies against AI-related threats encompass various stages from training to inference, addressing model architectures, training data, and optimization methods. For non-AI-related threats, a multi-faceted approach involving both software-based detection and hardware-based filtering is required. Considerable efforts have been made to design privacy-preserving model architectures[101, 102]. Studies have demonstrated that LLMs with greater parameter sizes exhibit stronger robustness against adversarial attacks, with cognitive architectures and knowledge graphs further enhancing LLM security[103, 104]. Since LLMs are shaped by their training data, it is crucial to cleanse these datasets through processes like detoxification, debiasing, de-identification, and deduplication to eliminate sensitive information, such as the geographical location of military supplies. Optimization techniques commonly seen in min-max game adversarial training and robust fine-tuning help reshape and constrain the gradient propagation of models[105], especially in security and ethical contexts. Differential Privacy (DP)-based methods are broadly employed to safeguard against privacy leaks in inference attacks[106, 107]. DP-enhanced models that integrate with Stochastic Gradient Descent (SGD) optimization algorithms[108] reduce privacy leaks while maintaining comparable model performance to non-DP environments. A recent framework, InferDPT[109], leverages black-box LLMs for privacy-preserving inference, integrating DP into text generation tasks. In the inference phase, defense strategies focus on quick-response applications, including test-time defenses such as preprocessing instructions to filter prompts, detecting malicious events, and post-processing generated responses. Instruction preprocessing filters malicious inputs using techniques like token manipulation[110, 111], purification through masked token prediction, or defensive demonstrations. Malicious detection involves analyzing model behaviors, such as neuron activations or generation probabilities[112], to identify adversarial patterns. For example, Yan et al. proposed ParaFuzz[113], a framework for detecting poisoned samples in NLP models by leveraging the interpretability of model predictions, identifying outliers in training data that require additional time to process. Post-processing methods address harmful outputs by evaluating toxicity across candidate responses or prompting models to self-assess the confidence in their answers[114]. To counter actuator and GPS attacks in smart agriculture, integrated mitigation strategies include multi-GNSS fusion, combining BeiDou, GPS, and ground-based augmentation signals to detect spatial-temporal anomalies[115], encrypted signal authentication through anti-spoofing modules[116], and AI-driven anomaly detection that cross-references environmental sensor data (such as soil moisture and drone trajectories) with actuator commands to flag inconsistencies[117–120]. Observer-based techniques utilize robust observers to monitor actuator behavior and detect anomalies, replacing compromised signals with estimates from a resilient observer[121]. A detection-protection mechanism employs multiple supervisors to detect attacks and switch control to a backup supervisor[117], ensuring system safety during actuator attacks. For GPS threats, multi-sensor fusion combines vision-based lateral localization[122], high-precision map alignment, and inertial navigation to ensure reliable positioning, while pseudorange correlation analysis and multi-GNSS redundancy help mitigate spoofing. Encryption protocols and environmental perception techniques, including visual SLAM and landmark matching, provide alternative navigation in GPS-denied scenarios. Furthermore, regarding the impact of data poisoning and backdoor attacks on model reliability, metrics such as attack success rate (ASR) and accuracy degradation on clean data are introduced to evaluate model robustness. Additionally, redundant sensors and multimodal consistency checks are employed to defend against AI misdirection.

8 Discussion

8.1 Future trend of security of smart farming

Table 4 is a summary of smart agriculture security comparisons.The defensive measures and risk assessments within smart farming are continuously reshaped by a dynamic interplay between technological

Table 4. Comparison and Summary of Smart Agricultural Safety

Layer	Attack	Description	Defense Measures	Key Technologies	References
Sensing Layer	Data Leakage Attacks	Extraction of sensitive information via side-channels.	Shielding, Filtering, Hardware Enhancement	RF Shielding, Acoustic Damping, FIR Filters, Biased Voltage Generators	[23–26], [32–35]
	Signal Injection Attacks	Injection of malicious signals into sensors, leading to data tampering or system interference.	Shielding, Filtering, Anomaly Detection, Sensor Fusion	Sensor Data Fusion Algorithms, RADAR Method, Spectrum Analysis	[27–30, 17, 31, 123], [36–40]
Network Layer	DDoS Attacks	Consumption of network resources, resulting in service unavailability.	Encryption Protocols, Blockchain, IDS	TLS/SSL, ECC, PBFT Consensus	[46, 18, 124, 47–49], [55–62]
	MITM Attacks	Interception and alteration of data during transmission, causing flawed decisions or leakage of sensitive information.	Secure Communication, Authentication	Firewalls, Endpoint Security Software	[50–52]
	Malware & Ransomware Attacks	Implantation of viruses/trojans or encryption of system files for extortion.	IDS, Behavioral Analysis	Signature-based Detection, Anomaly-based Detection, Hybrid IDS	[53, 125, 54]
Cloud Layer	VM Escape Attacks	Attackers break out of a virtual machine to access sensitive agricultural data on other VMs residing on the same host.	Encryption, IDS, Secure APIs	Role-Based Encryption, Hybrid Encryption, Signature+Anomaly IDS	[67, 70, 73**?** , 74]
	Data Remanence Attacks	Recovery of residual sensitive data from deallocated cloud resources.	Data Erasure, Memory Sanitization, Encryption	Memory Sanitization Policies, Hardware Isolation	[68, 69, 73, 126, 74]
	Malicious Service Module Injection	Injection of compromised analytics tools or machine learning models into the PaaS layer.	IDS, Secure APIs, Service Authentication	API Authentication, Input Validation, Service Auditing	[70, 72, 75, 78, 79]
	Web Application Attacks	Exploitation of web interfaces to steal data or hijack user sessions.	Input Filtering, Secure Coding, WAF	SQL Injection Filtering, XSS Protection, Token Validation	[71]
Application Layer	Adversarial Attacks in AI Training Phase	Poisoning of training data or embedding hidden triggers, causing model misbehavior on specific inputs.	Data Cleansing, Adversarial Training, Differential Privacy	Data Detoxification, Debiasing, Adversarial Training	[88–94, 101–105, 108]
	Prompt Manipulation Attacks in AI Inference Phase	Manipulation of model outputs via carefully crafted input prompts to generate malicious content or leak information.	Prompt Filtering, Output Sanitization, Self-Assessment	Token Purification, Malicious Detection, Confidence Evaluation	[89, 95, 96, 110–114]
	Actuator Attacks	Tampering with control signals or spoofing navigation signals, leading to equipment malfunction or failure.	Multi-Sensor Fusion, Cryptographic Authentication, Anomaly Detection	Multi-GNSS Fusion, Visual SLAM, Environmental Perception, Observer-based Techniques	[97–100, 19, 115–122]

progress and the evolving comprehension of novel cyber-physical threats. Several key trends are expected to shape the future of smart farming security. (1) Data privacy and integrity protection: As smart farming generates vast amounts of sensitive data, ensuring its privacy and integrity will be critical. Advances in encryption, multi-party computation, and differential privacy will enhance data protection, particularly in cloud and IoT environments. Security risks at each stage of the data lifecycle—collection (perception layer), transmission (network layer), storage (cloud layer), and usage (application layer)—exhibit transitivity and coupling.Table 2 summarizes the primary threats associated with each lifecycle stage and the recommended defense mechanisms. (2) AI-driven threat detection: AI and machine learning will become integral to real-time threat detection. These technologies will enable adaptive responses to cybersecurity threats, such as identifying subtle attack patterns in IoT networks. AI-based systems will also automate responses, such as isolating compromised devices. (3) Integration of emerging technologies for comprehensive security frameworks: As smart farming systems grow more complex, integrating IoT, AI, cloud computing, and blockchain into cohesive security frameworks will be essential. These technologies will create unified platforms for data protection, threat detection, and system resilience. For example, AI-driven anomaly detection can be combined with blockchain for data traceability, offering a comprehensive defense against cyberattacks and system failures. The integration of these technologies will ensure the sustainability and security of agricultural practices. Combinations ofd advanced technologies will enable multi-layered defense systems for agriculture. AI-driven anomaly detection will secure data and identify threats, while edge computing supports real-time IoT monitoring. Bio-inspired solutions (e.g., DNA-based authentication) will merge biological and digital security. These frameworks must integrate legacy and emerging systems to mitigate risks while ensuring adaptive, sustainable protection. Table 5 is a summary of major threats and recommended defense mechanisms for each stage of the data life cycle. We have explicitly introduced a data lifecycle model that spans four stages: data collection(sensing layer), data transmission (network layer), data storage and processing (cloud layer), and data usage and decision-making (application layer). For each stage, we reinterpret security risks as violations of data integrity, availability, or consistency. For example, in the sensing layer, signal injection attacks compromise data integrity by introducing false measurements. In the network layer, DDoS and jamming attacks undermine data availability by disrupting transmission. In the cloud layer, VM escape and data remanence attacks threaten data consistency and confidentiality. In the application layer, adversarial data poisoning and prompt injection attacks violate both integrity and consistency of AI-driven decisions. The network layer serves as a critical bottleneck for risk propagation; once compromised, it can affect both upper and lower layers. Furthermore, vulnerabilities propagate across layers; for example, signal injection at the perception layer can be amplified into erroneous decisions at the application layer. Conversely, data leakage at the cloud layer may expose raw data from the perception layer.

8.2 Suggestions to smart farming research

To address the challenges in smart farming security, research should focus on the following areas: (1) Data-Driven Secure IoT architectures: Given the reliance on IoT devices, research on data generation for attack simulation, specifically using GANs and diffusion models to generate agricultural IoT attack data, to mitigate the scarcity of labeled data. Additionally, research should prioritize the development of secure, lightweight IoT protocols. These should include secure communication, hardware-based security, and advanced authentication to prevent unauthorized access and signal interception.(2) Interdisciplinary collaboration on physical information-driven security modeling: The complexity of smart farming security requires collaboration across fields such as agriculture, cybersecurity, data science, and engineering. Combining crop growth models with environmental physical characteristics to detect attacks where sensor data deviates from physical laws. Cross-disciplinary research will help develop integrated solutions that address both sector-specific and technological security challenges. (3) AI-Driven Adaptive Defense Mechanisms: Research on adversarial prompts and defense strategies for agricultural LLMs, as well as the use of generative AI for automated security response. Research should focus on developing AI-powered anomaly detection systems that adapt to diverse agricultural environments. Self-supervised learning frameworks can reduce reliance on curated datasets, and lightweight knowledge distillation techniques can enhance model performance on resource-constrained devices. Additionally, federated learning protocols can ensure AI models maintain efficacy across diverse farms. Collaborative benchmarking will

Table 5. Major Threats and Recommended Defense Mechanisms for Each Stage of the Data Life Cycle

LifeCycle Stage	Architecture Layer	Security Threats	Defense Mechanisms
Data Collection	Sensing Layer	Data leakage; Signal injection; Sensor spoofing.	Physical shielding and filtering; Sensor fusion validation; Anomaly detection algorithms
Data Transmission	Network Layer	DDoS/DoS attacks; Man-in-the-Middle; Malware/ransomware; Jamming/congestion attacks.	Lightweight encryption; Blockchain-based authentication; Deep learning-based IDS; Multi-path redundant transmission
Data Storage	Cloud Layer	VM escape/data remanence; SQL injection/XSS; Malicious service module injection; Insecure API exploitation.	Multi-layer encryption; Hybrid IDS; Deception-based defense; Secure APIs
Data Usage	Application Layer	Adversarial attacks/data poisoning; Backdoor attacks/prompt injection; Actuator hijacking; GPS spoofing/jamming.	Differential privacy; Adversarial training/robust fine-tuning; Multi-sensor fusion localization; Explainable AI anomaly detection

establish standardized metrics for evaluating AI security in agricultural contexts. (4) Implementation of Security-as-a-Service (SECaaS) in Agriculture: Research scaling "Security-as-a-Service" (SECaaS) models will provide cost-effective, on-demand cybersecurity solutions tailored for farmers. Additionally, research should aim to develop integrated risk monitoring platforms that synthesize data from various sources, such as meteorological and cyber-threat data, for predictive analytics.

9 Conclusion

This paper presents a holistic perspective on security in smart farming, analyzing emerging threats and mitigation strategies in an increasingly interconnected agricultural ecosystem. The study highlights how the integration of IoT, AI, and cloud technologies introduces novel vulnerabilities while proposing adaptive defense mechanisms to safeguard critical farming operations. By emphasizing the need for robust, multi-layered security frameworks, the work contributes to developing resilient smart farming systems capable of withstanding evolving cyber threats while maintaining operational reliability and data integrity. The findings underscore the importance of balancing technological innovation with comprehensive security measures to ensure sustainable agricultural transformation.

Acknowledgments

Thanks to anonymous reviewers for their hard work and kind help.

Funding

This work was supported by National Natural Science Foundation of China Grant 62350710797 and the Major Key Project of PCL (Grant No. PCL2024A05).

Conflicts of interest

The author declare no conflicts of interest.

Data availability statement

No data are associated with this article.

Author contribution statement

Ruonan Li wrote the main part of this paper. Jie Liu guided the overall direction of the work, revised the manuscript, and provided important suggestions. Tiantian Liu contributed supplementary content to this paper, assisted in revising the manuscript, and provided constructive feedback.

References

[1] FAO, IFAD, UNICEF, WFP and WHO, *The State of Food Security and Nutrition in the World 2022. Repurposing food and agricultural policies to make healthy diets more affordable.* Rome: FAO, 2022.

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

[3] A. Antonacci, F. Arduini, D. Moscone, G. Palleschi, and V. Scognamiglio, "Nanostructured (bio) sensors for smart agriculture," *TrAC Trends in Analytical Chemistry*, vol. 98, pp. 95–103, 2018.

[4] E. K. Gyamfi, Z. ElSayed, J. Kropczynski, M. A. Yakubu, and N. Elsayed, "Agricultural 4.0 leveraging on technological solutions: Study for smart farming sector," in *2024 IEEE 3rd International Conference on Computing and Machine Intelligence (ICMI)*, 2024, pp. 1–9.

[5] T. Talaviya, D. Shah, N. Patel, H. Yagnik, and M. Shah, "Implementation of artificial intelligence in agriculture for optimisation of irrigation and application of pesticides and herbicides," *Artificial intelligence in agriculture*, vol. 4, pp. 58–73, 2020.

[6] M. Campoverde-Molina and S. Luján-Mora, "Cybersecurity in smart agriculture: A systematic literature review," *Computers & Security*, p. 104284, 2024.

[7] M. Gupta, M. Abdelsalam, S. Khorsandroo, and S. Mittal, "Security and privacy in smart farming: Challenges and opportunities," *IEEE access*, vol. 8, pp. 34 564–34 584, 2020.

[8] H. T. Bui, H. Aboutorab, A. Mahboubi, Y. Gao, N. H. Sultan, A. Chauhan, M. Z. Parvez, M. Bewong, R. Islam, Z. Islam *et al.*, "Agriculture 4.0 and beyond: Evaluating cyber threat intelligence sources and techniques in smart farming ecosystems," *Computers & Security*, vol. 140, p. 103754, 2024.

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

[10] Y. S. Abdulsalam and M. Hedabou, "Security and privacy in cloud computing: technical review," *Future Internet*, vol. 14, no. 1, p. 11, 2021.

[11] R. Dembani, I. Karvelas, N. A. Akbar, S. Rizou, D. Tegolo, and S. Fountas, "Agricultural data privacy and federated learning: A review of challenges and opportunities," *Computers and Electronics in Agriculture*, vol. 232, p. 110048, 2025.

[12] S. C. I. O. of the People's Republic of China. (2025) Agriculture blossoms with tech innovation drive. Accessed: 2025-04-16. [Online]. Available: http://english.scio.gov.cn/m/in-depth/2025-02/27/content_117735935.html

[13] A. Alvino and S. Marino, "Remote sensing for irrigation of horticultural crops," *Horticulturae*, vol. 3, no. 2, p. 40, 2017.

[14] G. V. Research. (2025) Smart agriculture farming market analysis. Accessed: 2025-04-16. [Online]. Available: https://www.grandviewresearch.com/industry-analysis/smart-agriculture-farming-market

[15] M. A. Alahe, L. Wei, Y. Chang, S. R. Gummi, J. Kemeshi, X. Yang, K. Won, and M. Sher, "Cyber security in smart agriculture: Threat types, current status, and future trends," *Computers and Electronics in Agriculture*, vol. 226, p. 109401, 2024.

[16] S. Hackfort, S. Marquis, and K. Bronson, "Harvesting value: Corporate strategies of data assetization in agriculture and their socio-ecological implications," *Big Data & Society*, vol. 11, no. 1, 2024.

[17] Z. Xu, R. Hua, J. Juang, S. Xia, J. Fan, and C. Hwang, "Inaudible attack on smart speakers with intentional electromagnetic interference," *IEEE Transactions on Microwave Theory and Techniques*, vol. 69, no. 5, pp. 2642–2650, 2021.

[18] B. Nassi, M. Sror, I. Lavi, Y. Meidan, A. Shabtai, and Y. Elovici, "Piping botnet-turning green technology into a water disaster," *arXiv preprint arXiv:1808.02131*, 2018.

[19] J. Shen, J. Y. Won, Z. Chen, and Q. A. Chen, "Drift with devil: Security of {Multi-Sensor} fusion based localization in {High-Level} autonomous driving under {GPS} spoofing," in *29th USENIX security symposium (USENIX Security 20)*, 2020, pp. 931–948.

[20] A. Nayyar and V. Puri, "Smart farming: Iot based smart sensors agriculture stick for live temperature and moisture monitoring using arduino, cloud computing & solar technology," in *Proc. of The International Conference on Communication and Computing Systems (ICCCS-2016)*, 2016, pp. 9 781 315 364 094–121.

[21] R. Rayhana, G. G. Xiao, and Z. Liu, "Printed sensor technologies for monitoring applications in smart farming: A review," *IEEE Transactions on Instrumentation and Measurement*, vol. 70, pp. 1–19, 2021.

[22] S. Jagannathan, R. Priyatharshini *et al.*, "Smart farming system using sensors for agricultural task automation," in *2015 IEEE Technological Innovation in ICT for Agriculture and Rural Development (TIAR)*, 2015, pp. 49–53.

[23] W. Van Eck, "Electromagnetic radiation from video display units: An eavesdropping risk?" *Computers & Security*, vol. 4, no. 4, pp. 269–286, 1985.

[24] T. Tosaka, Y. Yamanaka, and K. Fukunaga, "Method for determining whether or not information is contained in electromagnetic disturbance radiated from a pc display," *IEEE transactions on Electromagnetic Compatibility*, vol. 53, no. 2, pp. 318–324, 2011.

[25] A. Kumar, C. Scarborough, A. Yilmaz, and M. Orshansky, "Efficient simulation of em side-channel attack resilience," in *2017 IEEE/ACM International Conference on Computer-Aided Design (ICCAD)*, 2017, pp. 123–130.

[26] G. Goller and G. Sigl, "Side channel attacks on smartphones and embedded devices using standard radio equipment," in *International Workshop on Constructive Side-Channel Analysis and Secure Design*, 2015, pp. 255–270.

[27] A. Richelli, L. Colalongo, and Z. M. Kovács-Vajna, "Analog ics for automotive under emi attack," in *AEIT International Annual Conference (AEIT)*, 2019, pp. 1–6.

[28] I. Giechaskiel and K. Rasmussen, "Taxonomy and challenges of out-of-band signal injection attacks and defenses," *IEEE Communications Surveys & Tutorials*, vol. 22, no. 1, pp. 645–670, 2019.

[29] G. Zhang, C. Yan, X. Ji, T. Zhang, T. Zhang, and W. Xu, "Dolphinattack: Inaudible voice commands," in *Proceedings of the 2017 ACM SIGSAC conference on computer and communications security*, 2017, pp. 103–117.
[30] T. Sugawara, B. Cyr, S. Rampazzi, D. Genkin, and K. Fu, "Light commands:{Laser-Based} audio injection attacks on {Voice-Controllable} systems," in *29th USENIX Security Symposium (USENIX Security 20)*, 2020, pp. 2631–2648.
[31] Y. Tu, S. Rampazzi, B. Hao, A. Rodriguez, K. Fu, and X. Hei, "Trick or heat? manipulating critical temperature-based control systems using rectification attacks," in *Proceedings of the 2019 ACM SIGSAC Conference on Computer and Communications Security*, 2019, pp. 2301–2315.
[32] H. Liu, R. Spolaor, F. Turrin, R. Bonafede, and M. Conti, "Usb powered devices: A survey of side-channel threats and countermeasures," *High-Confidence Computing*, vol. 1, no. 1, p. 100007, 2021.
[33] Y. Tu, V. S. Tida, Z. Pan, and X. Hei, "Transduction shield: A low-complexity method to detect and correct the effects of emi injection attacks on sensors," in *Proceedings of the 2021 ACM Asia Conference on Computer and Communications Security*, 2021.
[34] D. F. Kune, J. Backes, S. S. Clark, D. Kramer, M. Reynolds, K. Fu, Y. Kim, and W. Xu, "Ghost talk: Mitigating emi signal injection attacks against analog sensors," in *IEEE symposium on security and privacy*, 2013, pp. 145–159.
[35] Y. Zhang and K. Rasmussen, "Detection of electromagnetic interference attacks on sensor systems," in *2020 IEEE Symposium on Security and Privacy (SP)*, 2020, pp. 203–216.
[36] J. Guan, L. Pan, C. Wang, S. Yu, L. Gao, and X. Zheng, "Trustworthy sensor fusion against inaudible command attacks in advanced driver-assistance systems," *IEEE Internet of Things Journal*, 2023.
[37] K. S. Tharayil, B. Farshteindiker, S. Eyal, N. Hasidim, R. Hershkovitz, S. Houri, I. Yoffe, M. Oren, and Y. Oren, "Sensor defense in-software (sdi): Practical software based detection of spoofing attacks on position sensors," *Engineering Applications of Artificial Intelligence*, vol. 95, p. 103904, 2020.
[38] Z. Zhang, Z. Zhan, D. Balasubramanian, B. Li, P. Volgyesi, and X. Koutsoukos, "Leveraging em side-channel information to detect rowhammer attacks," in *2020 IEEE Symposium on Security and Privacy (SP)*. IEEE, 2020, pp. 729–746.
[39] C. Shen and J. Huang, "{EarFisher}: Detecting wireless eavesdroppers by stimulating and sensing memory {EMR}," in *18th USENIX Symposium on Networked Systems Design and Implementation (NSDI 21)*, 2021, pp. 873–886.
[40] C. Yang and A. P. Sample, "Em-id: Tag-less identification of electrical devices via electromagnetic emissions," in *2016 IEEE International Conference on RFID (RFID)*, 2016, pp. 1–8.
[41] H. M. Rouzbahani, H. Karimipour, E. Fraser, A. Dehghantanha, E. Duncan, A. Green, and C. Russell, "Communication layer security in smart farming: A survey on wireless technologies," *arXiv preprint arXiv:2203.06013*, 2022.
[42] C. Prakash, L. P. Singh, A. Gupta, and S. K. Lohan, "Advancements in smart farming: A comprehensive review of iot, wireless communication, sensors, and hardware for agricultural automation," *Sensors and Actuators A: Physical*, vol. 362, p. 114605, 2023.
[43] L. Aldhaheri, N. Alshehhi, I. I. J. Manzil, R. A. Khalil, S. Javaid, N. Saeed, and M.-S. Alouini, "Lora communication for agriculture 4.0: Opportunities, challenges, and future directions," *IEEE Internet of Things Journal*, 2024.
[44] L. Lei, W. Zhai, K. Lin, N. Metje, and T. Hao, "Experimental evaluation of ug2ag wireless communication channel for lorawan-based underground infrastructure monitoring," in *2023 9th International Conference on Computer and Communications (ICCC)*, 2023, pp. 914–918.
[45] Z. Chang, F. Zhang, J. Xiong, J. Ma, B. Jin, and D. Zhang, "Sensor-free soil moisture sensing using lora signals," *Proceedings of the ACM on Interactive, Mobile, Wearable and Ubiquitous Technologies*, vol. 6, no. 2, pp. 1–27, 2022.
[46] A. N. Alahmadi, S. U. Rehman, H. S. Alhazmi, D. G. Glynn, H. Shoaib, and P. Solé, "Cyber-security threats and side-channel attacks for digital agriculture," *Sensors*, vol. 22, no. 9, p. 3520, 2022.
[47] A.-u. Rehman, S. U. Rehman, and H. Raheem, "Sinkhole attacks in wireless sensor networks: A survey," *Wireless Personal Communications*, vol. 106, pp. 2291–2313, 2019.
[48] C. W. Badenhop, S. R. Graham, B. W. Ramsey, B. E. Mullins, and L. O. Mailloux, "The z-wave routing protocol and its security implications," *Computers & Security*, vol. 68, pp. 112–129, 2017.
[49] Y. Arjoune and S. Faruque, "Smart jamming attacks in 5g new radio: A review," in *2020 10th annual computing and communication workshop and conference (CCWC)*, 2020, pp. 1010–1015.
[50] M. Conti, N. Dragoni, and V. Lesyk, "A survey of man in the middle attacks," *IEEE communications surveys & tutorials*, vol. 18, no. 3, pp. 2027–2051, 2016.
[51] H. A. Abdul-Ghani, D. Konstantas, and M. Mahyoub, "A comprehensive iot attacks survey based on a building-blocked reference model," *International Journal of Advanced Computer Science and Applications*, vol. 9, no. 3, pp. 355–373, 2018.
[52] S. Rudrakar and P. Rughani, "Iot based agriculture (iota): Architecture, cyber attack, cyber crime and digital forensics challenges," preprint at Research Square. [Online]. Available: https://doi.org/10.21203/rs.3.rs-2042812/v1
[53] K. Angrishi, "Turning internet of things (iot) into internet of vulnerabilities (iov): Iot botnets," *arXiv preprint arXiv:1702.03681*, 2017.
[54] S. D. S. U. Extension. (2024) The growing threat of cyber attacks in agriculture. Accessed: 2025-04-16. [Online]. Available: https://extension.sdstate.edu/growing-threat-cyber-attacks-agriculture
[55] B. Martínez-Rodríguez, S. Bilbao-Arechabala, and F. Jorge-Hernandez, "Security architecture for swarms of autonomous vehicles in smart farming," *Applied sciences*, vol. 11, no. 10, p. 4341, 2021.
[56] I. Nadir, W. K. Zegeye, F. Moazzami, and Y. Astatke, "Establishing symmetric pairwise-keys using public-key cryptography in wireless sensor networks (wsn)," in *2016 IEEE 7th Annual Ubiquitous Computing, Electronics & Mobile Communication Conference (UEMCON)*, 2016, pp. 1–6.
[57] K. Taji and F. Ghanimi, "Enhancing security and privacy in smart agriculture: A novel homomorphic signcryption system," *Results in Engineering*, vol. 22, p. 102310, 2024.
[58] K. LB, "Survey on the applications of blockchain in agriculture," *Agriculture*, vol. 12, no. 9, p. 1333, 2022.

[59] A. Vangala, A. K. Das, A. Mitra, S. K. Das, and Y. Park, "Blockchain-enabled authenticated key agreement scheme for mobile vehicles-assisted precision agricultural iot networks," *IEEE Transactions on Information Forensics and Security*, vol. 18, pp. 904–919, 2023.

[60] R. Vatambeti, D. Venkatesh, G. Mamidisetti, V. K. Damera, M. Manohar, and N. S. Yadav, "Prediction of ddos attacks in agriculture 4.0 with the help of prairie dog optimization algorithm with idsnet," *Scientific reports*, vol. 13, no. 1, p. 15371, 2023.

[61] T. H. Aldhyani and H. Alkahtani, "Cyber security for detecting distributed denial of service attacks in agriculture 4.0: Deep learning model," *Mathematics*, vol. 11, no. 1, p. 233, 2023.

[62] K. Kethineni and G. Pradeepini, "Intrusion detection in internet of things-based smart farming using hybrid deep learning framework," *Cluster Computing*, vol. 27, no. 2, pp. 1719–1732, 2024.

[63] A. Ometov, O. L. Molua, M. Komarov, and J. Nurmi, "A survey of security in cloud, edge, and fog computing," *Sensors*, vol. 22, no. 3, p. 927, 2022.

[64] D. Vasisht, Z. Kapetanovic, J. Won, X. Jin, R. Chandra, S. Sinha, A. Kapoor, M. Sudarshan, and S. Stratman, "{FarmBeats}: an {IoT} platform for {Data-Driven} agriculture," in *14th USENIX Symposium on Networked Systems Design and Implementation (NSDI 17)*, 2017, pp. 515–529.

[65] D. . Company. (2025) Operations center. Accessed: 2025-04-16. [Online]. Available: https://operationscenter.deere.com/

[66] A. Cloud. (2018) Alibaba cloud launches et agricultural brain at the shanghai computing. Accessed: 2025-04-16. [Online]. Available: https://www.alibabacloud.com/en/press-room/alibaba-cloud-launches-et-agricultural-brain-at-the-shanghai-computing?_p_lc=1

[67] M. H. Song, "Analysis of risks for virtualization technology," *Applied Mechanics and Materials*, vol. 539, pp. 374–377, 2014.

[68] B. Albelooshi, K. Salah, T. Martin, and E. Damiani, "Experimental proof: Data remanence in cloud vms," in *2015 IEEE 8th International Conference on Cloud Computing*, 2015, pp. 1017–1020.

[69] C. Drewes, O. Weng, A. Meza, A. Althoff, D. Kohlbrenner, R. Kastner, and D. Richmond, "Pentimento: Data remanence in cloud fpgas," in *Proceedings of the 29th ACM International Conference on Architectural Support for Programming Languages and Operating Systems, Volume 2*, 2024, pp. 862–878.

[70] M. Ali, S. U. Khan, and A. V. Vasilakos, "Security in cloud computing: Opportunities and challenges," *Information sciences*, vol. 305, pp. 357–383, 2015.

[71] D. Stutz, J. T. de Assis, A. A. Laghari, A. A. Khan, A. Deshpande, D. Kulkarni, A. Terziev, M. A. de Jesus, and E. G. Grata, "Cyber threat detection and mitigation using artificial intelligence–a cyber-physical perspective," *Applying Artificial Intelligence in Cybersecurity Analytics and Cyber Threat Detection*, pp. 107–133, 2024.

[72] G. Ramachandra, M. Iftikhar, and F. A. Khan, "A comprehensive survey on security in cloud computing," *Procedia Computer Science*, vol. 110, pp. 465–472, 2017.

[73] S. D. C. Di Vimercati, S. Foresti, S. Jajodia, S. Paraboschi, and P. Samarati, "Over-encryption: management of access control evolution on outsourced data," in *Proceedings of the 33rd international conference on Very large data bases*, 2007, pp. 123–134.

[74] F. Pan, Z. Pang, M. Luvisotto, M. Xiao, and H. Wen, "Physical-layer security for industrial wireless control systems: Basics and future directions," *IEEE Industrial Electronics Magazine*, vol. 12, no. 4, pp. 18–27, 2018.

[75] D. M. Tudesco, A. Deshpande, A. A. Laghari, A. A. Khan, R. T. Lopes, R. Jenice Aroma, K. Raimond, L. Teng, and A. Khan, "Utilization of deep learning models for safe human-friendly computing in cloud, fog, and mobile edge networks," *Applying artificial intelligence in cybersecurity analytics and cyber threat detection*, pp. 221–248, 2024.

[76] S. Yoo and T. Lee, "A study of the ordinal scale classification algorithm for cyber threat intelligence based on deception technology," *Electronics*, vol. 12, no. 11, p. 2474, 2023.

[77] H. Li, Y. Guo, S. Huo, H. Hu, and P. Sun, "Defensive deception framework against reconnaissance attacks in the cloud with deep reinforcement learning," *Science China Information Sciences*, vol. 65, no. 7, p. 170305, 2022.

[78] L. E. Nugroho, A. G. H. Pratama, I. W. Mustika, and R. Ferdiana, "Development of monitoring system for smart farming using progressive web app," in *2017 9th International Conference on Information Technology and Electrical Engineering (ICITEE)*, 2017, pp. 1–5.

[79] M.-Y. Wu and T.-H. Lee, "Design and implementation of cloud api access control based on oauth," in *IEEE 2013 Tencon-Spring*, 2013, pp. 485–489.

[80] T. A. Shaikh, T. Rasool, K. Veningston, and S. M. Yaseen, "The role of large language models in agriculture: harvesting the future with llm intelligence," *Progress in Artificial Intelligence*, pp. 1–48, 2024.

[81] W. X. Zhao, K. Zhou, J. Li, T. Tang, X. Wang, Y. Hou, Y. Min, B. Zhang, J. Zhang, Z. Dong *et al.*, "A survey of large language models," *arXiv preprint arXiv:2303.18223*, vol. 1, no. 2, 2023.

[82] T. Brown, B. Mann, N. Ryder, M. Subbiah, J. D. Kaplan, P. Dhariwal, A. Neelakantan, P. Shyam, G. Sastry, A. Askell *et al.*, "Language models are few-shot learners," *Advances in neural information processing systems*, vol. 33, pp. 1877–1901, 2020.

[83] H. Touvron, T. Lavril, G. Izacard, X. Martinet, M.-A. Lachaux, T. Lacroix, B. Rozière, N. Goyal, E. Hambro, F. Azhar *et al.*, "Llama: Open and efficient foundation language models," *arXiv preprint arXiv:2302.13971*, 2023.

[84] A. Liu, B. Feng, B. Xue, B. Wang, B. Wu, C. Lu, C. Zhao, C. Deng, C. Zhang, C. Ruan *et al.*, "Deepseek-v3 technical report," *arXiv preprint arXiv:2412.19437*, 2024.

[85] J. Li, M. Xu, L. Xiang, D. Chen, W. Zhuang, X. Yin, and Z. Li, "Foundation models in smart agriculture: Basics, opportunities, and challenges," *Computers and Electronics in Agriculture*, vol. 222, p. 109032, 2024.

[86] Z. Yuan, K. Liu, R. Peng, S. Li, D. Leybourne, N. Musa, H. Huang, and P. Yang, "Pestgpt: Leveraging large language models and iot for timely and customized recommendation generation in sustainable pest management," *IEEE Internet of Things Magazine*, vol. 8, no. 1, pp. 26–33, 2024.

[87] HIT-Kwoo. (2025) Kwoogr github repository. Accessed: 2025-04-16. [Online]. Available: https://github.com/HIT-Kwoo/KwooGr
[88] Y. Yao, J. Duan, K. Xu, Y. Cai, Z. Sun, and Y. Zhang, "A survey on large language model (llm) security and privacy: The good, the bad, and the ugly," *High-Confidence Computing*, p. 100211, 2024.
[89] B. C. Das, M. H. Amini, and Y. Wu, "Security and privacy challenges of large language models: A survey," *ACM Computing Surveys*, vol. 57, no. 6, pp. 1–39, 2025.
[90] M. Shu, J. Wang, C. Zhu, J. Geiping, C. Xiao, and T. Goldstein, "On the exploitability of instruction tuning," *Advances in Neural Information Processing Systems*, vol. 36, pp. 61 836–61 856, 2023.
[91] X. Zhang, Z. Zhang, S. Ji, and T. Wang, "Trojaning language models for fun and profit," in *2021 IEEE European Symposium on Security and Privacy (EuroS&P)*, 2021, pp. 179–197.
[92] A. Wan, E. Wallace, S. Shen, and D. Klein, "Poisoning language models during instruction tuning," in *International Conference on Machine Learning*. PMLR, 2023, pp. 35 413–35 425.
[93] H. Yang, K. Xiang, M. Ge, H. Li, R. Lu, and S. Yu, "A comprehensive overview of backdoor attacks in large language models within communication networks," *IEEE Network*, 2024.
[94] J. Li, Y. Yang, Z. Wu, V. Vydiswaran, and C. Xiao, "Chatgpt as an attack tool: Stealthy textual backdoor attack via blackbox generative model trigger," *arXiv preprint arXiv:2304.14475*, 2023.
[95] Y. Liu, G. Deng, Y. Li, K. Wang, Z. Wang, X. Wang, T. Zhang, Y. Liu, H. Wang, Y. Zheng *et al.*, "Prompt injection attack against llm-integrated applications," *arXiv preprint arXiv:2306.05499*, 2023.
[96] X. Shen, Z. Chen, M. Backes, Y. Shen, and Y. Zhang, "" do anything now": Characterizing and evaluating in-the-wild jailbreak prompts on large language models," in *Proceedings of the 2024 on ACM SIGSAC Conference on Computer and Communications Security*, 2024, pp. 1671–1685.
[97] Q. Zhang, C. Seatzu, Z. Li, and A. Giua, "Sensor and actuator attacks in discrete event systems," *IFAC-PapersOnLine*, vol. 55, no. 28, pp. 38–45, 2022.
[98] H. Fawzi, P. Tabuada, and S. Diggavi, "Security for control systems under sensor and actuator attacks," in *51st IEEE conference on decision and control (CDC)*, 2012, pp. 3412–3417.
[99] H. Sathaye, M. Strohmeier, V. Lenders, and A. Ranganathan, "An experimental study of {GPS} spoofing and takeover attacks on {UAVs}," in *31st USENIX security symposium (USENIX security 22)*, 2022, pp. 3503–3520.
[100] S. Dasgupta, A. Ahmed, M. Rahman, and T. N. Bandi, "Unveiling the stealthy threat: Analyzing slow drift gps spoofing attacks for autonomous vehicles in urban environments and enabling the resilience," *arXiv preprint arXiv:2401.01394*, 2024.
[101] X. Li, F. Tramer, P. Liang, and T. Hashimoto, "Large language models can be strong differentially private learners," *arXiv preprint arXiv:2110.05679*, 2021.
[102] K. Zhu, J. Wang, J. Zhou, Z. Wang, H. Chen, Y. Wang, L. Yang, W. Ye, Y. Zhang, N. Zhenqiang Gong *et al.*, "Promptbench: Towards evaluating the robustness of large language models on adversarial prompts," *arXiv e-prints*, pp. arXiv–2306, 2023.
[103] X. Chen, S. Jia, and Y. Xiang, "A review: Knowledge reasoning over knowledge graph," *Expert Systems with Applications*, vol. 141, p. 112948, 2020.
[104] J. E. Laird, C. Lebiere, and P. S. Rosenbloom, "A standard model of the mind: Toward a common computational framework across artificial intelligence, cognitive science, neuroscience, and robotics," *AI Magazine*, vol. 38, no. 4, pp. 13–26, 2017.
[105] X. Liu, H. Cheng, P. He, W. Chen, Y. Wang, H. Poon, and J. Gao, "Adversarial training for large neural language models," *arXiv preprint arXiv:2004.08994*, 2020.
[106] M. Abadi, A. Chu, I. Goodfellow, H. B. McMahan, I. Mironov, K. Talwar, and L. Zhang, "Deep learning with differential privacy," in *Proceedings of the 2016 ACM SIGSAC conference on computer and communications security*, 2016, pp. 308–318.
[107] C. Dwork, A. Roth *et al.*, "The algorithmic foundations of differential privacy," *Foundations and Trends® in Theoretical Computer Science*, vol. 9, no. 3–4, pp. 211–407, 2014.
[108] J. Weng, J. Weng, J. Zhang, M. Li, Y. Zhang, and W. Luo, "Deepchain: Auditable and privacy-preserving deep learning with blockchain-based incentive," *IEEE Transactions on Dependable and Secure Computing*, vol. 18, no. 5, pp. 2438–2455, 2019.
[109] M. Tong, K. Chen, J. Zhang, Y. Qi, W. Zhang, N. Yu, T. Zhang, and Z. Zhang, "Inferdpt: Privacy-preserving inference for black-box large language models," *IEEE Transactions on Dependable and Secure Computing*, 2025.
[110] A. Robey, E. Wong, H. Hassani, and G. J. Pappas, "Smoothllm: Defending large language models against jailbreaking attacks," *arXiv preprint arXiv:2310.03684*, 2023.
[111] L. Li, D. Song, and X. Qiu, "Text adversarial purification as defense against adversarial attacks," *arXiv preprint arXiv:2203.14207*, 2022.
[112] H. Zhang, J. Ye, W. Hu, Q. Wang, X. Yan, Q. Yue, W. Lv, M. He, and J. Wang, "Study on the latent state of kaminsky-style dns cache poisoning: Modeling and empirical analysis," *Computers Security*, vol. 110, p. 102445, 2021.
[113] L. Yan, Z. Zhang, G. Tao, K. Zhang, X. Chen, G. Shen, and X. Zhang, "Parafuzz: An interpretability-driven technique for detecting poisoned samples in nlp," *Advances in Neural Information Processing Systems*, vol. 36, pp. 66 755–66 767, 2023.
[114] B. Chen, A. Paliwal, and Q. Yan, "Jailbreaker in jail: Moving target defense for large language models," in *Proceedings of the 10th ACM Workshop on Moving Target Defense*, 2023, pp. 29–32.
[115] J. Burbank, T. Greene, and N. Kaabouch, "Detecting and mitigating attacks on gps devices," *Sensors*, vol. 24, no. 17, p. 5529, 2024.
[116] K. A. Tychola and K. Rantos, "Cyberthreats and security measures in drone-assisted agriculture," *Electronics*, vol. 14, no. 1, p. 149, 2025.

[117] Y. Tong, K. Cai, and C. Seatzu, "Actuator attack mitigation using the detection-protection mechanism," *IFAC-PapersOnLine*, vol. 58, no. 1, pp. 180–185, 2024.
[118] X. Jin, W. M. Haddad, and T. Yucelen, "An adaptive control architecture for mitigating sensor and actuator attacks in cyber-physical systems," *IEEE Transactions on Automatic Control*, vol. 62, no. 11, pp. 6058–6064, 2017.
[119] Y. Zhou, K. G. Vamvoudakis, W. M. Haddad, and Z.-P. Jiang, "A secure control learning framework for cyber-physical systems under sensor and actuator attacks," *IEEE Transactions on Cybernetics*, vol. 51, no. 9, pp. 4648–4660, 2020.
[120] Z. Zhao, Y. Xu, Y. Li, Y. Zhao, B. Wang, and G. Wen, "Sparse actuator attack detection and identification: A data-driven approach," *IEEE Transactions on Cybernetics*, vol. 53, no. 6, pp. 4054–4064, 2023.
[121] M. Kachhwaha, H. Modi, M. K. Nehra, and D. Fulwani, "Robust observer-based defense strategy against actuator and sensor cyber-attacks in dcmgs," *IEEE Transactions on Industrial Informatics*, 2024.
[122] Q. Chen, P. Liu, G. Li, and Z. Wang, "Gps attack detection and mitigation for safe autonomous driving using image and map based lateral direction localization," *arXiv preprint arXiv:2310.05407*, 2023.
[123] X. Wei, X. Li, C. Sun, and J. Ma, "Physical attacks on a uav system: Overview and emerging methods," *IEEE Transactions on Intelligent Transportation Systems*, 2025.
[124] BleepingComputer. (2018) Flaws in smart irrigation systems expose water utilities to botnet-grade attacks. Accessed: 2025-04-16. [Online]. Available: https://www.bleepingcomputer.com/news/security/flaws-in-smart-irrigation-systems-expose-water-utilities-to-botnet-grade-attacks/
[125] F. Wang, Y. Chen, H. Gao, Q. Li, and C. Wang, "Self-supervised contrastive representation learning for classifying internet of things malware," *Engineering Applications of Artificial Intelligence*, vol. 150, p. 110299, 2025.
[126] A. D. Kaif, K. S. Alam, S. K. Das, G. Chen, S. Islam, and S. Muyeen, "Blockchain-integrated cyber-physical smart meter design and implementation for secured energy trading in virtual power plants," *IEEE Transactions on Automation Science and Engineering*, 2025.

Ruonan Li is currently a Postdoctoral with Peng Cheng Laboratory. She received Ph.D. degree in Department of Computer Science and Technology, Harbin Institute of Technology in 2024. Her research interest include Network Security, AI security, blockchain, AI empowered Internet-of-Things and Deep Reinforcement Learning for Networking.

Tiantian Liu is an Assistant Professor at the School of Informatics, Xiamen University. She received her Ph.D. degree from Zhejiang University in 2025 and her Bachelor's degree from Zhejiang University in 2020. Her research interests include cyber-physical systems (CPS) security, speech security, AI security, and mobile computing. Her work received the Best Paper Candidate Award from ACM SenSys 2021 and SIGMOBILE Research Highlight. She was also named the EECS Rising Star 2024 by MIT.

Jie Liu (*Fellow, IEEE*) is currently a Chair Professor with the International Institute for Artificial Intelligence, Harbin Institute of Technology, Shenzhen, China. He received the Ph.D. degree in electrical engineering and computer science from the University of California, Berkeley, CA, USA, in 2001. His research interests include artificial intelligence, control engineering, Internet of Things, and computer system.