Array 8 (2020) 100048

Contents lists available at ScienceDirect

Array

journal homepage: www.elsevier.com/journals/array/2590-0056/open-access-journal

Security challenges to smart agriculture: Current state, key issues, and future directions

Angelita Rettore de Araujo Zanella [a,b,*], Eduardo da Silva [c], Luiz Carlos Pessoa Albini [b]

[a] Catarinense Federal Institute, Rod. SC 135, Km 125, Campo Experimental, Videira, Brazil
[b] Department of Informatics, Federal University of Paraná, Rua Cel. Francisco Heráclito dos Santos, 100, Curitiba, Brazil
[c] Catarinense Federal Institute, Rod BR 280, km 27, Araquari, Brazil

ARTICLE INFO

Keywords:
Smart agriculture
Security
Open-field agriculture

ABSTRACT

Smart agriculture integrates a set of technologies, devices, protocols, and computational paradigms to improve agricultural processes. Big data, artificial intelligence, cloud, and edge computing provide capabilities and solutions to keep, store, and analyze the massive data generated by components. However, smart agriculture is still emerging and has a low level of security features. Future solutions will demand data availability and accuracy as key points to help farmers, and security is crucial to building robust and efficient systems. Since smart agriculture comprises a wide variety and quantity of resources, security addresses issues such as compatibility, constrained resources, and massive data. Conventional protection schemes used in the traditional Internet or Internet of Things may not be useful for agricultural systems, creating extra demands and opportunities. This paper aims at reviewing the state-of-the art of smart agriculture security, particularly in open-field agriculture, discussing its architecture, describing security issues, presenting the major challenges and future directions.

1. Introduction

Agriculture is the most important provider of food and plays an essential role in economic growth. The Food and Agriculture Organization of the United Nations (FAO) states that global demand for food must grow to 70% by 2050 to meet demand. While current production suffices to feed the entire world population, 500 million people still suffer from malnutrition, and over 821 million go hungry. The United Nations estimates that the world's population will increase by over 2 billion people, most living in urban areas. More than half of this increase will occur in India, Nigeria, Pakistan, the Democratic Republic of Congo, Ethiopia, the United Republic of Tanzania, Indonesia, Egypt, and the United States. Projections show India and Nigeria to account for the increase of approximately 473 million people between 2019 and 2050 [1]. This population increase represents a challenge to reach the goal of zero hunger defined in the text *Sustainable Development Goals* (SDGs) [2]. These expectations for the coming years influence the global demand for food. It may be difficult to meet 40% of water demands by 2030, and the degradation of 20% of arable land will reduce food supply. Therefore, food production requires more resources than currently available and more sustainable systems to increase cultivation rates and reduce the use of natural resources [3].

Annual cereal production must increase by 3 billion tons, and meat production has to grow over 200% by 2050 to meet the demand [4]. Cereal supplies will depend on the increase in yields. This increase requires the improvement of cultivation practices, structural changes towards larger farms, and the ability to adapt technologies [5]. Although it may be possible to meet the growing demand, it is not clear how to achieve it sustainably and inclusively. Then, there is a crucial need to streamline the farming system transformation at extraordinary speed and scale-up [4]. At the same time, the *Fourth Industrial Revolution* (Industry 4.0) and the *Internet of Things* (IoT) provide new technologies and innovations. These new technologies and innovations applied in agriculture are called *smart agriculture*, *smart farming*, or *Agriculture 4.0*. These terms are used interchangeably throughout this paper. Agriculture 4.0 can provide information on improving plantation productivity without increasing the crop area, optimizing irrigation processes by consuming less water and energy, or providing resources to control pests more efficiently, for example. These will be possible by integrating technologies for environmental measurements, prediction, and automation tools. New capabilities created by smart farming can optimize agricultural processes, allowing production to escalate while using fewer natural

* Corresponding author. Catarinense Federal Institute, Rod. SC 135, Km 125, Campo Experimental, Videira, Brazil.
E-mail addresses: angelita.zanella@ifc.edu.br, gelirettore@gmail.com (A. Rettore de Araujo Zanella), eduardo.silva@ifc.edu.br (E. da Silva), albini@inf.ufpr.br (L.C. Pessoa Albini).

https://doi.org/10.1016/j.array.2020.100048
Received 22 July 2020; Received in revised form 13 October 2020; Accepted 16 October 2020
Available online 21 November 2020

resources.

Smart farming combines different technologies, devices, protocols, and computing paradigms to enable the farmers to make the most out of innovations. Innovations in agriculture are called the "*digital agricultural revolution*'' and will transform all aspects of agriculture, resulting in more productive, efficient, sustainable, inclusive, transparent, and resilient systems. Nevertheless, integrating technologies into the agricultural sector depends on the complexity and maturity of technologies such as mobile devices, precision agriculture, remote sensing, big data, cloud, analytics, cybersecurity, and intelligent systems [4]. Although there are several security issues related to the smart farming, such as compatibility, heterogeneity, constrained devices, processing, and protection of massive data, few resources have been incorporated in Agriculture 4.0 so far. Therefore, this paper addresses the security challenges in these systems.

To build robust and efficient systems, Agriculture 4.0 must ensure (i) the correct and complete generation, transfer, and processing of data, and (ii) that the system has adequate security features to prevent attacks. Data integrity is essential to enable the proper operation of data-driven technologies, such as analytics and smart systems. Malfunctioning hardware or attacks, whether directed to the system or using the system as an intermediary for external attacks, can put security at risk. Heterogeneity of resources raises a lot of security concerns, such as keeping privacy, maintaining trust and reliability, which can be crucial to meet the demand and potential of emerging applications [6,7].

Since smart agriculture integrates elements from the traditional Internet, IoT, cellular, and wireless networks, it may incorporate all security problems these technologies present. It also deals with new special security issues such as data and device integrity, data accuracy, and availability. In smart farming, the devices (sensors and actuators) and communication systems are exposed to climatic fluctuations (sun, rain, snow), natural events (lightning, hail), engines (used in agriculture), power line transmissions (common in some rural regions), wandering animals, people and agricultural machinery. These elements make smart farming vulnerable to problems that have not been addressed in other contexts so far.

For instance, smart agriculture has devices installed in open areas and exposed to external agents such as animals, humans, or agricultural machinery. These agents can unintentionally remove the sensor from the original location or damage them. Most times, the devices cannot use protection boxes to prevent these external agents from approaching as in other scenarios, such as in smart cities. The lack of protection leaves devices vulnerable to security incidents and reveals a distinctive feature concerning applications in agricultural systems.

Another threat is *agroterrorism*, which has been around since the 6^{th} century B.C [8]. This type of terrorism can have several objectives, such as causing financial damage, fear, and social instability [9,10]. Through crises in agriculture and the food industry, terrorists can stimulate social unrest and loss of trust in government, which can serve a variety of interests in the globalized world. For example, terrorists and governments in trade disputes may want to cause economic damage to a nation, economic opportunists may attempt to manipulate markets, and unbalanced or disgruntled people may commit attacks with idiosyncratic or narcissistic motivations [8]. New technologies, such as smart agriculture, can contribute to the evolution of agroterrorism, creating *cyberagroterrorism*. It might use computer systems in agricultural environments to damage crops, livestock, and generate financial losses. Cyberagroterrorists can act both locally, on farms, and online, operating the attacks through cyber resources.

This article presents special security issues in Agriculture 4.0. The aim is to highlight the main solutions in this area and discuss security threats. Section 2 reviews smart agriculture and the architecture used by most systems. Section 3 outlines the major security threats from a layered perspective. Section 4 summarizes the current state of intelligent agriculture applications. The last section presents the key challenges in this area and points to future directions.

2. Smart agriculture overview

Agriculture has undergone several revolutions, which improved the sector's efficiency and profitability. The plant domestication (10,000 BC) led to the world's first societies and civilization. In recent centuries, agricultural mechanization (between 1900 and 1930) introduced machines and implements to mechanize work, increasing farmworker's productivity. The Green Revolution (about the 1960s) enabled farmers to use new crop varieties and agrochemicals. In the late 20^{th} century and early 21^{st} century (from 1990 to 2005), biotechnology allowed the creation of plants with pre-selected traits, such as increased yield and resistance to pests, drought, and herbicide. Now, the digital revolution could help humanity to survive and thrive long into the future [4]. Fig. 1 presents an overview of major agricultural revolutions, that preceded the digital revolution.

The first steps toward the digital revolution focused on automation techniques, including few computational functionalities [11,12]. Next, smart agricultural systems had sensors to collect climate or environmental data. Sensors connect to a constrained border device, named gateway, linked to a local computer through a network connection, frequently wireless. The local computer receives data from the gateway, stores it in a database, and shows processed information on a web page. Local systems did not integrate with external systems or the Internet.

In recent years, the scenario has changed, with researches in artificial intelligence and machine learning focusing on agricultural contexts, irrigation, animals, and farms. In the irrigation field, monitoring, controlling, and decision-making solutions attempted to save water and improve production [13–18]. Some studies focus on hydroponic [19], horticulture [20], vineyards [21] and leaf disease detection [22]. General-purpose systems [23–25], just implement IoT technologies and resources or design web-services [26], alert services [27], traceability resources [28] and control on the cloud [12]. Although there are several solutions in Agriculture 4.0, they are still immature and provide a low level of intelligence. Many of these proposals are automation-restricted, with sensors and actuators sending data to the gateway. In most cases, there is no integration with the Internet, though in a few cases, local systems store data in the cloud.

The above systems have been built up in architecture (see Fig. 2) that consists of perception layer devices, network layer capabilities, edge resources, and cloud-based applications and services [29,30]. The perception layer includes sensors, GPS, tags RFID, cameras, actuators, and any other devices responsible for collecting data from the farm environment and acting to modify them. These devices do not have the computational capacity to process or store data and perform at the edge or the cloud. This layer connects to edge resources via network technologies, which is usually a Wireless Sensor Network (WSN).

The edge layer may contain a variety of resources such as security features, data filters, decision-making capability, diversified processing, in-out interface, and the gateway. Including one or more resources at the edge depends on the features of the appliance. Some appliances support only the retransmission of data, while others have the computational capability to perform more tasks. More robust gateways can process data, make decisions, send commands to actuators and data to the cloud. The Internet Service Provider (ISP) connects the gateway to the cloud. The cloud processes and stores data to provide end-users with information and services. Data processing is a challenge, considering a large mass of data produced by the perception devices reaching the Big Data world, and the financial cost of processing in the cloud.

Processing everything in the cloud, as proposed by many solutions, implies enormous bandwidth requirements and high financing costs. It can be advantageous to use a robust gateway and perform part of the processing at the edge. Moving part of the subsystems to the edge may reduce the financial costs of smart farming. Data consumed or preprocessed at the edge saves bandwidth and can reduce the computing resources required from the cloud, protects privacy, and preserves the battery life of some devices. Thus, the cloud could store and process

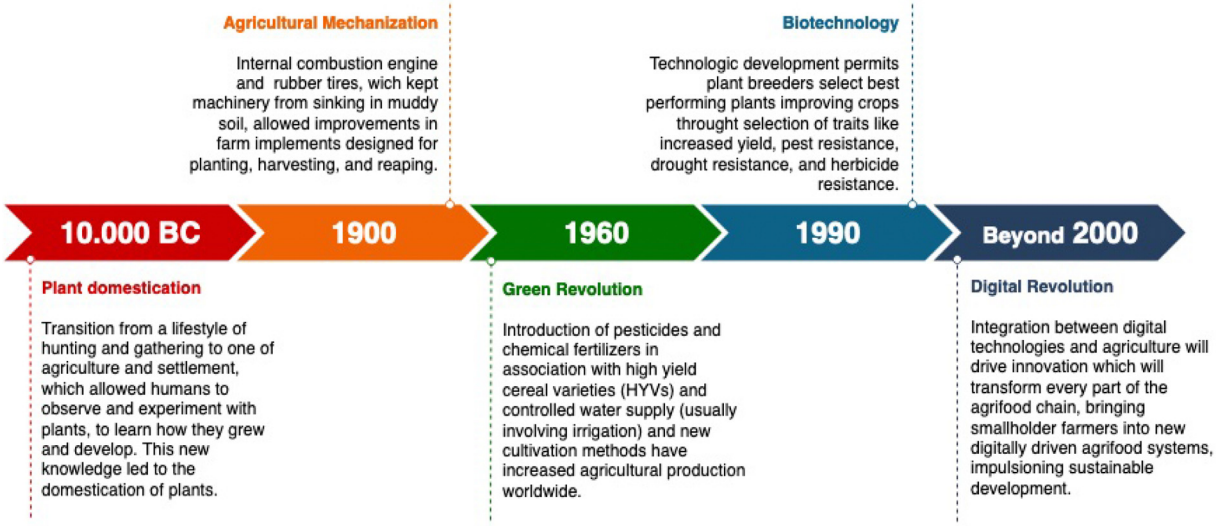

Fig. 1. Agricultural revolutions.

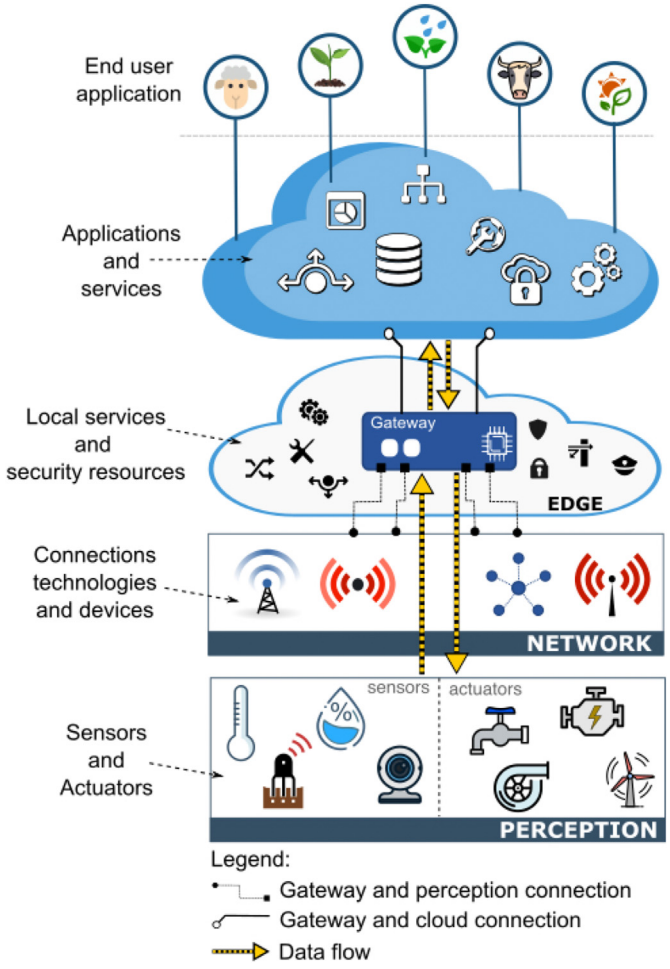

Fig. 2. Structure of smart agriculture components.

massive data, make decisions, and interact with the user. Processing big data to make decisions at the edge may require tools like artificial intelligence.

The improvement of devices and communication technologies will make it possible for more computational resources to be integrated into systems. Such integration aims at meeting different demands of agricultural automation, farm management, and precision farming [12,30]. Solutions must evolve to management systems rather than just monitoring, which can result in new challenges and possibilities. Another issue is the security of data. From the detection up to the storage and decision-making in the cloud, it is mandatory to provide data privacy, reliability, and accuracy. Security issues in smart farming are a great challenge and will be detailed in section 3.

3. Smart agriculture security threats

As discussed in Section 2, smart systems have four layers: (*i*) perception layer; (*ii*) network layer; (*iii*) edge; (*iv*) application. Table 1 shows the resources responsible for collecting, transporting, processing, and storing data at each layer. The set of devices, protocols, and technologies use the data to monitor environments and automate farming activities [29]. Storage, management, and data processing combined with Internet connectivity bring several issues and security threats. Fig. 3 summarizes attacks on smart agriculture in the layered perspective.

Security incidents may be accidental or intentional. Animals, farm working, and machinery can easily access farming environments and cause incidents. Additionally, smart systems comprise heterogeneous devices and software from distinct manufacturers installed between growth areas and the cloud. These specific features might make several security breaches and could result in incidents that compromise the smart system. Nevertheless, this topic has not been studied in most systems in use so far.

The system design should consider compatibility with distinct devices, protocols, subsystems, and multi-access methods. Smart Agriculture uses *machine-to-machine* (M2M) communication and devices manufactured by different vendors. However, most security mechanisms were developed for the communication model used by TCP/IP networks. These mechanisms usually ignore the existence of multiple heterogeneous devices communicating simultaneously. Security features created for TCP/IP networks can divide the relationship between smart farming devices, reducing their efficiency. Multi-access methods and heterogeneity hinder security, interoperability, and network coordination, increasing security vulnerabilities [31].

Agriculture 4.0 is exposed to a vast spectrum of cyberattacks. Security concern needs to be part of the system, maximizing their potential. Among these issues, there is also access control, management, information storage, data integrity, and reliability. Most of the security problems are quite common in other systems, but some are present only in those

Table 1
Smart agriculture elements.

Layer	Resource	Description
Perception	Sensor and Camera	Small devices to collecting environment data, such as humidity and temperature.
	Actuator	Devices or systems for changing the environment state. Example: sprinkler, ventilation, and irrigation systems.
	Tag RFID	Small devices to storing data, such as livestock identification number.
	GPS	A System that provides geolocation of agricultural machinery, farm resources and may assist precision farming system.
Network	Connection Technologies	Devices and technologies to interconnecting remote devices and transferring data. Example: router, access points, protocols.
Edge	Security features	Security protocols and schemes for ensuring the availability, integrity, and confidentiality of the system and data.
	In-out interface	Software and hardware interface for communication beyond the local area.
	Diverse resources	Software features applied to decision-making, processing data and so on.
	Gateway	System located at the edge of the network, connected with farm devices (perception layer) and the cloud. This system can process data, store small amount of data and communicate with the cloud.
Application	Database	System for storing data produced by the smart system.
	Web tools	Resources for exchanging data between the remote application and provide access to the end-user application on the Internet.
	Decision-making	System to making-decisions to change the state of the environment.
	End-user application	Software for presenting information to the user.

that operate in open-field systems, such as smart agriculture. Although privacy is unnecessary in most contexts, others might require it. This work addresses all security requirements regardless of the context. Therefore, the developer must select the features related to each system. Here we introduce some of the current security issues in Agriculture 4.0, describing the most relevant threats in each layer separately.

3.1. Security issues at perception layer

The perception layer mainly deals with physical devices, such as sensors and actuators. They can be installed in small farm areas, such as those found in Europe, or scattered along with large farms, current in the USA, Australia, and Brazil. Physical devices may malfunction because of accidental or intentional human action, viruses, malware, or cybercriminals. There are many kinds of sensors and technologies used by smart farming applications, and this variety enables several security threats just as follow:

Random sensor incidents - It is the unintentional physical modification of a perception device that diverts it from the regular operation. Smart systems developed for small or large farms may have devices installed outdoors. In many cases, these devices do not have tamper-resistant boxes, as this would make it expensive. The lack of tamper-resistant boxes exposes the device to interactions with external agents such as people, animals, or agricultural equipment. A farmworker or wild animal may accidently collide with a sensor, moving or removing the device from its original location, violating system integrity. Farm equipment, such as a tractor, may hit the device causing temporary or permanent physical damage, leading to data corruption, data unavailability, or damage to the device. This threat is not exclusive to smart farming but may be present in other contexts, such as smart cities. However, it is a relevant issue because it can have a deep impact on the reliability of the solution. In most cases, there is no way to avoid this threat, though it is necessary to identify it to avoid its effects.

Autonomous system hijacking - It consists in hijacking autonomous systems such as tractors, drones/UAV, and sowing robots. Several farming activities use autonomous systems, such as drones and robots. Drones could spray pesticides and fertilizers, and robots may perform weeding and disease detection. If a malicious agent hijacks an autonomous system, the hijacker can remotely control and guide without authorization. This type of attack could have several impacts, from the unavailability of the system to perform a task to its complete damage or crop damage.

Autonomous system disruption - It is an intentional modification of autonomous system resources. Autonomous tractors, robots, and UAV (Unmanned Aerial Vehicles) are technologies increasingly present in precision agriculture, especially in large farms. These equipment have a series of features that are essential to their operation, such as sensors, cameras, GPS, maps, and remote-control systems. If an opponent modifies one or more components, the autonomous system may work improperly or suffer/cause accidents. Malfunctions could result in severe losses, resulting from incorrect soil or crop management, damage to crops, buildings, equipment, and machinery, including the autonomous tractor itself.

Optical deformation - It is the deformation of images from cameras installed in robots or autonomous devices. Some autonomous systems have cameras to capture images. The cameras usually have an essential function in the system, and the captured images should have a minimum quality. Cameras are usually vital to the system. Pictures must meet a minimum quality standard in order to ensure the whole process to run smoothly. Below standard pictures may mislead the harvesting system into picking spoiled or unripe fruit or even damaging the fruit trees.

Irregular measurement - It consists of abnormal measurements or readings caused by data corruption, energy depletion, electromagnetic

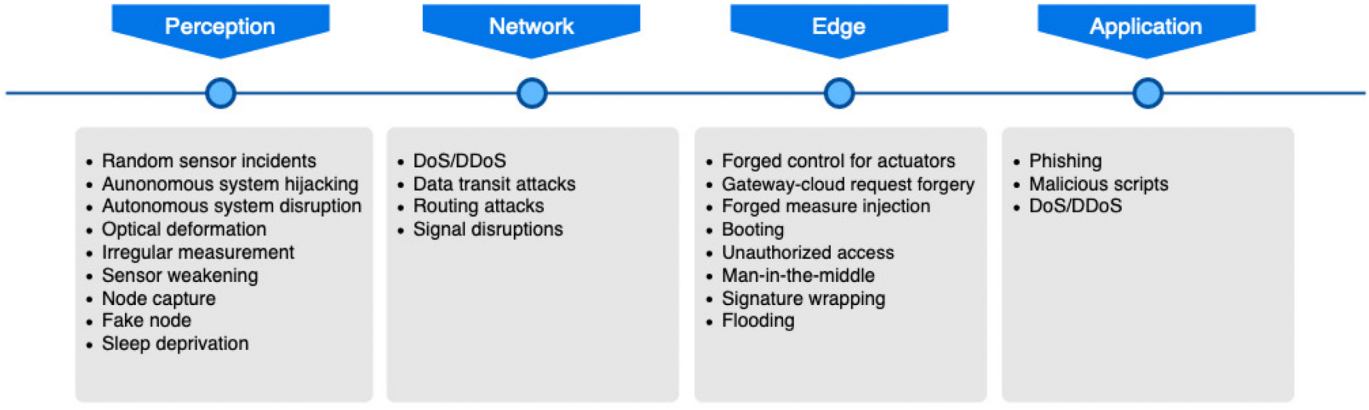

Fig. 3. Smart agriculture main attacks.

interference, interception of variable connectivity, severe weather, malfunctions, or false inputs. In some regions, usually in large farms, high-voltage grids pass over agricultural areas and can generate an electromagnetic field, causing distortions or data corruption. Power depletion of battery-powered devices, variable connectivity, or malfunctioning of some device components can cause irregular readings, compromising data availability or integrity, which results in inaccurate data. Inaccurate data can be dangerous for decision making, resulting in incorrect data analysis, and reducing system's accuracy.

Sensor weakening - This is the normal degeneration of sensors because of processes such as corrosion, oxidation, dust accumulation, and saturation. Some sensors used in smart farms can suffer gradual degradation for exposure to environmental conditions and physical-chemical or climatic phenomena. For example, wind speed sensors installed in dusty environments can suffer from dust accumulation, which gradually prevents the rods from moving. Humidity sensors can saturate when exposed to high humidity levels. Sensors built with copper may suffer oxidation. This way, the sensors register incorrect or irregular measurements. The natural degradation of the sensors requires their periodic replacement. However, some events may expect device degradation, causing failures earlier than expected. It is still not possible to avoid the natural degradation of the sensors. However, it is necessary to detect sensor weakening, to prevent the use of inaccurate data by the system.

Traditional network and IoT attacks can affect the security of smart farming applications, for example:

Node capture - It consists of the physical capture of a node or device. This operation could be performed by entirely replacing the device or modifying components of hardware or software [32,33]. Node capture may not generate a significant impact if performed on a single node and might not trigger other attacks. However, after capturing a device, the opponent may modify the hardware or software, gain access to the system, or inject false data. A node capture breaches the integrity of the system and can potentially interfere with decision-making. It might also damage the cultivation and cause financial loss. For example, a hostile actuator in an irrigation system could never start irrigation or flood the crop. A dissatisfied employee or commercial competitor who has physical or logical access to the system could perform this attack for several reasons.

Fake node - An adversary adds fake or malicious nodes to the system to disrupt their operation [31]. A node capture could trigger this attack and lead to node replication. This kind of attack usually aims at both to manipulate data or to shutdown services and devices. In a system with insufficient or fraudulent identity control, malicious sensors could send wrong data interfering with decision-making, or inject multiple packets into the network causing a denial of service, or sleep deprivation. Likewise, actuators may act maliciously, hostile gateways may send false commands to legitimate actuators, or act as black holes to cause harm.

Sleep deprivation - This attack aims to drain the battery of the device until depleting it. Smart farming sensors are energy-restricted and usually use power batteries. To reduce the power consumption and prolong battery life, the nodes should enter in sleep mode when they are not working [34,35]. Sleep deprivation attack sends sets of apparently legitimate requests so that the devices remain awake as long as possible. Therefore, the battery of the device will deplete, and the node shuts down [34,35]. Once the sensors turn off, sensed data is no longer sent, compromising decision-making, and system efficiency.

Since Agriculture 4.0 systems are open-field, they are susceptible to environmental conditions, climate fluctuations, and human action. Weak security measures could affect the reliability and trust of the system, exposing them to accidental use of corrupted data, remote control, and physical damage. Sensors do not have computational resources that allow the adoption of traditional security methods, such as cryptography, which makes security even more challenging. Therefore, adding innovative security solutions to this layer is as challenging, as necessary.

3.2. Security issues at network layer

The network layer transmits data from the perception layer to the most robust computational unit, usually the cloud. The transmission of a large amount of data over a wide transmission area makes this layer susceptible to attacks, which generally threaten confidentiality and integrity [36]. Although the existing communication network has relatively complete security protection measures, there are still some common threats that can compromise network resources [31,37]. Major security issues in the network layer are as follow:

DoS/DDoS - It is a transversal attack that affects all layers. Denial of Service (DoS) aims to prevent access to services or devices either by overloading the network or by exploiting protocol vulnerabilities that lead to the collapse of resources, such as CPU and memory [38]. There are several ways to achieve this attack, such as flooding servers or routers with numerous requests. Flooding attacks can cause network delays, disable devices, and make the service unavailable. When the attacker uses multiple sources to flood the target, then such an attack is termed as a Distributed Denial of Service attack (DDoS). Although such attacks were not designed specifically for smart systems, Internet connectivity, pervasiveness, heterogeneity, and high vulnerability of these systems make them prone to such attacks [39]. In farming systems, DoS attacks could prevent measurements from reaching the edge or cloud on time, delay commands to actuators, and make services unavailable.

Data Transit Attacks - Some attacks intend to intercept data exchanged between network components to find sensitive information [7]. Different connection technologies connecting distinct points on the network and wireless networking carrying clear (unencrypted) data make these systems susceptible to data breaches [7,40]. An opponent could conduct traffic interception through malicious access points or by man-in-the-middle attacks [40]. Traffic interception exposes sensitive information such as unique identifiers, access credentials, or cryptographic keys. Other transit attacks can corrupt network traffic, enabling malicious control, or even compromising the entire system.

Routing Attacks - They intend to alter network routes to achieve control of traffic. IoT networks may have malicious nodes that try to redirect routing paths during the data transmission process. Attacks such as sinkhole and wormhole could subvert the communication network and get unauthorized access. The sinkhole is routing attacks where a rival announces a shorter routing path and draws nodes to route traffic through it. Malicious routes allow disrupting the traffic flow [7,41]. In a wormhole, an opponent creates a tunnel between two nodes for fast packet transferring to create a shortcut on the network and control traffic [7,42]. During these attacks, the recipient may receive the information late, receive partial or changed information, or not receive one data [41,42].

Network layer resources on smart farming and IoT systems have some common security vulnerabilities. However, smart farming can consist of multiple systems and integrate technologies and subsystems from different vendors. Therefore, integrating systems and technologies requires caution to avoid incompatibilities. Likewise, the security features of these systems and technologies cannot be fully trusted, as they may contain vulnerabilities embedded in the system or generated by the integration process.

3.3. Security issues at edge

The edge contains critical elements monitoring and controlling subsystems, communicating with all layers, and accessing strategic resources. The processing of massive amounts of data generated by perception layer can be local, instead of centralized in the cloud. This would save energy, bandwidth and cloud-processing costs. Due to the distributed architecture of edge computing, this layer might provide services with faster response and higher quality, in contrast with cloud

computing [33]. Direct connection to cloud and perception resources make the edge a strategic point, making security a fundamental requirement to ensure system reliability. Major edge security issues are the following.

Forged controls for actuators - It is the injection of false measures/data to manipulate the system. The perception devices are usually resource constrained and do not support complex security features. Typically, the gateway receives the data in plain text. The gateway may receive data from the perception or cloud by Supervisory Control and Data Acquisition (SCADA) systems or other control systems. An opponent who knows the data patterns sent by the sensors to the gateway or cloud can use a computational device to inject the same data pattern into the system. If the control system receiving the data at the gateway does not have sufficient security mechanisms, the data will be accepted and may propagate through the system. False data will cause incorrect decision making. For example, to manipulate a smart irrigation system, an opponent could inject incorrect soil moisture measurements.

Gateway-cloud request forgery - Gateway and cloud are connected through an Internet Service Provider or cellular network. Usually, the cloud is connected to the Internet and therefore exposed to a wide variety of attacks. An Internet adversary could impersonate a gateway and forge requests for the cloud. From these requests, the adversary could modify parameters in smart farming, control requests for vulnerable services, or manipulate system resources. The gateway is usually a constrained resource, but the cloud has the computational capability to incorporate robust security mechanisms. These mechanisms must be incorporated into the system to maximize system reliability.

Forged measure injection - It consists of the injection of false measurements/readings to manipulate the system. Perception devices generally are resource-constrained and do not support complex security features. In general, data exchange with the gateway is done in plain text, creating several vulnerabilities. An opponent who knows the patterns of data sent by sensors to the gateway or the cloud can use a computational device to inject the same data pattern into the system. Sending false data could result in wrong decision-making. For instance, to manipulate an intelligent irrigation system, an opponent may inject incorrect soil moisture measurements.

Booting - IoT evolution has driven the development of low-cost and resource-constrained devices. These devices are becoming smaller and cheaper. However, innovations do not advance into the field of security [43]. Smart agriculture uses resource-constrained artifacts in the perception and edge layers. Usually, these artifacts have few security features and rarely include boot protection. Lack of security processes on booting, leaving devices vulnerable to attacks [44]. For instance, SD-cards and USB sticks may contain malicious scripts that could run at startup [43]. Malicious boot processes could trigger a series of attacks to the edge with weak protection. Those processes could open back doors or allow elevation of privileges. Insufficient computing resources and direct connection to perception and the cloud make it imperative to protect the start-up process.

Unauthorized access - Authentication and access control are crucial elements of security. Access control is a technology that satisfies properties such as confidentiality, integrity, and availability [45]. Providing adequate access control to the edge elements is essential as these can usually communicate with perception and the cloud. In particular, the gateway is a critical element as all data pass through it. Limited or insufficient authentication and access control mechanisms allow an opponent to access the gateway by cloud connection. For the large number of things communicating with edge devices or services, authentication methods need to be scalable, easily manageable, and requiring minimal human intervention [33,45]. However, several agricultural systems use gateways with weak or insufficient access controls. Researchers developing projects to smart agriculture do not discuss the use of access control resources, and existing commercial solutions rarely change the credentials after deployment.

Man-in-the-middle - In this attack, an opponent intercepts a communication to collect information or even replace it. Compromised devices or malicious nodes can trigger several internal or external attacks in systems with weak or missing security [46,47]. Many solutions use communication protocols that use the publish-subscribe model with a broker, which effectively acts as a proxy. These protocols allow decoupling the publishing and subscribing clients from each other, authorizing messages to be sent to an unknown destination. An attacker who achieves the broker control and becomes a man-in-the-middle may obtain full control of communication without being noticed by the clients [7].

Signature wrapping - This attack modifies the original message by injecting a fake element to perform an arbitrary Web Service request while authenticating yourself as a legitimate user [48]. Web services for edge to cloud communication usually use XML signatures. An adversary, who breaks the signature algorithm, can perform operations or change the heard message by exploiting protocol vulnerabilities, such as the step [7]. An opponent may control the actuators or manipulate the decision-making systems by using malicious messages.

Flooding - This is a DDoS attack where many packets are sent to a system or network to overload it. In farming systems, infected devices could start a flood attack toward the edge devices to compromise the Quality-of-Service (QoS) or even to stop it. A hostile device at the perception layer or a malicious portal in the cloud could send multiple requests to service until their exhaustion. These attacks could impact severely on the systems, overloading the edge and resulting in a denial of service. Flooding could also be performed at the network layer and in the cloud [6,7].

Edge resources provide computing services for clients or applications and can connect to distinct features from all layers. Both locally and externally processed data pass-through this layer. Protecting devices from remote access and using appropriate cryptographic resources are key security challenges. Therefore, it is imperative to achieve security features to avoid compromising data and edge resources.

3.4. Security issues at application layer

The application layer aims at providing services to end-users, storing data, and making decisions within the system. Security issues in this layer focus on preventing data theft and ensuring privacy and are specific to different applications. Some applications comprise a sub-layer, which supports services, and helps intelligent resource allocation [7,33]. Each application has distinct characteristics, and it is impossible to predict all vulnerabilities which could affect them. Therefore, the security issues listed below are some threats that might affect cloud-based applications and services.

Phishing - It is a virtual pest that aims to fraudulently obtain confidential user data, such as ID and password. Phishing usually achieves end-user from fraudulent emails or websites [49,50]. An opponent who accesses the system with administrative credentials may send fraudulent commands to actuators and change system settings. In critical cases, the attacker could interfere with decision-making processes or other internal processes. It is impossible to avoid this type of attack, but secure access control systems can mitigate it. However, the most efficient protection would be to have the users themselves keep vigilant while surfing the net [33].

Malicious scripts - The connectivity of agricultural solutions to the Internet allows them to interact with other online services and users. This interaction makes them targets for malicious scripts such as Java applets, Active-X scripts, and cross-site scripting (XSS) [33,36]. Malicious scripts can mislead customers, inject malicious information, access sensitive information, and break security mechanisms. Cybercriminals often make this attack by personal, financial, and political ends. From malicious scripts, they can damage or disrupt the service operation, displaying unwanted advertisements, and extorting money [51].

Denial of Services - This attack causes service interruptions by overloading the network traffic or by flooding the service with multiple requests [52]. Weak security configurations enable an adversary to start

this attack from the Internet or a subsystem [7]. Such attacks deprive legitimate users of using the services, prevent the proper processing or storage of non-persistent information, reduce the efficiency of critical systems (such as environmental controls in mushroom greenhouses), and may even cause a complete system shutdown.

The application layer includes cloud-based applications and services, so it has all cloud security issues. The cloud exposes applications and resources to Internet-based attacks becoming urgent to take preventive security measures. Usually, security focuses on privacy and access control to protect the many sensitive data stored and processed in the cloud. However, it is essential to consider more than just privacy and access control, adopting security measures to ensure the availability and integrity of the complete system.

Smart farming systems incorporate a set of devices, with greater or lesser levels of limitations, that interact with each other. Many weak points are because of the constraints of the devices, which make it impossible to use existing tools and security techniques. Technologies developed for other systems, such as IoT or Industry 4.0, support security, but using them requires processing and memory resources that some devices do not have. However, it is necessary to know the existing vulnerabilities and create mechanisms to mitigate the effects of incidents. Then, security measures can be done at the highest layers and on devices equipped with the necessary resources. Top-layer appliances with robust computing capabilities could adopt more robust security mechanisms to ensure efficient and reliable operation.

4. Current state of security in smart agriculture

In the past few years, there has been a growing effort to develop smart systems to improve agricultural activity. Farmers usually conduct these activities in open-field or greenhouses. This work focuses on open-field agriculture, as it is an immature area with security features limited to access control and web encryption. Therefore, it analyzes smart agriculture projects and explores information on the security features implemented by them.

In this scope, most efforts focus on irrigation processes, disease detection, crop management, and traceability. The control may be automatic or manual. In both cases, the system uses sensors for monitoring and actuators for changing the environment. The decision about actuators' actions may be made automatically by the system or manually by a user. Some projects only automate the farms, while others integrate industry 4.0 or IoT technologies.

It is relevant to show that most current smart agriculture projects are based on IoT technologies and may direct inherit its security flaws. Others do not consider security at all. Protocols such as MQTT and CoAP disable security features by default, and the developer must enable them according to the requirements of each project. Since researchers do not report security features enablement, they probably remain disabled. Table 2 presents a taxonomy of current smart agriculture security resources.

The paper of [13] presents a system to predict irrigation requirements based on climate and environmental information. The system uses data collected by sensors to predict soil moisture and provides irrigation suggestions. End-user interacts with the system from a web page. The authors do not show any security features, validation processes, or failure checks in the collecting, transferring, or storing phases. The lack of security makes systems vulnerable to all attacks presented in Section 3, i.e., the system is highly insecure. Incidents leading to corruption or inaccuracy of data result in prediction errors and wrong decisions. Wrong decisions can damage the cultivation and reduce the adoption of the system.

Similarly [17], develops a system to monitor fields through soil moisture, temperature, humidity, and light levels. Irrigation control can be manual or automatic through the web or mobile applications. The system description does not contain information on any security features, which exposes the system to the full range of attacks presented in the previous section. Control of actuators driven by commands from a web system without strict security features is an excellent opportunity for malicious opponents, who may use malicious scripts and unauthorized access to manipulate the system.

[18] propose a smart irrigation system to control irrigation devices. These devices are remotely controlled by a server and managed from a web application. There are no details about security resources, creating the chance for opportunistic adversaries to gain improper access to the system, inject forged measures, forge controls for actuators, or conduct any previously reported attacks to deviate the system from its regular operation.

[19] introduce a Hydroponic Farming Ecosystem (HFE) to monitor the growing environment. The control is automatic, and the user may use a web interface to monitor the farming. Automated systems require rigorous protection to avoid or detect random sensor incidents, sensor weakening, false data injection, and other threats that could corrupt data and disturb the system's reliability. However, HFE fails to provide mechanisms to avoid the threats introduced in Section 3.

[22] have designed an intelligent solution for the detection of leaf diseases. The system identifies leaf diseases based on data of sensors and images from cameras. The end-user interacts with the system by a mobile or web application. This paper does not discuss the implementation details or security. If this system is part of a disease control process and receives corrupted or malicious data, the images suffer optical deformation, or an opponent compromises system, then security incidents can hinder disease detection and cause misuse of agricultural resources. In critical cases, this may cause loss of the entire production.

[28] introduces NETPIE, a system that provides information about agricultural products. Using a set of perception devices, NETPIE controls and monitors the growing environment. The production information is summarized and saved in a QR code and available to the customer. Just like the other presented systems, NETPIE does not discuss security resources. Any of the attacks that disrupts data accuracy may break the reliability of the information summarized in the QR code.

[12] present a cloud-based Wireless Sensor and Actuator Network (WSAN) communication system to monitor and control farm devices. The system monitors environmental conditions, predicts the irrigation requirements, and acts automatically on the environment. The paper describes the system architecture, including appliances and protocols, allowing the WSAN to remain vulnerable to the attacks shown in Section 3.

Table 2
Taxonomy of security in smart agriculture.

Security target	Security Resources	Solutions
Not considered	None	Sales et al. [12], Goap et al. [13], Mahalakshmi [14], Rajalakshmi and Mahalakshmi [17], Zhao et al. [18], Ruengittinun et al. [19], Thorat et al. [22], Yoon et al. [23], Wongpatikaseree et al. [28]
Data Exchange	HTTPS	Khelifa et al. [11], Minh et al. [25]
Access Control	IP Authentication	Nageswara Rao and Sridhar [15]
	User and Device Management	Oliver et al. [21]

Likewise [23], propose a smart farming system for data exchange between the server, the gateway, and the nodes. The paper describes the construction of the system but does not mention any user interaction or remote control and does not demonstrate any security concerns. Because it is a system for data exchange, the most critical attacks are those that affect the network layer, such as DoS, signal disruption, data transit, and routing.

Similarly [14], introduces an automated irrigation system. The paper presents the step-by-step construction of the system, which monitors and controls water flow remotely. Although the system controls and monitors irrigation devices, there is no evidence of the addition of security capabilities. Attacks on the perception layer, as well as attacks that cause a denial of service, can damage correct system operation. Unauthorized access, malicious scripts, and false data injection can deliberately manipulate the system.

On the other hand, some solutions add a small level of security. The [11] strategy, for instance, includes encryption in the communication between cloud and user applications. This proposal intends to create a smart irrigation system controlled remotely by the user. Farmers manage the irrigation process from a mobile application. This strategy uses HTTPS to encrypt the communication between the server and smartphone. The use of cryptography protects data in transit, preventing an adversary from intercepting the communication, obtaining sensitive information, and impersonating the mobile application. However, there is no information about other security features deployed by the system, which exposes the system to other previously presented attacks.

Another proposal that uses HTTPS is that of [25], which has developed an intelligent system to manage and control mushroom and hybrid maize farms. This system automatically controls the production environments remotely. The webserver uses HTTPS for user communication, protecting data in transit. However, this security feature is insufficient, considering that the system automatically controls the water pumps, light levels, and fans. Automated controls, especially for environmental control systems for crops as sensitive as mushrooms, demands accurate security features to avoid that Random Sensor Incident, Irregular Measurement, and Sensor Weakening, Forged Measure Injection, or Forged Controls for Actuators affect the system accuracy.

On the other hand [21], introduce a system called SEnviro. This system is designed to remotely monitor vineyards and predicts some diseases. The paper presents the developed platform and does not discuss prediction. The system includes a user and device manager, which permits to manage authorized users and devices to interact with the system. Access control prevents unauthorized devices or users from gaining access to the system and acting maliciously. Nevertheless, this resource is insufficient to protect a platform designed to predict disease and remotely monitor, as it does not prevent events that could interfere with the accuracy of the data or that could take the system to an unreliable state.

In the same way [15], proposes a remote crop-field and automatic irritation monitoring system using IoT technologies. The system uses collected data from sensors to estimate the quantity of water required for irrigation. The system uses measurement data to estimate the volume of water for irrigation. As well as the access control presented by Ref. [21], the authentication scheme used by Ref. [15] avoids unauthorized access to the service but does not protect the edge and other subsystems. Weak protection of automatic control systems is critical, as incidents that affect data accuracy or cause system malfunctions can result in significant losses to the plantation.

Summarizing the related papers, from a security perspective, they use sensors and actuators without any security features. Besides, there is no security information on the gateway. Systems developed so far do not present information about transmission privacy or device authentication. Features such as access control, identity management, or encryption add a bit of security to Internet communication. Table 3 shows that little security in farming systems is limited to privacy and reliable data transmission between the user and the cloud or between the gateway and the cloud.

Table 3
Security features added to Agriculture 4.0

Layer	Security issues	Security Resources	Papers
Application	Data thefts	HTTPS	Khelifa et al. [11], Minh et al. [25]
	Sniffing	HTTPS	Khelifa et al. [11], Minh et al. [25]
	Access Control	IP Authentication	Nageswara Rao and Sridhar [15]
		User and Device Management	Oliver et al. [21]
	Phishing attack	Use not reported	Open issue
	Malicious scripts	Use not reported	Open issue
	Deny of services	Use not reported	Open issue
Edge	Man-in-the-middle	Use not reported	Open issue
	Booting vulnerabilities	Use not reported	Open issue
	Unauthorized access	Use not reported	Open issue
	Signature wrapping	Use not reported	Open issue
	Flooding	Use not reported	Open issue
	Forged control for actuators	Use not reported	Open issue
	Gateway-cloud request forgery	Use not reported	Open issue
	Forged measure injection	Use not reported	Open issue
Network	DoS/DDoS	Use not reported	Open issue
	Data transit attacks	Use not reported	Open issue
	Routing attacks	Use not reported	Open issue
	Signal disruptions	Use not reported	Open issue
Perception	Random sensor incidents	Use not reported	Open issue
	Autonomous system hijacking	Use not reported	Open issue
	Autonomous system disruption	Use not reported	Open issue
	Optical deformation	Use not reported	Open issue
	Irregular measurement	Use not reported	Open issue
	Sensor weakening	Use not reported	Open issue
	Node capture	Use not reported	Open issue
	Fake node	Use not reported	Open issue
	Sleep deprivation	Use not reported	Open issue

Many solutions for smart farming only include security mechanisms in the application layer. While [12,13] use HTTPS for communication between the cloud and the end-user application, most systems use the HTTP, CoAP, and MQTT protocols without any integration with SSL or TLS protocols. Similarly, many proposals do not implement access control or use it with limited resources. The absence of robust security features for communication between the cloud and the end-user creates several security breaches. There is no information about configuring security features in database management systems or using secure data search techniques in web applications. Thus, these features are probably not included.

Currently, smart agriculture is an easy target for malicious agents. Attacks may have several motivations, such as commercial, ideological, or even terrorist reasons. For instance, terrorist groups can inflict economic harm to a nation, economic opportunists may try to manipulate markets, and an individual employee may proceed with an attack for a variety of reasons [8]. Thus, it is urgent to add security as an essential resource for smart farming, contributing to the development and popularization of reliable and efficient systems.

5. Improvements and enhancements required for upcoming applications

Devices from traditional Internet have many security features built into them, like firewalls, authentication, and access control schemes, and so on. However, these security shields are missing on Agriculture 4.0 or limited in use. Sometimes this is due to smart farming is still emerging,

sometimes because the resources are inadequate for this technology or the absence of professionals to manage these resources. Also, a well-defined framework and standard to guide an end-to-end application development are not available yet. Usually, solutions are not standalone, but it is an embedded product that integrates many individuals and industries and requires an architecture that can handle heterogeneity, interoperability, and numerous devices. This architecture should allow multiple access, in a secure and coordinated way, to avoid data loss and compromise the system efficiency. Security resources presented in Table 4 may improve smart farm security in different scenarios.

On the perception layer, devices could be resistant packaging to prevent some sensor incidents and autonomous system disruption. However, this can be very expensive to use for some low-cost systems or those using many sensors. If it is not possible to avoid incidents, then it is necessary to use techniques to prevent disrupted data from affecting system accuracy and influencing decision-making. Therefore, it is essential to develop security schemes to detect sensor or incidents and avoid the use of corrupt or inconsistent data. On the other hand, Autonomous Tractor is robust equipment that requires more precision and reliability. The tractors have a structure to support the inclusion of tamper-resistant boxes. Thus, it is possible to prevent a malicious employee or a commercial competitor from modifying or damaging these subsystems, for example.

GPS is an essential component of many autonomous systems, whether tractors, drones, or UAVs, and requires security to prevent threats that affect their accuracy [53,54]. Therefore, it is necessary to invest in mechanisms to protect the GPS used by autonomous systems. Violations of the GPS can result in significant physical damage to the Autonomous System, the crop, or the farm. Similarly, manufacturers of these systems must create strategies to protect the remote control system, including, but not limiting to, features such as data encryption and access control.

Irregular measurement, sensor weakening, optical deformation, and signal disruption could trigger inconsistent data resulting in incorrect decision-making. Usually, it is not possible or quite difficult to avoid such threats, but it is necessary to prevent inconsistent data from propagating through the system. Inconsistencies can be misinterpreted as attacks and inadequately handled by security systems. Thus, it is essential to identify both attacks to the system, Sensor Weakening, Irregular Measurement, Optical Deformation, and Signal Disruption to prevent the system from generating or using incorrect data that makes the system operate unreliably. Some solutions designed for errors, faults, and failures detection, such as those proposed by Ref. [55,56], could be adapted for this purpose.

Table 4
Security resources to improve security in smart agriculture.

Security resources	IoT Resource	Security threats
IDS	Cloud, gateway	DoS/DDoS, autonomous system hijacking, forged control for actuators, gateway-cloud request forgery, forged measure injection, flooding, XSS attack, SQL injection, infiltration, port scan, backdoors, worms, routing attacks, and others cyberattacks
Anomaly detection system	Data, services	Random sensor incidents, autonomous system disruption, optical deformation, irregular measurement, sensor weakening, gateway-cloud request forgery, forged measure injection, data transit attacks and others cyberattacks
Cryptography	Data, communication link	Forged measure injection, false data injection, eavesdropping, traffic interception, man-in-the-middle, data capture
Authentication	Services, devices	Forged control for actuators, gateway-cloud request forgery, fake node, forged measure injection, false data injection, advanced persistent attack, malicious scripts, unauthorized access
Access Control	Services, devices	Unauthorized access
Firewall	Cloud, gateway	Unauthorized access
Anti-virus/ malware	Cloud	Phishing, virus, worm
Specialized solutions	Applications, services, protocols	Node capture, autonomous system hijacking, routing attacks, sleep deprivation, signature wrapping
Open Issue		Booting

Other preventive measures include the use of big data algorithms to filter data [57], and Intrusion Detection Systems (IDS) to detect data intruders. However, including IDS in smart farming can be challenging as there is usually no IT department to manage the system, and the farmer does not have the technical knowledge to maintain this resource. Therefore, IDSs developed for Agriculture 4.0 need to be transparent, as far as possible, and easy to manage. Besides, most IDSs analyze network traffic patterns [58,59], which may be efficient in identifying DoS/DDoS, forged control for actuators, gateway-cloud request forgery, forged measure injection, and other network-bound attacks but is inefficient in identifying failures, data noise, and false data injection. For these threats, it is possible to use a set of strategies, such as anomaly detection, encryption, and authentication.

Some attacks require additional preventive measures. For example, integrity verification protocols [32] or schemes capable of identifying malicious nodes [60,61] could identify or mitigate autonomous system hijacking, node capture attacks. Systems designed for low power consumption networks may detect sleep deprivation [62]. Artificial intelligence algorithms and machine learning could discover forged control for actuators, gateway-cloud request forgery, forged measure injection, and false data injection [63]. Solutions like XPath and FastXPath can mitigate signature wrapping attacks [48].

Authentication services applied to devices and services at all layers can make it difficult or limit forged control for actuators, gateway-cloud request forgery, forged measure injection, and prevent unauthorized access. The edge is the middle element, and it becomes a critical security point, which needs strict access controls, and schemes to avoid false data injection. However, the current access control systems may not be efficient in the context of smart agriculture. Access controls that require human intervention are impractical in intelligent agriculture because of the characteristics of the machines and users involved. For example, end-user authentication may use user and password-based or biometric schemes. Key-based access schemes could be feasible for systems that include up to a hundred devices or services, as long as they do not require periodic modification. However, some solutions may incorporate more features or demand periodical key updating to achieve an adequate level of security. The large number and variety of devices used by smart farming require new authentication schemes to manage them by the user [37,64], who usually does not have the technical knowledge to manage authentication services. New authentication schemes must be transparent to the user, lightweight to operating on constrained devices, and efficient.

Gateways must have security features to prevent unauthorized remote access and control by malicious agents. Barriers like firewalls, Intrusion Prevention Systems (IPS), authentication, and access control schemes can be useful, but gateways have restricted resources, requiring lightweight and efficient controls [6,37]. Some gateways are more restricted, making it impossible to use most security mechanisms, which makes this task even more challenging. Others have more computational resources and include a small operating system, limited processor, and little memory. The software developed for these devices should be lightweight and easy to manage to be operated by farmers. Once the gateway accesses many resources and devices, and intermediates communication between the perception and cloud layers, it is a critical element in the smart system and compromising it may affect the whole system.

Traditional cryptographic schemes may be unsuitable in smart systems. The perception layer has constrained devices that do not have the memory, processing power, and energy to compute traditional

algorithms [64]. Encryption is an efficient tool to minimize attacks such as traffic interception, data theft, and sniffing and may be used to hinder attacks such as forged measure injection. This tool can provide reliable data transfer between perception layer devices and the gateway. However, the use of cryptography in intelligent agriculture requires new encryption schemes that are lighter and more efficient than those currently in use.

DoS attacks may affect all services and devices in the system. The perception layer does not have the computational power to run intrusion detection systems. Therefore, firmware should prevent excessive requests from draining system resources. Edge services must accept a limited amount of connections to avoid delays and service disruption. Furthermore, IDSs or anomaly detectors designed for the edge may provide a way to mitigate such attacks. These detectors may identify several threats such as jamming and false data injection [65], malicious devices [66,67], and several routing attacks [68–70]. The cloud could use robust security schemes to mitigate DoS, such as traditional IDSs or anomaly detectors, while configuring services to prevent them from being affected by an excessive amount of requests, both from the system itself and the Internet.

Communication between devices could use one or more technologies, such as LoRa, LoRaWan, Sigfox, Zigbee, and LTE. Some standards allow connecting devices over wide areas, simplifying management and reducing installation and maintenance costs. However, only these features are not enough to guarantee data transmission security. Technologies that support some level of encryption can maximize data transmission security, reducing the risk of traffic interception.

Networks operating over TCP/IP, whether in the perception, edge or cloud, could maximize communication security using protocols lighter and more flexible than HTTP. The HTTP protocol used on the traditional Internet is not suitable for systems such as smart farming because it is computationally complex, incurs an enormous overhead, and is potentially insecure [7]. There are several alternative protocols such as MQTT, SMQTT, CoAP, XMPP, UPNP, AMQP, M3DA, DDS, JMS, and JavascriptIoT. These protocols were developed for industrial communications or IoT and are more suitable for smart agriculture. Some of them have cryptography support, appropriate for networks that have no secrecy in the communication layer. It is important to emphasize that, even if the sensors' data are not sensitive, the system usually exchange private information over the network, such as identifiers and access credentials. Any sensible data transmitted over the network requires secure communication.

The application layer should have more security resources because of the Internet connection. Robust and rigorous access control is essential to prevent unauthorized access and remote control of services and applications. In the cloud, it is imperative to add features such as firewalls for perimeter protection, antivirus, and antiphishing to reduce risks with phishing, malicious scripts, and viruses/worms. Cloud services must restrict connections to other services or users as much as possible to prevent data leakage and denials of service. Using microservices favors environment security if properly configured.

In summary, edge and gateway protection schemes should include features such as compatibility, low resource consumption, and effectiveness. The identity management system must be transparent to end-user and able to work with numerous and different devices, protecting the devices and services. Data must be protected at all stages to ensure system reliability and efficiency. However, system constraints require light and efficient algorithms. The cloud can use security schemes developed for the traditional Internet since this layer has the necessary computational resources for its execution.

6. Conclusion

The agricultural methods modernization is essential to increase production rates and preserve natural resources. Smart agriculture can enhance farming tasks by providing efficient control of actuators, optimizing utility and resource use, managing production, maximizing profit, and minimizing costs. However, to achieve this goal, smart systems must include more computational capabilities, such as edge computing, handling massive data, artificial intelligence resources, and security features. Security requires special attention as constrained devices generate a large volume of data and forward them to the gateway or the cloud. The farming system must protect the data from the detection through to decision-making and storage.

Although many security threats can affect agricultural systems, they still incorporate a few security resources. Possibly this is because these solutions are still in their early stages of development. Most times, there are only automation resources implemented, and these have few computational resources. Thus, security features are not yet on the list of system requirements. However, reaching an additional level of smart farming demands solutions with security mechanisms that give them enough reliability and accuracy to implement these systems on a large scale. As smart farming creates an extra set of challenges, it also presents fresh research opportunities both in security and in other areas of computer science.

Declaration of competing interest

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

References

[1] United Nations, Department of Economic, Affairs Social, Division Population. World population prospects 2019: highlights. 2019.
[2] Nation United. Sustainable development goals. https://sdgs.un.org/goals; 2017.
[3] Food and Agriculture Organization of the United Nations - FAO. Strengthened global partnerships needed to end hunger and malnutrition. 2019. http://www.fao.org/news/story/en/item/1194310/icode/.
[4] Trendov NM, Varas S, Zeng M. Digital technologies in agriculture and rural areas - status report, Tech. Rep., Nations. Rome, Italy: Food and Agriculture Organization of the United; 2019.
[5] OECD. Food, A. O. Of the united nations, OECD-FAO agricultural outlook 2020-2029. 2020. https://doi.org/10.1787/1112c23b-en. https://www.oecd-ilibrary.org/content/publication/1112c23b-en.
[6] Varga P, Plosz S, Soos G, Hegedus C. Security threats and issues in automation IoT. In: IEEE international workshop on factory communication systems - proceedings, WFCS, IEEE, trondheim, Norway, ISBN 9781509057887. p. 6. https://doi.org/10.1109/WFCS.2017.7991968}.
[7] Hassija V, Chamola V, Saxena V, Jain D, Goyal P, Sikdar B. A survey on IoT security: application areas, security threats, and solution architectures, vols. 1–1. IEEE Access; 2019. ISSN 2169-3536.
[8] Olson D. Agroterrorism: threats to America's economy and food supply. https://leb.fbi.gov/articles/featured-articles/agroterrorism-threats-to-americas-economy-and-food-supply; 2012.
[9] Ózvvári L, Kasza G, Lakner Z. Historical and economic aspects of bioterrorism. In: Management, organizations and society; 2017. p. 179–86. https://doi.org/10.18515/dBEM.M2017.n01.ch18. chap. 18, http://real.mtak.hu/39950/1/Management_Organizations_and_Society-Agroinform-2017jan08-DOI_CrossRef-Chapter_3.2.pdf.
[10] Monke J. Agro-terrorism: threats and preparedness, tech. Rep., congressional research service. 2008 {March12,2007}.
[11] Khelifa B, Amel D, Amel B, Mohamed C, Tarek B. Smart irrigation using internet of things. In: 4th international conference on future generation communication technology, FGCT 2015. Luton, UK: IEEE; 2015, ISBN 9781479982660. p. 91–6. https://doi.org/10.1109/FGCT.2015.7300252}. ISSN 2377-262X.
[12] Sales N, Remedios O, Arsenio A. Wireless sensor and actuator system for smart irrigation on the cloud. In: IEEE world forum on Internet of things. Milan; Italy: WF-IoT, IEEE; 2015, ISBN 9781509003655. p. 693–8. https://doi.org/10.1109/WF-IoT.2015.7389138. ISSN 0954-4089.
[13] Goap A, Sharma D, Shukla AK, Rama Krishna C. An IoT based smart irrigation management system using Machine learning and open source technologies. Comput Electron Agric 2018;155:41–9. https://doi.org/10.1016/j.compag.2018.09.040}. ISSN 01681699.
[14] Mahalakshmi M. Distant monitoring and controlling of solar driven irrigation system through IoT. In: National power engineering conference (NPEC). Madurai, India: IEEE; 2018, ISBN 9781538638033. p. 1–5.
[15] Nageswara Rao R, Sridhar B. IoT based smart crop-field monitoring and automation irrigation system. In: 2nd international conference on inventive systems and control, ICISC 2018. Coimbatore, India: IEEE; 2018, ISBN 9781538608074. p. 478–83. https://doi.org/10.1109/ICISC.2018.8399118}. ISSN 1472-4472.

[16] Navarro-Hellín H, Martínez-del Rincon J, Domingo-Miguel R, Soto-Valles F, Torres-Sánchez R. A decision support system for managing irrigation in agriculture. Comput Electron Agric 2016;124:121–31. https://doi.org/10.1016/j.compag.2016.04.003}. ISSN 01681699.

[17] Rajalakshmi P, Mahalakshmi SD. IOT based crop-field monitoring and irrigation automation. In: 10th international conference on intelligent systems and control, ISCO 2016. IEEE, Coimbatore; India; 2016, ISBN 9781467378079. p. 1–6. https://doi.org/10.1109/ISCO.2016.7726900}. ISSN 0018-9197.

[18] Zhao W, Lin S, Han J, Xu R, Hou L. Design and implementation of a smart irrigation system based on LoRa. In: IEEE globecom workshops. Singapore: IEEE, Singapore; 2017, ISBN 978-1-78561-238-1. p. 1–6. https://doi.org/10.1049/cp.2016.1357}.

[19] Ruengittinun S, Phongsamsuan S, Sureeratanakorn P. Applied internet of thing for smart hydroponic farming ecosystem (HFE). In: 10th international conference on ubi-media computing and workshops with the 4th international workshop on advanced E-learning and the 1st international workshop on multimedia and IoT: networks, systems and applications (Ubi-Media 2017). IEEE Inc, Beach RoadPattaya; Thailand; 2017, ISBN 9781538627617. p. 1–4. https://doi.org/10.1109/UMEDIA.2017.8074148}.

[20] Lee M, Kim H, Yoe H. Intelligent environment management system for controlled horticulture. In: 4th NAFOSTED conference on information and computer science, NICS 2017 - proceedings. Hanoi; Vietnam: IEEE Inc; 2017, ISBN 9781538632109. p. 116–9. https://doi.org/10.1109/NAFOSTED.2017.8108049}.

[21] Oliver ST, González-Pérez A, Guijarro JH. An IoT proposal for monitoring vineyards called SEnviro for agriculture. In: Proceedings of the 8th international conference on the Internet of things - IOT '18, 1, ACM New York, santa barbara; United States, ISBN 9781450365642. p. 1–4. https://doi.org/10.1145/3277593.3277625}.

[22] Thorat A, Kumari S, Valakunde ND. An IoT based smart solution for leaf disease detection. In: International conference on big data, IoT and data science, BID 2017, 2018-Janua. Pune, India: IEEE; 2018, ISBN 9781509065936. p. 193–8. https://doi.org/10.1109/BID.2017.8336597}. ISSN 13456652.

[23] Yoon C, Huh M, Kang S-G, Park J, Lee C. Implement smart farm with IoT technology. In: 20th international conference on advanced communication technology (ICACT). Korea (South), Korea (South): IEEE, Chuncheon-si Gangwon-do; 2018, ISBN 9791188428007. p. 749–52. https://doi.org/10.23919/ICACT.2018.8323908}. ISSN 17389445.

[24] Musat GA, Colezea M, Pop F, Negru C, Mocanu M, Esposito C, Castiglione A. Advanced services for efficient management of smart farms. J Parallel Distr Comput 2018;116:3–17. https://doi.org/10.1016/j.jpdc.2017.10.017}. ISSN 07437315.

[25] Minh QT, Phan TN, Takahashi A, Thanh TT, Duy SN, Thanh MN, Hong CN. A cost-effective smart farming system with knowledge base. In: 8th international symposium on information and communication technology - SoICT 2017. Nha Trang; Vietnam: ACM New York; 2017, ISBN 9781450353281. p. 309–16. https://doi.org/10.1145/3155133.3155151}. ISSN 00243795.

[26] Colezea M, Musat G, Pop F, Negru C, Dumitrascu A, Mocanu M. CLUeFARM: integrated web-service platform for smart farms. Comput Electron Agric 2018;154(August):134–54. https://doi.org/10.1016/j.compag.2018.08.015}. ISSN 01681699.

[27] Raducu IG, Bojan VC, Pop F, Mocanu M, Cristea V. Real-time alert service for cyber-infrastructure environments. In: 10th international conference on P2P, parallel, grid, cloud and Internet computing, 3PGCIC 2015. Poland: IEEE, Krakow; 2015, ISBN 9781467394734. p. 296–303. https://doi.org/10.1109/3PGCIC.2015.122}.

[28] Wongpatikaseree K, Kanka P, Ratikan A. Developing smart farm and traceability system for agricultural products using IoT technology. In: IEEE/ACIS 17th international conference on computer and information science (ICIS). Singapore: IEEE, Singapore; 2018, ISBN 9781538658925. p. 180–4. https://doi.org/10.1109/ICIS.2018.8466479}.

[29] Mekala MS, Viswanathan P. A Survey: smart agriculture IoT with cloud computing. In: International conference on microelectronic devices, circuits and systems, ICMDCS 2017. Vellore, India: IEEE; 2017, ISBN 9781538617168. p. 1–7. https://doi.org/10.1109/ICMDCS.2017.8211551}.

[30] Ray PP. Internet of things for smart agriculture: technologies, practices and future direction. J Ambient Intell Smart Environ 2017;9(4):395–420. https://doi.org/10.3233/AIS-170440. ISSN 18761364.

[31] Zhao K, Ge L. A survey on the internet of things security. In: 2013 ninth international conference on computational intelligence and security. Leshan, China: IEEE; 2013, ISBN 9781479925483. p. 663–7. https://doi.org/10.1109/CIS.2013.145}. ISSN 2316-9451.

[32] Agrawal S, Das ML, Lopez J. Detection of node capture attack in wireless sensor networks. IEEE Systems Journal 2019;13(1):238–47. https://doi.org/10.1109/JSYST.2018.2863229. ISSN 19379234.

[33] Lin J, Yu W, Zhang N, Yang X, Zhang H, Zhao W. A survey on internet of things: architecture, enabling technologies, security and privacy, and applications. IEEE Internet of Things Journal 2017;4(5):1125–42. https://doi.org/10.1109/JIOT.2017.2683200}. ISSN 23274662.

[34] Sarma R, Barbhuiya FA. Internet of things: attacks and defences. In: 2019 7th international conference on smart computing and communications, ICSCC 2019. Sarawak, Malaysia: IEEE; 2019, ISBN 9781728115573. p. 1–5. https://doi.org/10.1109/ICSCC.2019.8843649}.

[35] Syed A, Shah SH. A comprehensive security model for internet of things. Int J Comput Commun Netw 2019;1(2):38–46.

[36] Kumar SA, Vealey T, Srivastava H. Security in internet of things: challenges, solutions and future directions. In: Proceedings of the annual Hawaii international conference on system sciences. Koloa, HI, USA: IEEE; 2016, ISBN 9780769556703. p. 5772–81. https://doi.org/10.1109/HICSS.2016.714}. ISSN 15301605.

[37] Chahid Y, Benabdellah M, Azizi A. Internet of things security. In: 2017 international conference on wireless technologies, embedded and intelligent systems, WITS 2017. IEEE; 2017, ISBN 9781509066810. p. 1–6. https://doi.org/10.1109/WITS.2017.7934655}.

[38] Vasques AT, Gondim JJ. Amplified reflection DDoS attacks over iot mirrors: a saturation analysis. In: WCNPS 2019 - workshop on communication networks and power systems. IEEE, Brasília, Brasil; 2019, ISBN 9781728129204. p. 1–6. https://doi.org/10.1109/WCNPS.2019.8896290}.

[39] Kolias C, Kambourakis G, Stavrou A, Voas Jeffrey. DDoS in the IoT: mirai and other botnets. Computer 2017;50(7):80–4.

[40] Capellupo M, Liranzo J, Bhuiyan MZA, Hayajneh T, Wang G. Security and attack vector analysis of IoT devices. In: Security, privacy, and anonymity in computation, communication, and storage. Cham: Springer International Publishing; 2017. 978-3-319-72395-2, 593–606.

[41] Pundir S, Wazid M, Singh DP, Das AK, Rodrigues JJ, Park Y. Designing efficient sinkhole attack detection mechanism in edge-based IoT deployment. Sensors 2020;20(5):1300. https://doi.org/10.3390/s20051300}. ISSN 14248220.

[42] Goyal M, Dutta M, IEEE. Intrusion detection of wormhole attack in IoT: a review. In: 2018 international conference on circuits and systems in digital enterprise technology, ICCSDET 2018. Kottayam, India: IEEE; 2018, ISBN 9781538605769. p. 1–5. https://doi.org/10.1109/ICCSDET.2018.8821160}.

[43] Schulz S, Schaller A, Kohnhäuser F, Katzenbeisser S, Boot Attestation. Secure remote reporting with off-the-shelf IoT sensors. In: Computer security – ESORICS 2017, vol. 1. Cham, Oslo, Norway: Springer; 2017. p. 437–55.

[44] L. Garcia, L. Parra, J. M. Jimenez, J. Lloret, IoT-based smart irrigation systems : an overview on the recent trends on sensors and IoT systems for irrigation in precision agriculture, Sensors 20 (4).

[45] Ouaddah A, Mousannif H, Abou Elkalam A, Ait Ouahman A. Access control in the Internet of Things: big challenges and new opportunities. Comput Network 2017;112:237–62.

[46] Navas RE, Bouder HL, Cuppens N, Cuppens F, Papadopoulos GZ. Demo: do not trust your neighbors! A small IoT platform illustrating a man-in-the-middle attack. In: DHOC-NOW: international conference on ad hoc networks and wireless, september. Cham, Saint-Malo, France.: Springer; 2018, ISBN 9783030002473. p. 1–6. https://doi.org/10.1007/978-3-030-00247-3}.

[47] Stojmenovic I, Wen S. The Fog computing paradigm: scenarios and security issues. In: 2014 federated conference on computer science and information systems, FedCSIS 2014, vol. 2. Warsaw, Poland: IEEE; 2014, ISBN 9788360810583. p. 1–8. https://doi.org/10.15439/2014F503}.

[48] Gajek S, Jensen M, Liao L, Schwenk J. Analysis of signature wrapping attacks and countermeasures. In: 2009 IEEE international conference on web services, ICWS 2009. Los Angeles, USA: IEEE; 2009. p. 575–82.

[49] Benavides E, Fuertes W, Sanchez S, Sanchez M. Classification of phishing attack solutions by employing deep learning techniques : a systematic literature review. In: Developments and advances in defense and security. Singapore: Springer Singapore; 2020. p. 51–64.

[50] Guarda T, Augusto MF, Lopes I. The art of phishing. In: Advances in intelligent systems and computing. Cham, Bogots, Colombia: Springer; 2019, ISBN 9783030118891. p. 683–90. https://doi.org/10.1007/978-3-030-11890-7_64}. ISSN 21945357.

[51] Khan N, Abdullah J, Khan AS. Defending malicious script attacks using machine learning classifiers. Wireless Communications and Mobile Computing 2017 2017:9.

[52] Shurman MM, Khrais RM, Yateem AA. IoT denial-of-service attack detection and prevention using hybrid IDS. In: International arab conference on information technology (ACIT), vol. 3. IEEE, Al Ain, United Arab Emirates; 2019.

[53] Manesh MR, Kenney J, Hu WC, Devabhaktuni VK, Kaabouch N. Detection of GPS spoofing attacks on unmanned aerial systems. In: 2019 16th IEEE annual consumer communications networking conference (CCNC). IEEE; 2019. p. 1–6.

[54] Bonebrake C, O'Neil LR. Attacks on GPS time reliability. IEEE Security Privacy 2014;12(3):82–4.

[55] Di Modica G, Gulino S, Tomarchio O. IoT fault management in cloud/fog environments. In: ACM international conference on the Internet of things. New York, USA: ACM; 2019, ISBN 9781450372077. p. 1–4. https://doi.org/10.1145/3365871.3365882}.

[56] Power A, Kotonya G. Complex patterns of failure: fault tolerance via complex event processing for iot systems. In: International conference on Internet of things (iThings) and IEEE green computing and communications (GreenCom) and IEEE cyber, physical and social computing (CPSCom) and IEEE smart data (SmartData). Atlanta, USA: IEEE; 2019. p. 986–93.

[57] García-Gil D, Luengo J, García S, Herrera F. Enabling smart data: noise filtering in big data classification. Inf Sci 2019;479(2019):135–52. https://doi.org/10.1016/j.ins.2018.12.002}. ISSN 00200255.

[58] Liu L, Xu B, Zhang X, Wu X. An intrusion detection method for internet of things based on suppressed fuzzy clustering. EURASIP J Wirel Commun Netw 2018;(1).

[59] Santos L, Rabadao C, Goncalves R. Intrusion detection systems in Internet of Things: a literature review. In: 13th iberian conference on information systems and technologies (CISTI). Caceres: IEEE; 2018. p. 1–7.

[60] Dimitriou T, Alrashed EA, Karaata MH, Hamdan A. Imposter detection for replication attacks in mobile sensor networks. Comput Network 2016;108:210–22. https://doi.org/10.1016/j.comnet.2016.08.019}. ISSN 13891286.

[61] Smache M, Mrabet NE, Gilquijano JJ, Tria A, Riou E, Gregory C. Modeling a node capture attack in a secure wireless sensor networks. In: 2016 IEEE 3rd world forum on Internet of things, WF-IoT 2016. Reston, USA: IEEE; 2016. p. 188–93.

[62] Jahir Husain A, Maluk Mohamed MA. IMBF counteracting denial-of-sleep attacks in 6LoWPAN based internet of things. J Inf Sci Eng 2019;35(2):361–74.

[63] Mode GR, Calyam P, Hoque KA. False data injection attacks in internet of things and deep learning enabled predictive analytics. In: EEE/IFIP network operations and ManagementSymposium. Budapest, Hungary: IEEE; 2020. p. 1–11.

[64] Partra L, Rao UP. Internet of Things — architecture, applications, security and other major challenges. In: 2016 3rd international conference on computing for sustainable global development (INDIACom). New Delhi, India: IEEE; 2016. p. 1201–6.
[65] Fu Y, Yan Z, Cao J, Koné O, Cao X. An automata based intrusion detection method for Internet of things. Mobile Information Systems; 2017.
[66] Sohal AS, Sandhu R, Sood SK, Chang V. A cybersecurity framework to identify malicious edge device in fog computing and cloud-of-things environments. Comput Secur 2018;74:340–54.
[67] J. Pacheco, S. Hariri, Anomaly behavior analysis for IoT sensors, Transactions on Emerging Telecommunications Technologies 29 (4).
[68] Razaa S, Wallgren L, Voigt T. SVELTE: real-time intrusion detection in the internet of things. Ad Hoc Netw 2013;11(8):2661–74.
[69] Sun Z, Xu Y, Liang G, Zhou Z. An intrusion detection model for wireless sensor networks with an improved V-detector algorithm. IEEE Sensor J 2018;18(5): 1971–84. ISSN 1530437X.
[70] Sedjelmaci H, Senouci SM, Al-Bahri M. A lightweight anomaly detection technique for low-resource IoT devices: a game-theoretic methodology. In: IEEE international conference on communications, ICC 2016, vol. 6. Kuala Lumpur: IEEE; 2016.