sensors

MDPI

Review

Survey on Security Threats in Agricultural IoT and Smart Farming

Konstantinos Demestichas *, Nikolaos Peppes and Theodoros Alexakis

Institute of Communication and Computer Systems, Zografou, 15773 Athens, Greece; npeppes@cn.ntua.gr (N.P.); talexakis@cn.ntua.gr (T.A.)

* Correspondence: cdemest@cn.ntua.gr; Tel.: +30-210-772-1478

Received: 13 September 2020; Accepted: 6 November 2020; Published: 12 November 2020

Abstract: The agriculture sector has held a major role in human societies across the planet throughout history. The rapid evolution in Information and Communication Technologies (ICT) strongly affects the structure and the procedures of modern agriculture. Despite the advantages gained from this evolution, there are several existing as well as emerging security threats that can severely impact the agricultural domain. The present paper provides an overview of the main existing and potential threats for agriculture. Initially, the paper presents an overview of the evolution of ICT solutions and how these may be utilized and affect the agriculture sector. It then conducts an extensive literature review on the use of ICT in agriculture, as well as on the associated emerging threats and vulnerabilities. The authors highlight the main ICT innovations, techniques, benefits, threats and mitigation measures by studying the literature on them and by providing a concise discussion on the possible impacts these could have on the agri-sector.

Keywords: agriculture; IoT; cybersecurity; threats; security; precision agriculture; smart farming

1. Introduction

According to the latest research results of the United Nations' Food and Agriculture organization [1], the world will be in need of producing 70% more food in 2050, in comparison with today's production, in order to feed the constantly growing Earth population, estimated to reach almost 10 billion in 2050 [2]. The market size of the smart agriculture sector is also expected to significantly grow in order to address these needs, supported by the anticipated increase in the number of Internet of Things (IoT) devices employed for agricultural purposes [3].

The continuous and rapid digitization at a global level, underpinned by the progress made in Information and Communication Technologies (ICT), is a trend that deeply transforms many market sectors and has created opportunities in several areas of global economies and societies [4]. The agricultural domain has demonstrated a rapid technological growth in recent years by engaging a variety of emerging ICT solutions. Although Agriculture 4.0 is expected to be the new norm, physical threats and risks in this particular domain is a critical factor that may impede their wide-spread acceptability and adoption. Some of these threats remain traditionally the same, throughout the years, such as weather conditions, but others are associated with the vast evolution of the technological solutions. A brief and accurate list of the physical threats in agriculture is provided by Calicioglu et al. [5], whose work assumes the following classifications: (i) climate change impacts and extreme weather effects; (ii) rapid growth of world population, urbanization and aging; (iii) advanced food production systems and impacts in farmlands and farmers; (iv) pests and diseases.

The most prominent of the aforementioned physical threats for the agriculture sector throughout the years has been the weather conditions, especially in recent decades due to climate change. In this direction, there are several studies aiming to research and elaborate on this type of threat. According to

Devendra [6], the problem of climate change is global and affects both developed and developing countries. The authors of this work distinguish the following main effects of the climate change: (i) Earth will become warmer; (ii) soil moisture will decline because of increased temperatures; and (iii) sea level will continue to rise because of the frost melt down. However, although climate change is a major threat for the agricultural sector, agriculture is responsible for part of the problem too. Horrigan et al. claim that about 20% of green-house gases originate from agriculture activities [7].

The physical threats will always be one of major and unpredictable risks in agriculture but there is an upward trend in the recent decades to attempt to minimize their impact by engaging new technologies. To this end, the agricultural domain applications are taking advantage of robust and trustworthy connectivity of different types of equipment, Internet of Things (IoT) networks, and cloud computing infrastructures. For example, the development of smart and precision agriculture applications in order to reduce the existing risks and maximize the production efficiency. Those innovations are only some of the notable achievements that have come as a result of the huge growth of ICT capabilities. On the other hand, with the rapid development of ICT, significant threats of different forms that attempt to exploit security-related vulnerabilities arise as well.

Particularly, the rapid development and adoption pace of IoT has created not only many technological and market opportunities, but also a significant gap and attack surface in terms of security. Despite the fact that many research efforts have concentrated on designing network security protocols, cryptography solutions and device security, several challenges still remain, especially with respect to data integrity, service trustworthiness and the lack of metrics for device security [4]. These challenges are often hard to deal with effectively, due to their range of possible cyber and physical security threats.

Nowadays, ICT systems are the number one cyber-criminal means worldwide for stealing money, intellectual properties, business secrets and other assets. The associated term of cyber-security refers to the combination of techniques, skills and processes in order to ensure a high degree of protection for network, computers, programs and data, against malware, attacks, damage and unauthorized access. In this context, on a daily basis, new types of cyber threats are emerging, including ransomware, endpoint attacks, phishing, third party attacks, supply chain attacks, artificial intelligence and Machine Learning-driven attacks, crypto-jacking, cyber physical attacks, state sponsored attacks, IoT attacks, threats to smart devices, attacks on connected, semi-autonomous or autonomous, vehicles [8]. The significant increase in terrorism, financial devastation and physical injuries or deaths are the result of these types of cyber-attacks. The aforementioned types of threats, alongside the existing physical hazards in agriculture [9], form the basis for creating models that can be used to detect system and network vulnerabilities. The application of cyber tools and (cyber) physical infrastructures as well as of new stronger cybersecurity measures and techniques are of the utmost importance in order to encounter these attacks successfully.

This paper is an extensive literature review of the benefits, the security issues and threats as well as theeffective mitigation strategies posed by the introduction of modern ICT solutions in the domain of agriculture. Advantages, security issues, cybersecurity and IoT-related threats as well as mitigation measures are organized and presented into distinct sections. The remainder of this paper is structured as follows: Section 2 presents an overview of ICT applications and benefits in the agricultural domain; Section 3 focuses on the vulnerabilities, risks and threats in Agriculture 4.0; Section 4 focuses on mitigation strategies and techniques concerning the risks presented in the previous section and finally, Section 5 concludes the paper.

2. State-of-the-Art ICT in Agriculture: Definitions, Technologies, Applications and Benefits

Over the last years, the role of ICT and IoT in agriculture is increasingly important [3]. ICT and IoT consists the backbone of the fourth industrial revolution [10], contributing into sustainable growth and development, especially in the agricultural sector of developing countries [11]. The demand for greatly increased productivity and efficiency, at a global level, in conjunction with the need to decrease costs and increase the occupation time, from the employers' point of view, render these technologies an attractive choice for farmers and companies in the agricultural domain. The integration of IoT into agriculture has resulted in a number of notable applications [12], such as the analysis of crop productivity, crop health monitoring, soil nutrition management, rainfall monitoring, water management and pest infestation monitoring [3]. Systems and IoT applications, such as decision support tools, automated irrigation, frost protection, remote monitoring and fertilization systems, are some typical examples of IoT-based tools that can be deployed and used in the agricultural sector [12,13].

This new form of agriculture which engages ICT and IoT technologies is often denoted as Precision Farming (PF) or Precision Agriculture (PA). Precision Farming or Precision Agriculture, according to Wolf and Wood, is a technological innovation which takes full advantage of the Global Positioning System (GPS) and digitalization of agriculture measurements so as to enhance the accuracy and efficiency of crop production in terms of fertilizer, pest and water management [14]. From this early definition of PA in 1997, the technology evolved rapidly together with the concept of PA itself. Nowadays, Precision Agriculture can be applied and presented also as satellite farming or site-specific crop management (SSCM). PA or SSCM is a farming management concept based on gathering measurements, analyzing and responding to inter- and intra-field variability in crops or livestock [15].

The goal of PA-related research is to design a decision support system (DSS) for the entire farm management, capable to maximize the outcomes by minimizing the inputs and preserving resources [16–18]. PA engages a plethora of IoT and electronic sensors for monitoring and controlling the production. Furthermore, until a few years ago, the agricultural domain was typically considered as a heavily mechanized, offline industrial sector. The PA concept came to change that, as there is an increasing trend to move agriculture online. More and more crop and livestock farms interconnect their systems, making them remotely accessible, so that they can easily be monitored and controlled [19]. As already highlighted, PA adopts digital technologies to achieve its purposes [20]. According to the European Commission, object identification, georeferencing, measurement of physical and chemical parameters, satellite navigation, connectivity, data storage and analysis, process automation and vehicle driving are currently the most adopted technologies of PA [20,21].

Thanks to IoT, farmers can get access to collected data in real time and without human intervention. Due to the evolution of technology, the size and shape of sensors is getting smaller and more sophisticated, while in parallel the general cost of the IoT devices is getting lower. The combination of daily-life tools, such as smart phones and/or laptops, with IoT technologies (spanning sensors, gateways, network and middleware devices, as well as additional components for various purposes, e.g., low altitude air-borne hyperspectral imaging system) [22] lead the innovation in the agricultural sector and establish a new domain of interest, often referred to as "Smart Farming". The ambition of the aforementioned innovations is to confront the industry problems that have occurred over recent decades since the first agriculture revolution in 1970 [3,11].

Some well-known areas where the integration and usage of IoT in agriculture has been applied, are shown in Table 1:

Table 1. Overview of Internet of Things (IoT) usage and integration areas and corresponding studies.

Area	Studies
Continuous land monitoring	[3,23–27]
Water management	[1,28–30]
Monitoring and reporting of crop growth	[25,31–35]
Identification and management of soil characteristics	[36–40]
Detection and recognition of diseases in crops and/or plants	[41–45]
Enhanced food preservation and quality control	[46–49]
Smart livestock	[50–53]

Based on the above applications and analysis of IoT and ICT in agriculture, there are several benefits from the integration of IoT in the agricultural sector. Thus, according to [12,13,54–57], the benefits from IoT and ICT integration in the agri-sector can be summarized as follows:

- Crop monitoring, decreasing the overall costs;
- Logistic and qualitative traceability of food production combining decision making processes with real-time data for reducing the waste of inputs and overall costs;
- Capitalizing on Big Data resources, at hardware and software level, establishing new agriculture communities in urban and rural areas;
- Generating novel business models in the sector, creating a new retailer–consumer relationship;
- Automatic irrigation systems development that adjust their operations based on the humidity, temperature and soil moisture values which are retrieved through the embedded sensors;
- Collection of environmental parameters, in an automatic way using IoT, which are usable for further analysis;
- Big Data analytic processes and tools for enhancing productivity using decision support systems.

New standards, in combination with the rapid technological advance, lead the agricultural sector, as well as many others, in a new promising future [58]. For agriculture, the main focus of this evolution is the development and innovation of processes that use fewer resources with better production results, keeping in mind that food production is of significant importance for the entire human population.

As digital transformation progresses in the agricultural industry, many businesses face new emerging challenges posed by cyber criminals, who are looking for sectors and organizations that are digitally exposed and might not have built adequate security systems and defensive mechanisms [59]. With the agricultural sector getting more and more dependent on ICT systems, new emerging vulnerabilities, threats and risks, which are described in more detail in the next section, also arise.

3. Security Threats in Modern Agriculture

The rapid evolution and the use of smart communication technologies [60] as well as the integration of IoT in addition to the digitization and automation of business, bring new risks and dangers in terms of ICT security in the global market [61]. Potential attacks in various different smart agricultural systems can lead to serious security issues in the dynamic and distributed cyber-physical environment [60,62]. These types of threats and attacks can result in severe disruptions of interconnected businesses. Furthermore, in the heavily mechanized landscape of agriculture, smart technologies and remote administration used in PA and smart farming are something brand new for its stakeholders, with most of the new threats in this specific domain being strongly connected with similar threats that exist in other industries [63]. These threats are mostly related to cybersecurity, data integrity and data loss [64,65]. In addition, because of the fact that the PA sector utilizes heavy machinery connected online, there are many emerging vulnerabilities that can potentially lead to disastrous consequences [65].

The next paragraphs of this section offer a detailed approach on the security threats met in modern agriculture. The extensive literature review performed in this section is focused on the cybersecurity

and IoT-related threats in agriculture, which are nonetheless interwoven strongly with PA, Agriculture 4.0 and smart farming [64].

3.1. Equipment and Data Vulnerabilities, Risks and Threats in Modern Agriculture

As discussed earlier, the agricultural sector is directly influenced by harsh environmental conditions, such as high temperatures, humidity, rain, winds and other phenomena, which can cause serious damage to electromechanical equipment [66]. All these sensors are susceptible to malfunction, making it possible to provide false measurements and commands which may lead to production disaster [67]. In addition to monitoring and controlling sensors, the wireless networks used in the agri-sector, which are mainly low power such as LoRaWAN, Zigbee, etc., can be affected by the harsh environmental conditions, such as temperature, humidity, obstacles and human presence as well, an impact that leads in turn to communication and data loss [68–70]. Moreover, sensors as well as network devices in many cases are physically accessible. This consists a major risk for farmlands, since anyone with malicious intentions can access them either to damage or compromise them in order to make them malfunction [71].

The collected data from IoT sensors and other machinery in agriculture are now transferred online, which constitutes another potential security risk as well. Data privacy and ownership are a major security issue within the agricultural sector [72], as farmers can suffer serious damage, both in financial and personal terms, in the case of a data breach. The threats to confidentiality are classified into four discrete categories in [65], namely: (i) intentional data theft through smart applications and platforms that are not compliant with confidentiality standards; (ii) internal data thefts from a stakeholder in the supply chain in order to damage an agri-business or a farmer; (iii) unethical data sale to minimize profits for farmers or to damage them; (iv) unattended foreign access to sensitive and confidential data through equipment such as drones, sensors, cameras, in order to use them against farmers or to compromise public security [64,73].

In the light of the above, since PA is mainly focused on automated data collection, analysis and decision-making, it is of utmost importance to ensure the integrity and availability of data [64,65,67,74]. Falsification of data, either intentional or unintentional, can have severe consequences, especially since this can affect the decisions made by artificial intelligence (e.g., Machine Learning) algorithms and automation systems leading to the disruption or even the destruction of production [75]. Additionally, false data could lead to dangerous conditions both for the agri-products and human health, possibly resulting in the overuse of fertilizers or pesticides which may travel from the farm to the plate [65].

Alongside the integrity issue, the availability of data and equipment holds a major role in modern agriculture. An elaborate survey for PA in Australia [76] concluded that the majority of farmers make use of GPS systems and are, thus, susceptible to malfunctions that can lead to missing routes for autonomous vehicles and drones and, consequently, to problems in the cultivation procedure [76]. Through this example, it is clear that, in time-precise sectors such as agriculture, the availability of the equipment and systems utilized by farmers is critical [64,65,77].

The aforementioned risks, vulnerabilities and threats exist in every agriculture application which engages modern ICT and IoT technologies. Complementing the aforementioned threats, the next subsection is mainly focused on cybercrime activities and exploitable vulnerabilities in ICT technologies and provides a more detailed and elaborate presentation of the dangers and their causes in terms of cybersecurity in the agri-sector.

3.2. Cybercrime and Cybersecurity in Agriculture

Cybercrime is defined as a crime where a computer or a smart device is the object of the crime and/or is used as a tool to commit an offense. A cybercriminal may use a device to access a user's personal information, confidential business information, government information, or disable a device [78]. Selling or eliciting the abovementioned information online is also considered as a cybercrime. Currently,

cybercrime is a worldwide criminal activity and the persons (attackers) that get involved are highly motivated to acquire new technologies, discover and identify new or already existing vulnerabilities and breaches, in order to reach their target and perform an unethical action [60,79,80].

An enormous amount of heterogeneous types of data is transferred through the networks using connected smart devices. The increasing accessibility to smart technology also means that there are multiple access points within users' homes, offices and any other kind of application or space for hackers to exploit. While law enforcement attempts to tackle this growing issue, crime numbers continue to grow, taking advantage of the anonymity of the internet [78]. Hackers can gain unauthorized access to these types of devices by discovering vulnerabilities at many different layers of ICT systems, such as middleware, network or application layer. It is important for agricultural stakeholders to recognize and protect the ICT environment, as well as to ensure adherence to the current privacy regulations, taking into account the inherent risks of ICT and IoT systems [80].

As an answer to cybercrime, cybersecurity has been an ever-evolving area in recent decades and it will continue to be such, as our world shifts to become more and more online. Individual organizations are highly dependent on supply chains and networks [81], which makes it extremely difficult to manage risks due to the fact that every type of defense is only as strong as its weakest link. Additionally, the existence of one or more possible weaknesses in a third-party application could also put the entire adopted system at risk [82]. Furthermore, even larger firms or companies may have difficulty to recruit the necessary experts, in order to design and develop an adequate defense system against cyber threats and attacks. The larger an organization is, the greater the possibilities are to find weaknesses somewhere in the supply chain [81]. Such weaknesses can provide an access point for cyber criminals, enabling them to launch illegal, devastating attacks on critical infrastructures, such as water or power systems [82–85].

Nowadays, a cyber-attack to an agricultural or food company is more feasible as the digitization and the use of many devices that are connected to the internet, offer more opportunities to the potential (cyber)criminal in a domain that previously was too difficult to strike or too distant to physically approach [61]. Hence, a possible cyber-attack or security issue in an agricultural company could result in significant human or financial consequences. This suggests that relevant security challenges, arising from the massive and daily use of IoT technology as well as the rise of agroterrorism, demand sufficient attention, security planning and counter measures [61].

Many types of cyber-attacks can cause significant financial and security implications in the agricultural sector, as the majority of system operations are network-based, and on many occasions may not be secured from cyber-threats [86]. Complex combinations of network systems, and especially the dependencies of such systems, amplify vulnerabilities to possible threats by creating possibilities for various cyber threats and causing a cascading effect to materialize. According to Jahn et al. there are five main factors that strengthen these risks in the agriculture sector: (i) the increasing farm consolidation and the associated heavy reliance on technology; (ii) the vertical integration across the food supply chains, where producers may directly trade products and execute processes; (iii) the absence of compliance with food safety, traceability and insurance requirements and regulations; (iv) the increasing dependence of components among food-related systems in smart markets, which leads to greater exposure to failures and faults and (v) the lack of systematic surveillance of food-related systems, social media and markets in a secured, dynamic and near real-time manner, in order to detect significant digital and security issues, which might be the cause of important information breaches and system flaws [87].

This increased risk of cyber-attacks can lead to various ways through which these attacks can impact the agricultural domain. Duncan et al. in [84] classify these ways as: (i) disruption of delivery; (ii) interception of confidential information; (iii) alteration of formulations; and (iv) tampering threats. Obviously, these threats are strongly attached to the adoption and the usage of technological advances in agriculture and food industries. Bogaardt et al. as well as Cooper et al. recognize the main technological advancement areas which are widely adopted in the agri-sector and consist susceptible points for malicious cyber-attacks as follows [86,88]:

- Wireless connections (e.g., Wi-Fi);
- Radio Frequency Identification (RFID);
- Air, soil and crop and infrastructure sensors;
- Unmanned Aerial Vehicles (UAVs), e.g., drones;
- Automation systems focused on PA (e.g., Real Time Kinematic Technology);
- Mobile devices (e.g., laptops, mobile phones, GPS trackers);
- Vertical farming and smart agriculture;
- The combination of biotechnology and nanotechnology with Artificial Intelligence (AI).

The agricultural sector is mainly interwoven with people's nutrition so every risk, vulnerability and threat represents a major risk for public health. Cybersecurity is, in general, an open and evolving research field and when it comes to the agricultural domain and its application, its significance is of utmost importance. The survey conducted for cybersecurity in agriculture and its threats can be summarized in Table 2.

Table 2. Overview of possible attacks per security aspect in agricultural cybersecurity.

Security Aspect	Examples of Attacks	Agriculture Consequences	Studies
Privacy	Physical Attack Replay Attack Masquerade Attack	The collection of information regarding the type and possible usage of devices concerning agriculture projects. These security leaks can be used in order to get access to infrastructure and production standards as well as getting privacy data and compromising the privacy of the system. Theft and vandalism purposes can be the outcome of a possible violation of privacy.	[62,78,79,89–92]
Confidentiality	Tracing Attack Brute Force Attack Known-Key Attack	The usage of various communication devices in a smart farming or an agriculture system based on ICT can outcome into data travelling through several interconnected devices and protocols from source to destination. Possible confidentiality problems can lead to the persistence, on many occasions, of loss of privacy and data or information breaches. The unauthorized access to important data as a result of the confidentiality loss could lead to theft of key information and also cause serious threats over the involved agriculture system users' confidential information.	[29,62,79,93,94]
Integrity	Forgery Attack Man-In-The-Middle Attack (MITM) Biometric Template Attack Trojan Horse Attack	As a result of possible unauthorized or improper changes in the trustworthiness of data or resources, information between agriculture ICT or smart farming systems can be no longer reliable or accurate. The transmitted information data between the devices and/or the people/farmers/stakeholders that are involved in an agriculture business or even a process can lead to possible financial or authentication frauds due to the lack of the assurance that the information is sufficiently accurate for its purpose.	[62,79,91,95,96]
Availability	Denial of Service (DoS) attacks (SYN Flood, Ping of Death, Botnets)	A smart farming environment is meant for real or near-real time operations in order to keep a real-world impact. An attacker can suspend the activities of the installed smart farming network or even establish the services unavailable to the farmers. The lack of availability of the provided services can lead to business disruption, possible loss of customer's confidence and revenue.	[62,79,92,97,98]
Authenticity	Attacks against Authentication (Dictionary attack, Session Hijacking, Spoofing)	Authenticity ensures the authentication of certain information provided from a valid/authorized source. Forged attackers' identities can mimic legal/authorized persons and gain access to the smart farming system. Possible results can be the data breach/loss and/or alternation, service unavailability, loss of devices connectivity or even smart farming agriculture system corruption and/or destruction.	[62,79,99–101]
Non-Repudiation	Malicious Code Attack Repudiation Attack	During the authentication process, a commonly known service that provides proof of the integrity as well as the origin of data, both in an unforgeable relationship, and can be verified by any third party at any time with high assurance and genuineness, is non-repudiation. The repudiation of information allows an attacker to repudiate all the power consumption, generated information and production processes of an agriculture ICT system, which can lead to a situation of refusing services, authentication information or data transmissions, through the nodes of the system.	[62,79,102,103]

3.3. IoT Vulnerabilities, Risks and Threats in Agriculture

The main cybersecurity threats were extensively presented in the previous subsection. Every and each of these threats are also applicable to IoT technologies and consist a threat for the associated agricultural applications. In the following paragraphs, a more detailed and focused survey on the IoT domain and its threats in agriculture is presented. IoT technologies are widely adopted by agricultural stakeholders in every part of the world and in every phase from production to supply chain. Thus, their role and their susceptibilities and risk are of high importance and worthy of study.

IoT technology is consisted of four major systems, which render the communication between two endpoints (nodes) feasible. An IoT system technology is composed of: (i) the sensing technology; (ii) IoT gateways; (iii) cloud server/data storage and (iv) remote control using mobile applications.

Current along with new risks and vulnerabilities come along with new as well as older types and architectures of IoT systems in agriculture. Such vulnerabilities can be attributed to hardware and software issues of the IoT devices, communication protocols, as well as data storage and processing solutions (e.g., in cloud infrastructures, data centers and smartphones) [2,11]. A brief but accurate categorization of the main causes of low security in IoT include, according to [2,104,105], the following:

- Unpatched firmware and/or extended use of default passwords, which allow for compromising the devices within an IoT network;
- Limited computational resources of smart devices, which hinders the implementation of complex cryptographic algorithms, due to the efforts of vendors to reduce the costs of their products in a competitive environment;
- Vulnerabilities in the communication protocols used by smart devices (e.g., ZigBee, Bluetooth);
- Low security level of the old version of the Wi-Fi Protected Access (WPA) protocol, which is still used in many cases;
- Search engines that can be used for executing passive vulnerability detection;
- The danger of organizing millions of smart devices in a powerful botnet (e.g., Mirai), due to the relatively easy detection of vulnerabilities by means of internet scanning;
- General lack of attention to the security of smart devices.

Concisely, the overall lack of security of smart devices is caused by the general absence of standards or mandatory official recommendations for the security of IoT. The lack of legislative acts that regulate the responsibility between the manufacturer, the seller and the client, as well as the existence of a diversity of devices, combined with the need for costs savings, jointly affect the security of IoT [2,78].

Finally, IoT vulnerabilities, risks and threats can be classified using several different criteria. These threats apply to IoT applications in general, also including the agricultural domain. Firstly, there are two main classification categories of security threats in IoT applications in the agricultural sector, namely: (i) internal vs. external threats; (ii) passive vs. active threats [79]. Another interesting classification of threats for IoT follows a layer-based approach. Hassija et al. [22] propose that each of the following layers combines diverse technologies that bring a number of possible vulnerability issues, breaches and/or security threats. The architecture of IoT depends upon five distinct layers: (i) the application layer; (ii) the middleware layer; (iii) the internet layer, (iv) the access gateway layer and (v) the edge technology layer. Taking into account the layered architecture of a typical IoT system and the diverse technologies that it adopts, there is a significant number of possible vulnerability issues, security breaches and threats, which can result in major issues and/or problems for the organizations into the agriculture domain. Possible attacks on each layer of a typical IoT system are classified as depicted in Table 3:

Table 3. Overview of security threats in agriculture across different IoT layers.

Layer	Security Threats	Smart Farming Effects	Studies
Application	Data Thefts Access Control Attacks Service Interruption Attacks Malicious Code Injection Attacks Sniffing Attacks Reprogram Attacks	The top of the stack in the already mentioned IoT layer architecture. Possible effects or problems could be considered the lack of the delivery of services between the respective users from various domains such as farmers, retailers and/or other stakeholders. Accessibility problems for the involved users and lack of security and privacy are also major issues.	[62,79,106–108]
Middleware	Man-In-the Middle Attack (MITM) SQL Injection Attack Signature Wrapping Attack Cloud Malware Injection Flooding Attack in Cloud	This layer operates in two-way mode. More specifically, this layer stands between (in the middle) of the application and the hardware layer and also acts as an interface between them. Major problems that come as a result of attacks on this layer can affect data and/or device (nodes installed into the agriculture infrastructure) management and other types of issues such as device information discovery, access control by the users and data analysis as well.	[62,79,107,109]
Internet	Phishing Site Attack Access Attack DDoS/DoS Attack Data transit Attacks Routing Attacks	The most crucial layer concerning the establishment of the communication between two distinct endpoints, such as device-to-device, device-to-cloud, device-to-gateway and back end data-sharing. In case of a failure the communication is being disrupted and the ICT system is, practically, out of service. Improper communication services and/or lack of automatic updates could lead to privacy concerns among the users' private information (e.g., access credentials)	[62,79,107,110]
Access Gateway	Secure on-Boarding Extra Interfaces End-to-End Encryption Firmware Updates	Access GW layer contributes to the handling of the very first data as well as to bridging the gap between the client (farmers, stakeholders, retailers) and the end point (node or device). Messages routing, identification and subscribing problems between the smart farming nodes could be possible outcomes to the client side concerning the final form of the received message. This message may also include the desired information as well as lack of transport encryption/integrity verification, so sensitive data could easily then be intercepted.	[62,79,107,108,111]
Edge Technology	Node Capturing Malicious Code Injection attack False data Injection Attack Side-Channel Attacks Eavesdropping and Interference Sleep Deprivation Attacks Booting Attacks	This layer is consisted of the majority of hardware parts (e.g., sensors, Radio-Frequency Identification (RFID) tags) and has a significant role for the communication between the involved devices as well as the data collection within the network and the servers that are deployed on the installed ICT smart farming system. Possible attacks on the entities of this layer could lead to important problems of monitoring or sensing various phenomena. Additionally, information theft and/or tampering could also be possible results.	[62,79,107–109]

4. Mitigation Measures and Strategies for Security Threats in Agriculture

In the previous section, the main vulnerabilities, risks and threats in agriculture concerning the adoption and utilization of state-of-the-art technology, techniques and tools were discussed. Thus, it is of high importance for agriculture stakeholders to invest and adopt measures and strategies which can mitigate the risks and avoid disastrous consequences. Nevertheless, despite the increasing concern related to cyber agroterrorism, a large number of companies are still not investing sufficiently in the improvement of the cybersecurity protection of IoT and ICT systems [61]. Although, many larger corporations and industries have invested in safe and efficient security systems and measures, smaller agricultural companies and farms often lack in terms of financial resources, time and plans to design and implement adequate measures and/or systems against possible cyber-attacks [83].

Agriculture stakeholders must focus on the possible attacks featured in detail previously such as: data privacy and integration, risk management (also in relation to third parties), integrity protection, non-repudiation, trusted origin, access control, scalability and robustness in terms of points of failure [62,79,80,112] in order to enhance cybersecurity. To address these challenges, some emerging architectures embedded blockchain technology in order to ensure data privacy and integrity, addressing

space, fault tolerance, trusted origin and accountability, access control, removal of third-party risks, prevention of illegal use of personal (private) data, as well as protection of the sharing of IoT network information [112,113]. In summary, prior research for the enhancement of security and privacy in IoT and ICT applications in the agricultural sector falls under six main categories according to Ferrag et al. [79]: (i) privacy-preserving solutions; (ii) data integrity solutions; (iii) authentication solutions; (iv) access control solutions; (v) data confidentially solutions; and (vi) blockchain-based solutions and consensus algorithms.

Cybersecurity and mitigation measures and strategies is a very wide, open and rapidly evolving research field. Every day new threats and risks are emerging and thus new countermeasures become available. Table 4 features a list of countermeasures that can be taken against security aspect threats and IoT layer threats as those described in Tables 2 and 3.

Table 4. Mitigation countermeasures against cybersecurity threats and attacks.

Mitigation Measures	Short Description	Security Aspect Threat	IoT Layer Threat	Studies
Firmware Update	It is important to be checked if an update mechanism is installed or even turned on in the device, in order to prevent various online and offline attacks.	Privacy, Confidentially, Availability	Application	[92,106,107,114–120]
Block Unnecessary Ports	Block unnecessary, vulnerable or overlooked ports, so to prevent a possible cyberattack or device exploitation.	Privacy, Authenticity, Non-Repudiation	Internet	[100,101,107,110,114–118,120,121]
Disable Telnet	Telnet is a great security risk due the fact of sending passwords and usernames in clear text. It should be ensured that is turned off.	Privacy, Authenticity, Non-Repudiation	Internet	[100,101,107,110,114–118,120,122]
Encrypted Communication Usage (SSL/TLS)	Using a secure protocol such as SSL/TLS consists an essential step towards a device security through transport encryption.	Confidentially, Integrity, Authenticity	Access Gateway	[93,94,108,111,114–117,119,120]
Strong Passwords	A token could be used to increase the security level of the device.	Privacy, Confidentially, Authenticity	Middleware	[93,94,100,107,109, 114–117,120,123]
Encryption of Drives	Keep the data inaccessible in case of a device theft.	Privacy, Integrity	Middleware, Edge Technology	[93,94,100,101,107–109,114–117,120,123]
Accounts Lockout	Account lockout mechanism(s) should be incorporated in the device so as to allow a legitimate user to access and retrieve information.	Privacy, Confidentially, Authenticity	Edge Technology	[93,94,100,101,107–109,114–117,123]
Periodic Assessment of Devices	Devices need periodic cybersecurity assessments in order to check and avoid possible new vulnerabilities of any type.	Privacy, Availability	Edge Technology	[93,94,100,101,107–109,114–117,120]
Secure Password Recovery	Helps to retrieve back missed credentials in a secure way.	Privacy, Confidentially, Authenticity	Middleware	[93,94,100,107,109, 114–120]
Two-Factor Authentication	Keep data encrypted and protected as well.	Privacy, Confidentially, Authenticity	Middleware	[93,94,100,107,109, 114–118,120]
Disable UPnP	In order to avoid possible exposure of the network to aspiring attackers, the UPnP must be disabled as it does not require any authentication, which renders it an important security flaw.	Privacy, Confidentially, Availability	Internet	[93,94,100,107,110, 114–117,120]

Lastly, regarding agricultural cyber-security, researchers intensify their efforts in designing Machine Learning (ML) and Deep Learning (DL) methods for anomaly behavior detection and network analysis of intrusion detection systems (IDS) [124]. Traditional Machine and Deep Learning applications applied for cybersecurity in agriculture include [125,126]:

- Support Vector Machine (SVM);
- K-Nearest Neighbor;
- Decision Trees;
- Deep Belief Network (DBN);
- Recurrent Neural Networks (RNN);
- Convolutional Neural Networks (CNN);
- Artificial Neural Networks (ANN);

- Self-Organizing Maps (SOMs);
- Natural Language Processing (NLP);
- Biologically inspired techniques, such as Deep Neural Networks (DNN) and/or Generative Adversarial Networks (GANs).

The emergence of such methods has enabled efficient handling and analysis of large amounts of data (e.g., files extracted from server logs, communication equipment, security solutions and blogs related to information security, in different types of structured and unstructured formats), so as to support a variety of conceptual models, security activities and knowledge generation mechanisms. This leads to efficient decision making or automation of security responses without the need for human interception [127].

5. Conclusions

The goal of this study was to conduct a thorough literature research on the benefits and the security threats imposed by the introduction of novel ICT technologies in the agricultural sector nowadays as well as on the associated mitigation measures and strategies. Research began with the advantages of ICT technologies and their importance in the agri-sector and then focused on the threats emerging alongside the evolution of smart agriculture or Agriculture 4.0. Also, research conducted in the context of this paper showed that, despite the rapid evolution in technology, stakeholders throughout the entire agricultural sector need to exercise caution on how they adopt and exploit new technologies and tools. The agri-sector tends to be even more vulnerable compared to other sectors that engage digital tools, so the mitigation of security threats is and will be an ever-open research subject.

The new era in agriculture employs concepts and assets from Industry 4.0 that facilitate the transition to Agriculture 4.0 and the smart farming era. The increasing complexity of methods used for cultivation and production of agri-products leads to even more potential threats on various facets. By making the agriculture ecosystem smart and connected, multiple "backdoors" have opened with stakeholders and security specialists urged work together to block them entirely, in order to guarantee the safety and efficiency of all the new possibilities offered to farmers.

To conclude, in order to characterize a new method or system as successful, it should be able to: (i) reduce costs; (ii) save time; (iii) increase trust; (iv) reduce risk. Stakeholders in agriculture should be willing to adopt new ways of working only when they are convinced that the newly proposed method or system is secure, safe and usable, increases productivity and brings added value. Taking the above into account, it becomes clear that the consolidation of new technologies in the sensitive sector of agriculture is an enormous challenge which should be carried out step by step, and only by efficiently engaging the directly affected stakeholders across the supply chain in security-preserving activities and investments.

Funding: This research received no external funding.

Conflicts of Interest: The authors declare no conflict of interest.

References

1. Roopaei, M.; Rad, P.; Choo, K.R. Cloud of Things in smart agriculture: Intelligent irrigation monitoring by thermal imaging. *IEEE Cloud Comput.* **2017**, *4*, 10–15. [CrossRef]
2. Karlov, A.A. Cybersecurity of internet of things—Risks and opportunities. In Proceedings of the XXVI International Symposium on Nuclear Electronics & Computing (NEC'2017), Budva, Montenegro, 25–29 September 2017; pp. 182–187.
3. Malavade, V.N.; Akulwar, P.K. Role of IoT in agriculture. *IOSR J. Comput. Eng.* **2016**, *2016*, 56–57.
4. Prasad, R.; Rohokale, V. *Cyber Security: The Lifeline of Information and Communication Technology*; Springer International Publishing: Cham, Switzerland, 2020; ISBN 978-3-030-31702-7.
5. Calicioglu, O.; Flammini, A.; Bracco, S.; Bellú, L.; Sims, R. The future challenges of food and agriculture: An integrated analysis of trends and solutions. *Sustainability* **2019**, *11*, 222. [CrossRef]

6. Devendra, C. *Climate Change Threats and Effects: Challenges for Agriculture and Food Security*; ASM Series on Climate Change; Academy of Sciences Malaysia: Kuala Lumpur, Malaysia, 2012.
7. Horrigan, L.; Lawrence, R.S.; Walker, P. How sustainable agriculture can address the environmental and human health harms of industrial agriculture. *Environ. Health Perspect.* **2002**, *110*, 445–456. [CrossRef]
8. O'Brien, D. The A to Z of Cyber Security. Available online: https://medium.com/threat-intel/the-a-to-z-of-cyber-security-93150c4f336c (accessed on 7 September 2020).
9. Ivanov, I. *Cyber Security and Cyber Threats: Eagle VS "New Wars"?* Academia.edu: San Francisco, CA, USA, 2019.
10. Koerner, J.; Dinesh, D.; Loboguerrero, A.M.; Campbell, B. Lessons learnt from CCAFS—10 Years Scaling Climate-Smart Agriculture: Insights from the Review of CCAFS Scaling Activities. 2019. Available online: https://ccafs.cgiar.org/publications/lessons-learnt-ccafs-10-years-scaling-climate-smart-agriculture-insights-review-ccafs#.X6vmtVVR0uU (accessed on 1 January 2020).
11. Misra, N.N.; Dixit, Y.; Al-Mallahi, A.; Bhullar, M.S.; Upadhyay, R.; Martynenko, A. IoT, big data and artificial intelligence in agriculture and food industry. *IEEE Internet Things J.* **2020**. [CrossRef]
12. Gómez-Chabla, R.; Real-Avilés, K.; Morán, C.; Grijalva, P.; Recalde, T. IoT applications in Agriculture: A systematic literature review. In *ICT for Agriculture and Environment*; Valencia-García, R., Alcaraz-Mármol, G., del Cioppo-Morstadt, J., Vera-Lucio, N., Bucaram-Leverone, M., Eds.; Springer International Publishing: Cham, Switzerland, 2019; pp. 68–76.
13. Muangprathub, J.; Boonnam, N.; Kajornkasirat, S.; Lekbangpong, N.; Wanichsombat, A.; Nillaor, P. IoT and agriculture data analysis for smart farm. *Comput. Electron. Agric.* **2019**, *156*, 467–474. [CrossRef]
14. Wolf, S.A.; Wood, S.D. Precision farming: Environmental legitimation, commodification of information, and industrial coordination. *Rural Sociol.* **1997**, *62*, 180–206. [CrossRef]
15. Dwivedi, A.; Naresh, R.; Kumar, R.; Yadav, R.; Kumar, R. *Precision Agriculture*; Parmar Publishers & Distributors: Dhanbad, India, 2017; pp. 83–105.
16. Milella, A.; Reina, G.; Nielsen, M. A multi-sensor robotic platform for ground mapping and estimation beyond the visible spectrum. *Precis. Agric.* **2019**, *20*, 423–444. [CrossRef]
17. McBratney, A.; Whelan, B.; Ancev, T.; Bouma, J. Future directions of precision agriculture. *Precis. Agric.* **2005**, *6*, 7–23. [CrossRef]
18. Whelan, B.; Mcbratney, A. Definition and interpretation of potential management zones in Australia. In Proceedings of the 6th International Conference on Precision Agriculture and Other Precision Resources Management, Geelong, Australia, 2–6 February 2003.
19. Zarco-Tejada, P.J.; Hubbard, N.; Loudjani, P.; European Parliament; Joint Research Centre (JRC); Monitoring Agriculture Resources (MARS). *Precision Agriculture: An Opportunity for EU-Farmers—Potential Support with the AP 2014–2020*; European Union: Brussels, Belgium, 2014.
20. Trivelli, L.; Apicella, A.; Chiarello, F.; Rana, R.L.; Fantoni, G.; Tarabella, A. From precision agriculture to Industry 4.0: Unveiling technological connections in the agrifood sector. *Br. Food J.* **2019**, *121*, 8. [CrossRef]
21. Schrijver, R.; Poppe, K.; Daheim, C. *Precision Agriculture and the Future of Farming in Europe*; Scientific Foresight Study; EPRS—European Parliamentary Research Service: Brussels, Belgium, 2016.
22. Hassija, V.; Chamola, V.; Saxena, V.; Jain, D.; Goyal, P.; Sikdar, B. A Survey on IoT security: Application areas, security threats, and solution architectures. *IEEE Access* **2019**, *7*, 82721–82743. [CrossRef]
23. Symeonaki, E.; Arvanitis, K.; Piromalis, D. A context-aware middleware cloud approach for integrating precision farming facilities into the IoT toward agriculture 4.0. *Appl. Sci.* **2020**, *10*, 813. [CrossRef]
24. Keerthana, K.T.E.; Karpagavalli, S.; Posonia, A.M. Smart system monitoring agricultural land Using IoT. In Proceedings of the 2018 International Conference on Emerging Trends and Innovations. In Engineering And Technological Research (ICETIETR), Ernakulam, India, 11–13 July 2018; pp. 1–7.
25. Sreekantha, D.K.; Kavya, A.M. Agricultural crop monitoring using IOT—A study. In Proceedings of the 2017 11th International Conference on Intelligent Systems and Control (ISCO), Coimbatore, India, 5–6 January 2017; pp. 134–139.
26. Moulat, M.E.; Debauche, O.; Mahmoudi, S.; Brahim, L.A.; Manneback, P.; Lebeau, F. Monitoring system using Internet of Things for potential landslides. *Procedia Comput. Sci.* **2018**, *134*, 26–34. [CrossRef]
27. Elijah, O.; Abd Rahman, T.; Orikumhi, I.; Leow, C.Y.; Hindia, M. An overview of Internet of Things (IoT) and Data Analytics in agriculture: Benefits and challenges. *IEEE Internet Things J.* **2018**, *5*, 3758–3773. [CrossRef]

28. Kamienski, C.; Soininen, J.-P.; Taumberger, M.; Fernandes, S.; Toscano, A.; Cinotti, T.; Maia, R.; Neto, A. SWAMP: An IoT-based Smart Water Management Platform for Precision Irrigation in Agriculture. In Proceedings of the 2018 Global Internet of Things Summit (GIoTS), Bilbao, Spain, 4–7 June 2018.
29. Kamienski, C.; Soininen, J.-P.; Taumberger, M.; Toscano, A.; Cinotti, T.; Dantas, R.; Maia, R.; Neto, A.; Ferreira, F. Smart water management platform: IoT-based precision irrigation for agriculture. *Sensors* **2019**, *19*, 276. [CrossRef]
30. Patil, S.J.; Patil, A. Precision Agriculture for water management using IOT. In *International Journal on Recent and Innovation Trends in Computing and Communication*; Auricle Technologies Pvt. Ltd.: Rajasthan, India, 2017; Volume 5, pp. 142–144.
31. Hu, X.; Qian, S. IoT application system with crop growth models in facility agriculture. In Proceedings of the 2011 6th International Conference on Computer Sciences and Convergence Information Technology (ICCIT), Seogwipo, Korea, 29 November–1 December 2011; pp. 129–133.
32. Stočes, M.; Vaněk, J.; Masner, J.; Pavlík, J. Internet of Things (IoT) in agriculture—Selected aspects. *Agris on-Line Pap. Econ. Inform.* **2016**, 83–88. [CrossRef]
33. Ghanshala, K.K.; Chauhan, R.; Joshi, R.C. A novel framework for smart crop monitoring using Internet of Things (IoT). In Proceedings of the 2018 First International Conference on Secure Cyber Computing and Communication (ICSCCC), Jalandhar, India, 15–17 December 2018; pp. 62–67.
34. Kajol, R.; Akshay, K.; Keerthan Kumar, T.G. Automated agricultural field analysis and monitoring system using IoT. *Int. J. Inf. Eng. Electron. Bus.* **2018**, *10*, 17–24. [CrossRef]
35. Kuaban, G.S.; Czekalski, P.; Molua, E.L.; Grochla, K. An architectural framework proposal for IoT driven agriculture. In *Computer Networks*; Gaj, P., Sawicki, M., Kwiecień, A., Eds.; Springer International Publishing: Cham, Germany, 2019; pp. 18–33.
36. Pandithurai, O.; Aishwarya, S.; Aparna, B.; Kavitha, K. Agro-tech: A digital model for monitoring soil and crops using internet of things (IoT). In Proceedings of the 2017 Third International Conference on Science Technology Engineering Management (ICONSTEM), Chennai, India, 23–24 March 2017; pp. 342–346.
37. Burton, L.; Dave, N.; Fernandez, R.E.; Jayachandran, K.; Bhansali, S. Smart gardening IoT soil sheets for real-time nutrient analysis. *J. Electrochem. Soc.* **2018**, *165*, B3157–B3162. [CrossRef]
38. Na, A.; Isaac, W.; Varshney, S.; Khan, E. An IoT based system for remote monitoring of soil characteristics. In Proceedings of the 2016 International Conference on Information Technology (InCITe)—The Next Generation IT Summit on the Theme—Internet of Things: Connect Your Worlds, Noida, India, 6–7 October 2016; pp. 316–320.
39. Zhang, X.; Zhang, J.; Li, L.; Zhang, Y.; Yang, G. Monitoring citrus soil moisture and nutrients using an IoT based system. *Sensors* **2017**, *17*, 447. [CrossRef]
40. Athani, S.; Tejeshwar, C.H.; Patil, M.M.; Patil, P.; Kulkarni, R. Soil moisture monitoring using IoT enabled arduino sensors with neural networks for improving soil management for farmers and predict seasonal rainfall for planning future harvest in North Karnataka—India. In Proceedings of the 2017 International Conference on I-SMAC (IoT in Social, Mobile, Analytics and Cloud) (I-SMAC), Palladam, India, 10–11 February 2017; pp. 43–48.
41. Ampatzidis, Y.; De Bellis, L.; Luvisi, A. iPathology: Robotic applications and management of plants and plant diseases. *Sustainability* **2017**, *9*, 1010. [CrossRef]
42. Khattab, A.; Habib, S.E.D.; Ismail, H.; Zayan, S.; Fahmy, Y.; Khairy, M.M. An IoT-based cognitive monitoring system for early plant disease forecast. *Comput. Electron. Agric.* **2019**, *166*, 105028. [CrossRef]
43. Shi, Y.; Wang, Z.; Wang, X.; Zhang, S. Internet of Things application to monitoring plant disease and insect pests. In Proceedings of the 2015 International conference on Applied Science and Engineering Innovation, Jinan, China, 30–31 August 2015; pp. 31–34.
44. Wang, X.F.; Wang, Z.; Zhang, S.W.; Shi, Y. Monitoring and discrimination of plant disease and insect pests based on agricultural IoT. In Proceedings of the 4th International Conference on Information Technology and Management Innovation, Shenzhen, China, 12–13 September 2015; pp. 112–115.
45. Nawaz, M.; Khan, T.; Rasool, R.; Kausar, M.; Usman, A.; Bukht, F.; Ahmad, R.; Ahmad, J.; Multan, P. Pakistan Plant disease detection using Internet of Thing (IoT). *Int. J. Adv. Comput. Sci. Appl.* **2020**, *11*, 5.
46. Liu, Y.; Han, W.; Zhang, Y.; Li, L.; Wang, J.; Zheng, L. An Internet-of-Things solution for food safety and quality control: A pilot project in China. *J. Ind. Inf. Integr.* **2016**, *3*, 1–7. [CrossRef]

47. Popa, A.; Hnatiuc, M.; Paun, M.; Geman, O.; Hemanth, D.J.; Dorcea, D.; Son, L.H.; Ghita, S. An intelligent IoT-based food quality monitoring approach using low-cost sensors. *Symmetry* **2019**, *11*, 374. [CrossRef]
48. Bhatia, M.; Manocha, A. Cognitive framework of food quality assessment in IoT-inspired smart restaurants. *IEEE Internet Things J.* **2020**. [CrossRef]
49. Fennema, O. An over-all view of low temperature food preservation. *Cryobiology* **1966**, *3*, 197–213. [CrossRef]
50. Iwasaki, W.; Morita, N.; Nagata, M.P.B. 14—IoT sensors for smart livestock management. In *Chemical, Gas, and Biosensors for Internet of Things and Related Applications*; Mitsubayashi, K., Niwa, O., Ueno, Y., Eds.; Elsevier: Amsterdam, The Netherlands, 2019; pp. 207–221. ISBN 978-0-12-815409-0.
51. Houngue, P.; Sagbo, R.; Kedowide, C. An hybrid novel layered architecture and case study: IoT for smart agriculture and smart liveStock. In *Society with Future: Smart and Liveable Cities*; Pereira, P., Ribeiro, R., Oliveira, I., Novais, P., Eds.; Springer International Publishing: Cham, Germany, 2020; pp. 71–82.
52. Pan, L.; Xu, M.; Xi, L.; Hao, Y. Research of livestock farming IoT system based on RESTful web services. In Proceedings of the 2016 5th International Conference on Computer Science and Network Technology (ICCSNT), Changchun, China, 10–11 December 2016; pp. 113–116.
53. Saravanan, K.; Saraniya, S. Cloud IoT based novel livestock monitoring and identification system using UID. *Sens. Rev.* **2018**, *38*, 21–33. [CrossRef]
54. Dolci, R. IoT solutions for precision farming and food manufacturing: Artificial Intelligence applications in digital food. In Proceedings of the 2017 IEEE 41st Annual Computer Software and Applications Conference (COMPSAC), Turin, Italy, 4–8 July 2017; pp. 384–385.
55. Kaewmard, N.; Saiyod, S. Sensor data collection and irrigation control on vegetable crop using smart phone and wireless sensor networks for smart farm. In Proceedings of the 2014 IEEE Conference on Wireless Sensors (ICWiSE), Subang, Malaysia, 26–28 October 2014; pp. 106–112.
56. Nandyala, S.; Kim, H.-K. Green IoT agriculture and healthcare application (GAHA). *Int. J. Smart Home* **2016**, *10*, 289–300. [CrossRef]
57. Cambra, C.; Sendra, S.; Lloret, J.; Garcia, L. An IoT service-oriented system for agriculture monitoring. In Proceedings of the 2017 IEEE International Conference on Communications (ICC), Paris, France, 21–25 May 2017; pp. 1–6.
58. Ferris, J.L. Data privacy and protection in the agriculture industry: Is federal regulation necessary? *Minn. J. Law Sci. Technol.* **2017**, *18*, 309.
59. Alrajhi, A.M. A survey of Artificial Intelligence techniques for cybersecurity improvement. *Int. J. Cyber-Secur. Digit. Forensic* **2020**, *9*, 34–41.
60. Salam, A. Internet of Things for sustainability: Perspectives in privacy, cybersecurity, and future trends. In *Internet of Things for Sustainable Community Development: Wireless Communications, Sensing, and Systems*; Salam, A., Ed.; Springer International Publishing: Cham, Germany, 2020; pp. 299–327. ISBN 978-3-030-35291-2.
61. Barreto, L.; Amaral, A. Smart farming: Cyber security challenges. In Proceedings of the 2018 International Conference on Intelligent Systems (IS), Funchal, Portugal, 25–27 September 2018; pp. 870–876.
62. Gupta, M.; Abdelsalam, M.; Khorsandroo, S.; Mittal, S. Security and privacy in smart farming: Challenges and opportunities. *IEEE Access* **2020**, *8*, 34564–34584. [CrossRef]
63. European Commission. *Industry 4.0 in Agriculture: Focus on IoT Aspects*; Digital Transformation Monitor; European Commission: Brussels, Belgium, 2017.
64. Window, M. Security in Precision Agriculture: Vulnerabilities and Risks of Agricultural Systems. Master's Thesis, Department of Computer Science, Electrical and Space Engineering, Luleå University of Technology, Luleå, Sweden, 2019.
65. Champion, S.; Linsky; Mutschler, P.; Ulicny, B.; Reuters, T.; Barrett, L.; Bethel, G.; Matson, M.; Strang, T.; Ramsdell, K.; et al. *Threats to Precision Agriculture*; 2018 Public-Private Analytic Exchange Program Report; United States Department of Homeland Security and Office of Intelligence and Analysis: Washington, DC, USA, 2020.
66. McCartney, L.; Lefsrud, M. Protected agriculture in extreme environments: A review of controlled environment agriculture in tropical, arid, polar and urban locations. *Appl. Eng. Agric.* **2018**, *34*, 455–473. [CrossRef]
67. Tzounis, A.; Katsoulas, N.; Bartzanas, T.; Kittas, C. Internet of Things in agriculture, recent advances and future challenges. *Biosyst. Eng.* **2017**, *164*, 31–48. [CrossRef]

68. Bannister, K.; Giorgetti, G.; Sandeep, K. Wireless sensor networking for hot applications: Effects of temperature on signal strength, data collection and localization. In Proceedings of the 5th Workshop on Embedded Networked Sensors (HotEmNets' 08), Charlottesville, VA, USA, 2–3 July 2008.
69. Boano, C.A.; Tsiftes, N.; Voigt, T.; Brown, J.; Roedig, U. The Impact of temperature on outdoor industrial sensornet applications. *IEEE Trans. Ind. Inform.* **2010**, *6*, 451–459. [CrossRef]
70. Thelen, J.; Goense, D.; Langendoen, K. Radio Wave Propagation in Potato Fields. Available online: https://scholar.google.com/scholar?hl=en&as_sdt=0%2C5&q=70.%09Thelen%2C+J.%3B+Goense%2C+D.%3B+Langendoen%2C+K.+Radio+wave+propagation+in+potato+fields&btnG= (accessed on 3 September 2020).
71. Lopez, J.; Roman, R.; Alcaraz, C. Analysis of security threats, requirements, technologies and standards in wireless sensor networks. In *Foundations of Security Analysis and Design V: FOSAD 2007/2008/2009 Tutorial Lectures*; Aldini, A., Barthe, G., Gorrieri, R., Eds.; Springer: Berlin/Heidelberg, Germany, 2009; pp. 289–338. ISBN 978-3-642-03829-7.
72. El Bilali, H.; Allahyari, M.S. Transition towards sustainability in agriculture and food systems: Role of information and communication technologies. *Inf. Process. Agric.* **2018**, *5*, 456–464. [CrossRef]
73. Begemann, S. 13 Ways Precision Ag Advances Leave Farmers Vulnerable to Attack. Available online: https://www.agprofessional.com/article/13-ways-precision-ag-advances-leave-farmers-vulnerable-attack (accessed on 3 September 2020).
74. Vogt, W. 4 Tips for Improved Farm Data Integrity. Available online: https://www.farmprogress.com/data/4-tips-improved-farm-data-integrity (accessed on 3 September 2020).
75. Bughin, J.; Hazan, E.; Ramaswamy, S.; Chui, M.; Allas, T.; Dahlström, P.; Henke, N.; Trench, M. *Artificial Intelligence: The Next Digital Frontier?* McKinsey & Company: New York, NY, USA, 2017.
76. Jochinke, D.C.; Noonon, B.J.; Wachsmann, N.G.; Norton, R.M. The adoption of precision agriculture in an Australian broadacre cropping system—Challenges and opportunities. *Field Crop. Res.* **2007**, *104*, 68–76. [CrossRef]
77. Talaviya, T.; Shah, D.; Patel, N.; Yagnik, H.; Shah, M. Implementation of artificial intelligence in agriculture for optimisation of irrigation and application of pesticides and herbicides. *Artif. Intell. Agric.* **2020**, *4*, 58–73. [CrossRef]
78. Zhou, W.; Jia, Y.; Peng, A.; Zhang, Y.; Liu, P. The Effect of IoT new features on security and privacy: New threats, existing solutions, and challenges yet to be solved. *IEEE Internet Things J.* **2019**, *6*, 1606–1616. [CrossRef]
79. Ferrag, M.A.; Shu, L.; Yang, X.; Derhab, A.; Maglaras, L. Security and privacy for green IoT-based agriculture: Review, blockchain solutions, and challenges. *IEEE Access* **2020**, *8*, 32031–32053. [CrossRef]
80. Parmar, D. Cyber security techniques for internet of things in agriculture. *Guj. J. Ext. Educ.* **2019**, *30*, 185–190.
81. Kohl, K.D. The Increase of Cybersecurity Threats to the Food and Agriculture Sector from Smart Agriculture. Master's Thesis, Utica College, New York, NY, USA, 2017.
82. Okupa, H. Cybersecurity and the Future of Agri-Food Industries. Master's Thesis, Department of Agricultural Economics College of Agriculture, Kansas State University, Manhattan, KS, USA, 2020.
83. Lezzi, M.; Lazoi, M.; Corallo, A. Cybersecurity for Industry 4.0 in the current literature: A reference framework. *Comput. Ind.* **2018**, *103*, 97–110. [CrossRef]
84. Duncan, S.E.; Reinhard, R.; Williams, R.C.; Ramsey, F.; Thomason, W.; Lee, K.; Dudek, N.; Mostaghimi, S.; Colbert, E.; Murch, R. Cyberbiosecurity: A New Perspective on Protecting U.S. Food and Agricultural System. *Front. Bioeng. Biotechnol.* **2019**, *7*, 63. [CrossRef] [PubMed]
85. Manninen, O. Cybersecurity in Agricultural Communication Networks: Case Dairy Farms. Master's Thesis, JAMK University of Applied Sciences, Jyväskylä, Finland, 2018.
86. Bogaardt, M.; Poppe, K.; Viool, V.; van Zuidam, E. *Cybersecurity in the Agrifood Sector*; Capgemini Consulting: Wien, Austria, 2016.
87. Jahn, M.; Oemichen, W.; Treverton, G.; David, S.; Rose, M.; Brosig, M.; Jayamaha, B.; Hutchison, W.; Rimestad, B. Cyber Risk and Security Implications in Smart Agriculture and Food Systems. Available online: https://jahnresearchgroup.webhosting.cals.wisc.edu/wp-content/uploads/sites/223/2019/01/Agricultural-Cyber-Risk-and-Security.pdf (accessed on 10 September 2020).
88. Cooper, C. Cybersecurity and food and agriculture. In *Protecting Our Future, Volume 2: Educating a Cybersecurity Workforce*; Hudson Whitman/ECP: New York, NY, USA, 2015.

89. Altawy, R.; Youssef, A.M. Security, privacy, and safety aspects of civilian drones: A survey. *ACM Trans. Cyber Phys. Syst.* **2016**, *1*, 1–25. [CrossRef]
90. Ametepe, A.F.; Ahouandjinou, S.A.R.M.; Ezin, E.C. Secure encryption by combining asymmetric and symmetric cryptographic method for data collection WSN in smart agriculture. In Proceedings of the 2019 IEEE International Smart Cities Conference (ISC2), Casablanca, Morocco, 10–17 October 2019; pp. 93–99.
91. Mekala, M.S.; Viswanathan, P. A Survey: Smart agriculture IoT with cloud computing. In Proceedings of the 2017 International Conference on Microelectronic Devices, Circuits and Systems (ICMDCS), Vellore, India, 10–12 August 2017; pp. 1–7.
92. Vangala, A.; Das, A.K.; Kumar, N.; Alazab, M. Smart secure sensing for IoT-based agriculture: Blockchain perspective. *IEEE Sens. J.* **2020**. [CrossRef]
93. Khanna, A.; Kaur, S. Evolution of Internet of Things (IoT) and its significant impact in the field of Precision Agriculture. *Comput. Electron. Agric.* **2019**, *157*, 218–231. [CrossRef]
94. Yu, S.; Lou, W.; Ren, K. Chapter 15—Data Security in Cloud Computing. In *Handbook on Securing Cyber-Physical Critical Infrastructure*; Das, S.K., Kant, K., Zhang, N., Eds.; Morgan Kaufmann: Boston, MA, USA, 2012; pp. 389–410. ISBN 978-0-12-415815-3.
95. Chamarajnagar, R.; Ashok, A. Integrity threat identification for distributed IoT in precision agriculture. In Proceedings of the 2019 16th Annual IEEE International Conference on Sensing, Communication, and Networking (SECON), Boston, MA, USA, 10–13 June 2019; pp. 1–9.
96. Davcev, D.; Mitreski, K.; Trajkovic, S.; Nikolovski, V.; Koteli, N. IoT agriculture system based on LoRaWAN. In Proceedings of the 2018 14th IEEE International Workshop on Factory Communication Systems (WFCS), Imperia, Italy, 13–15 June 2018; pp. 1–4.
97. Nesarani, A.; Ramar, R.; Pandian, S. An efficient approach for rice prediction from authenticated Block chain node using machine learning technique. *Environ. Technol. Innov.* **2020**, *20*, 101064. [CrossRef]
98. Bisogni, F.; Cavallini, S.; Trocchio, S. Cybersecurity at European level: The role of information availability. *Commun. Strateg.* **2011**, *1*, 105–124.
99. Palm, T. Impact of authenticity on sense making in word problem solving. *Educ. Stud. Math.* **2008**, *67*, 37–58. [CrossRef]
100. National Academies of Sciences, Engineering, and Medicine; Policy and Global Affairs; Government-University-Industry Research Roundtable. *Authenticity, Integrity, and Security in a Digital World: Proceedings of a Workshop–In Brief*; Whitacre, P., Ed.; The National Academies Press: Washington, DC, USA, 2019.
101. Bothe, A.; Bauer, J.; Aschenbruck, N. RFID-assisted Continuous user authentication for IoT-based smart farming. In Proceedings of the 2019 IEEE International Conference on RFID Technology and Applications (RFID-TA), Pisa, Italy, 25–27 September 2019; pp. 505–510.
102. Mccullagh, A.; Caelli, W. Non-repudiation in the digital environment. *First Monday* **2000**, *5*. [CrossRef]
103. Holkar, A.M.; Holkar, N.S.; Nitnawwre, D. Investigative analysis of repudiation attack on MANET with different routing protocols. *Int. J. Emerg. Trends Technol. Comput. Sci.* **2013**, *2*, 356–359.
104. Mishra, P.K. Bluetooth security threats. *Int. J. Comput. Sci. Eng. Technol.* **2013**, *4*, 147–151.
105. Seri, B.; Vishnepolsky, G. BlueBorne: The Dangers of Bluetooth Implementations: Unveiling Zero Day Vulnerabilities and Security Flaws in Modern Bluetooth Stacks. Available online: https://kryptera.se/assets/uploads/2017/09/blueborne-technical-white-paper.pdf (accessed on 11 September 2020).
106. Glaroudis, D.; Iossifides, A.; Chatzimisios, P. Survey, comparison and research challenges of IoT application protocols for smart farming. *Comput. Netw.* **2020**, *168*, 107037. [CrossRef]
107. Farooq, M.S.; Riaz, S.; Abid, A.; Abid, K.; Naeem, M.A. A survey on the role of IoT in agriculture for the implementation of smart farming. *IEEE Access* **2019**, *7*, 156237–156271. [CrossRef]
108. Triantafyllou, A.; Tsouros, D.C.; Sarigiannidis, P.; Bibi, S. An architecture model for smart farming. In Proceedings of the 2019 15th International Conference on Distributed Computing in Sensor Systems (DCOSS), Santorini Island, Greece, 29–31 May 2019; pp. 385–392.
109. Aluthgama Acharige, R.; Halgamuge, M.; Wirasagoda, H.; Syed, A. Adoption of the Internet of Things (IoT) in agriculture and smart farming towards urban greening: A review. *Int. J. Adv. Comput. Sci. Appl.* **2019**, *10*, 11–28. [CrossRef]
110. Ahmed, N.; De, D.; Hussain, I. Internet of Things (IoT) for smart precision agriculture and farming in rural areas. *IEEE Internet Things J.* **2018**, *5*, 4890–4899. [CrossRef]

111. Ryu, M.; Yun, J.; Miao, T.; Ahn, I.-Y.; Choi, S.; Kim, J. Design and implementation of a connected farm for smart farming system. In Proceedings of the 2015 IEEE SENSORS, Busan, Korea, 1–4 November 2015; pp. 1–4.
112. Chinnaiyan, R.; Balachandar, S. Reliable administration framework of drones and IoT sensors in agriculture farmstead using blockchain and smart contracts. In *2020 2nd International Conference on Big Data Engineering and Technology*; Association for Computing Machinery: New York, NY, USA, 2020; pp. 106–111.
113. Demestichas, K.; Peppes, N.; Alexakis, T.; Adamopoulou, E. Blockchain in Agriculture Traceability Systems: A Review. *Appl. Sci.* **2020**, *10*, 4113. [CrossRef]
114. Zhang, H.; Wei, X.; Zou, T.; Li, Z.; Yang, G. Agriculture Big Data: Research status, challenges and countermeasures. In *Computer and Computing Technologies in Agriculture VIII*; Li, D., Chen, Y., Eds.; Springer International Publishing: Cham, Germany, 2015; pp. 137–143.
115. Daoliang, L. Internet of things and wisdom agriculture. *Agric. Eng.* **2012**, *2*, 1–7.
116. Yousuf, T.; Mahmoud, R.; Aloul, F.; Zualkernan, I. Internet of Things (IoT) security: Current status, challenges and countermeasures. *Int. J. Inf. Secur. Res.* **2015**, *5*, 608–616. [CrossRef]
117. Butun, I.; Österberg, P.; Song, H. Security of the Internet of Things: Vulnerabilities, attacks, and countermeasures. *IEEE Commun. Surv. Tutor.* **2020**, *22*, 616–644. [CrossRef]
118. Ghadeer, H. Cybersecurity issues in Internet of Things and countermeasures. In Proceedings of the 2018 IEEE International Conference on Industrial Internet (ICII), Seattle, WA, USA, 21–23 October 2018; pp. 195–201.
119. Mentsiev, A.U.; Magomaev, T.R. Security threats of NB-IoT and countermeasures. *IOP Conf. Ser. Mater. Sci. Eng.* **2020**, *862*, 052033. [CrossRef]
120. Pfleeger, C.P.; Pfleeger, S.L. *Analyzing Computer Security: A Threat/Vulnerability/Countermeasure Approach*; Pearson Education, Inc.: Hoboken, NJ, USA, 2012; ISBN 978-0-13-278946-2.
121. Beaver, K. Commonly hacked ports. In *Hacking For Dummies*; For Dummies; John Wiley & Sons: Hoboken, NJ, USA, 2018.
122. Throwe, T.; Viren, B. Turning off Telnet Access (Telnetd) 2018. Available online: https://www.phy.bnl.gov/cybersecurity/old/telnet.html (accessed on 11 September 2020).
123. El Mouaatamid, O.; Lahmer, M.; Belkasmi, M. Internet of Things security: Layered classification of attacks and possible countermeasures. *Electron. J. Inf. Technol.* **2016**, *9*, 24–37.
124. West, J. A prediction model framework for cyber-attacks to precision agriculture technologies. *J. Agric. Food Inf.* **2018**, *19*, 307–330. [CrossRef]
125. Xin, Y.; Kong, L.; Liu, Z.; Chen, Y.; Li, Y.; Zhu, H.; Gao, M.; Hou, H.; Wang, C. Machine learning and deep learning methods for cybersecurity. *IEEE Access* **2018**, *6*, 35365–35381. [CrossRef]
126. Zeadally, S.; Adi, E.; Baig, Z.; Khan, I.A. Harnessing Artificial Intelligence capabilities to improve cybersecurity. *IEEE Access* **2020**, *8*, 23817–23837. [CrossRef]
127. Andrade, R.; Ontaneda, N.; Silva, A.; Tello Oquendo, L.; Cadena, S.; Quiroz, D.; Fuertes, W.; Nacional, E. Application of Big Data Analytic in Cybersecurity. In Proceedings of the 2019 International Conference on Applied Cognitive Computing, Las Vegas, NV, USA, 29 July–1 August 2020.