A Survey on Smart Agriculture: Development Modes, Technologies, and Security and Privacy Challenges

Xing Yang, *Student Member, IEEE,* Lei Shu, *Senior Member, IEEE,* Jianing Chen, Mohamed Amine Ferrag, Jun Wu, *Member, IEEE,* Edmond Nurellari, *Member, IEEE,* and Kai Huang

***Abstract*—With the deep combination of both modern information technology and traditional agriculture, the era of agriculture 4.0, which takes the form of smart agriculture, has come. Smart agriculture provides solutions for agricultural intelligence and automation. However, information security issues cannot be ignored with the development of agriculture brought by modern information technology. In this paper, three typical development modes of smart agriculture (precision agriculture, facility agriculture, and order agriculture) are presented. Then, 7 key technologies and 11 key applications are derived from the above modes. Based on the above technologies and applications, 6 security and privacy countermeasures (authentication and access control, privacy-preserving, blockchain-based solutions for data integrity, cryptography and key management, physical countermeasures, and intrusion detection systems) are summarized and discussed. Moreover, the security challenges of smart agriculture are analyzed and organized into two aspects: 1) agricultural production, and 2) information technology. Most current research projects have not taken agricultural equipment as potential security threats. Therefore, we did some additional experiments based on solar insecticidal lamps Internet of Things, and the results indicate that agricultural equipment has an impact on agricultural security. Finally, more technologies (5G communication, fog computing, Internet of Everything, renewable energy management system, software defined network, virtual reality, augmented reality, and cyber security datasets for smart agriculture) are described as the future research directions of smart agriculture.**

***Index Terms*—Smart agriculture, Agricultural Internet of Things, Agricultural Artificial intelligence, Security, Agricultural automation.**

I. INTRODUCTION

AGRICULTURE is the primary industry in the world, and it plays an important role in social stability and economic development [1]. Overcoming the contradiction between the population explosion and the limited grain yield is a challenge that motivates an increasing number of studies on smart agriculture. The development of agriculture is based on both the improvement in productivity and the restrictions of the era, and the progress of science and technology drives the revolution of agriculture [2]. Fig. 1 is used to help readers understand the characteristics and confronted issues of agriculture development (from Agriculture 1.0 to Agriculture 4.0).

- **Agriculture 1.0**: the traditional agricultural era (between 1784 and around 1870) dominated by human and animal resources, the main issue of agriculture was the low efficiency of operation.
- **Agriculture 2.0**: the era of mechanized agriculture (in the 20th century), the main issue was the inefficient use of resources.
- **Agriculture 3.0**: the era of high-speed development of automatic agriculture (between 1992 to 2017), the main issue was the low level of intelligence.
- **Agriculture 4.0**: the era of smart agriculture (which is characterized by unmanned operations, begin at 2017) is mainly marked by the use of modern information technology to both serve agriculture and develop it intelligently.

Smart agriculture is a new agricultural production mode, that contributes to agricultural information perception, quantitative decision-making, intelligent control, precise investment, and personalized service through the deep integration of modern information technologies, e.g., the internet, Internet of Things (IoT), big data, cloud computing, and Artificial Intelligence (AI) with agriculture. In short, the new mode is a smart agricultural solution that combines agriculture with modern information technology. Although modern information technology brings new opportunities to the development of agricultural production, it also creates great demands and challenges to security and privacy in the field of smart agriculture. For instance, both intellectual and unmanned operations are the development goals of smart agriculture, whose characteristics not only increase productivity but also increase the security risks of equipment and data.

A. Motivation for the article

This article has three motivational factors:

Manuscript received August 27, 2020; revised October 1, 2020, accepted November 17, 2020. This work was supported in part by the National Natural Science Foundation of China under Grant 62072248, and in part by the National Natural Science Foundation of China under Grant 61902188, and in part by China Postdoctoral Science Foundation under Grant 2019M651713. *(Corresponding author: Lei Shu.)*

X. Yang and K. Huang are with the College of Engineering, Nanjing Agricultural University, Nanjing, 210031 China e-mail: (harryyangx@gmail.com, kai_huang@njau.edu.cn).

L. Shu is with the College of Engineering, Nanjing Agricultural University, Nanjing, 210031 China and also with the School of Engineering, University of Lincoln, Lincoln, LN67TS, UK email: (lei.shu@njau.edu.cn).

J. Chen and J. Wu are with the School of Cyber Security, Shanghai Jiao Tong University, Shanghai, 200240 China email: (jonnychen1996@sjtu.edu.cn, junwuhn@sjtu.edu.cn).

M. A. Ferrag is with Department of Computer Science, Guelma University, B.P. 401, 24000, Algeria e-mail: ferrag.mohamedamine@univ-guelma.dz

E. Nurellari is with the School of Engineering, University of Lincoln, Lincoln, LN67TS UK email: (ENurellari@lincoln.ac.uk).

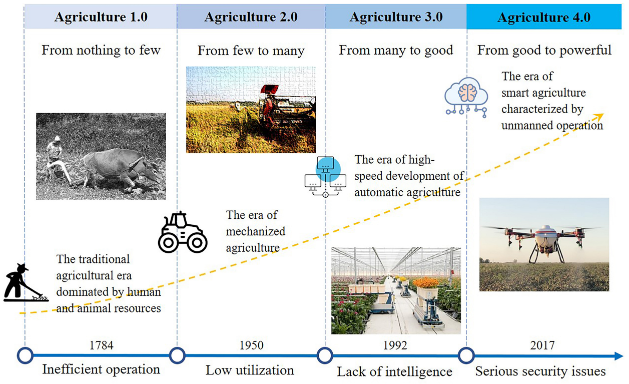


Fig. 1. Characteristics and confronted issues of agriculture development (from Agriculture 1.0 to Agriculture 4.0).

1) Smart agriculture is an emerging paradigm that extends information technology to traditional agriculture, and it has the potential as the development trend of agriculture due to the limited productivity of traditional agriculture and the wide application of information technology. Therefore, it is very important to summarize the existing production mode and specific researches.
2) Although smart agriculture has been extensively studied, little work has been done on the analysis of security challenges compared with industrial security solutions.
3) There is a great difference between urban (industry) conditions and rural (agriculture) conditions, as shown in Table I. It indicates that security countermeasures based on urban conditions may not suitable for rural conditions. Therefore, it is critical to analyze the characteristics of security issues under the smart agriculture scenarios.

For the above factors, this article aims to present a survey of the security topics that arise from smart agriculture, which naturally leads to a large number of open research issues.

B. Related works

1) Works related to smart agriculture: Some of the articles related to smart agriculture and its security issues are listed in Table III. In [3], typical applications of cloud computing technology in agricultural IoT were discussed, and a simple IoT agriculture model was addressed with a wireless network. Gondchawar *et al.* sought to make agriculture smart by using automation and IoT technology, e.g., smart GPS-based remote-controlled robot, smart irrigation with decision-making system, and smart warehouse management [4]. Antonacci *et al.* discussed the application of nanostructured sensors to support farmers in accessing fast and accurate analyses [5]. In [6], IoT deployment challenges and specific issues were discussed. In addition, the wireless communication technologies that are associated with agricultural applications were analyzed. Elijah *et al.* depicted the applications of IoT and data analytics in agriculture and analyzed the benefits of these applications [7]. Khanna *et al.* highlighted the applications of IoT in precision agriculture [8]. In [9], the research initiatives and scientific literature of smart agriculture were discussed in detail. The applications of big data in smart agriculture were discussed in [10], especially in terms of the food supply chain. In addition, the study mentioned that ensuring privacy and security is one of the greatest challenges of big data. Bacco *et al.* presented ground and aerial vehicles, along with the vision systems of UAVs in smart agriculture scenarios [11]. To identify the differences between UAV missions, the study also proposed a simple taxonomy. In [12] and [13], climate-smart agriculture was mainly used in precision agriculture by monitoring and predicting meteorological factors and environmental conditions. Various applications, services, and sensors based on IoT devices and communications techniques in smart agriculture were introduced in [14]. In [3]–[10], these studies also mentioned security issues without further discussion.

2) Works related to security issues in smart agriculture: Security issues in smart agriculture have been studied in [15]–[20], among them privacy-oriented blockchain-based solutions were introduced in [15], [16] proposed a holistic study on security and privacy in a smart agriculture ecosystem, and [17] studied the cyber security in smart agriculture. A prediction model framework for cyber-attacks in precision agriculture was presented in [18], and it is suggested that anomaly detection is needed to eliminate false alarms. Furthermore, Haseeb *et al.* proposed a security mechanism based on symmetric data encryption in agricultural sensors and a robust transmission strategy for IoT-based smart agriculture applications [19]. Moreover, Farooq *et al.* made a brief overview of security requirements, security challenges, stack challenges, thread model, and attack taxonomy on smart agriculture without further discussion about them [20]. Although the above surveys reviewed various smart agriculture applications and described security issues from the aspect of various information technologies, there is little discussion about security challenges in agricultural production.

C. Contribution

The contributions of this paper are listed as follows.

1) The development status of smart agriculture is summarized and classified into three typical development modes: precision agriculture, facility agriculture, and order agriculture. Furthermore, 7 key technologies and 11 key applications are discussed.
2) Security and privacy countermeasures are summarized as (1) authentication and access control, (2) privacy-preserving, (3) blockchain-based solutions for data integrity, (4) cryptography and key management, (5) physical countermeasures, and (6) intrusion detection systems.
3) Potential security challenges of smart agriculture are highlighted and divided into two aspects: (1) agricultural production and (2) information technology.
4) Agricultural equipment will also affect the security strategy. For instance, it is suggested that high voltage discharge interference of Solar Insecticidal Lamps Internet of Things (SIL-IoT) should be considered as attacks or have an impact on security strategy. In [25], [26], we did some experiments and the results indicate

TABLE I
COMPARISON OF SECURITY ISSUES BETWEEN URBAN (INDUSTRY) AND RURAL (AGRICULTURE)

	Urban-industry	Rural-agriculture	Security issue for rural
Communication	More base stations	Fewer base stations	Vulnerable to false base station attacks
Resident	More security-conscious	Lack of security-conscious	Hard to deal with security threats
Facility density	High	Low	Data of the attacked node cannot be replaced by neighbor nodes
Facility deployment	Mostly deployed indoor	Mostly deployed outdoor	Facilities are vulnerable to be stolen or damaged
Facility characteristics	QoS preferential	Low power consumption, low cost	Complex security methods cannot be applied in facility
Production data	Strong security measures	Weak security measures	Vulnerable to unauthorized access, data theft attacks
Production cycle	Production line, short production cycle	Based on crop growth cycle, long production cycle	More loss due to the attacks
Transport	Perfect transportation facilities	Farmland environment, bad traffic	Facilities cannot be repaired timely when they are stolen or damaged
Facility Ascription	Public space	Private facilities for farmers	Private devices contain more privacy information
Management system	Mature architecture, a lot of security measures	Immature architecture, lack of security measures	Vulnerable to control system intrusion and key theft

that the interference of high voltage discharge affects data transmission. Then, we found that the interference has an impact on data acquisition from the results of our additional experiments in this paper. Furthermore, the electromagnetic interference of photovoltaic power generation may also be potential attacks in photovoltaic agricultural Internet of Things.

The remaining part of this paper is structured as Fig. 2: Section II describes the development modes of smart agriculture. Section III lists some key technologies and applications in smart agriculture. Section IV summaries the security and privacy countermeasures for smart agriculture. Section V discusses the security challenges of smart agriculture. Section VI summarizes the future trends and opportunities of smart agriculture and Section VII concludes the article. To help readers understand this paper, acronyms found in this paper are shown in II.

II. DEVELOPMENT MODES OF SMART AGRICULTURE

At present, smart agriculture is the common goal of agricultural development in all countries worldwide. The world's typical smart agriculture development modes are divided into three types, as shown in Table IV. Considering the characteristics of the vast territory and uneven population distribution in China, the development modes need to be modified before they are applied to the different regions of China. These modes have a strong impact on promoting production management, industrial operation, and unmanned development of agriculture. Fig. 3 shows three types of development modes and their characteristics in smart agriculture.

A. *Precision agriculture*

According to the environmental conditions of each operation unit in the field and the temporal-spatial differences of crop yield, various agronomic measures should be carefully and accurately applied to optimize the quantity, quality and timing of water, fertilizer, seeds, pesticides, etc., so as to obtain the highest yield and maximum economic benefits, and protect the agricultural ecological environment and protect the agricultural natural resources. Precision agriculture is an advanced technology to improve crop yields, in which Wireless Sensor Networks (WSNs) is the main developmental driving force [30]. The combination of WSNs and agriculture can effectively reduce the potential risks of the production process and help farmers make favorable decisions by deploying a large number of low-power, multi-function, wireless communication sensors on farmland to collect relevant data throughout the agricultural production process (e.g., environmental data, crop growth data, and livestock health data) [31].

The modern information technology used in precision agriculture is mainly "3S", which includes remote sensing technology (RS), geographic information system (GIS), and global positioning system (GPS) [15]. Various types of data (e.g., GPS data, GIS data, RS data), as well as AI methods, are used in precision agriculture to deduce the crop growth process and propose crop production management in an expert decision system, which is different from the traditional agricultural production management methods based on subjective experience. The functions of precision agriculture include:

- Reducing environmental pollution by reasonably controlling the pesticide dosage;
- Reducing the waste of resources by improving the efficiency of agricultural irrigation;
- Enhancing the land utilization by improving the ecological environment of farmland;
- Improving the yield and quality of agricultural products by analyzing the law of crop growth and thereby maintaining the best crop growth conditions.

The main security threats in precision agriculture are:

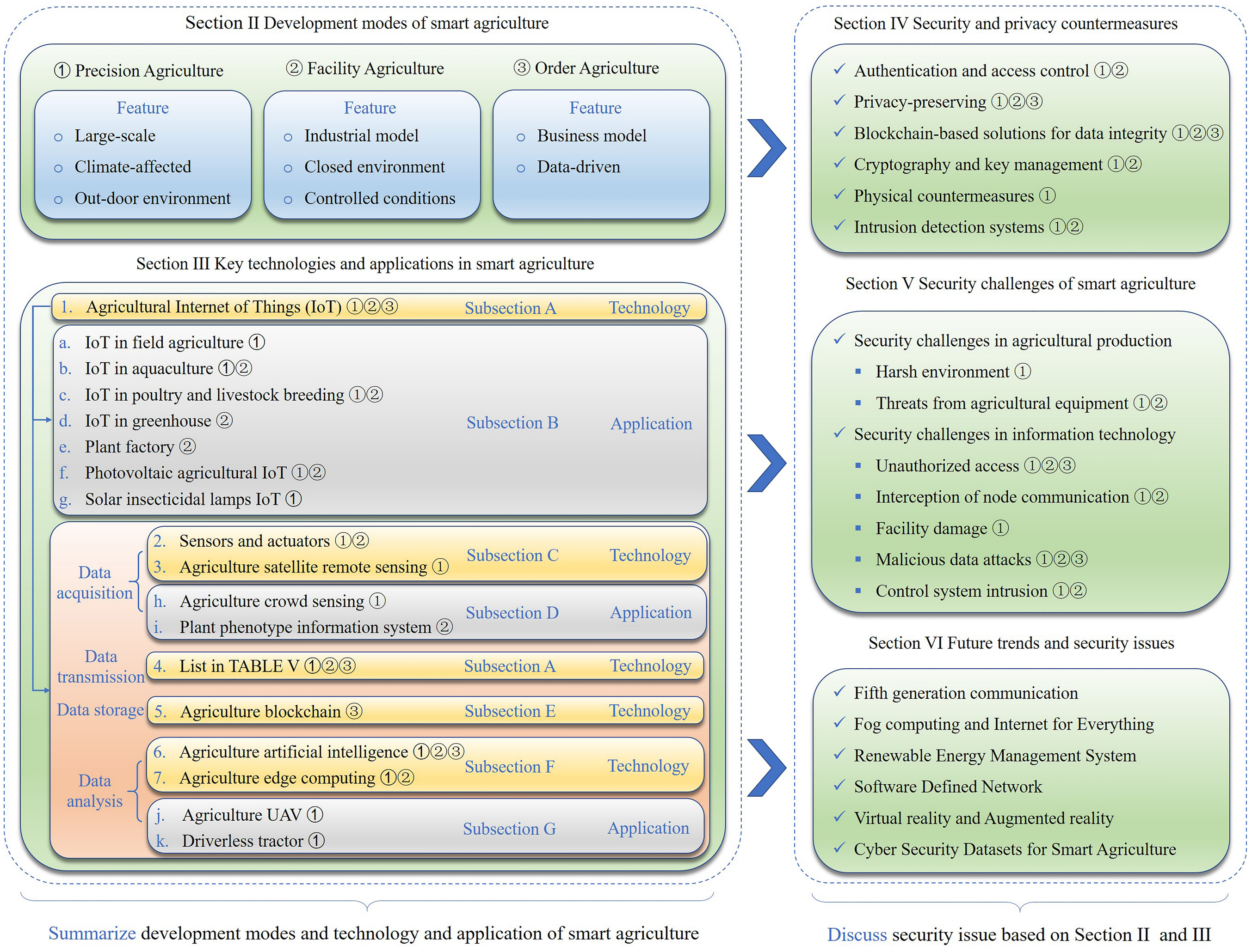

Section II Development modes of smart agriculture
① Precision Agriculture
② Facility Agriculture
③ Order Agriculture
Feature
○ Large-scale
○ Climate-affected
○ Out-door environment
Feature
○ Industrial model
○ Closed environment
○ Controlled conditions
Feature
○ Business model
○ Data-driven
Section III Key technologies and applications in smart agriculture
1. Agricultural Internet of Things (IoT) ①②③ Subsection A Technology
a. IoT in field agriculture ①
b. IoT in aquaculture ①②
c. IoT in poultry and livestock breeding ①②
d. IoT in greenhouse ②
e. Plant factory ②
f. Photovoltaic agricultural IoT ①②
g. Solar insecticidal lamps IoT ①
Subsection B Application
Data acquisition
2. Sensors and actuators ①②
3. Agriculture satellite remote sensing ①
Subsection C Technology
h. Agriculture crowd sensing ①
i. Plant phenotype information system ②
Subsection D Application
Data transmission
4. List in TABLE V ①②③ Subsection A Technology
Data storage
5. Agriculture blockchain ③ Subsection E Technology
Data analysis
6. Agriculture artificial intelligence ①②③
7. Agriculture edge computing ①②
Subsection F Technology
j. Agriculture UAV ①
k. Driverless tractor ①
Subsection G Application
Section IV Security and privacy countermeasures
✓ Authentication and access control ①②
✓ Privacy-preserving ①②③
✓ Blockchain-based solutions for data integrity ①②③
✓ Cryptography and key management ①②
✓ Physical countermeasures ①
✓ Intrusion detection systems ①②
Section V Security challenges of smart agriculture
✓ Security challenges in agricultural production
▪ Harsh environment ①
▪ Threats from agricultural equipment ①②
✓ Security challenges in information technology
▪ Unauthorized access ①②③
▪ Interception of node communication ①②
▪ Facility damage ①
▪ Malicious data attacks ①②③
▪ Control system intrusion ①②
Section VI Future trends and security issues
✓ Fifth generation communication
✓ Fog computing and Internet for Everything
✓ Renewable Energy Management System
✓ Software Defined Network
✓ Virtual reality and Augmented reality
✓ Cyber Security Datasets for Smart Agriculture
Summarize development modes and technology and application of smart agriculture
Discuss security issue based on Section II and III

Fig. 2. Organization of this paper. Development modes, 7 key technologies, and 11 applications of smart agriculture are summarized in Section II and III, which contribute to discuss security issues in Section IV, V and VI.

- Sensors being vulnerable to eavesdrop, steal and inject malicious data due to signal loss from their long-distance of deployment strategy and harsh environment;
- Location tampering of outdoor sensors and actors resulting in agricultural facilities failure and abnormal operation.

B. Facility agriculture

Facility agriculture has the goal of good quality and high yield, and this agricultural production mode is in the industrial style. This type of agriculture is a remarkable sign in the development of modern agriculture, and it is characterized by high demand for capital, technology, and labor. Using engineering technology, facility agriculture can provide man-made conditions suitable for crop growth, and facility protection; it can also remove the environmental restrictions on agricultural production and improve the efficiency of automatic production. Compared with traditional agriculture, facility agriculture can meet the multi-level consumption demands derived from societal development without the constraints of the natural environment and seasonal agricultural products [32].

Moreover, facility agriculture, facility horticulture, and facility breeding share a similar mode of production, and all of them are outfitted with the technologies, i.e., biotechnology, engineering technology, meteorology technology, IoT technology, and computer technology. The cores of the above three production modes consist of prediction models and decision-making management systems that are based on historical data, e.g., environmental data, crop growth data under different conditions, and crop growth data with different types of genes. Considering the different environmental requirements of crops, elements in the facility (e.g., temperature, air pressure, relative humidity, light intensity, and fertilizer application rate) are monitored and controlled in real time to ensure crops grow in the most favorable conditions. The most typical example is the intelligent greenhouse. The differences between specific studies (i.e., greenhouse, aquaculture, plant factory and poultry and livestock breeding) include different environmental elements, different sensor devices, and specific computer-controlled programs. The functions of facility agriculture include:

- Ensuring sustainable and efficient production within a completely closed environment with the function of in-

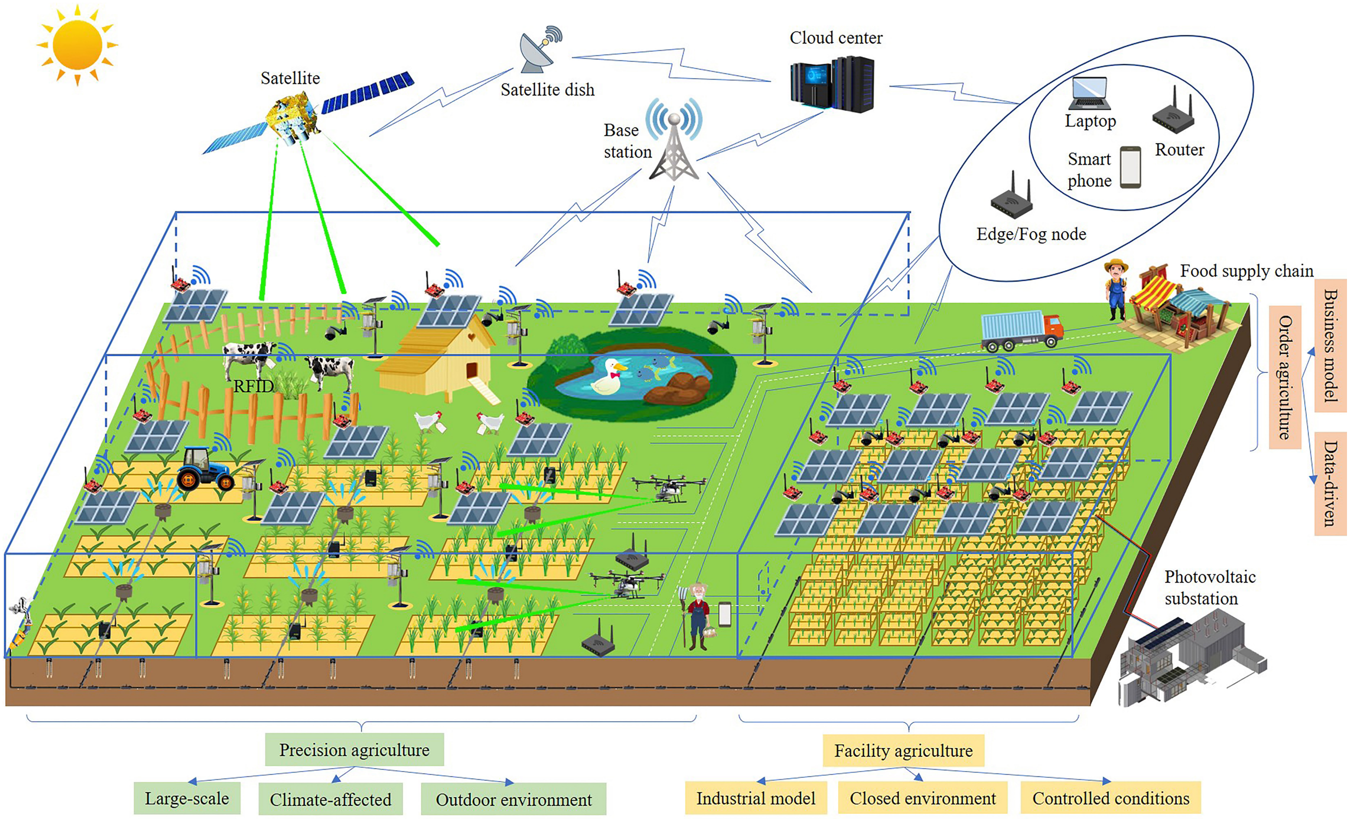


Fig. 3. Research fields of smart agriculture based on 1) precision agriculture, 2) facility agriculture, and 3) order agriculture.

telligent control;

- Ensuring agricultural production against the restriction of geographical conditions;
- Shortening the production cycle of agricultural products;
- Improving the quality and yield of products.

As a combination of both agriculture and industry, facility agriculture, will be the development trend of agriculture, and it has become a pillar industry in developed countries e.g., the U.S., the Netherlands, and Japan. Due to the characteristics of centralized administration and automatic management, facility agriculture is vulnerable to control system intrusion and unauthorized access.

C. Order agriculture

With the advancement of urbanization in China, urban development is rapid, while rural development is slow. There are three main problems that hamper rural development:

- A weak agricultural foundation,
- Hidden dangers in the quality and security of agricultural products,
- Information island transactions within agricultural products [33].

It implies that on its own, advanced agricultural production technologies are not sufficient, and it helps to create value only when it meets an enabling market opportunity [34]. Therefore, order agriculture has achieved an effective business model by outsourcing the production demand for agricultural products in advance, which can reduce the planting and breeding risks, and avoid blind production [29]. Besides, to ensure food security and manage agricultural products, a traceability system which makes consumers obtain the appropriate information agricultural productions is applied to agricultural product supply chain. Furthermore, agricultural product supply chain plays a vital role in the market supervision of agricultural products trade. The functions of agricultural product supply chain include:

- Improving the transparency of agricultural product information by modern e-commerce and blockchain technology;
- Eliminating the information island of an agricultural product transaction [35];
- Reducing the information asymmetry between farmers and suppliers;
- Reducing the imbalance between the supply of and demand for agricultural products.

For instance, Leng *et al.* [36] proposed a public agricultural supply chain system based on double chain architecture to provide a security guarantee mechanism for the public platform and improve the utilization of business resources. In [37], an agricultural provenance system based on blockchain was presented to solve the trust crisis in product supply chain.

D. Summary

Precision agriculture, facility agriculture, and order agriculture are the main development modes of smart agriculture, which combine traditional agricultural forms (outdoor),

TABLE II
ACRONYMS FOUND IN THIS PAPER

Acronym	Description
5G	Fifth generation communication
IoT	Internet of Things
WSNs	Wireless Sensor Networks
FC	Fog Computing
IoE	Internet of Everything
SDN	Software Defined Network
AI	Artificial Intelligence
GPS	Global Positioning System
UAV	Unmanned Aerial Vehicle
UGV	Unmanned Ground Vehicle
GSM	Global System/Standard for Mobile Communication
CDMA	Code Division Multiple Access
3GPP	3rd Generation Partnership Project
LET	Limited Technical Evaluation
TMSI	Temporary Mobile Subscriber Identity
WEP	Wired Equivalent Privacy
WPA	Wi-Fi Protected Access
AES	Advanced Encryption Standard
DES	Data Encryption Standard
SUPI	Subscription Permanent Identifier
RFID	Radio Frequency Identification
SIL	Solar Insecticidal Lamps
DAS	Direct Attached Storage
NAS	Network Attached Storage
SAN	Storage Area Network
GNSS	Global Navigation Satellite System
TTP	Trusted Third Party
RS	Remote Sensing
GIS	Geographic Information System
IP	Internet Protocol
PCA	Principal Components Analysis
ICS	Industrial Control Systems
SVM	Support Vector Machine
DDoS	Distributed Denial Of Service attack
EMS	Energy Management System
VR	Virtual Reality
AR	Augmented Reality

emerging agricultural forms (indoor), and agricultural products industry chain with emerging technologies. Various applications of smart agriculture based on the above development modes contribute to the improvement of grain products and the quality of agricultural products, the reduction of agricultural production costs, and the transparency of agricultural products trading.

III. Key technologies and applications in smart agriculture

In this section, 7 key technologies and 11 key applications in smart agriculture based on the three development modes mentioned in Section II are introduced. The arrangement of this section is shown in Fig. 2. Agricultural IoT (key technology, introduced in Subsection A) is the information carrier of the other technologies and applications in smart agriculture. Seven Typical applications of it (introduced in Subsection B) are: 1) IoT in field agriculture, 2) IoT in aquaculture, 3) IoT in poultry and livestock breeding, 4) IoT in greenhouse, 5) plant factory, 6) photovoltaic agricultural IoT, and 7) SIL-IoT). Besides, agricultural IoT has the functions of data acquisition, data transmission, data storage, and data analysis. According to the four functions, six key technologies are: 1) sensors and actuators, and 2) agriculture satellite remote sensing (data acquisition technologies, introduced in Subsection C); 3) various data transmission technologies (listed in V); 4) agriculture blockchain (data storage technology, introduced in Subsection E); 5) agriculture AI and 6) agriculture edge computing (data analysis technologies, introduced in Subsection F). And four key applications are: 1) agriculture crowd sensing, and 2) plant phenotype information system (data acquisition applications, introduced in Subsection D); 3) agriculture UAV, and 4) driverless tractor (data analysis applications, introduced in Subsection G).

A. Agricultural Internet of Things technology

Agricultural IoT is a key technology in smart agriculture which makes it possible to quantify the environmental factors, crop growth, and process of agricultural production by automatic processing, analysis, and access [38]. According to the definition of IoT, IoT architecture can be divided into perception layer, transmission layer, and application layer, as shown in Fig. 4.

In the perception layer, various types of sensors are used to collect both field environment information and crop growth information, and these sensors are also used to describe the state of the environment [39].

The transmission layer includes all types of network communication protocols in which the data collected by the perception layer can be transmitted to the application layer based on these protocols. Various wireless communication technologies and their parameters are listed in Table V (adapted from [6], [7], [38], [40], [41], and Wikipedia). Due to the characteristics of the large-scale and outdoor environment in precision agriculture, technologies with low transmission range (e.g., WiFi and Thread) and high energy consumption (e.g., WiFi) cannot apply to precision agriculture. In addition, low data rate technologies (e.g., 2G(GSM), Z-Wave, LoRa) are not applicable for some technologies with high throughput data transmission (e.g., plant phenotype information system).

The application layer plays a vital role in agriculture, and it can be the cloud-based (i.e., multiple servers) and local-based (i.e., edge computing based on the gateway) system. The application layer consists of the following functions:

TABLE III
RELATED WORKS

Reference	Main technology	Scenario	Security
Mekala *et al.* [3]	IoT, cloud computing	Water and energy management, crop monitoring	Metioned
Gondchawar and Kawitkar [4]	Automation, IoT	Smart machinery, smart irrigation, smart warehouse management	Theft detection by motion detector
Antonacci *et al.* [5]	Nanotechnology, sensors	Climate-smart agriculture, sensing systems	Working without interference from electric or magnetic fields
Ray *et al.* [6]	IoT	Bee keeping, greenhouse service platform, wheat disease detection, tomato pest control, UAV based precision agriculture	Metioned
Elijah *et al.* [7]	IoT, WSNs, data analysis	Monitoring, tracking and tracing, agricultural machinery, precision agriculture, greenhouse production	Metioned
Khanna *et al.* [8]	IoT	Precision agriculture	Metioned
Wolfert *et al.* [10]	Big data	Farm management, network management, data chain	Metioned
Bacco *et al.* [11]	UAVs, UGVs	Agriculture UAVs, agriculture UGVs	Not metioned
Bacco *et al.* [9]	Digitisation	Cloud/edge-based systems, unmanned vehicles, satellite-based activities	Metioned
Makate [12]	Scale agriculture, climate-smart agriculture	Approaches, policy and strategy in climate-smart agriculture	Not metioned
Totin *et al.* [13]	Climate-smart agriculture	A systematic review in climate-smart agriculture	Not metioned
Ayaz *et al.* [14]	IoT	Various applications, services and sensors in smart agriculture	Not metioned
Koksal and Tekinerdogan [21]	IoT	Farm management information systems	Metioned
Malche *et al.* [22]	IoT	Environmental monitoring system for smart city	Authenticating IoT sensor device and sending encrypted data
Munir *et al.* [23]	IoT, blockchain	Intelligent and secure smart watering system	Decentralized storage of irrigation and plants database by implementing the concept of blockchain
Ferrer [24]	Blockchain	Swarm robotic systems for precision farming	Public key cryptography by blockchain
Farooq *et al.* [20]	IoT	Livestock management, precision farming, greenhouse monitoring	Brief overview of security requirements, security challenges, stack challenges, thread model, and attack taxonomy on smart agriculture
Ferrag *et al.* [15]	Blockchain, IoT	Security and privacy in green-IoT based agriculture	Privacy-oriented blockchain-based solutions
Gupta *et al.* [16]	IoT, AI	Precision agriculture based multi-layered security and privacy architecture	A holistic study on security and privacy in a smart agriculture ecosystem
Barreto *et al.* [17]	Smart agriculture IoT	Water Management, Fertigation, Livestock Safety and Maturity Monitoring, Crop Communication, Drilling, Seeding and Spraying, Aerial Crop Monitoring, Supply Chain Monitoring	Cyber security in smart agriculture
West [18]	Parameters detection, IoT system	Precision agriculture threat prediction model based Common Vulnerability Scoring System	A prediction model framework for cyber-attacks in precision agriculture
Haseeb *et al.* [19]	WSNs, data encryption	Efficient and secure cluster routing for IoT-based smart agriculture applications	A security mechanism based on symmetric data encryption between agricultural sensors and a robust transmission
Our paper	Agricultural IoT, sensors and actuators, satellite remote sensing, blockchain, artificial intelligence, and edge computing	Smart agriculture based 6 security and privacy countermeasures and 7 security challenges	Summarizing development modes, technologies and applications of smart agriculture, and discussing security issues based on smart agriculture scenarios

TABLE IV
THREE TYPICAL DEVELOPMENT MODES OF SMART AGRICULTURE

Type	Country	Feature	Trends	Characteristics of type
Precision agriculture [27]	U.S.	Less population, more land, and developed industry	Develop field agriculture, replace manpower with mechanization, and decrease manpower operation.	Large-scale, climate affected, ourdoor environment
Facility agriculture [28]	Japan	More population and less land, scientific and technological progress	Improve crop genes, improve production conditions, and improve the land utilization rate.	Industrial model, closed environment, controlled conditions
Order agriculture [29]	Western Europe	Moderate population and land, developed economy	Increase agricultural scale, develop agricultural management, increase output rate.	Business model, data-driven

TABLE V
COMPARISON OF THE EXISTING WIRELESS COMMUNICATION TECHNOLOGIES

Year	Technology	Standard(s)	Transmission range	Frequency Bands	Data rate	Power	Security
1991	2G(GSM)	GSM,CDMA	Mobile network area	865MHz, 2.4GHz	50-100kb/s	Medium	TMSI
1999	WiFi	IEEE 802.11/a/c/b /d/g/n	20-100m	2.4, 3.6, 5, 60GHz	1Mb/s-6.75Gb/s	High	WEP, WPA, WPA2
1999	Bluetooth	IEEE 802.15.1	<100m	2.4GHz	1-24Mb/s	Medium	56/128bit
2001	WiMAX	IEEE 802.16	<50km	2-66GHz	1Mb/s-1Gb/s	Medium	AES, DES
2001	ZigBee	IEEE 802.15.4	<1km	2.4GHz	250kb/s	Low	128bit
2001	3G	UMTS, CDMA2000	Mobile network area	865MHz, 2.4GHz	0.2-100Mb/s	Medium	SNOW 3G, Stream Cipher
2004	Z-Wave	Z-Wave	<100m	908.42MHz	100kb/s	Low	Triple DES
2009	4G	UMTS, CDMA2000	Mobile network area	865MHz, 2.4GHz	100Mb/s-1Gb/s	Medium	SNOW 3G, Stream Cipher
2010	SigFox	SigFox	Rural: 30-50km	908.42MHz	10-1000b/s	N/A	N/A
2014	Thread	IEEE 802.15.4	<30m	686/915/ 2450MHz	250kb/s	Low	N/A
2015	LoRa	LoRaWAN	<20km	Various sub-GHz	0.3-50kb/s	Very low	AES 128bit
2015	NB-IoT	3GPP Rel.13	LTE/4G base stations	180kHz	DL:234.7kb/s, DI:204.8kb/s	Low	LTE encryption
2019	5G	3GPP, ITU, IMT-2020	Mobile network area	0.6-6GHz, 26,28, 38,60Hz	3.5-20Gb/s	Medium	SUPI

- **Data storage**, e.g., cloud-based platform and Hadoop distributed file system for quick and safe accessing to data [42];
- **Data management**, e.g., Supervisory Control And Data Acquisition (SCADA) for monitoring real-time data [18];
- **Data analytics**, e.g., decision-making system, yield models and plant instructions for automatic control in agricultural production [43];
- **Data marketing**, e.g., data visualization, traceability system of agricultural products for ownership, privacy, new business models [44].

B. Agricultural Internet of Things application

1) Internet of Things in field agriculture: Field crops mainly refer to such products as wheat, rice, and corn, which are of great significance to ensuring grain security [45]. In field agriculture, the main research topics include field resource management and agricultural condition monitoring, and IoT plays an important role in both of these areas. Based on the characteristics of various regions in field agriculture, it is difficult to apply wired transmission in that setting. Therefore, WSNs technology is mainly used instead of wired transmission in field agriculture [46]. After analyzing the data transmitted by the transmission layer, the application layer can be expanded into a variety of digital tools that benefit the agricultural production e.g., decision support systems, expert

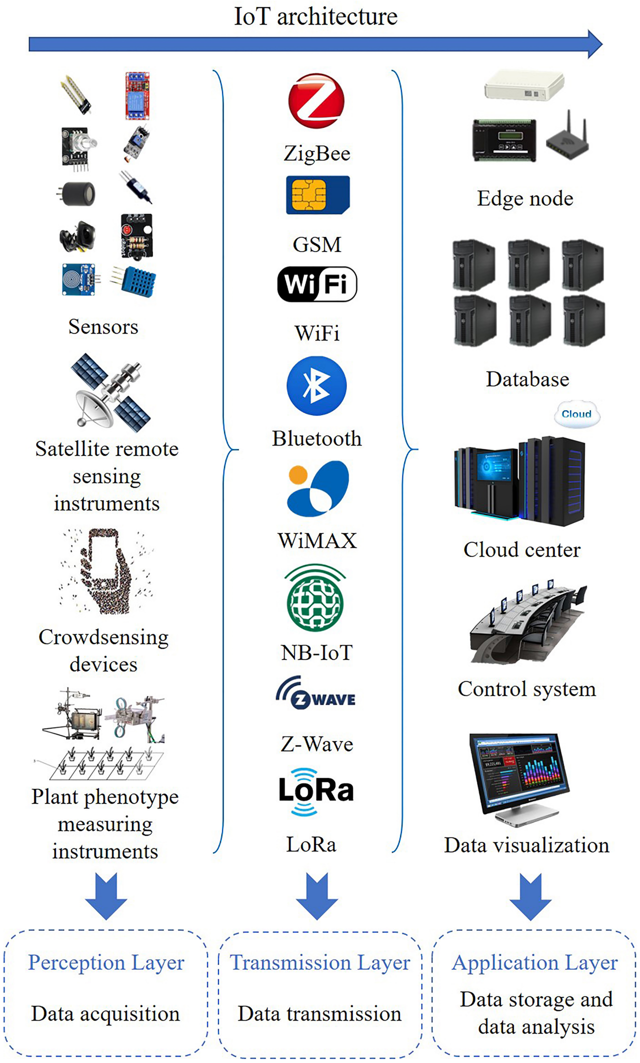


Fig. 4. Various technologies and applications based on IoT architecture.

systems, and cloud data storage.

Although IoT technology improves the efficiency and quality of field agricultural production, it also entails some security problems (e.g., agricultural facility damage).

2) Internet of Things in aquaculture: China has become the largest aquaculture country with aquaculture production that accounts for approximately two-thirds of the world's production [47]. Currently, aquaculture is transferred from traditional extensive aquaculture to industrialized and precise aquaculture. IoT in aquaculture is a symbol of the transformation of aquaculture, it is an intelligent aquaculture system based on WSNs that collects environmental data for real-time monitoring, early warning analysis, and auxiliary decision-making [48]. Special facilities, e.g., water quality parameter sensors, underwater robots, underwater cameras, and meteorological stations, are applied to monitor environment elements such as the water temperature, dissolved oxygen, pH value, salinity, and chloride in real time. In addition, actuators are used to adjust the water quality of the culture pond to ensure the most suitable environmental conditions for the growth of aquatic organisms [49].

The differences between IoT in aquaculture and IoT in field agriculture include not only the monitoring objects but also the complex aquaculture environment and various influencing factors during the growth of aquatic organisms. Thus, it is difficult to implement accurate and effective monitoring, detection, and optimization management [50].

3) Internet of Things in poultry and livestock breeding: Compared with the other forms of agricultural production, poultry and livestock breeding have higher production scales and requirements in terms of the technology, facility, and funds [51]. IoT in poultry and livestock breeding is based on both indoor conditions and outdoor environment, as shown in Fig. 5. Indoor conditions include facilities e.g., environmental control equipment (to ensure environmental stability), automatic feeding equipment (to ensure forage supply), video monitoring equipment (to monitor animal behavior). In addition, to track the growth status of each animal under indoor conditions and outdoor environment and increase the traceability of meat products, Radio Frequency Identification (RFID) technology is generally used to set the electronic identification, assign a serial number to each animal, and simplify data storage and tracing [52]. Hence, the advantages of monitoring, identification, and positioning of animals through RFID technology are:

- Effectively strengthening the detection of the breeding environment;
- Preventing the spread of various epidemic diseases among animals;
- Ensuring the price stability of meat products [53].

For instance, the recent sharp rise in the price of pork in China, which resulted from African swine fever in 2019, will not happen again if IoT technology is well applied in poultry and livestock breeding. Currently, important studies of IoT in poultry and livestock breeding include the electronic identification of animals, database management of animal information, the quality control and safety traceability of product, and auxiliary disease diagnosis using AI technology [54]. Due to the high production value of poultry and livestock breeding, high data sensitivity is required for the decision-making system. Failures in sensors, links, and decision-making systems may lead to irreparable economic losses to farmers.

4) Internet of Things in greenhouse: Through the environmental control system, IoT in a greenhouse provides a closed growing environment to ensure the healthy growth of crops without the restrictions of an external environment, which helps improve the yield and quality of crops [55]. Agriculture production of IoT in greenhouse can be divided into the following steps:

- Collecting the environmental data through sensors, including the temperature, relative humidity, carbon dioxide concentration, light intensity, soil temperature, soil humidity, and pH value;
- Uploading the collected data to the control system through signal transmission facilities;
- Modeling and analyzing the heterogeneous data through the prediction model in the control system [56].

(a) Indoor facility for chicken farm

(b) Outdoor environment for sheep breeding

(c) Indoor facility for hog farm

(d) Outdoor environment for cattle breeding

Fig. 5. Indoor conditions and outdoor environment of poultry and livestock breeding, e.g., (a) indoor conditions for chicken farm, (b) outdoor environment for sheep breeding, (c) indoor conditions for hog farm, and (d) outdoor environment for cattle breeding.

Through the above three steps, the facilities in a greenhouse, e.g., the sprinkler irrigation facility, drip irrigation facility, and temperature regulation facility, can execute commands intelligently and automatically to maintain steady environmental conditions.

5) Plant factory: Due to the growing scarcity of both arable land and water sources, a type of low-consumption, environmental-protection, high-yield, and safe agricultural production mode has emerged as the most suitable mode for agriculture. The plant factory is one of the representative technologies, which is a reflection of the transformation from traditional agriculture to modern industry [57]. The plant factory's characteristics include:

- No limitation due to the environmental conditions;
- Less pollution;
- Less waste of resources;
- A controllable production cycle, these features ensure the agriculture production even with a deterioration of the ecological environment [58].

Similar to the production mode of IoT in a greenhouse, a plant factory cultivates crops under the controlled conditions of factors such as the temperature, humidity, carbon dioxide concentration, and light intensity. The differences are that the plant factory has:

- Higher mechanization;
- Higher automation;
- More hydroponics;
- A higher space utilization rate;
- Proximity to a city;
- A closed and clean environment.

At present, plant factories are mainly distributed among East Asia, Europe, and the U.S., and artificial light plant factories are being developed rapidly in Japan. Due to the reduction of arable land, frequent natural disasters, and the shortage of rural labor, agriculture is also trending to plant factories in China [59]. The key technologies of the plant factory are as follows:

- Three-dimensional and multi-layer soilless cultivation technology;
- Artificial lighting luminous technology;
- Intelligent environment control technology;
- Automatic control technology of the plant production space.

The above technologies are associated with the production efficiency and production cost of a plant factory [60]. A plant factory is confronted with the following issues:

- The high cost of the initial construction and maintenance;
- Limited types of crop cultivation;
- A low level of intelligent production;
- Low security and privacy [60].

Because the above issues hinder the development of plant factories, they should gain more attention and emphasis.

6) Photovoltaic agricultural Internet of Things: With the reduction of natural resources and the aggravation of environmental pollution, clean and renewable energy plays an indispensable role in the energy transformation of the world [61]. In China, photovoltaic power generation occupies a significant position in new energy power generation, and there is vast potential for its development [62]. In addition, photovoltaic power generation has the advantages of low operation cost, no greenhouse gas emissions, and a low maintenance cost [63]. However, the development of photovoltaic power generation is limited by the low energy conversion efficiency, the high correlation with meteorological factors, and the waste of residual power after the grid connection [64], [65]. With the combination of photovoltaic power generation and agricultural IoT, the residual power can be utilized effectively.

Generally, if the actual generation exceeds the demand of the grid, power will be limited to protect the grid, which leads to energy waste. With the application of residual power for agricultural IoT facilities through battery storage, the wasted power and farm operation costs can be effectively reduced. For example, photovoltaic energy was used for the irrigation of farmland, and SolarCoin (similar to Bitcoin) was proposed for energy and water trading [66]. In addition, because a large area of land is required for both field agricultural production and photovoltaic power generation, deploying photovoltaic panels over farmland can optimize land usage [67]. Moreover, sensors for monitoring field crops can acquire power from a photovoltaic system and monitor photovoltaic power generation facilities [68]. However, this technology also brings some security challenges. For instance, photovoltaic power generation may have a great impact on information transmission and further increase the risk of receiving malicious data.

7) Solar insecticidal lamps Internet of Things: Solar insecticidal lamps (SIL) kill migratory pests by releasing a high voltage pulse current, which contributes to reducing the usage of pesticides [69]. At present, SIL are widely applied in China, for instance, 20000 SIL have been deployed for pest control in Xinyu City, Jiangxi Province, China. With a low level of intelligence, most of the traditional SIL are deployed only for killing pests among the fields. However, pest information cannot be obtained to make forecasts of pests and adjust the work time of insecticidal lamps adaptively.

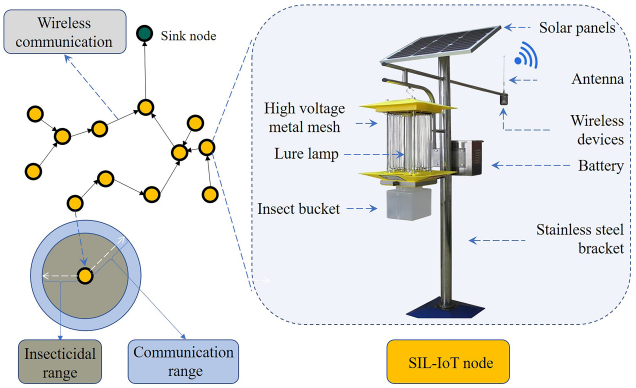


Fig. 6. SIL-IoT component and communication diagram. The insecticidal range is smaller than the communication range, which ensures that the SIL-IoT nodes deployed in the field meet the communication requirements.

Therefore, the application situation of SIL was investigated and the structure diagram of SIL-IoT node was introduced in [69]. It has been found that the effective killing distance of SIL (SIL deployment radius $\leqslant 110m$) [70] is in the valid communication radius of wireless sensor nodes (e.g., ZigBee, LoRa), as shown in Fig. 6. Due to the advantages of SIL-IoT (i.e., pollution-free, high insecticidal efficiency, and easy for scheduling), SIL-IoT will be applied widely for pest prevention and control, as well as the data acquisition of field agriculture. Recently, Yang *et al.* [70] proposed a node deployment strategy based on partition structure for SIL-IoT. The node deployment problem is transformed into a secondary allocation problem by using the natural partition structure of farmland, and the problem is solved by genetic algorithm. Under the constraint of ensuring full coverage, this strategy significantly reduces the number of SIL-IoT nodes. In addition, Huang *et al.* [25], [26] found that high voltage pulse discharge released by SIL has been as an interference to ZigBee-based device in SIL-IoT. It is metioned that the device in [25], [26] can be used as a method to attack WSNs, leading to the abnormal working state, and it is suggested that the installing space between SIL and ZigBee-based device is at least 25cm. Moreover, Yang *et al.* [71] mentioned that the interference will affect fault diagnosis of SIL-IoT and thereby affect the reliability of SIL-IoT. In [71], the characteristics and challenges of fault diagnosis in SIL-IoT are analyzed and it is highlighted that security attacks will lead to the failure of fault diagnosis.

Although the application of IoT technology expands the functions of insecticidal lamps and improves their utilization rate, it entails some new security challenges. For example, signal interference is serious when the insecticidal lamp is discharged, and traditional signal transmission security methods may not suitable for this situation.

C. Data acquisition technology

Data acquisition is an interface that uses a device to collect data from the outside of the system and input them into the internal system. Data acquisition technology mainly includes:

- RS232, RS485 serial ports for connecting multiple detection instruments to implement automatic data acquisition;
- USB interface for outputting data;
- The wireless communication module for transmit data;
- Various sensors for collecting data and various actuators for maintaining the controlled variable;
- Satellite for obtaining, measuring and processing the related data through the interaction between electromagnetic wave and object.

These technologies can be applied to agriculture crowd sensing and plant phenotype information system, which obtain data from perception module of mobile devices, camera, spectrometer, various weather sensors, etc..

1) Sensors and actuators: Agricultural sensors are mainly used to collect both environmental conditions and crop growth information [39] and then transmit the data to the cloud [38]. Various sensors in smart agriculture can be classified into location sensors, photoelectric sensors, mechanical sensors, electrochemical sensors, airflow sensors, and optical sensors, as shown in Table VI (adapted from [5], [7], [72]). These sensors are applied to collect meteorological information (e.g., temperature, humidity, carbon dioxide concentration), crop information (e.g., crop growth conditions, crop disease), soil information (e.g., tensiometers, soil type, and moisture level of the soil), location information (e.g., precision location of crops), etc..

Then, these information are transmitted to the cloud. If the data collected by the sensor meet certain judgment conditions, actuators will activate or deactivate agricultural equipment. The main actuators in facility agriculture are:

- Irrigation equipment to ensure the sufficient moisture for crop growth;
- Lighting control equipment to ensure the suitable lighting conditions for crop growth;
- Air circulation to ensure the carbon dioxide concentration in closed growth conditions;
- Crop disease control to ensure the healthy growth of the crop.

2) Agricultural satellite remote sensing: Agricultural satellite remote sensing is a technology that monitors:

- Various types of agricultural systems e.g., field planting and aquaculture;
- The process of agricultural production;
- Multiple elements of agriculture i.e., production, environment, and ecology information [73].

It is mainly applied to the following fields: area estimation, crop growth monitoring, pest information monitoring, yield prediction, grassland vegetation monitoring, and agricultural resources mapping [74]. Moreover, the trends of agricultural satellite remote sensing development in the world include both joint observation and high spatial-temporal resolution monitoring.

In China, the demand for sky-air-ground-integration in agriculture was proposed in the "Outline of the National Rural Development Plan of Sky-air-ground Digital Agriculture (2018-2025)". The requirements also include realizing (1) the digitalization of all factors and all production processes, and

TABLE VI
SENSORS IN SMART AGRICULTURE

Type of sensors	Function	Application
Location sensors	Locate precision location of crops	Locate precision location of crops
Photoelectric sensors	Analyze signal by photoelectric effect	Monitor temperature, illumination, humidity, carbon dioxide
Mechanical sensors	Convert the measured quantity (physical quantity) to mechanical quantity	Tensiometers to detect the force used by the roots in water absorption
Electrochemical sensors	Detect specific ions in the soil by electrodes	Monitor temperature, humidity, gas composition
Airflow sensors	Convert a gas volume fraction into a corresponding electrical signal	Measure compaction, structure, soil type, and moisture level of the soil
Nanostructured (bio)sensors	Exploit features of nanomaterials for different purposes	Analyze soil humidity, water and soil nutrients/pesticides, and plant pathogens

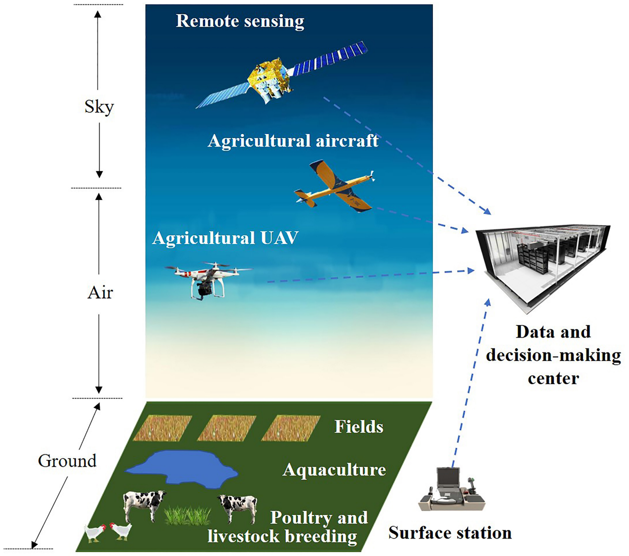


Fig. 7. Massive data fusion among satellites, aircraft, UAVs, and surface stations.

(2) intelligent dynamic monitoring in field planting, animal husbandry, and related areas [75]. To implement sky-air-ground-integration, several problems must be solved, e.g., we need both cooperative observation among satellites, and massive data fusion among satellites, aircraft, UAVs, and surface stations, as shown in Fig. 7.

D. Data acquisition application

1) Agricultural crowd sensing: Crowd sensing employs the functions of perception computing, common measurement, and information sharing by a large number of personal mobile devices (e.g., smartphones and wearable devices) to complete large-scale and complex perception tasks [76]. Mobile terminal equipment is used as the basic sensing unit to complete the collection of sensing data through the wireless network. Furthermore, with the combination of the ideas of both mobile perception and crowdsourcing, crowd sensing has the advantages of low cost, strong scalability, and strong mobility. The emphases of crowd sensing are:

- The data processing technology;
- The incentive mechanism;
- The crowd sensing software platform.

To date, crowd sensing has been widely used in intelligent transportation, public security, environmental monitoring, and other applications. It is mainly applied in urban environments, and there have been few applications in rural ones. Due to the increasing proportion of farmers with smartphones and the demands of collecting agricultural data, agricultural crowd sensing has huge potential for data acquisition [77]. For instance, Ginige *et al.* [78] proposed a mobile-based information system which consists of a smart computing framework, and was studied for farmers to report pest and disease outbreak events. As a new IoT sensing technology, agriculture crowd sensing will inevitably entail a variety of security challenges [79]. For example, a SmartfLAIr system was proposed for an increased resolution of leaf area index and a perturbation based privacy mechanism with Trusted Third Party (TTP) architecture was designed to ensure user privacy [80].

2) Plant phenotype information system: The plant phenotype information system is a technology that quantitatively analyses the interaction effect of both the genotype and the environment on crop products' quality and other traits. It has the following functions:

- Monitoring the growth of crops by deploying various types of sensors and measuring instruments under Specified conditions [81];
- Analyzing the data from both UAVs and satellite remote sensing to quantify the growth state and yield of crops under different genes and environmental factors;
- Selecting stable and high-yield crop genes and their suitable growth environment.

All the functions are based on abundant plant phenotype information, which is mainly composed of massive images, videos, and text data. To make the data suitable for analytics, the main studies of plant phenotypic information systems are:

- Massive data annotation [82], management [83] and integration [84] (i.e., data annotation, data association and data storage by knowledge graph technology);
- Massive image data analysis [85], [86] (e.g., machine learning, and deep learning algorithms).

Due to the characteristics of interdisciplinary fusion, multi-team cooperation is required for a plant phenotype information system. Hence, Ubbens *et al.* [87] proposed a deep plant phenomics system, which was an easy platform by providing a pre-trained model for plant scientists. In addition, a plant phenotype information system involves various technologies, e.g., sensor facility, network communication, big data platform, and data processing method, which entails many security issues.

E. Data storage technology

Data storage objects include temporary files generated by data stream or information that needs to be searched in the process of processing. At present, the main data storage methods include:

- **Direct Attached Storage (DAS)**, a storage device directly connected to the host system without centralized management solution;
- **Network Attached Storage (NAS)**, a device with data storage function connected to the network;
- **Storage Area Network (SAN)**, a network in which storage devices are connected to each other and connected to a server or group of servers.

Moreover, database is the most commonly used data storage software, which consists of:

- **Relational database**, the relational model is used to organize data in database, e.g., Oracle, SQLServer, MySQL;
- **Non-relational database**, removing the relational characteristics of relational database to ensure the scalability of data, e.g., Redis, MongoDb, Neo4J).

From the aspects of storage mode, traditional databases mostly adopts centralized storage mode, which are confronted with capacity bottleneck issue. Therefore, distributed database is presented, which provides scalable service capacity and storage capacity by the way of sub database and sub table, and provides transparent data access and smooth capacity expansion and reduction by database agent. Similar to the characteristics of distributed database, blockchain is a decentralized distributed database, which collectively maintains a reliable database by decentralizing and trusting mechanisms.

1) Agriculture blockchain: Blockchain technology was proposed by scholars with the pseudonym of ”Satoshi Nakamoto” in 2008. It is a point-to-point distributed data-storage-architecture scheme, and it uses a variety of consensus mechanisms to achieve collaborative trust among multiple participants [88]. Furthermore, the application of cryptographic methods ensures the security of data transmission. At present, the intelligent operation of node data can be implemented by deploying smart contracts (a kind of script code) on distributed nodes [89]. Blockchain supplies a reliable technical guarantee for both the integrity and immutability of information, and it is widely used in product information traceability [90].

In agriculture, blockchain has the following functions: (1) establishing the backtracking mechanism of agricultural products. Reliable and safe information about agricultural products including their planting, processing, and selling are provided to improve information transparency. In addition, the distributed information storage method based on digital encryption and verification technology ensures the information security of agricultural products [91]; (2) establishing a new agricultural product trading market. The distributed storage technology of blockchain is used to digitize the upstream and downstream information of agricultural products. Moreover, the information is shared across the entire agricultural blockchain alliance [92]. Although blockchain can be used as an information security solution, it is essentially data storage and releases technology. Because blockchain technology is still in the exploration stage in agriculture, the security challenges of blockchain remain to be explored.

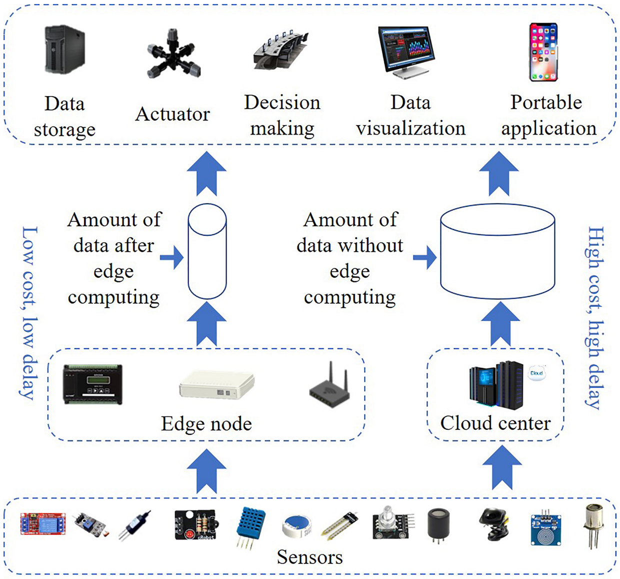


Fig. 8. Comparison of edge computing and cloud computing. The advantages of edge computing are low cost and low delay, which benefit to high time efficiency tasks, e.g., SIL-IoT, agricultural UVAs, driverless tractors.

F. Data analysis technology

Data analysis is a process of detailed research and summary of data to extract useful information, which uses appropriate methods (e.g., statistical analysis method, machine learning method) to analyze the large amount of data. Artificial intelligence is an emerging technology which contributes to the accuracy of data analysis. In addition, edge computing technology greatly reduces the traffic amount and delay by deploying artificial intelligence algorithms on the device rather than cloud server.

1) Agricultural artificial intelligence: With the development of IoT technology, the amount of agricultural data has increased dramatically. AI technology can provide an expert system to analyze agricultural big data, select valuable information, and increase agricultural productivity finally [93], [94]. At present, there are many studies and applications in agriculture AI [95], [96]. The main studies of agriculture AI include:

- Intelligent robots based on pre-set machine learning models and computer vision technology that complete basic agricultural tasks much more quickly than manpower and traditional robots, e.g., intelligent seeding robot and intelligent harvesting robots;
- Crop and soil monitoring, which have applied both computer vision technology and deep learning algorithms to analyze the crop growth data and soil health data;
- Predictive analysis, which forecasts the impact of weather changes on crop harvests by training machine learning model [97].

Based on the above studies, manual operations are being replaced by intelligent machines and decision-making systems, which contribute to the development of smart agriculture [10]. However, AI technology will result in huge losses (e.g., a wrong decision for the irrigation system and plant factory environment control) if it suffers from attacks.

2) Agricultural edge computing: Cloud computing provides scalable, on-demand, and virtualized resources for users [98]. Therefore, cloud computing has been widely applied in planting, aquaculture, poultry and livestock breeding, plant factories, and related applications [54]. However, it is difficult to use the centralized data processing method of cloud computing to meet the growing amount of data, which stem from the explosive growth of agricultural data. Although cloud computing has the advantages of both strong computing power and fast processing speed, the demands of data analysis cannot be fully met by it due to its disadvantages (e.g., high cost, high delay, and low capacity of protecting the privacy of users).

Thus, edge computing is applied in agriculture to solve these problems, as shown in Fig. 8. The "edge" refers to any network and computing resources between the data source (e.g., sensors) and the cloud data center [99]. For instance, the smartphone is the edge between the user and the cloud. By transmitting sensor data to edge devices for calculation, communication delay can be reduced effectively [100]. Therefore, edge computing is suitable for tasks with both low computational cost and high timeliness requirements [101].

In the area of SIL-IoT, if insect pest location data are transmitted to the cloud for decision-making and then returned to an actuator, the pest outbreak area may be transferred before the implementation of relevant measures. However, if the data are transmitted to the edge nodes and then returned to the actuator, the delay caused by the data transmission will be greatly reduced. Therefore, it is important to promote agricultural edge computing and find its potential security problems [102].

G. Data analysis application

1) Agricultural unmanned aerial vehicle: With the development of "3S" technology, UAVs have become widely used in agriculture, industry, and commerce. Furthermore, the UAVs' characteristics of labor-saving and high efficiency are consistent with the development goal of smart agriculture. At present, the studies of agricultural UAVs mainly focus on plant protection operations, forestry monitoring, crop pollination, and herd positioning [103].

Due to the advantages of high operating efficiency, low pollution, and no poisoning risks for farmers in agricultural applications, the development of agricultural UAVs has been rapidly growing in some countries e.g., the U.S., Russia, South Korea, and especially Japan. With more than 2400 registered agricultural UAVs and more than 14000 operators, Japan has become the country that has the largest number of agricultural UAVs [104]. Compared with the above countries in the fields of UAVs, the development of Chinese UAVs has lagged, but the investment in agricultural UAVs has increased in recent years.

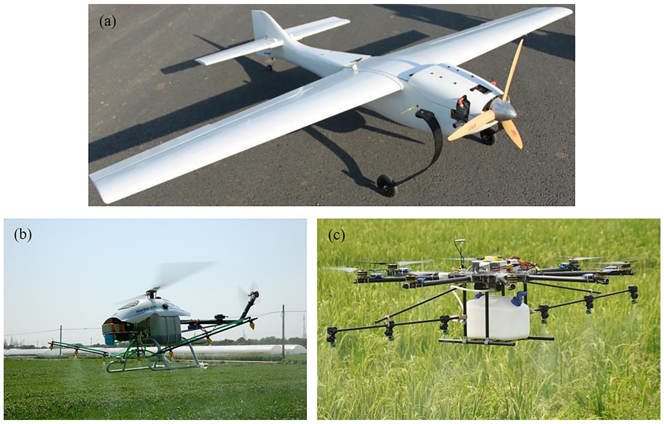


Fig. 9. (a) Fixed-wing UAV, (b) single-rotor hydraulic UAV, and (c) multi-rotor electric UAV. Currently, electric multi-rotor UAVs have a major market share due to their low cost, low failure rate, simple operation, and environmental protection.

There are various types of agricultural UAVs on the market, as shown in Fig. 9. For instance, UAVs can be divided into both hydraulic UAVs and electric UAVs according to the dynamic system. Furthermore, UAVs can be divided into fixed-wing UAVs, single-rotor UAVs, and multi-rotor UAVs according to the model structure. Currently, electric multi-rotor UAVs have a major market share due to their low cost, low failure rate, simple operation, and environmental protection. Besides, the plant protection UAV is one of the most common applications of agricultural UAVs, based on high operating efficiency, good spraying effect, low pollution level, and operation without limitations due to the crop height. The technology gaps in the production areas where plant protection cannot be carried out manually are addressed by agricultural UAVs [103].

2) Driverless tractor: The traditional tractor is indispensable power machinery in field agriculture, as it provides traction for cultivating machines, traction seeders, a machine that spray insecticide, harvesters, etc. [105]. The driverless tractor is a combination of the traditional tractor and modern driverless technology. The advantages of driverless tractors include both optimal operation path planning by the map transmission system and dynamic obstacle avoidance by lidar, which contribute to improving the quality and efficiency of operations, and maximizing the utilization rates of land, seed and fertilizer [106], [107].

Currently, the applications of the global navigation satellite system (GNSS) and laser system in driverless tractors have been generalized in Europe, so as to avoid obstacles and operate in the appointed paths effectively [108]. In [109], further studies have been conducted in North America on the key components of automatic navigation, including navigation sensors, vehicle motion models, navigation plan devices, and steering controllers. Liu *et al.* [110] proposed an artificial vehicle powertrain system to build a general framework for data-driven intelligent control, which can be applied to the driverless tractor.

Furthermore, China has begun to develop driverless tractors in recent years. For instance, the major research program "Cognitive Computing of Audio-visual Information" of the National Natural Science Fund of China (NSFC) was established in 2008, and it has provided finance and policy support for driverless driving.

H. Summary

In this section, we described 7 key technologies and 11 key applications in smart agriculture based on IoT architecture (perception layer for data acquisition, transmission layer for data transmission, and application layer for data storage and data analysis). Some applications of agricultural IoT are introduced: IoT in field agriculture, IoT in aquaculture, IoT in poultry and livestock breeding, IoT in greenhouse, plant factory, photovoltaic agricultural IoT, and SIL-IoT, which have unique characteristics in specific agricultural scenarios and are confronted with various security threats (e.g., agricultural facility damage for IoT in field agriculture, failures in sensors for IoT in poultry and livestock breeding, control system intrusion for IoT in greenhouse and plant factory, malicious data attacks for photovoltaic agricultural IoT, and signal interference for SIL-IoT).

In addition, sensors and actuators, and agriculture satellite remote sensing are introduced as data acquisition technologies, which contribute to the applications of data acquisition (agriculture crowd sensing, and plant phenotype information system). There are some security threats for data acquisition technologies and applications, e.g., facility damage and interception of node communication for sensors and actuators, unauthorized access for agriculture satellite remote sensing, privacy leaks for agriculture crowd sensing, and control system intrusion for plant phenotype information system.

Agriculture blockchain is described as a distributed data storage technology to ensure data storage security, which is also confronted with security threats (e.g., access control failure, unsafe consensus agreement).

Moreover, agriculture artificial intelligence and agriculture edge computing are introduced as data analysis technologies. They are confronted with various security threats e.g., malicious data attacks, unauthorized access, and control system intrusion. The above data analysis technologies are applied in agriculture UAV and driverless tractor for path planning, automatic operation, local information processing, etc.. There are some security threats for agriculture UAV and driverless tractor, e.g., false location information by malicious data attacks, facility damage by control system intrusion, data interception by interception of node communication.

Therefore, effective security and privacy countermeasures play a vital role in ensuring security of smart agriculture.

IV. Security and Privacy Countermeasures

The summary of existing security and privacy countermeasures which are suitable for smart agriculture are presented in Table VII. The relationship between some key technologies and applications in smart agriculture and security and privacy countermeasures are shown in Fig. 10.

A. Authentication and access control

To enhance the security and privacy of smart agriculture, user authentication systems should ensure the following security and performance requirements: resilience to various attacks, device anonymity, session key agreement, mutual authentication, and unlinkability. Lee *et al.* [111] proposed a three-factor anonymous user authentication scheme, which can be applied in a network model composed of three types of nodes, namely, a mobile node, a sensor node, and a gateway. Based on the bio-hash function, Lee *et al.*'s scheme can satisfy user anonymity, users untraceability, and resists stolen mobile device attacks. For achieving cross-domain permission delegation and access control, Gauhar *et al.* [112] proposed a decentralized blockchain-based framework, named xDBAuth, which the blockchain technology is used for providing transparent to all the users in the IoT network. The xDBAuth framework considers a network model composed of five main elements, including, smart contract, IoT devices, blockchain manager, overlay network, and underlay network. Based on the two algorithms, namely, cross-domain resource access algorithm and proof-of-authenticity/integrity algorithm, the xDBAuth framework can provide authentication/authorization, availability, integrity, and non-repudiation.

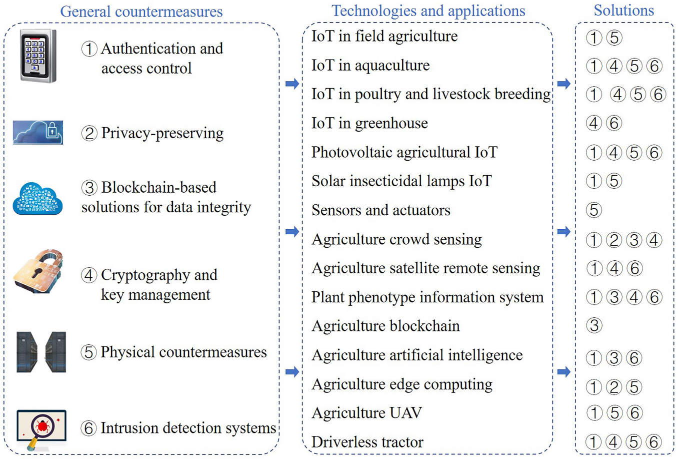

General countermeasures
① Authentication and access control
② Privacy-preserving
③ Blockchain-based solutions for data integrity
④ Cryptography and key management
⑤ Physical countermeasures
⑥ Intrusion detection systems
Technologies and applications
IoT in field agriculture
IoT in aquaculture
IoT in poultry and livestock breeding
IoT in greenhouse
Photovoltaic agricultural IoT
Solar insecticidal lamps IoT
Sensors and actuators
Agriculture crowd sensing
Agriculture satellite remote sensing
Plant phenotype information system
Agriculture blockchain
Agriculture artificial intelligence
Agriculture edge computing
Agriculture UAV
Driverless tractor
Solutions
①⑤
①④⑤⑥
①④⑤⑥
④⑥
①④⑤⑥
①⑤
⑤
①②③④
①④⑥
①③④⑥
③
①③⑥
①②⑤
①⑤⑥
①④⑤⑥

Fig. 10. Different security and privacy countermeasures for 7 key technologies and 11 key applications in smart agriculture.

In addition, Shin *et al.* [113] designed a privacy-preserving authentication scheme for wireless sensor networks in 5G-integrated IoT, which the IoT architecture is based on a wireless sensor network, gateways, cloud computing, and with three types of layers, including, network layer, application layer, and support layer. The Shin *et al.*'s scheme uses elliptic curve cryptography to guarantees gateway anonymity, user anonymity with untraceability, and resistant to four types of attacks, including, offline password guessing attacks, mobile device loss attacks, stolen verifier attacks, and user impersonation attacks.

B. Privacy-preserving

For achieving privacy-preserving, Wang *et al.* [114] proposed a privacy-preserving spectrum sharing framework for the IoT network, which can be applied for smart agriculture by considering at the same time the spatial spectrum reuse and truthfulness. Specifically, the proposed framework considers three units, including, a cryptographic authority, multiple bidders, and an auctioneer. Based on the Elgamal

TABLE VII
Summary of security and privacy countermeasures for Smart Agriculture

Authentication model	**Scheme**	**Year**	**Network model**	**Security analysis**	**Performance (+)**	**Limitation (-)**	**Performance analysis**
Informal security analysis	Lee *et al.* [111]	2020	The network model composed of three types of nodes, namely, a mobile node, a sensor node, and a gateway	Mutual authentication	+ Resistance to stolen mobile device attack + Ensures a session key agreement	- Location privacy is not considered	High communication cost
Informal security analysis	Gauhar *et al.* [112]	2020	The network model is composed of five main elements: smart contract, IoT devices, blockchain manager, Overlay network, and underlay network	Authentication and Authorization	+ Protects the network availability + Provides non-repudiation	- Stolen mobile device attacks	Medium overhead ratio
Privacy-Preserving	Shin *et al.* [113]	2020	The IoT architecture is based on a wireless sensor network, gateways, cloud computing, and with three types of layers, including, network layer, application layer, and support layer	BAN logic	+ Guarantees gateway anonymity and the user anonymity with untraceability + Resistant to offline password guessing and mobile device loss attacks	- The network availability is not considered	Medium computation cost
Privacy-Preserving	Wang *et al.* [114]	2020	The network model is composed of three units, including, a cryptographic authority, multiple bidders, and an auctioneer	Simulation-based	+ Can hide the user's bid + Achieving user satisfaction ratio	- There is no security analysis against attacks	High communication cost
Privacy-Preserving	Wei *et al.* [115]	2020	A cloud-centric network model with smart devices	Informal security analysis	+ Message authenticity and integrity + Preserving the location and identity privacy	- Non-repudiation is not considered	Low computation cost
Privacy-Preserving	Zhang *et al.* [116]	2020	The network model is composed of four parts, namely, a trusted authority, edge servers, control center, and cloud server	q-strong Diffie–Hellman (q-SDH) assumptions	+ Privacy-preserving and integrity verification	- Location privacy is not considered	Medium computation cost
Intrusion detection system	Ferrag *et al.* [117]	2020	Three-tier fog computing architecture (i.e., cloud computing, fog computing, and IoT devices)	Simulation-based	+ Detecting cyber attack	- Authentication and privacy are not achieved	High accuracy and detection rates
Data integrity	Hang *et al.* [118]	2020	The network model is composed of four main components, including, end-user, blockchain network, fish farm, and data storage	Simulation-based	+ Provides reliable and secure storage	- There is no security analysis against attacks	Low computation cost
Data integrity	Shahid *et al.* [119]	2020	The network architecture is composed of three layers, including, data layer, blockchain layer, and storage layer	Simulation-based	+ Achieves accountability and authenticity + Robust against denial of service attacks	- Location privacy is not considered	Low computation cost
Intrusion detection system	Anthi *et al.* [120]	2019	Three layers, including, layer 1 for scanning the network, layer 2 for classifying the packets, and layer 3 for classifying malicious packets	Simulation-based	+ Detecting cyber attack + Identifying malicious packets	- Authentication and privacy are not achieved	High F-measure rates
Physical countermeasure	Li *et al.* [121]	2019	Learning-based IoT security system	Simulation-based	+ Detect physical attacks and threats + Use only energy audit data	- Non-repudiation is not considered	Medium storage cost
Intrusion detection system	Ahmim *et al.* [122]	2018	Learning-based IoT security system	Simulation-based	+ Detecting cyber attack	- Authentication and privacy are not achieved	High accuracy and detection rates
Key management	Esposito *et al.* [123]	2018	Group nodes with the cluster head and the border nodes	Simulation-based	+ Lower the costs of rekeying + Achieves confidentiality	- Integrity is not achieved	Low computation cost
Physical countermeasure	Ali and Awad [124]	2018	The network model of composed of three parts, including, IoT devices, a gateway, and a web server.	Information risk assessment	+ Highlight various security vulnerabilities + Mitigating the identified risks	- Authentication and privacy are not achieved	Efficient for resource-constrained devices
Key management	Wazid *et al.* [125]	2017	The network model is composed of three different nodes, including, the sensing nodes, the gateway node, and cluster head nodes	AVISPA tool	+ Resilience against sensing node capture attack + Providing anonymity and untraceability	- The network availability is not considered	Medium computation cost
Intrusion detection system	Sforzin *et al.* [126]	2016	The network model is based on a small, portable device, pre-packaged with an intrusion detection system	Simulation-based	+ Detecting cyber attack	- Authentication and privacy are not achieved	Efficient for resource-constrained devices

encryption scheme, the proposed framework can keep the bidders¡¯ bids confidential and achieving user satisfaction ratio. Therefore, in order to enable offline/online computation and support IoT devices with various cryptographic settings, Wei *et al.* [115] designed privacy-preserving message authentication scheme, named SAMA, for IoT networks, which can be applied for smart agriculture. The SAMA scheme uses various systems such as RSA-type and ElGamal-type for preserving the location and identity privacy of a data source as well as message authenticity and integrity. Zhang *et al.* [116] proposed a privacy-preserving data aggregation scheme, named LVPDA, which can be applied for the edge-computing-enabled smart agriculture. During the data aggregation process, the LVPDA scheme combines an online/offline signature technique and Paillier homomorphic encryption method for privacy-preserving and integrity verification. Based on the q-strong Diffie¨CHellman (q-SDH) assumptions, the LVPDA scheme is proven unforgeable under the chosen message attack.

C. Blockchain-based solutions for data integrity

The blockchain technology is used as a security solution to provide data integrity in smart agriculture. To provide automated data processing in fish farming, Hang *et al.* [118] designed a blockchain-based fish farm platform, which is based on smart contracts. The proposed platform uses four main components, including, end-user, blockchain network, fish farm, and data storage. Based on the blockchain network, the proposed platform can provide reliable and secure storage. Therefore, to provide traceability and trust in the agri-food supply chain, Shahid *et al.* [119] proposed a security solution deployed over the Ethereum blockchain network. The proposed solution considers an agri-food supply chain with a layered architecture and is categorized into three layers, including, data layer, blockchain layer, and storage layer. To achieve accountability and authenticity, the proposed solution uses an interplanetary file storage system that receives the data and returns a hash of these data to the blockchain network.

D. Cryptography and key management

The symmetric encryption/decryption along with the cryptographic hash function are used by Wazid *et al.* [125] for designing a secure user authenticated key management protocol, which can be applied in smart agriculture. The network model used by the proposed protocol is composed of three different nodes, including, the sensing nodes, the gateway node, and cluster head nodes. To verify the biometric authentication, the proposed protocol uses the fuzzy extractor technique. To ensure confidentiality with end-to-end security guarantees, Esposito *et al.* [123] proposed a clustered and distributed key management framework, which is based on the group-based keys. Specifically, the proposed framework uses a network model composed of group nodes with the cluster head and the border nodes. In addition, within the proposed protocol, the key to be shared, is divided into encoded parts, and only a part of the received parts is transmitted by the cluster head to its neighboring nodes.

E. Physical countermeasures

Both cyber and physical attacks are in high demand in smart agriculture. Li *et al.* [121] proposed an auditing and analytics-based IoT monitoring mechanism. The proposed mechanism uses disaggregation-aggregation architecture using the evaluation of the power usage of the system's sub-components. Therefore, the proposed mechanism adopts two deep learning models, including, the aggregation model and disaggregation model. Therefore, to provide a comprehensive view of the security status of smart homes in smart agriculture, Ali and Awad [124] proposed the operationally critical threat, asset, and vulnerability evaluation methodology, named OCTAVE, which focuses on information assets. The OCTAVE method is applied in the network model composed of three parts, including, IoT devices, a gateway, and a web server. In addition, the OCTAVE method uses four main phases to allow comprehensive risk assessment, including: 1) establish drivers phase, 2) profile assets phase, 3) identify threats phase, and 4) risk mitigation phase.

F. Intrusion detection systems

Cyber-attacks for smart agriculture infrastructures are emerging as an increasingly important concern for both organizations and nations. To detect these cyber-attacks in smart agriculture, security researchers have proposed intrusion detection systems based on machine learning and data mining algorithms. Ferrag *et al.* [117] and Maglaras *et al.* [127] designed a hybrid intrusion detection system, named RDTIDS, for internet-of-things networks, which can be applied for smart agriculture. Specifically, the RDTIDS system uses decision tree and rules-based concepts to classify the network traffic as attack/benign. The experimental results on the BoT-IoT dataset and the CICIDS2017 dataset shows that the RDTIDS system achieves the highest accuracy with 96.995% and 96.665%, respectively.

In addition, Anthi *et al.* [120] designed a three-layer intrusion detection system for detecting a series of cyber-attacks on IoT networks, which can be applied for smart agriculture. The proposed system uses a supervised approach to classifies attacks such as replay attack, reconnaissance attack, man-in-the-middle attack, spoofing attack, and denial of service attack. The experimental results on cyber attacks dataset show that the proposed system achieves an F-measure of: 1) 96.2%, 2) 90.0%, and 3) 98.0%. Sforzin *et al.* [126] proposed an intrusion detection architecture for the IoT network, named RPiDS, which can be applied for smart agriculture. The RPiDS architecture uses a small, portable device, pre-packaged with an intrusion detection system for detecting an active attack and or suspicious network-related activity. The experimental results on Raspberry Pi equipped with Snort show that RPiDS architecture is adapted to conduct intrusion detection in an IoT framework. Ahmim *et al.* [122] designed an intrusion detection system that can be applied for smart agriculture. Specifically, the proposed system can be installed at the fog computing layer for detecting cyber-attack using the combination of the probability predictions of a tree of classifiers. The experimental results on KDD'99 and NSL©datasets show

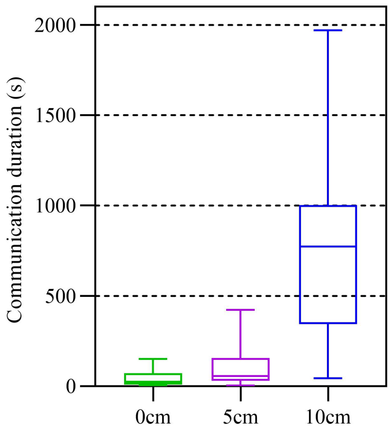


Fig. 11. Interference on different distances between SIL and receiving node. Average communication duration values of 0cm, 5cm, and 10cm are 45.6s, 116.5s, and 765.9s. Maximum values of 0cm, 5cm, and 10cm are 151s, 422s, and 1970s. Minimum values of 0cm, 5cm, and 10cm are 4s, 4s, and 45s.

that the proposed system achieves the highest accuracy with 96.27% and 89.75%, respectively.

V. Security challenges of smart agriculture

Most of the existing security and privacy countermeasures are based on industrial scenarios or only based on simulation performance, without considering the actual application scenarios. Therefore, it is necessary to analyze security challenges based on smart agriculture, which contributes to applying the above security and privacy countermeasures to various smart agriculture scenarios.

A. Security challenges in agricultural production

1) Harsh environment: The modes of agricultural production mainly include large-scale field farming, small-scale greenhouse farming, aquaculture, and poultry and livestock breeding. However, the maintenance problems of sensors and farm implements by the above modes cannot be ignored. The primary maintenance problems include hardware protection for the facilities and the energy consumption design of the facilities. Due to the characteristics of sparse deployment and the absence of supervision in agricultural IoT facilities, sensor nodes may be stolen and used by malicious users, which would lead to serious security problems (e.g., data leakage and network paralysis). In addition, agricultural IoT facilities are required to have reliable long-distance signal transmissions, and they must reduce their energy consumption to ensure their long-term stable operation. Therefore, a balance between energy consumption and the reliability of the signal transmission is critical for agricultural IoT facilities.

2) Threats from agricultural equipment: Except for the harsh environment, the security issues caused by the working characteristics of agricultural equipment cannot be ignored. For instance, SIL release high voltage (2̃150V to 6̃000V) pulse discharge while migratory insects with phototaxis feature contact with the metal mesh, which has a great impact on ZigBee [25]. In [25], [26], we did some experiments and the results indicate that the interference of high voltage discharge affects data transmission. In this paper, we did the following experiments under the same experimental devices [26] (parameter, evaluating indicator, purpose, and device are shown in Table VIII). The first experiment (only indicating that the interference affects sending node) has been done in [26] before, we did that again with three evaluating indicators and extended it to two additional experiments, which are used to verify whether the interference has an impact on receiving node and sensors.

- Observing the interference of high voltage pulse discharge for sending node under the distances of 10, 15, 20, and 25cm. Table IX illustrates that the interference is stronger to ZigBee with the closer distance between SIL and sending node (there is a positive correlation between FET and interference intensity). It is mentioned in [26] that the interference (quantified by FET times) has an impact on the ZigBee-based device. However, the influences of the interference on data transmission and data acquisition are not mentioned. Therefore, we did the next two experiments.
- Observing the interference of high voltage pulse discharge for receiving node under the distances of 0, 5, and 10cm. The results are depicted in Fig. 11, and communication duration is the time difference between node receiving data normally and not receiving data normally. It is observed from the results that the communication duration has a positive correlation with the distance between SIL and receiving node. Moreover, when the distance between SIL and receiving node is more than 10cm, the interference is not obvious under the existing experimental equipment and conditions. The distance may increase with the increase of the interference intensity generated by the equipment.
- Observing the interference of high voltage pulse discharge for sensors under the distances of 0 and 5cm. The sensors with ID 1 and 2 were used for the experiment (distances between them and SIL are 0 and 5cm), and the sensor with ID 3 was used as the control group (distance between it and SIL is 1m). As shown in 12, when we turn on the discharge module at 15:34:30, the data acquisition is abnormal and the device reset after a few seconds. The proportion of abnormal data (the proportion of abnormal data to all data in a certain period) and the proportion of device reset are shown in Table X. When the distance is 0cm, sensors with ID 1 and 2 can hardly collect data normally. The interference is not obvious when the distance between SIL and sensors is more than 5cm. However, in the case of a harsh environment and aging equipment, the effective range and extent of injury of interference may be unpredictable.

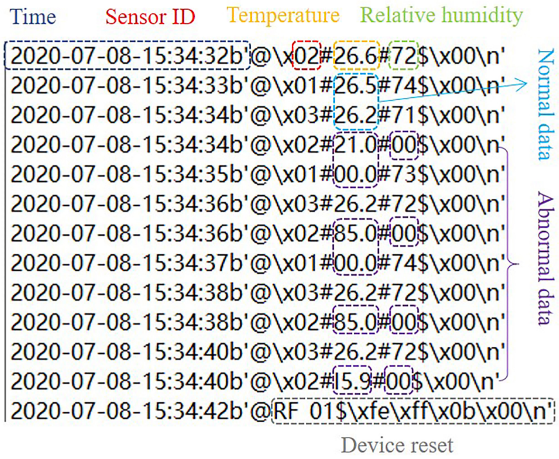
The above experiments indicate that the interference of high voltage pulse discharge has an impact on data transmission and data acquisition. The interference is a kind of security threat and may mislead the execution of security strategy. For instance, if the receiving node cannot receive data normally

TABLE VIII
INTERFERENCE EXPERIMENTS FOR DIFFERENT DEVICES

Experiment	Parameter	Evaluating indicator	Purpose	Affected Device
1	1. Discharge frequency: 4 2. Distances between SIL and the sending node: 10, 15, 20, 25 cm 3. Experimental duration: 5min	1. Average Packet Reception Ratio (PRR) 2. Average CRC error times newline 3. Average Falling Edge Trugger (FET) times	Verifying the interference of high voltage pulse discharge for sending node	ZigBee (Webee)
2	1. Discharge frequency: 4 2. Distances between SIL and the receiving node: 0, 5, 10 cm	Communication duration	Verifying the interference of high voltage pulse discharge for receiving node	ZigBee (Webee)
3	1.Discharge frequency:4 2.Distances between SIL and the sensors: 0, 5 cm	1. Proportion of abnormal data 2. Proportion of device reset	Verifying the interference of high voltage pulse discharge for data acquisition	Sensors (DHT11)

TABLE IX
INTERFERENCE ON DIFFERENT DISTANCES BETWEEN SIL AND SENDING NODE

Distance	Average PRR	Average CRC times	Average FET times
10cm	99.96%	0.017	34.4
15cm	99.98%	0.03	33.11
20cm	99.98%	0.017	24.18
25cm	99.99%	0.02	9.62



```
2020-07-08-15:34:32b'@\x02#26.6#72$\x00\n'
2020-07-08-15:34:33b'@\x01#26.5#74$\x00\n'
2020-07-08-15:34:34b'@\x03#26.2#71$\x00\n'
2020-07-08-15:34:34b'@\x02#21.0#00$\x00\n'
2020-07-08-15:34:35b'@\x01#00.0#73$\x00\n'
2020-07-08-15:34:36b'@\x03#26.2#72$\x00\n'
2020-07-08-15:34:36b'@\x02#85.0#00$\x00\n'
2020-07-08-15:34:37b'@\x01#00.0#74$\x00\n'
2020-07-08-15:34:38b'@\x03#26.2#72$\x00\n'
2020-07-08-15:34:38b'@\x02#85.0#00$\x00\n'
2020-07-08-15:34:40b'@\x03#26.2#72$\x00\n'
2020-07-08-15:34:40b'@\x02#I5.9#00$\x00\n'
2020-07-08-15:34:42b'@RF_01$\xfe\xff\x0b\x00\n'
```

Fig. 12. Data acquisition under interference. For the first line, “2020-07-08-15-15:34:32” is time format, “02” is sensor ID in red dotted box, “26.6” is temperature (°C) in yellow dotted box, and “72” is relative humidity (%) in green dotted box. Besides, data in blue dotted box are normal data, data in violet dotted box are abnormal data, and data in grey dotted box are device reset information.

due to interference, the security strategy may classify it as a DDoS attack.

B. Security challenges in information technology

1) Unauthorized access: Unauthorized access refers to unauthorized use of system resources and unauthorized access to a database, which results in serious network security challenges. To access data and control agricultural IoT facilities beyond the limit of users’ authority, hackers attack the access control mechanism of the system by forging a counterfeit identity [128]. The main reasons for unauthorized access are:

TABLE X
INTERFERENCE ON DIFFERENT DISTANCES BETWEEN SIL AND SENSORS

Distance	Sensor ID	Proportion of abnormal data	Proportion of device reset
0cm	1	78.61%	10.98%
	2	89.45%	3.52%
	3	0%	0%
5cm	1	45.31%	3.01%
	2	57.27%	1.48%
	3	0%	0%

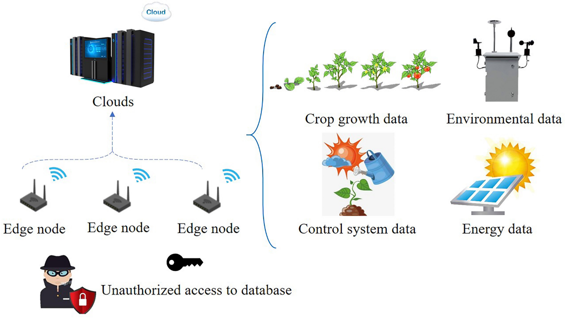


Fig. 13. When a variety of data is transmitted to the cloud or edge node, hackers access the database through unauthorized access.

- Rapid change of accessing the particular user account from the unrecognized location;
- Accessing the user account with an unrecognized device;
- Sudden IP, server domain and gateway change [128].

Identity authentication, which identifies legal users by their passwords and biometrics, is applied to prevent unauthorized access [129]. Furthermore, access control strategies should be set up to manage user rights, and to ensure the security of various resources in the system. As shown in Fig. 13, hackers can illegally access edge nodes and cloud databases to obtain crop growth data and modify control system information, which would have an impact on crop growth and data quality.

2) Interception of node communication: Wireless communication technology is widely applied in various agricultural IoT facilities. Unfortunately, the information transmitted by wireless communication is easily copied and stolen [130].

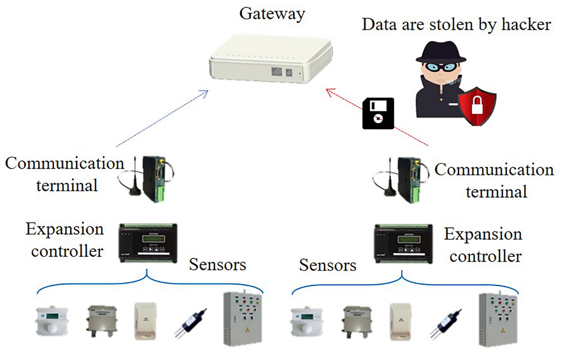


Fig. 14. In the process of node communication, hackers intercept data by invading receiving nodes.

The information usually contains both environmental data collected by sensors and facility control signals in agricultural production. Data tampering and interception by hackers may have serious consequences [131]. To ensure the security of wireless communication, appropriate encryption strategies for wireless devices are required to encrypt data [132]. Simultaneously, various wireless sensors may not be able to support complex encryption algorithms for communication security. Therefore, a balance between the encryption strength and the facility capacity must be sought. As presented in Fig. 14, data collected by sensors can be sent to a gateway through the communication terminal. Hackers steal data by invading wireless communications, which results in serious consequences.

3) Facility damage: Due to the complex conditions in an agricultural production environment, facilities that are deployed in an agricultural environment may send incorrect data, be damaged, or lose the capacity to collect data. Facility damage may result in data distorted and missing, which would affect the data analysis and the decision-making system [133]. Therefore, it is necessary to establish a facility detection mechanism. If the facility stops working or the data collected by the sensors deviate from the normal range, faults should be detected and related measures should be implemented promptly by the neighboring nodes or diagnosis nodes. Fig. 15 shows various faults that result from facility damage, which have negative impacts on the daily operation of agricultural UAVs.

4) Malicious data attacks: AI technology can be applied with its ability to analyze massive data and sensory data is the main factor in any decision-making process [134]. In addition, a pre-trained model with optimal environmental parameter settings contributes to improving the yield and quality of agricultural products. However, by inserting malicious data into the database, the model training process is affected, which would cause a deviation in the model results. The primary solutions include the privacy protection of agricultural IoT facilities [135], and online and real-time monitoring system [136]. As presented in Fig. 16, due to malicious data attacks, the solar insecticidal lamps in an actual pest outbreak area are sleeping, which leads to crops damage. Simultaneously, we have a waste of energy caused by incorrect responses of the solar insecticidal lamps that are in the false pest outbreak area.

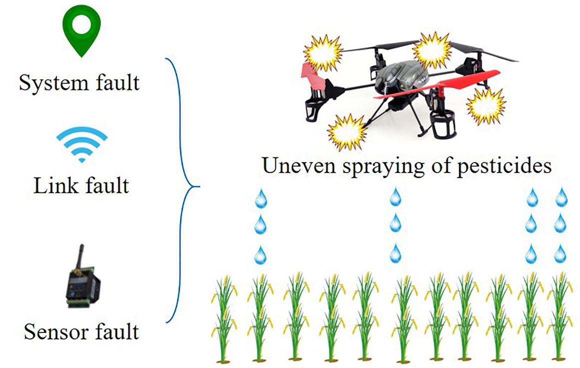


Fig. 15. System fault, link fault, sensor fault, and other factors lead to uneven spraying of pesticides.

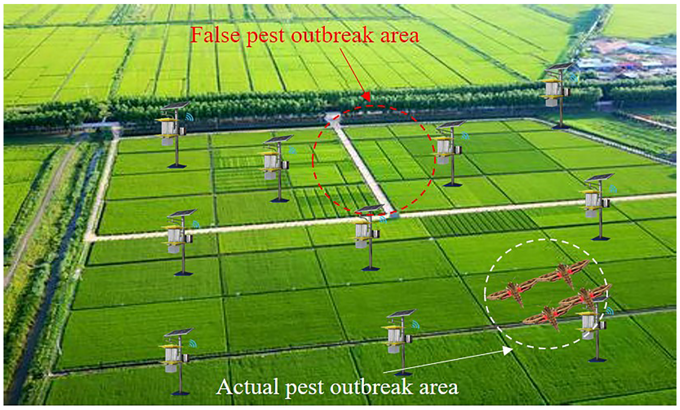


Fig. 16. Due to malicious data attacks, the solar insecticidal lamps in an actual pest outbreak area are sleeping, which leads to crops damage. Simultaneously, we have a waste of energy caused by incorrect responses of the solar insecticidal lamps that are in the false pest outbreak area.

5) Control system intrusion: After the data collection and analysis, the control system sends commands to the machinery to complete the corresponding production operation. Therefore, the security of the control system plays a vital role in agricultural production. Control system intrusion may lead to no response from the production machinery [137], which would have a strong impact on agricultural production. Therefore, protecting the decision-making system from intrusion, and protecting the control signals from interference has a great impact on the performance of agricultural production. Fig. 17 illustrates a driverless tractor operating on the wrong route after a control system intrusion.

C. Summary

Due to the harsh environment and threats from agricultural equipment, the protection measures and anti-interference design of the agricultural equipment are very important. Furthermore, severe weather prediction and interference filtering at the software layer contribute to the security of agricultural production. However, ensuring the security of agricultural production is a very complex task, mainly because of changeable

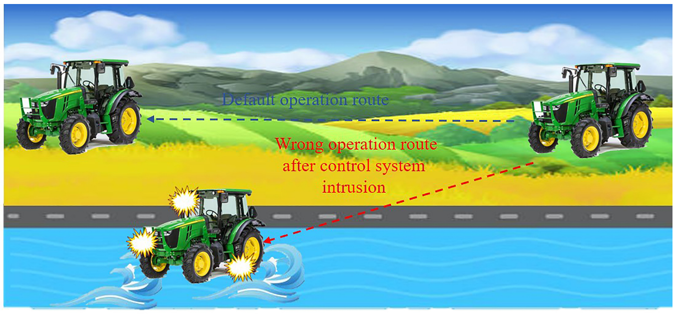


Fig. 17. A driverless tractor operating on the wrong route after a control system intrusion.

climatic conditions, large-scale and harsh environments, and various agricultural equipment with different standards.

In addition, recent works related to information security are shown in Table XI. Key distribution and authentication mechanisms are a major research direction of unauthorized access, and among these works, machine learning algorithms have been used to improve the accuracy of the classifications [138]. Furthermore, hypothesis testing is a method that can estimate false alarm rate and false negative rate (i.e., 5% false rejection rate with four PCA dimensions [129]).

Recent studies of the interception of node communication focus on the decode-and-forward protocol, and the affected layer is typically the cyber-physical layer. Intercept probability is mainly used to estimate the performance of model, increasing power-splitting factor signal power, and the number of relays may improve the security of wireless transmission [130], [132], [139]. In addition, Zou and Wang [131] demonstrated that sensor scheduling method contributes to against eavesdropping attack.

The perception layer is the main affected layer in facility damage. Various methods are used to protect sensors and actuators, and the effective ones include node privacy and source encryption methods [140].

Malicious data attacks mainly happen in smart grids and position systems, and statistical methods and deep learning algorithms have primarily been applied to mitigate this problem [136]. In [141], an analytical method based on no previous knowledge of attack was adapted to multiple and simultaneous cyber-attacks. Alromilh *et al.* [134] proposed a randomized watermarking filtering method to ensure data security in transmission layer and save as up to 85% more energy than Cui *et al.* [142]. In addition, an online robust PCA-based algorithm was proposed to reconstruct the original data when the corruption rate is no more than 20% [136].

Industrial control systems (ICS) are the major attack target of control system intrusions, which have strong impacts on these systems' transmission layer and application layer. Modbus/TCP oriented attack is a major type of control system intrusion. Ndona and Sadre [143] proposed a two-level intrusion detection system to efficient against Modbus/TCP oriented attacks with a small impact on communication latency. In [144], a new intrusion detection algorithm based on one-class SVM was presented with advantages of fast and strong generalization ability, less support vector, simple mode, and great practical value. Moreover, A stereo depth intrusion detection system with a low rate of false positive (not exceed 0.045%) was proposed [145]. With the development of smart agriculture, agricultural production will be the novel attack target, and above intrusion detection algorithms will contribute to the security of the agricultural control system.

In summary, analyzing types of attacks for different smart agriculture researches and security strategies suitable for various agricultural scenarios is critical to ensuring the security of smart agriculture.

VI. Future trends and security issues

The following issues may be the future research trends of smart agriculture, and they may result in novel security challenges. We briefly describe the concepts below.

A. *Fifth generation communication (5G)*

5G is the next generation wireless communication technology with characteristics of high-frequency electromagnetic wave and low latency. Compared with the existing wireless communication technology, 5G provides faster data transmission speed and larger data throughput, which support the device communication, AI algorithm deployed in user end, distributed fault diagnosis method, and complex security strategy. However, 5G is also vulnerable to security threats, e.g., interception of node communication. In addition, the security defined in the 3rd Generation Partnership Project (3GPP) focuses on resistance to network attacks, authenticity, integrity, and confidentiality. However, some emerging cryptographic techniques, e.g., public key infrastructure, anonymization, security mechanisms of IPsec, and differential privacy, etc., can be considered for achieving security and privacy requirements. To design efficient and secure privacy-preserving schemes using these techniques for 5G-enabled smart agriculture networks, the following critical challenges need to be solved:

- How to protect the confidentiality of transmitted data between network entities?
- How to authenticate the source of the received data?
- How to protect the integrity of transmitted data between different network entities?
- How to detect and prevent attacks (e.g., falsification of multiple identities and replays data between network entities)?

A possible research direction in this topic could be related to developing an efficient secure and privacy-preserving scheme for 5G-enabled smart agriculture networks. For instance, the physical-layer threats in UAVs' communication based on 5G was discussed in [148].

B. *Fog computing (FC) and Internet of Everything (IoE)*

FC is a computing paradigm that reduces communication delays by moving the cloud computing facilities and services to the access network. Since the FC is designed upon traditional networking components, it is highly vulnerable to security attacks (e.g., wiretapping, tampering, loss of information,

TABLE XI
SUMMARY OF RECENT WORKS RELATED TO INFORMATION SECURITY

Security issue	**Reference**	**Model**	**Affected layer**	**Performance**	**Object**
Unauthorized access	Rumyantsev *et al.* [146]	A two-pass auto-compensation fiber-optic quantum key distribution system	Transmission layer	Improve the effectiveness of the preliminary stage synchronization algorithm QKDS by eliminating false solutions	Fiber-optic communication
	Joe *et al.* [128]	Two novel authentication mechanisms based on Multi kernel Fuzzy C-Means and group search optimizer algorithms	Application layer	Two authentication procedures are more effective than password, privacy, e-mail authentication	Authentication algorithms in Online Social Network platform
	Fukami *et al.* [129]	An authentication system based on steady state visual evoked potential and principal component analysis	Application layer	Lowest false rejection rate of 5% with four PCA dimensions 9% equal error rate considering unregistered individuals	Authentication system based on electroencephalography evoked by sensory stimuli
	Kim *et al.* [138]	SVM, C4.5, KNN, and MLP applied in unauthorized access point dataset created by round trip time	Transmission layer	KNN and C4.5 have the most accurate (%92.9)in True Positive value KNN is the closest to ROC curve compared with SVM, C4.5 and MLP	Wireless access point
Interception of node communication	Milošević *et al.* [130]	New close-form expressions for the intercept probability of decode-and-forward relaying system	Physical layer	The increasing signal power at the source/relay enhance	Wireless communication over Nakagami-m faded environment system performance up
	Zou and Wang [131]	An optimal sensor scheduling method for wireless communication against eavesdropping attack	Physical layer	The proposed scheme outperforms the conventional round-robin scheduling in terms of the intercept probability	Industrial WSN sensor schedule
	Jameel *et al.* [132]	A system based on two-way decode-and-forward relay assisting transmission	Physical layer	Increasing power-splitting factor from 0.1 to 0.7 causes the intercept probability to increase from 0.48 to 0.80	Energy harvesting relays
	Ding *et al.* [139]	A so-called secrecy maximization oriented relay selection method (SMORS)	Physical layer	SMORS scheme outperforms the traditional max-min relay selection scheme in intercept probability Increasing the number of relays can improve the physical-layer security of wireless transmissions based on SMORS	Cooperative relay network consisting of a source, a destination, and multiple decode- and-forward (DF) relays
Facility damage	Mohamed *et al.* [140]	SMASheD framework under Android ecosystem	Perception layer	Consumes few resources, utilizes various channels to send the extracted data to the malware owner, wipes out all attack traces with touch injects	Android¡¯s sensor security model
	Milošević *et al.* [133]	An actuator security index and a method for computing the index in small-scale systems	Perception layer	Actuator security can be increased by placing additional sensors Proposed index can characterize actuators vulnerable in any realization	Actuator security
Malicious data attacks	Bretas *et al.* [141]	An analytical method for smart grids cyber-physical security	Physical layer	Highlight the improved accuracy under multiple and simultaneous cyber-attacks A previous knowledge of attack is not required	Smart grids cyber-physical security
	Che *et al.* [135]	A cybersecured corrective dispatch method (CSCD)	Perception layer	Mitigate the physical overloads and under an assumed risk level of cyber-overloads attack	Operator¯s security-constrained economic dispatch
	Alromih *et al.* [134]	A randomized watermarking filtering method (RWFS)	Transmission layer	RWFS can save as up to 85% more energy than Cui *et al.* [142] Network lifetime of RWFS is almost twice as that of Cui *et al.* [142]	IoT applications
	Mahapatra *et al.* [136]	An online robust principal component analysis-based algorithm	Application layer	Reconstruct the original data from the corrupted signal when corruption is present in 20% of the total number of signals at any instant	Wide-area mode metering application
Control system intrusion	Ndonda and Sadre [143]	A two-level intrusion detection system for industrial control systems (ICS) networks	Transmission layer	Only a small impact on communication latency in the ICS Efficient against Modbus/TCP oriented attacks	Industrial Control Systems
	Shang *et al.* [144]	A new intrusion detection algorithm based on one-class support vector machine	Application layer	Fast and strong generalization ability, less support vector, simple mode, and great practical value	Industrial Control Systems
	Wang *et al.* [145]	A stereo depth intrusion detection system based on rule extraction and deep inspection	Transmission layer	A low rate of false positive (not exceed 0.045%) and false negative	Modbus over TCP/IP protocol
	Teng *et al.* [147]	An adaptive collaboration intrusion detection method	Application layer	Higher accuracy (89.02%), lower error (12.19%) and less training time (7.247s) compared with SingleType-Support Vector Machine	KDD CUP 1999 data set

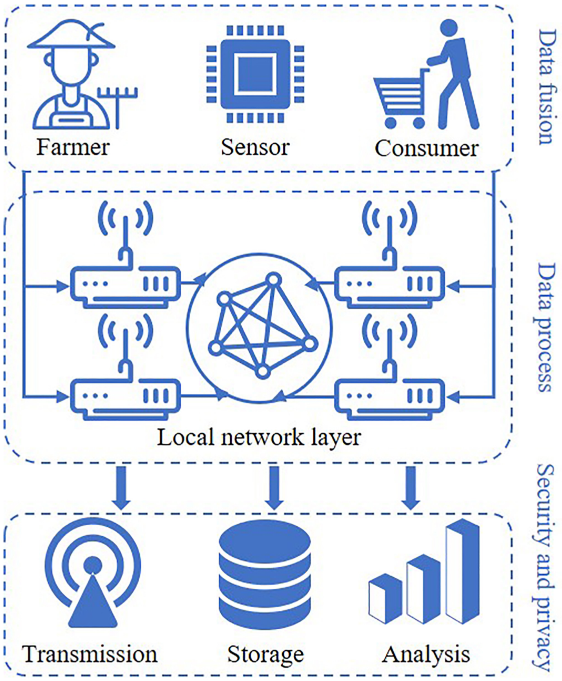


Fig. 18. The novel mode of agricultural production by FoE architecture.

and Trojan horses) [149]. IoT mainly focuses on machine-to-machine sensor-based smart facility communication, as well as IoE aims at providing services to people by IoT. Due to the resource-limited sensors and bandwidth-limited wireless communication, the Fog of Everything (FoE) was proposed in [150] to set up a complexity system. It will contribute to SIL-IoT and photovoltaic agricultural IoT which have multi-tasking requirements (i.e., operating, monitoring, and scheduling).

In addition, data of farmers, consumers and sensors are fused by FoE, and part of processing modules of agricultural information, agricultural products trading and other data can be deployed in the local network layer, as shown in Fig. 18. With the application of new generation of communication technology, e.g., 5G, FoE can meet more intelligent agricultural production demands, and improve the security of existing smart agriculture applications. Simultaneously, in the process of data fusion, transmission, storage and analysis, new security issues will inevitably arise due to the application of novel computing paradigm and information carrier, especially cyber security at the edge.

C. Renewable Energy Management System (Renewable EMS)

With the aggravation of the global energy crisis, considerable attention has been paid to the study of integrating and using high penetration of renewable energy in past decades [151]. Renewable energy has been widely applied in various domains, and agriculture is one of the most potential application scenarios. Energy management plays a vital role in smart multi-microgrids for agriculture (e.g., energy management of photovoltaic agricultural IoT), and it can ensure the energy supply of sensors deployed outdoors with the combination of wireless charging technology.

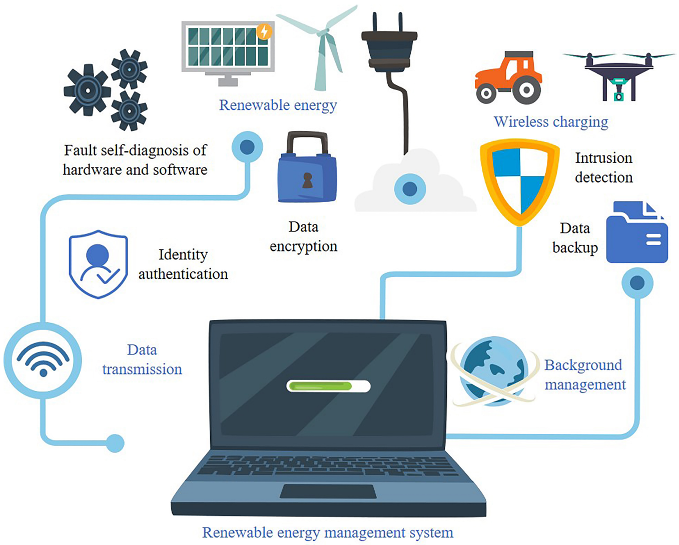


Fig. 19. The security scheme of renewable EMS, including 1) fault self-diagnosis of hardware and software in agricultural facilities and renewable energy equipment, 2) identity authentication and data encryption in data transmission layer, 3) intrusion detection and data backup in background management.

At present, the security scheme of renewable EMS usually includes fault self-diagnosis of hardware and software, identity authentication, data encryption, intrusion detection, and data backup, as shown in Fig. 19. Because agricultural facilities are mainly deployed in outdoor environment, fault self-diagnosis of hardware and software is very important to ensure the security scheme. In addition, blockchain technology may contribute to the security of renewable energy management system.

D. Software Defined Network (SDN)

Software defined network is characterized as a centrally-control network. With user-defined virtualization and programming, the relaying and controlling are performed separately, which can provide flexibility and reliability to the network management [152]. In recent years, SDN has been a hot subject, especially multi-domain SDN that controls large-scale networks, i.e., precision agriculture [153]. Moreover, It can effectively simplify the network, and manage heterogeneous network equipment. The SDN controller can monitor the security situation of whole network in real-time.

However, centralizing the network control plane and enabling network programmability are the emphases of hacking, and may lead to new security challenges, controllers¡¯ safety from applications, controller¡¯s scalability and availability, resilience and placement, etc. [154]. For instance, a plant phenotype information system integrates multiple data sources, and SDN architecture can improve its performance and security, but new security threats are an urgent problem. As shown in Fig. 20, if hackers attack the SDN controller, it will transmit wrong control instructions, which results in abnormal data flow and affects the trust between the SDN controller and the plant phenotype information system applications.

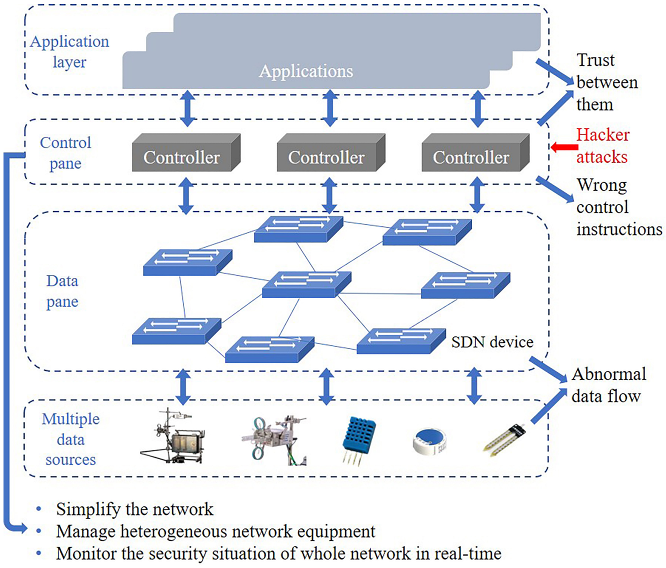


Fig. 20. A plant phenotype information system based on SDN architecture (including multiple data sources, control pane, data pane, and application layer) and security issues (trust between applications and controller, wrong control instructions, and abnormal data flow) result from hacker attacks.

E. Virtual reality (VR) and augmented reality (AR)

VR is a simulated experience that can be similar to or completely different from the real world. AR is the technology of superimposing virtual objects upon the real world [155]. Although VR has been widely applied as an educational method in industry, there are a few researches about VR in agriculture domain. For instance, Kim *et al.* developed an educational simulator by VR technology for a better farmer education compared with two-dimensional screens [156]. Besides, a VR simulator that contributes to technical training of maintenance of agricultural machinery was developed [157]. Huuskonen *et al.* designed a wearable AR equipment to aid and guide the farmer to collect soil samples [158]. Both VR and AR technologies contribute to the automation and intelligence of agriculture. For instance, farmers can remotely and precisely control agricultural robots through VR and AR equipment in the control center. In addition, farmers can study the fault diagnosis and security countermeasures by VR educational simulator, which contribute to the improvement of security-conscious and prevention skills of farmers.

However, both VR and AR technologies are vulnerable to various types of attacks, which have an impact on reliability of systems as they are designed to replace our perception of the physical world (e.g., tracking attacks) [159].

F. Cyber security datasets for smart agriculture

When proposing intrusion detection systems, it is struggling to find comprehensive and valid cyber security datasets to test and evaluate the performance of cyber security intrusion detection. The study in [160] reviewed the most cyber security datasets used in deep learning approaches for cyber security intrusion detection such as NSL-KDD dataset, KDD Cup 1999 dataset, and UNSW-NB15 dataset. These datasets are not simulated for smart agriculture environments. Therefore, the development of a new dataset to build a network intrusion detector under a smart agriculture environment is one of the significant research challenges. In addition, we believe that a comparative study of machine learning approaches for cyber security intrusion detection is needed for smart agriculture environments.

G. Summary

The integration of the above issues and agriculture provides the opportunity to promote intelligent and automatic agriculture. In addition, faster data transmission speed (5G), lower communication cost and latency (FC), lower energy consumption (renewable energy management system), separate relaying and controlling (SDN), simulation environment (VR and AR), and datasets for evaluating model (Cyber security datasets for smart agriculture) contribute to the development of smart agriculture, as shown in Fig. 21. However, the above issues are confronted with more severe security challenges because security threats of them have not been fully explored. When the above issues are widely used in smart agriculture, there will be a quantity of security problems. And these problems may lead to serious consequences, e.g., tracking attacks to VR equipment will result in improper positioning and harm to users.

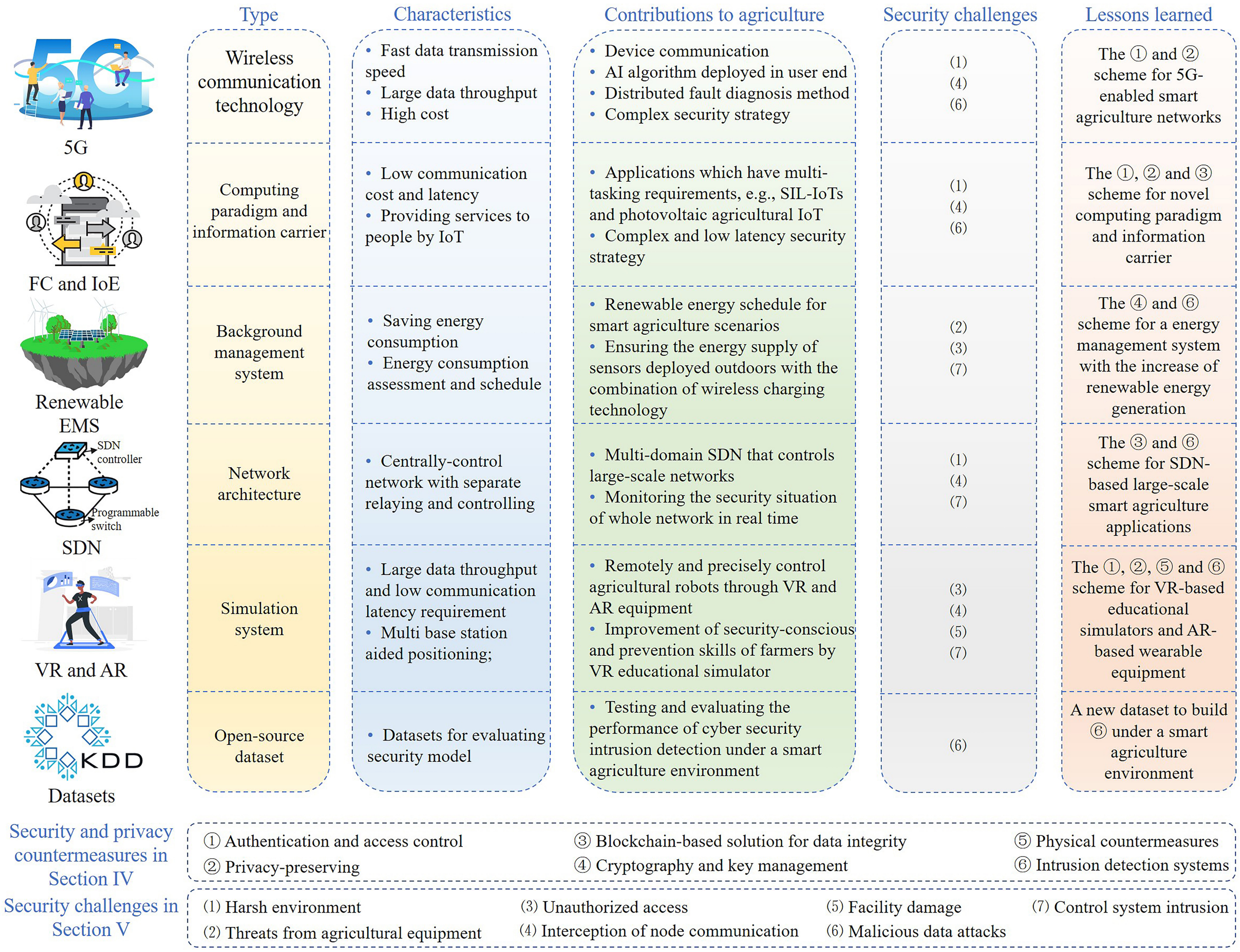
Therefore, secure and privacy-preserving schemes play a vital role in reliability of smart agriculture. Researches on the existing security and privacy countermeasures in the above issues can prevent security threats of them in smart agriculture. For instance, the authentication and access control and privacy-preserving scheme for 5G-enabled smart agriculture networks is required with the rapid development of smart agriculture. To ensure the security of 5G in agriculture, the researches on existing security and privacy countermeasures, and specific strategies will become hot issues in this field and promote the development of smart agriculture.

From the above sections, it is suggested that:

- Expanding and improving the existing security and privacy countermeasures in smart agriculture (most of them are in the theoretical stage, and few actual cases).
- Analyzing the characteristics and challenges of security issues in smart agriculture scenarios, and applying the existing security and privacy countermeasures mainly for industrial scenarios to smart agriculture scenarios (industrial scenarios are widely used, but the characteristics of agricultural production are not taken into consideration).
- Following the development of novel technologies, applying them to smart agriculture scenarios, and highlighting the new security issues brought by them simultaneously.

VII. Conclusion

With rapidly advancing modern technology, smart agriculture, which is a combination of agriculture and information technology, is becoming a trend of agricultural development. However, information technology also entails various security challenges. This paper surveys the state-of-the-art works related to smart agriculture and discusses the security challenges


5G
SDN controller
Programmable switch
KDD

	Type	Characteristics	Contributions to agriculture	Security challenges	Lessons learned
5G	Wireless communication technology	• Fast data transmission speed • Large data throughput • High cost	• Device communication • AI algorithm deployed in user end • Distributed fault diagnosis method • Complex security strategy	(1) (4) (6)	The ① and ② scheme for 5G-enabled smart agriculture networks
FC and IoE	Computing paradigm and information carrier	• Low communication cost and latency • Providing services to people by IoT	• Applications which have multi-tasking requirements, e.g., SIL-IoTs and photovoltaic agricultural IoT • Complex and low latency security strategy	(1) (4) (6)	The ①, ② and ③ scheme for novel computing paradigm and information carrier
Renewable EMS	Background management system	• Saving energy consumption • Energy consumption assessment and schedule	• Renewable energy schedule for smart agriculture scenarios • Ensuring the energy supply of sensors deployed outdoors with the combination of wireless charging technology	(2) (3) (7)	The ④ and ⑥ scheme for a energy management system with the increase of renewable energy generation
SDN	Network architecture	• Centrally-control network with separate relaying and controlling	• Multi-domain SDN that controls large-scale networks • Monitoring the security situation of whole network in real time	(1) (4) (7)	The ③ and ⑥ scheme for SDN-based large-scale smart agriculture applications
VR and AR	Simulation system	• Large data throughput and low communication latency requirement • Multi base station aided positioning;	• Remotely and precisely control agricultural robots through VR and AR equipment • Improvement of security-conscious and prevention skills of farmers by VR educational simulator	(3) (4) (5) (7)	The ①, ②, ⑤ and ⑥ scheme for VR-based educational simulators and AR-based wearable equipment
Datasets	Open-source dataset	• Datasets for evaluating security model	• Testing and evaluating the performance of cyber security intrusion detection under a smart agriculture environment	(6)	A new dataset to build ⑥ under a smart agriculture environment

Security and privacy countermeasures in Section IV

① Authentication and access control
② Privacy-preserving
③ Blockchain-based solution for data integrity
④ Cryptography and key management
⑤ Physical countermeasures
⑥ Intrusion detection systems

Security challenges in Section V

(1) Harsh environment
(2) Threats from agricultural equipment
(3) Unauthorized access
(4) Interception of node communication
(5) Facility damage
(6) Malicious data attacks
(7) Control system intrusion

Fig. 21. Future research trends, security challenges, and lessons learned about smart agriculture.

of smart agriculture. We introduce three smart agriculture development modes (precision agriculture, facility agriculture, and order agriculture), and investigate 7 key technologies and 11 key applications of smart agriculture. It is followed by a summary of security and privacy countermeasures for smart agriculture. Authentication and access control, privacy-preserving, blockchain-based solutions for data integrity, cryptography and key management, physical countermeasures, and intrusion detection systems are introduced and discussed in detail. Then, we discuss the security challenges in agricultural production and information technology. In addition, we did some experiments based on SIL-IoT, and the results indicate that the interference of high voltage pulse discharge has an impact on data transmission and data acquisition. Moreover, we present six issues which may be the future research trends of smart agriculture and introduce the novel security challenges.

References

[1] L. Ma, H. Long, Y. Zhang, S. Tu, D. Ge, and X. Tu, "Agricultural labor changes and agricultural economic development in China and their implications for rural vitalization," *J. Geogr. Sci.*, vol. 29, no. 2, pp. 163–179, 2019.

[2] Y. Liu, X. Ma, L. Shu, G. P. Hancke, and A. M. Abu-Mahfouz, "From industry 4.0 to agriculture 4.0: current status, enabling technologies, and research challenges," *IEEE Trans. Ind. Informat.*, 2020. [Online]. Available: DOI: 10.1109/TII.2020.3003910

[3] M. S. Mekala and P. Viswanathan, "A survey: smart agriculture IoT with cloud computing," in *Prof. Int. Conf. Microelectronic Devices, Circuits and Systems*. Vellore, India: IEEE, 2017, pp. 1–7.

[4] N. Gondchawar and R. Kawitkar, "IoT based smart agriculture," *Int. J. Adv. Res. Comput. Commun. Eng.*, vol. 5, no. 6, pp. 838–842, 2016.

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

[6] P. P. Ray, "Internet of things for smart agriculture: Technologies, practices and future direction," *J. Ambient Intell. Smart Environ.*, vol. 9, no. 4, pp. 395–420, 2017.

[7] O. Elijah, T. A. Rahman, I. Orikumhi, C. Y. Leow, and M. N. Hindia, "An overview of Internet of Things (IoT) and data analytics in agriculture: benefits and challenges," *IEEE Internet Things J.*, vol. 5, no. 5, pp. 3758–3773, 2018.

[8] A. Khanna and S. Kaur, "Evolution of Internet of Things (IoT) and its significant impact in the field of precision agriculture," *Comput. Electron. Agric.*, vol. 157, pp. 218–231, 2019.

[9] M. Bacco, P. Barsocchi, E. Ferro, A. Gotta, and M. Ruggeri, "The digitisation of agriculture: a survey of research activities on smart farming," *Array*, vol. 3, p. 100009, 2019.

[10] S. Wolfert, L. Ge, C. Verdouw, and M.-J. Bogaardt, "Big data in smart farming–a review," *Agric. Syst.*, vol. 153, pp. 69–80, 2017.

[11] M. Bacco, A. Berton, E. Ferro, C. Gennaro, A. Gotta, S. Matteoli, F. Paonessa, M. Ruggeri, G. Virone, and A. Zanella, "Smart farming:

opportunities, challenges and technology enablers," in *Proc. IoT Vertical and Topical Summit on Agriculture*. Tuscany, Italy: IEEE, 2018, pp. 1–6.

[12] C. Makate, "Effective scaling of climate smart agriculture innovations in african smallholder agriculture: a review of approaches, policy and institutional strategy needs," *Environ. Sci. Policy*, vol. 96, pp. 37–51, 2019.

[13] E. Totin, A. C. Segnon, M. Schut, H. D. Affognon, R. B. Zougmore, T. S. Rosenstock, and P. K. Thornton, "Institutional perspectives of climate-smart agriculture: a systematic literature review," *Sustain.*, vol. 10, no. 6, p. 1990, 2018.

[14] M. Ayaz, M. Ammaduddin, Z. Sharif, A. Mansour, and E. M. Aggoune, "Internet-of-things IoT-based smart agriculture: toward making the fields talk," *IEEE Access*, vol. 7, pp. 129 551–129 583, 2019.

[15] M. A. Ferrag, L. Shu, X. Yang, A. Derhab, and L. Maglaras, "Security and privacy for green IoT-based agriculture: review, blockchain solutions, and challenges," *IEEE Access*, vol. 8, pp. 32 031–32 053, 2020.

[16] 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.

[17] L. Barreto and A. Amaral, "Smart farming: cyber security challenges," in *Proc. Int. Conf. Intelligent Systems*. Madeira, Portugal: IEEE, 2018, pp. 870–876.

[18] J. West, "A prediction model framework for cyber-attacks to precision agriculture technologies," *J. Agric. Food Inf.*, vol. 19, no. 4, pp. 307–330, 2018.

[19] H. Khalid, U. D. Ikram, A. Ahmad, and I. Naveed, "An energy efficient and secure IoT-based wsn framework: an application to smart agriculture," *Sensors*, vol. 20, no. 7, p. 2081, 2020.

[20] M. S. Farooq, S. Riaz, A. Abid, K. Abid, and M. A. Naeem, "A survey on the role of IoT in agriculture for the implementation of smart farming," *IEEE Access*, vol. 7, pp. 156 237–156 271, 2019.

[21] O. Koksal and B. Tekinerdogan, "Architecture design approach for IoT-based farm management information systems," *Precis. Agric.*, vol. 20, no. 5, pp. 926–958, 2019.

[22] T. Malche, P. Maheshwary, and R. Kumar, "Environmental monitoring system for smart city based on secure Internet of Things (IoT) architecture," *Wirel. Pers. Commun.*, vol. 107, no. 4, pp. 2143–2172, 2019.

[23] M. S. Munir, I. S. Bajwa, and S. M. Cheema, "An intelligent and secure smart watering system using fuzzy logic and blockchain," *Comput. Electr. Eng.*, vol. 77, pp. 109–119, 2019.

[24] E. C. Ferrer, "The blockchain: a new framework for robotic swarm systems," in *Proc. Future Technologies Conf.* Cham: Springer, 2017, pp. 1037–1058.

[25] H. Kai, L. Kailiang, S. Lei, and Y. Xing, "Demo abstract: high voltage discharge exhibits severe effect on ZigBee-based device in solar insecticidal lamps internet of things," in *IEEE Int. Conf. Computer Communications*. Virtual conference: IEEE, 2020.

[26] K. Huang, K. Li, L. Shu, X. Yang, T. Gordon, and X. Wang, "High voltage discharge exhibits severe effect on ZigBee-based device in solar insecticidal lamps internet of things," *IEEE Wireless Commun.*, pp. 1–6, 2020. [Online]. Available: 10.1109/MWC.001.2000082

[27] N. Zhang, M. Wang, and N. Wang, "Precision agriculture—a worldwide overview," *Comput. Electron. Agric.*, vol. 36, no. 36, pp. 113–132, 2002.

[28] L. Zhou, L. Song, C. Xie, and J. Zhang, "Applications of Internet of Things in the facility agriculture," in *Computer and Computing Technologies in Agriculture VI*. Berlin, Heidelberg: Springer, 2012, pp. 297–303.

[29] M. F. Bellemare and J. R. Bloem, "Does contract farming improve welfare? a review," *World Dev.*, vol. 112, pp. 259–271, 2018.

[30] M. Srbinovska, C. Gavrovski, V. Dimcev, A. Krkoleva, and V. Borozan, "Environmental parameters monitoring in precision agriculture using wireless sensor networks," *J. Clean. Prod.*, vol. 88, pp. 297–307, 2015.

[31] D. D. Wu, D. L. Olson, and J. R. Birge, "Risk management in cleaner production," *J. Clean. Prod.*, vol. 53, pp. 1–6, 2013.

[32] V. V. hari Ram, H. Vishal, S. Dhanalakshmi, and P. M. Vidya, "Regulation of water in agriculture field using internet of things," in *Proc. IEEE Technological Innovation in ICT for Agriculture and Rural Development*. Chennai, India: IEEE, 2015, pp. 112–115.

[33] Y. Lin, J. R. Petway, J. Anthony, H. Mukhtar, S. Liao, C. Chou, and Y. Ho, "Blockchain: the evolutionary next step for ict e-agriculture," *Environ.*, vol. 4, no. 3, p. 50, 2017.

[34] D. Dalohoun, A. Hall, and P. Van Mele, "Entrepreneurship as driver of a "self- organizing system of innovation": the case of nerica in benin," *Int. J. Technol. Manag. Sustain. Dev.*, vol. 8, no. 2, pp. 87–101, 2009.

[35] M. P. Caro, M. S. Ali, M. Vecchio, and R. Giaffreda, "Blockchain-based traceability in agri-food supply chain management: a practical implementation," in *Proc. IoT Vertical and Topical Summit on Agriculture*. Tuscany, Italy: IEEE, 2018, pp. 1–4.

[36] K. Leng, Y. Bi, L. Jing, H. Fu, and I. Van Nieuwenhuyse, "Research on agricultural supply chain system with double chain architecture based on blockchain technology," *Future Gener. Comput. Syst.*, vol. 86, pp. 641–649, 2018.

[37] J. Hua, X. Wang, M. Kang, H. Wang, and F.-Y. Wang, "Blockchain based provenance for agricultural products: a distributed platform with duplicated and shared bookkeeping," in *Proc. IEEE Intelligent Vehicles Symp.* Changshu, China: IEEE, 2018, pp. 97–101.

[38] A. Villahenriksen, G. T. C. Edwards, L. Pesonen, O. Green, and C. G. Sorensen, "Internet of things in arable farming: implementation, applications, challenges and potential," *Biosyst. Eng.*, vol. 191, pp. 60–84, 2020.

[39] S. Wang, Y. Lin, Y. Qin, and C. Chen, "Security enhancement of internet of things using service level agreements and lightweight security," in *Advances in Information and Communication Networks*. Springer, 2018, pp. 221–235.

[40] A. Tzounis, N. Katsoulas, T. Bartzanas, and C. Kittas, "Internet of things in agriculture, recent advances and future challenges," *Biosyst. Eng.*, vol. 164, pp. 31–48, 2017.

[41] J. P. S. Sundaram, W. Du, and Z. Zhao, "A survey on lora networking: Research problems, current solutions, and open issues," *IEEE Commun. Surveys Tuts.*, vol. 22, no. 1, pp. 371–388, 2019.

[42] Z. Zong, R. Fares, B. Romoser, and J. Wood, "Faststor: improving the performance of a large scale hybrid storage system via caching and prefetching," *Cluster Comput.*, vol. 17, no. 2, pp. 593–604, 2014.

[43] L. Xiufeng, C. Shouhe, and G. Leifeng, "Technological innovation of agricultural information service in the age of big data," *J. Agric. Sci. Technol.*, vol. 16, no. 4, pp. 10–15, 2014.

[44] D. Ko, Y. Kwak, and S. Song, "Real time traceability and monitoring system for agricultural products based on wireless sensor network," *Int. J. Distrib. Sens. Netw.*, vol. 10, no. 6, p. 832510, 2014.

[45] S. Kang, X. Hao, T. Du, L. Tong, X. Su, H. Lu, X. Li, Z. Huo, S. Li, and R. Ding, "Improving agricultural water productivity to ensure food security in China under changing environment: from research to practice," *Agric. Water Manag.*, vol. 179, pp. 5–17, 2017.

[46] J. Muangprathub, N. Boonnam, S. Kajornkasirat, N. Lekbangpong, A. Wanichsombat, and P. Nillaor, "IoT and agriculture data analysis for smart farm," *Comput. Electron. Agric.*, vol. 156, pp. 467–474, 2019.

[47] P. Edwards, W. Zhang, B. Belton, and D. C. Little, "Misunderstandings, myths and mantras in aquaculture: its contribution to world food supplies has been systematically over reported," *Mar. Policy*, vol. 106, p. 103547, 2019.

[48] A. J. Embug, A. A. A. Ibrahim, M. Hamzah, and M. F. Asli, "A review on visual water quality monitoring system in precision aquaculture," in *Appl. Mech. Mater.*, vol. 892. Trans Tech Publ, 2019, pp. 23–30.

[49] J. Trevathan and R. Johnstone, "Smart environmental monitoring and assessment technologies (semat) - a new paradigm for low-cost, remote aquatic environmental monitoring," *Sensors*, vol. 18, no. 7, p. 2248, 2018.

[50] C. Dupont, P. Cousin, and S. Dupont, "IoT for aquaculture 4.0 smart and easy-to-deploy real-time water monitoring with IoT," in *Proc. Global Internet of Things Summit*. Bilbao, Spain: IEEE, 2018, pp. 1–5.

[51] F. Li, Q. Liu, S. Dong, and H. Cheng, "Agricultural development status and key cooperation directions between China and countries along "the belt and road"," in *Proc. IOP Conf. Series: Earth and Environmental Science*, vol. 190, no. 1. Irkutsk, Russia: IOP Publishing, 2018, p. 012058.

[52] M. Ariff and I. Ismail, "Rfid application development for a livestock monitoring system," in *Bioresources Technology in Sustainable Agriculture*. Apple Academic Press, 2018, pp. 81–94.

[53] I. Halachmi, M. Guarino, J. Bewley, and M. Pastell, "Smart animal agriculture: application of real-time sensors to improve animal well-being and production," *Annu. Rev. Anim. Biosci.*, vol. 7, pp. 403–425, 2019.

[54] X. Shi, X. An, Q. Zhao, H. Liu, L. Xia, X. Sun, and Y. Guo, "State-of-the-art internet of things in protected agriculture," *Sensors*, vol. 19, no. 8, p. 1833, 2019.

[55] M. Kang, X.-R. Fan, J. Hua, H. Wang, X. Wang, and F.-Y. Wang, "Managing traditional solar greenhouse with cpss: a just-for-fit philosophy," *IEEE Trans. Syst., Man, Cybern.*, vol. 48, no. 12, pp. 3371–3380, 2018.

[56] M. A. Akkas and R. Sokullu, "An IoT-based greenhouse monitoring system with micaz motes," *Procedia Comput. Sci.*, vol. 113, pp. 603–608, 2017.

[57] T. Kozai, "Resource use efficiency of closed plant production system with artificial light: concept, estimation and application to plant factory," *Proc. Japan Academy, Series B*, vol. 89, no. 10, pp. 447–461, 2013.

[58] W. Hu, C. Lin, C. Yang, and M. Hwang, "A framework of the intelligent plant factory system," *Procedia Comput. Sci.*, vol. 131, pp. 579–584, 2018.

[59] F. Ijaz, A. A. Siddiqui, B. K. Im, and C. Lee, "Remote management and control system for led based plant factory using ZigBee and internet," in *Proc. 14th Int. Conf. Advanced Communication Technology*. PyeongChang, South Korea: IEEE, 2012, pp. 942–946.

[60] R. R Shamshiri, F. Kalantari, K. C. Ting, K. R. Thorp, I. A. Hameed, C. Weltzien, D. Ahmad, and Z. M. Shad, "Advances in greenhouse automation and controlled environment agriculture: A transition to plant factories and urban agriculture," *Int. J. Agric. Biol. Eng.*, vol. 11, no. 1, pp. 1–22, 2018.

[61] D. Gielen, F. Boshell, D. Saygin, M. D. Bazilian, N. Wagner, and R. Gorini, "The role of renewable energy in the global energy transformation," *Energy Strategy Rev.*, vol. 24, pp. 38–50, 2019.

[62] E. Kabir, P. Kumar, S. Kumar, A. A. Adelodun, and K.-H. Kim, "Solar energy: potential and future prospects," *Renew. Sust. Energ. Rev.*, vol. 82, pp. 894–900, 2018.

[63] N. M. Shatar, M. A. A. A. Rahman, S. A. Z. S. Salim, M. H. M. Ariff, M. N. Muhtazaruddin, and A. K. A. Badlisah, "Design of photovoltaic-thermoelectric generator (pv-teg) hybrid system for precision agriculture," in *Proc. IEEE 7th Int. Conf. Power and Energy*. Kuala Lumpur, Malaysia: IEEE, 2018, pp. 50–55.

[64] M. Bey, A. Hamidat, B. Benyoucef, and T. Nacer, "Viability study of the use of grid connected photovoltaic system in agriculture: case of algerian dairy farms," *Renew. Sust. Energ. Rev.*, vol. 63, pp. 333–345, 2016.

[65] N. M. Kumar, K. Atluri, and S. Palaparthi, "Internet of Things (IoT) in photovoltaic systems," in *Proc. National Power Engineering Conf.* Madurai, India: IEEE, 2018, pp. 1–4.

[66] F. M. Enescu, N. Bizon, A. Onu, M. S. Răboacă, P. Thounthong, A. G. Mazare, and G. Šerban, "Implementing blockchain technology in irrigation systems that integrate photovoltaic energy generation systems," *Sustain.*, vol. 12, no. 4, p. 1540, 2020.

[67] F. Yang, L. Shu, Y. Liu, K. Li, K. Huang, Y. Zhang, and Y. Sun, "Poster: photovoltaic agricultural internet of things the next generation of smart farming," in *Int. Conf. Embedded Wireless Systems and Networks*, 2019, pp. 236–237.

[68] K. Huang, L. Shu, K. Li, F. Yang, G. Han, X. Wang, and S. Pearson, "Photovoltaic agricultural internet of things towards realizing the next generation of smart farming," *IEEE Access*, 2020.

[69] K. Li, L. Shu, K. Huang, Y. Sun, F. Yang, Y. Zhang, Z. Huo, Y. Wang, X. Wang, Q. Lu *et al.*, "Research and prospect of solar insecticidal lamps internet of things," *Smart Agric.*, vol. 1, no. 3, p. 13, 2019, in Chinese with English Abstract.

[70] Y. Fan, S. Lei, H. Kai, L. Kailiang, H. Guangjie, and L. Ye, "A partition-based node deployment strategy in solar insecticidal lamps Internet of Things," *IEEE Internet Things J.*, vol. 7, no. 11, pp. 11 223–11 237, 2020.

[71] X. Yang, L. Shu, K. Huang, Z. Huo, Y. Wang, X. Wang, Q. Lu, and Y. Zhang, "Characteristics analysis and challenges for fault diagnosis in solar insecticidal lamps internet of things," *Smart Agric.*, vol. 2, no. 2, pp. 11–27, 2020, in Chinese with English Abstract.

[72] S. Li, A. L. Simonian, and B. A. Chin, "Sensors for agriculture and the food industry," *Electrochem. Soc. Interface*, vol. 19, no. 4, pp. 41–46, 2010.

[73] A. O. Onojeghuo, G. A. Blackburn, J. Huang, D. Kindred, and W. Huang, "Applications of satellite "hyper-sensing" in chinese agriculture: challenges and opportunities," *Int. J. Appl. Earth Obs. Geoinf.*, vol. 64, pp. 62–86, 2018.

[74] D. J. Mulla, "Twenty five years of remote sensing in precision agriculture: key advances and remaining knowledge gaps," *Biosyst. Eng.*, vol. 114, no. 4, pp. 358–371, 2013.

[75] Z. Chen, H. Pan, C. Liu, and Z. Jiang, "Chapter 7 - agricultural remote sensing and data science in China," in *Federal Data Science*, F. A. Batarseh and R. Yang, Eds. Academic Press, 2018, pp. 95–108. [Online]. Available: http://www.sciencedirect.com/science/article/pii/B9780128124437000077

[76] K. Ota, M. Dong, J. Gui, and A. Liu, "Quoin: incentive mechanisms for crowd sensing networks," *IEEE Netw.*, vol. 32, no. 2, pp. 114–119, 2018.

[77] Y. Sun, W. Ding, L. Shu, K. Huang, K. Li, Y. Zhang, and Z. Huo, "When mobile crowd sensing meets smart agriculture: poster," in *Proc. ACM Turing Celebration Conference*, 2019, pp. 1–2.

[78] A. Ginige and J. Sivagnanasundaram, "Enhancing agricultural sustainability through crowdsensing: a smart computing approach," *J. Adv. Agric. Technol. Vol*, vol. 6, no. 3, pp. 161–165, 2019.

[79] Y. Wang, X. Jia, Q. Jin, and J. Ma, "Mobile crowdsourcing: framework, challenges, and solutions," *Concurr. Comput.*, vol. 29, no. 3, p. e3789, 2017.

[80] L. Huning, J. Bauer, and N. Aschenbruck, "A privacy preserving mobile crowdsensing architecture for a smart farming application," in *Proc. First ACM Workshop on Mobile Crowdsensing Systems and Application*. Delft, Netherlands: ACM, 2017, pp. 62–67.

[81] D. Reynolds, J. Ball, A. Bauer, R. Davey, S. Griffiths, and J. Zhou, "Cropsight: a scalable and open-source information management system for distributed plant phenotyping and IoT-based crop management," *Gigascience*, vol. 8, no. 3, pp. giz009, 2019.

[82] A. Adamblondon, M. Alaux, C. Pommier, D. Cantu, Z. Cheng, G. R. Cramer, C. Davies, S. Delrot, L. Deluc, G. Di Gaspero *et al.*, "Towards an open grapevine information system," *Hort. Res.*, vol. 3, no. 1, pp. 1–8, 2016.

[83] R. Shrestha, L. Matteis, M. Skofic, A. Portugal, G. McLaren, G. Hyman, and E. Arnaud, "Bridging the phenotypic and genetic data useful for integrated breeding through a data annotation using the crop ontology developed by the crop communities of practice," *Front. Physiol.*, vol. 3, p. 326, 2012.

[84] Y.-F. Li, G. Kennedy, F. Ngoran, P. Wu, and J. Hunter, "An ontology-centric architecture for extensible scientific data management systems," *Future Gener. Comput. Syst.*, vol. 29, no. 2, pp. 641–653, 2013.

[85] M. W. Libbrecht and W. S. Noble, "Machine learning applications in genetics and genomics," *Nat. Rev. Genet.*, vol. 16, no. 6, pp. 321–332, 2015.

[86] P. J. Navarro, F. Pérez, J. Weiss, and M. Egeacortines, "Machine learning and computer vision system for phenotype data acquisition and analysis in plants," *Sensors*, vol. 16, no. 5, p. 641, 2016.

[87] J. R. Ubbens and I. Stavness, "Deep plant phenomics: a deep learning platform for complex plant phenotyping tasks," *Front. Plant Sci.*, vol. 8, p. 1190, 2017.

[88] X. Huang, D. Ye, R. Yu, and L. Shu, "Securing parked vehicle assisted fog computing with blockchain and optimal smart contract design," *IEEE/CAA J. Automat. Sinica*, vol. 7, no. 2, pp. 426–441, 2020.

[89] S. Roy, M. Ashaduzzaman, M. Hassan, and A. R. Chowdhury, "Blockchain for IoT security and management: current prospects, challenges and future directions," in *Proc. 5th Int. Conf. Networking, Systems and Security*. Dhaka, Banglades: IEEE, 2018, pp. 1–9.

[90] J. F. Galvez, J. Mejuto, and J. Simal-Gandara, "Future challenges on the use of blockchain for food traceability analysis," *Trends Analyt. Chem.*, vol. 107, pp. 222–232, 2018.

[91] J. Lin, Z. Shen, A. Zhang, and Y. Chai, "Blockchain and IoT based food traceability for smart agriculture," in *Proc. 3rd Int. Conf. Crowd Science and Engineering*. Singapore: ACM, 2018, pp. 1–6.

[92] O. Bermeo-Almeida, M. Cardenas-Rodriguez, T. Samaniego-Cobo, E. Ferruzola-Gómez, R. Cabezas-Cabezas, and W. Bazán-Vera, "Blockchain in agriculture: a systematic literature review," in *Technologies and Innovation*, Cham, 2018, pp. 44–56.

[93] Y. Cheng, K. Chen, H. Sun, Y. Zhang, and F. Tao, "Data and knowledge mining with big data towards smart production," *J. Ind. Inf. Integration*, vol. 9, pp. 1–13, 2018.

[94] M. G. Jonathan, "The need for fuzzy AI," *IEEE/CAA J. Automat. Sinica*, vol. 6, no. 3, pp. 610–622, 2019.

[95] K. Jha, A. Doshi, P. Patel, and M. Shah, "A comprehensive review on automation in agriculture using artificial intelligence," *Artif. Intell. Agric.*, vol. 2, pp. 1–12, 2019.

[96] M. Kang and F. Wang, "From parallel plants to smart plants: intelligent control and management for plant growth," *IEEE/CAA J. Automat. Sinica*, vol. 4, no. 2, pp. 161–166, 2017.

[97] E. Alreshidi, "Smart Sustainable Agriculture (SSA) solution underpinned by Internet of Things (IoT) and Artificial Intelligence (AI)," *Int. J. Adv. Comput. Sci. Appl.*, vol. 10, no. 5, 2019. [Online]. Available: http://dx.doi.org/10.14569/IJACSA.2019.0100513

[98] M. Ghahramani, M. Zhou, and C. T. Hon, "Toward cloud computing QoS architecture: analysis of cloud systems and cloud services," *IEEE/CAA J. Automat. Sinica*, vol. 4, no. 1, pp. 6–18, 2017.

[99] W. Shi, J. Cao, Q. Zhang, Y. Li, and L. Xu, "Edge computing: vision and challenges," *IEEE Internet Things J.*, vol. 3, no. 5, pp. 637–646, 2016.

[100] D. Fan and S. Gao, "The application of mobile edge computing in agricultural water monitoring system," in *Proc. 4th Int. Conf. Water Resource and Environment*, vol. 191, no. 1. Kaohsiung, Taiwan: IOP Publishing, 2018, p. 012015.

[101] K. Zhang, S. Leng, Y. He, S. Maharjan, and Y. Zhang, "Mobile edge computing and networking for green and low-latency internet of things," *IEEE Commun. Mag.*, vol. 56, no. 5, pp. 39–45, 2018.

[102] F. J. Ferrández-Pastor, J. M. García-Chamizo, M. Nieto-Hidalgo, and J. Mora-Martínez, "Precision agriculture design method using a distributed computing architecture on internet of things context," *Sensors*, vol. 18, no. 6, p. 1731, 2018.

[103] L. Wang, Y. Lan, Y. Zhang, H. Zhang, M. N. Tahir, S. Ou, X. Liu, and P. Chen, "Applications and prospects of agricultural unmanned aerial vehicle obstacle avoidance technology in China," *Sensors*, vol. 19, no. 3, p. 642, 2019.

[104] Y. Lan and S. Chen, "Current status and trends of plant protection uav and its spraying technology in China," *Int. J. Precis. Agric. Aviat.*, vol. 1, no. 1, pp. 1–9, 2018.

[105] S. Fountas, C. G. Sorensen, Z. Tsiropoulos, C. Cavalaris, V. Liakos, and T. Gemtos, "Farm machinery management information system," *Comput. Electron. Agric.*, vol. 110, pp. 131–138, 2015.

[106] A. S. Matveev, M. Hoy, J. Katupitiya, and A. V. Savkin, "Nonlinear sliding mode control of an unmanned agricultural tractor in the presence of sliding and control saturation," *Robot. Auton. Syst.*, vol. 61, no. 9, pp. 973–987, 2013.

[107] R. Bogue, "Robots poised to revolutionise agriculture," *Ind. Robot Int. J.*, vol. 43, no. 5, pp. 450–456, 2016.

[108] R. Keicher and H. Seufert, "Automatic guidance for agricultural vehicles in europe," *Comput. Electron. Agric.*, vol. 25, no. 1-2, pp. 169–194, 2000.

[109] J. F. Reid, Q. Zhang, N. Noguchi, and M. Dickson, "Agricultural automatic guidance research in north america," *Comput. Electron. Agric.*, vol. 25, no. 1-2, pp. 155–167, 2000.

[110] T. Liu, B. Tian, Y. Ai, and F. Wang, "Parallel reinforcement learning-based energy efficiency improvement for a cyber-physical system," *IEEE/CAA J. Automat. Sinica*, vol. 7, no. 2, pp. 1–10, 2020.

[111] H. Lee, D. Kang, J. Ryu, D. Won, H. Kim, and Y. Lee, "A three-factor anonymous user authentication scheme for internet of things environments," *J. Inf. Secur. Appl.*, vol. 52, p. 102494, 2020.

[112] A. Gauhar, N. Ahmad, Y. Cao, S. Khan, H. Cruickshank, E. A. Qazi, and A. Ali, "xdbauth: blockchain based cross domain authentication and authorization framework for internet of things," *IEEE Access*, vol. 8, pp. 58 800–58 816, 2020.

[113] S. Shin and T. Kwon, "A privacy-preserving authentication, authorization, and key agreement scheme for wireless sensor networks in 5g-integrated internet of things," *IEEE Access*, vol. 8, pp. 67 555–67 571, 2020.

[114] X. Wang, M. Umehira, B. Han, H. Zhou, P. Li, and C. Wu, "An efficient privacy preserving spectrum sharing framework for internet of things," *IEEE Access*, vol. 8, pp. 34 675–34 685, 2020.

[115] J. Wei, T. V. X. Phuong, and G. Yang, "An efficient privacy preserving message authentication scheme for internet-of-things," *IEEE Trans. Ind. Informat.*, 2020.

[116] J. Zhang, Y. Zhao, J. Wu, and B. Chen, "Lvpda: a lightweight and verifiable privacy-preserving data aggregation scheme for edge-enabled IoT," *IEEE Internet Things J.*, vol. 7, no. 5, pp. 4016–4027, 2020.

[117] M. A. Ferrag, L. Maglaras, A. Ahmim, M. Derdour, and H. Janicke, "Rdtids: rules and decision tree-based intrusion detection system for internet-of-things networks," *Future Internet*, vol. 12, no. 3, p. 44, 2020.

[118] L. Hang, I. Ullah, and D.-H. Kim, "A secure fish farm platform based on blockchain for agriculture data integrity," *Comput. Electron. Agric.*, vol. 170, p. 105251, 2020.

[119] A. Shahid, A. Almogren, N. Javaid, F. A. Al-Zahrani, M. Zuair, and M. Alam, "Blockchain-based agri-food supply chain: a complete solution," *IEEE Access*, vol. 8, pp. 69 230–69 243, 2020.

[120] E. Anthi, L. Williams, M. Słowińska, G. Theodorakopoulos, and P. Burnap, "A supervised intrusion detection system for smart home IoT devices," *IEEE Internet Things J.*, vol. 6, no. 5, pp. 9042–9053, 2019.

[121] F. Li, Y. Shi, A. Shinde, J. Ye, and W. Song, "Enhanced cyber-physical security in internet of things through energy auditing," *IEEE Internet Things J.*, vol. 6, no. 3, pp. 5224–5231, 2019.

[122] A. Ahmim, M. Derdour, and M. A. Ferrag, "An intrusion detection system based on combining probability predictions of a tree of classifiers," *Int. J. Commun. Systems*, vol. 31, no. 9, pp. e3547.1–e3547.17, 2018.

[123] C. Esposito, M. Ficco, A. Castiglione, F. Palmieri, and A. De Santis, "Distributed group key management for event notification confidentiality among sensors," *IEEE Trans. Dependable Secure Comput.*, vol. 17, no. 3, pp. 566–580, 2018.

[124] B. Ali and A. I. Awad, "Cyber and physical security vulnerability assessment for IoT-based smart homes," *Sensors*, vol. 18, no. 3, p. 817, 2018.

[125] M. Wazid, A. K. Das, V. Odelu, N. Kumar, M. Conti, and M. Jo, "Design of secure user authenticated key management protocol for generic IoT networks," *IEEE Internet Things J.*, vol. 5, no. 1, pp. 269–282, 2017.

[126] A. Sforzin, F. G. Mármol, M. Conti, and J.-M. Bohli, "Rpids: Raspberry pi ids—a fruitful intrusion detection system for IoT," in *Proc. Intl IEEE Conf. Ubiquitous Intelligence & Computing, Advanced and Trusted Computing, Scalable Computing and Communications, Cloud and Big Data Computing, Internet of People, and Smart World Congress*. Toulouse, France: IEEE, 2016, pp. 440–448.

[127] A. Ahmim, L. Maglaras, M. A. Ferrag, M. Derdour, and H. Janicke, "A novel hierarchical intrusion detection system based on decision tree and rules-based models," in *Proc. 15th Int. Conf. Distributed Computing in Sensor Systems*. Santorini Island, Greece: IEEE, 2019, pp. 228–233.

[128] M. M. Joe and B. Ramakrishnan, "Novel authentication procedures for preventing unauthorized access in social networks," *Peer Peer Netw. Appl.*, vol. 10, no. 4, pp. 833–843, 2017.

[129] T. Fukami, Y. Abe, T. Shimada, and B. Ishikawa, "Authentication system preventing unauthorized access of a third person based on steady state visual evoked potentials," *Int. J. Innov. Comput. Inf. Control.*, vol. 14, no. 6, pp. 2091–2100, 2018.

[130] N. D. Milošević, J. A. Anastasov, A. M. Cvetković, D. M. Milović, and D. N. Milić, "On the intercept probability of df relaying wireless communication," *Wirel. Pers. Commun.*, vol. 104, no. 4, pp. 1523–1533, 2019.

[131] Y. Zou and G. Wang, "Intercept behavior analysis of industrial wireless sensor networks in the presence of eavesdropping attack," *IEEE Trans. Ind. Informat.*, vol. 12, no. 2, pp. 780–787, 2015.

[132] F. Jameel, Z. Chang, and T. Ristaniemi, "Intercept probability analysis of wireless powered relay system in kappa-mu fading," in *Proc. IEEE 87th Vehicular Technology Conference*. Porto, Portugal: IEEE, 2018, pp. 1–6.

[133] J. Milošević, A. Teixeira, K. H. Johansson, and H. Sandberg, "Actuator security indices based on perfect undetectability: computation, robustness, and sensor placement," *IEEE Trans. Automat. Contr.*, pp. 3816–3831, 2020.

[134] A. Alromih, M. Alrodhaan, and Y. Tian, "A randomized watermarking technique for detecting malicious data injection attacks in heterogeneous wireless sensor networks for internet of things applications," *Sensors*, vol. 18, no. 12, p. 4346, 2018.

[135] L. Che, X. Liu, and Z. Li, "Mitigating false data attacks induced overloads using a corrective dispatch scheme," *IEEE Trans. Smart Grid*, vol. 10, no. 3, pp. 3081–3091, 2018.

[136] K. Mahapatra and N. R. Chaudhuri, "Online robust pca for malicious attack-resilience in wide-area mode metering application," *IEEE Trans. Power Syst.*, vol. 34, no. 4, pp. 2598–2610, 2019.

[137] A. W. Aldabbagh, Y. Li, and T. Chen, "An intrusion detection system for cyber attacks in wireless networked control systems," *IEEE Trans. Circuits Syst. II*, vol. 65, no. 8, pp. 1049–1053, 2017.

[138] D. Kim, D. Shin, and D. Shin, "Unauthorized access point detection using machine learning algorithms for information protection," in *Proc. 17th IEEE Int. Conf. Trust, Security And Privacy In Computing And Communications/ 12th IEEE Int. Conf. Big Data Science And Engineering*, 2018, pp. 1876–1878.

[139] X. Ding, T. Song, Y. Zou, and X. Chen, "Intercept probability analysis of relay selection for wireless communications in the presence of multiple eavesdroppers," in *Proc. IEEE Wireless Communications and Networking Conf.* Doha, Qatar: IEEE, 2016, pp. 1–6.

[140] M. Mohamed, B. Shrestha, and N. Saxena, "Smashed: sniffing and manipulating android sensor data for offensive purposes," *IEEE Trans. Inf. Forensics Security*, vol. 12, no. 4, pp. 901–913, 2016.

[141] A. S. Bretas, N. G. Bretas, B. Carvalho, E. Baeyens, and P. P. Khargonekar, "Smart grids cyber-physical security as a malicious data attack: An innovation approach," *Electr. Power Syst. Res.*, vol. 149, pp. 210–219, 2017.

[142] J. Cui, L. Shao, H. Zhong, Y. Xu, and L. Liu, "Data aggregation with end-to-end confidentiality and integrity for large-scale wireless sensor networks," *Peer Peer Netw. Appl.*, vol. 11, no. 5, pp. 1022–1037, 2018.

[143] G. K. Ndonda and R. Sadre, "A two-level intrusion detection system for industrial control system networks using p4," in *Proc. 5th Int. Symp. ICS & SCADA Cyber Security Research*. University of Hamburg, Germany: Electronic Workshops in Computing, 2018, pp. 31–40.

[144] W. Shang, P. Zeng, M. Wan, L. Li, and P. An, "Intrusion detection algorithm based on ocsvm in industrial control system," *Secur. Commun. Netw.*, vol. 9, no. 10, pp. 1040–1049, 2016.

[145] W. Yusheng, F. Kefeng, L. Yingxu, L. Zenghui, Z. Ruikang, Y. Xiangzhen, and L. Lin, "Intrusion detection of industrial control system based on modbus tcp protocol," in *Proc. IEEE 13th Int. Symp. Autonomous Decentralized System*. Bangkok, Thailand: IEEE, 2017, pp. 156–162.

[146] K. Rumyantsev and A. Pljonkin, "Preliminary stage synchronization algorithm of auto-compensation quantum key distribution system with an unauthorized access security," in *Proc. Int. Conf. Electronics, Information, and Communications*. Da Nang, Vietnam: IEEE, 2016, pp. 1–4.

[147] S. Teng, N. Wu, H. Zhu, L. Teng, and W. Zhang, "Svm-dt-based adaptive and collaborative intrusion detection," *IEEE/CAA J. Automat. Sinica*, vol. 5, no. 1, pp. 108–118, 2018.

[148] N. Wang, P. Wang, A. Alipourfanid, L. Jiao, and K. Zeng, "Physical-layer security of 5g wireless networks for IoT: challenges and opportunities," *IEEE Internet Things J.*, vol. 6, no. 5, pp. 8169–8181, 2019.

[149] P. Zhang, M. Zhou, and G. Fortino, "Security and trust issues in fog computing: a survey," *Future Gener. Comput. Syst.*, vol. 88, pp. 16–27, 2018.

[150] E. Baccarelli, P. G. V. Naranjo, M. Scarpiniti, M. Shojafar, and J. H. Abawajy, "Fog of everything: energy-efficient networked computing architectures, research challenges, and a case study," *IEEE Access*, vol. 5, pp. 9882–9910, 2017.

[151] B. Huang, Y. Li, H. Zhang, and Q. Sun, "Distributed optimal co-multi-microgrids energy management for energy internet," *IEEE/CAA J. Automat. Sinica*, vol. 3, no. 4, pp. 357–364, 2016.

[152] Y. Duan, W. Li, X. Fu, Y. Luo, and L. Yang, "A methodology for reliability of wsn based on software defined network in adaptive industrial environment," *IEEE/CAA J. Automat. Sinica*, vol. 5, no. 1, pp. 74–82, 2018.

[153] T. Huang, S. Yan, F. Yang, and J. Liu, "Multi-domain sdn survivability for agricultural wireless sensor networks," *Sensors*, vol. 16, no. 11, p. 1861, 2016.

[154] I. Ahmad, S. Namal, M. Ylianttila, and A. Gurtov, "Security in software defined networks: a survey," *IEEE Commun. Surveys Tuts.*, vol. 17, no. 4, pp. 2317–2346, 2015.

[155] R. Azuma, "A survey of augmented reality," *Presence (Camb)*, vol. 6, no. 4, pp. 355–385, 1997.

[156] R. Kim, J. Kim, I. Lee, U. Yeo, and S. Lee, "Development of a vr simulator for educating cfd-computed internal environment of piglet house," *Biosyst. Eng.*, vol. 188, pp. 243–264, 2019.

[157] V. Figueredo, A. V. dos Reis, F. Garcia, and F. C. Araújo, "Virtual reality for agribusiness in the development of a maintenance simulator for agricultural machinery for senar goiás," in *Proc. 21st Symp. Virtual and Augmented Reality*, Rio de Janeiro, Brazil, 2019, pp. 17–19.

[158] J. Huuskonen and T. Oksanen, "Soil sampling with drones and augmented reality in precision agriculture," *Comput. Electron. Agric.*, vol. 154, pp. 25–35, 2018.

[159] M. U. Rafique and S. S. Cheung, "Tracking attacks on virtual reality systems," *IEEE Consum. Electron.*, vol. 9, no. 2, pp. 41–46, 2020.

[160] M. A. Ferrag, L. Maglaras, S. Moschoyiannis, and H. Janicke, "Deep learning for cyber security intrusion detection: approaches, datasets, and comparative study," *J. Inf. Secur. Appl.*, vol. 50, p. 102419, 2020.

Xing Yang (M'20) received the M.S. degree in control engineering from Nanjing University of Information Science and Technology, China, in 2018. He is currently working toward the Ph.D. degree in the college of engineering, Nanjing Agricultural University, China. His current research interests include fault diagnosis in wireless sensor networks, agricultural Internet of Things reliability, and machine learning algorithm.

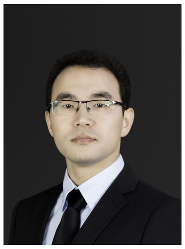
Lei Shu (SM'07) received the B.S. degree in computer science from South Central University for Nationalities, China, in 2002, and the M.S. degree in computer engineering from Kyung Hee University, South Korea, in 2005, and the Ph.D. degree from the Digital Enterprise Research Institute, National University of Ireland, Galway, Ireland, in 2010. Until 2012, he was a Specially Assigned Researcher with the Department of Multimedia Engineering, Graduate School of Information Science and Technology, Osaka University, Japan. He is currently a Distinguished Professor with Nanjing Agricultural University, China, and a Lincoln Professor with the University of Lincoln, U.K. He is also the Director of the NAU-Lincoln Joint Research Center of Intelligent Engineering. He has published over 400 papers in related conferences, journals, and books in the areas of sensor networks and Internet of Things. His current H-index is 58 and i10-index is 218 in Google Scholar Citation. His current research interests include wireless sensor networks and Internet of Things. He has also served as a TPC member for more than 150 conferences,suchasICDCS,DCOSS,MASS,ICC,GLOBECOM,ICCCN, WCNC, and ISCC. He was a recipient of the 2014 Top Level Talents in Sailing Plan of Guangdong Province, China, the 2015 Outstanding Young Professor of Guangdong Province, and the GLOBECOM 2010, ICC 2013, ComManTel 2014, WICON 2016, SigTelCom 2017 Best Paper Awards, the 2017 and 2018 IEEE Systems Journal Best Paper Awards, the 2017 Journal of Network and Computer Applications Best Research Paper Award, and the Outstanding Associate Editor Award of 2017, and the 2018 IEEE ACCESS. He has also served over 50 various Co-Chair for international conferences/workshops, such as IWCMC, ICC, ISCC, ICNC, Chinacom, especially the Symposium Co-Chair for IWCMC 2012, ICC 2012, the General Co-Chair for Chinacom 2014, Qshine 2015, Collaboratecom 2017, DependSys 2018, and SCI 2019, the TPC Chair for InisCom 2015, NCCA 2015, WICON2016, NCCA2016, Chinacom2017, InisCom2017, WMNC 2017, and NCCA 2018.

Jianing Chen received the B.S. degree (with Hons.) from the School of Electronic and Information Engineering in Beihang University, Beijing, China, in 2018. He is currently working toward the M.S. degree at the School of Electronic Information and Electrical Engineering, Shanghai Jiao Tong University, Shanghai, China. His current research interests include industrial control systems (ICS), blockchain and cryptography.

Mohamed Amine Ferrag received the Bachelor's degree (June, 2008), Master's degree (June, 2010), Ph.D. degree (June, 2014), HDR degree (April, 2019) from Badji Mokhtar- Annaba University, Algeria, all in Computer Science. Since October 2014, he is a senior lecturer at the Department of Computer Science, Guelma University, Algeria. Since July 2019, he is a Visiting Senior Researcher, NAU-Lincoln Joint Research Center of Intelligent Engineering, Nanjing Agricultural University, China. His research interests include wireless network security, network coding security, and applied cryptography. He has been conducting several research projects with international collaborations on these topics. He has published more than 60 papers in international journals and conferences in the above areas. Some of his research findings are published in top-cited journals, such as the IEEE Communications Surveys & Tutorials, IEEE Internet of Things Journal, IEEE Transactions on Engineering Management, IEEE Access, Journal of Information Security and Applications (Elsevier), Transactions on Emerging Telecommunications Technologies (Wiley), Telecommunication Systems (Springer), International Journal of Communication Systems (Wiley), Sustainable Cities and Society (Elsevier), Security and Communication Networks (Wiley), and Journal of Network and Computer Applications (Elsevier). He has participated in many international conferences worldwide, and has been granted short-term research visitor internships to many renown universities including, De Montfort University, UK and Istanbul Technical University, Turkey. He is currently serving on various editorial positions such as Editorial Board Member in Journals (Indexed SCI & Scopus) such as, IET Networks and International Journal of Internet Technology and Secured Transactions (Inderscience Publishers). He has served as an Organizing Committee Member (Track Chair, Co-Chair, Publicity Chair, Proceedings Editor, Web Chair) in numerous international conferences such as ICNAS'13'15'17, ASD'16, EUSPN'17, (AINIS) Symposium'17, ANT'17, SEIT'17, IEEE ICCE'18'19, and IEEE ITIA'20.

Jun Wu (M'08) received the Ph.D. degree in information and telecommunication studies from Waseda University, Japan. He was a Post-Doctoral Researcher with the Research Institute for Secure Systems, National Institute of Advanced Industrial Science and Technology, Japan, from 2011 to 2012. He was a Researcher with the Global Information and Telecommunication Institute, Waseda University, from 2011 to 2013. He is currently an Associate Professor of Electronic Information and Electrical Engineering with Shanghai Jiao Tong University, China. His research interests include the advanced computation and communications techniques of smart sensors, wireless communication systems, industrial control systems, wireless sensor networks, and smart grids. He has hosted and participated in several research projects for the National Natural Science Foundation of China, National 863 Plan, and 973 Plan projects. He has been a Guest Editor of the IEEE SENSORS journal and a TPC Member of several international conferences, including WINCON 2011 and GLOBECOM 2015.

Edmond Nurellari received his B.Sc and his M.Sc degree in Electrical and Electronic Engineering, both from Eastern Mediterranean University, Northern Cyprus, in 2010 and in 2012 respectively. From September 2010 to February 2013, he served as a Research and Teaching Assistant in the department of Electrical and Electronic Engineering at Eastern Mediterranean University. In 2013, he was awarded the Leeds International Research Scholarship (LIRS) to pursue his Ph. D. at the School of Electronics and Electrical Engineering, University of Leeds, United Kingdom. Since April 2017, he has been a faculty member with the School of Engineering at the University of Lincoln, United Kingdom, where he is currently a Lecturer in Electrical Engineering/Robotics. His research interests includes distributed signal processing, signal processing on graphs, resource allocations, distributed decisions and network security analysis in wireless sensor networks by employing tools from graph theory and game theory. He has served as an Invited Reviewer for the IEEE Transactions on Signal and Information Processing over Networks, IEEE Communication Letter, Springers Wireless Networks Journal, Springers Digital Signal Processing Journal and IEEE Flagship conferences.



Kai Huang received the Ph.D. degree in agricultural engineering from China Agricultural University, Beijing, China, in 2018. He is currently a postdoctoral researcher in the department of Electrical Engineering at Nanjing Agricultural University, Nanjing, China. His main research ?elds include agricultural Internet of Things. He has guest edited the special issue ?¡ÀSmart Agricultural Applications with Internet of Things?¡À in Sensors. He has served as a PC Members in the IoT Computing Systems area of 3PGCIC-2019.