

Article

A Review on Security of Smart Farming and Precision Agriculture: Security Aspects, Attacks, Threats and Countermeasures

Abbas Yazdinejad ¹, Behrouz Zolfaghari ¹, Amin Azmoodeh ¹, Ali Dehghantanha ^{1,*}, Hadis Karimipour ², Evan Fraser ³, Arthur G. Green ³, Conor Russell ³ and Emily Duncan ³

¹ Cyber Science Lab, University of Guelph, Guelph, ON N1G 2W1, Canada; ayazdine@uoguelph.ca (A.Y.); bbehrouz@cybersciencelab.org (B.Z.); aazmoodeh@uoguelph.ca (A.A.)

² School of Engineering, University of Guelph, Guelph, ON N1G 2W1, Canada; hkarimi@uoguelph.ca

³ Geography, Environment and Geomatics, University of Guelph, Guelph, ON N1G 2W1, Canada; frasere@uoguelph.ca (E.F.); agreen18@uoguelph.ca (A.G.G.); conchobh@uoguelph.ca (C.R.); edunca01@uoguelph.ca (E.D.)

* Correspondence: adehghan@uoguelph.ca

Abstract: In recent years, Smart Farming (SF) and Precision Agriculture (PA) have attracted attention from both the agriculture industry as well as the research community. Altogether, SF and PA aim to help farmers use inputs (such as fertilizers and pesticides) more efficiently through using Internet of Things (IoT) devices, but in doing so, they create new security threats that can defeat this purpose in the absence of adequate awareness and proper countermeasures. A survey on different security-related challenges is required to raise awareness and pave the way for further research in this area. In this paper, we first itemize the security aspects of SF and PA. Next, we review the types of cyber attacks that can violate each of these aspects. Accordingly, we present a taxonomy on cyber-threats to SF and PA on the basis of their relations to different stages of Cyber-Kill Chain (CKC). Among cyber-threats, we choose Advanced Persistent Threats (APTs) for further study. Finally, we studied related risk mitigation strategies and countermeasure, and developed a future road map for further study in this area. This paper's main contribution is a categorization of security threats within the SF/PA areas and provide a taxonomy of security threats for SF environments so that we may detect the behavior of APT attacks and any other security threat in SF and PA environments.

Keywords: smart farming; precision agriculture; cyber-threats; advanced persistent threats; cyber-kill chain; security threats



Citation: Yazdinejad, A.; Zolfaghari, B.; Azmoodeh, A.; Dehghantanha, A.; Karimipour, H.; Fraser, E.; Green, A.G.; Russell, C.; Duncan, E.A. Review on Security of Smart Farming and Precision Agriculture: Security Aspects, Attacks, Threats and Countermeasures. *Appl. Sci.* **2021**, *11*, 7518. <https://doi.org/10.3390/app11167518>

Academic Editors: Gregory Epiphanou and Carsten R. Maple

Received: 28 May 2021

Accepted: 1 August 2021

Published: 16 August 2021

Publisher's Note: MDPI stays neutral with regard to jurisdictional claims in published maps and institutional affiliations.



Copyright: © 2021 by the authors. Licensee MDPI, Basel, Switzerland. This article is an open access article distributed under the terms and conditions of the Creative Commons Attribution (CC BY) license (<https://creativecommons.org/licenses/by/4.0/>).

1. Introduction

Population growth, climate change, and rising affluence leading to more resource-intensive diets all mean that today, global food security is seen as a major challenge. According to the United Nations' Food and Agriculture Organization (FAO), global food production needs to be increased by 70% in order to feeding 10 billion people by 2050 [1,2]. Keeping pace with this growing demand for food while also working towards sustainable development requires new approaches to agriculture [2,3]. To this end, different cutting edge technologies that use IoT are supporting food industries [4] and industrial agriculture [5]. However, the development in these industries and their applications brings about a broad range of security challenges [6–8].

Moreover, the increased population will cause constraints in terms of land and water that will encourage adoption of farming techniques designed to improve agriculture resource utilization and crop yield. Applying IoT technology is a viable solution towards increased efficiency to tackle the challenges facing modern agriculture. As a result, we are observing the emergence of Smart Farming (SF) and Precision Agriculture (PA). Recent literature comes with numerous research works focusing on SF [9–11] and PA [12,13].

In general, both PA and SF refer to the use of modern technologies such as Internet of Things (IoT), drones, robotics and Artificial Intelligence (AI) in the control and management of farms in order to improve productivity and yield, while reducing input, land, and labor requirements.

A typical multi-layer SF architecture is shown in Figure 1. This architecture has been used as the reference architecture in several research projects [14–17]. In the architecture of Figure 1, the “Cloud”, “Network Communication”, “Edge” and “Physical” layers connect various smart IoT devices such as sensors and actuators as well as heterogeneous Cyber-Physical System (CPSs) to each other and to the internet [18,19]. A SF platform with the architecture of Figure 1 collects data from IoT devices, and then forms, processes, and controls data to provide various applications as well as various access levels to the users [20,21].

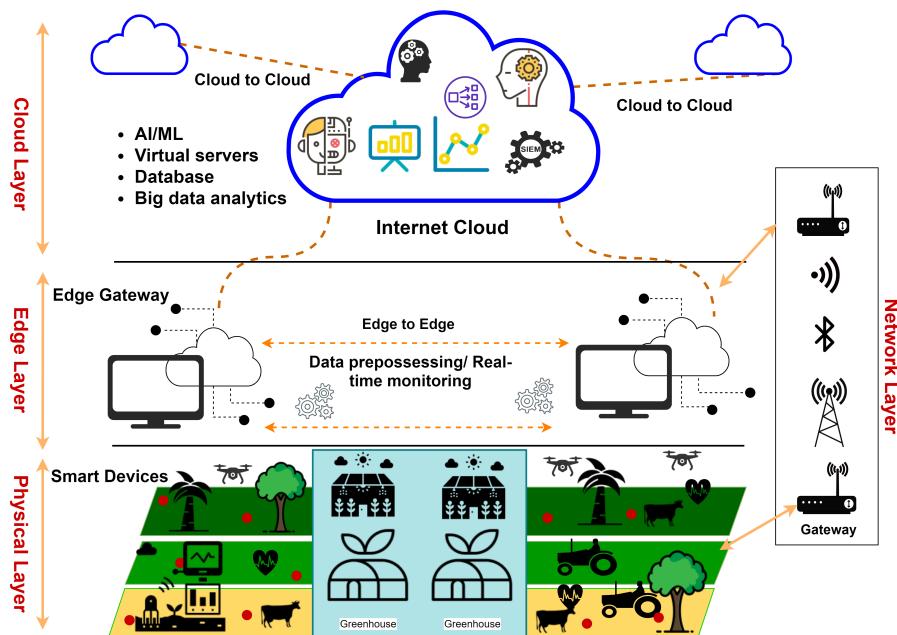


Figure 1. A typical SF architecture.

PA is distinct from SF in that it specifically refers to IoT-based approaches aiming at improving the efficiency of input use through providing farmers with tools that increase the granularity of decision making. In other words, PA is so sensitive and accurate that the minimum adversaries' activities simply can change the control system, target and damage valuable resources. Indeed, the PA is highly related to data and information of the system that can lead to costly, disruptive decisions and actions from the farmers via invalid data during run time.

For instance, in terms of crops, PA allows farmers the ability to move from managing fields to tailoring management to square meters or even individual plants within fields. For livestock farmers, PA means using IoT to shift from flock/herd scale management to being able to manage the needs of individual animals. A wide range of enabling technologies such as fog computing [22], AI [23], Unmanned Aerial Vehicles (UAVs) [24,25] and sensor networks [26] have been used to support both PA and SF.

Especially, IoT can be considered as one of the most important technologies for SF [27–29] and PA [30] due to its capabilities of remote sensing and operation without human interference. However, these IoT-based technologies create new cyber-security vulnerabilities and cyber-threats [1,3], which can be exploited to gain control on on-field actuators, sensors, and autonomous vehicles such as tractors, drones, sprayers, and planters, Refs. [1,3,31] as well as related databases and applications. A cyber-attack could have severe consequences on a farm. For instance, unauthorized changes to data could deceive a farmer to make changes that negatively influence the health of a herd. Poultry production relies

on sensors to control temperature and air quality within barns. In this case, a cyber-attack could cause the mortality of thousands of birds. Similar sensitivities are in greenhouse growing conditions where a breach in cyber-security could result in a devastating amount of profit for the farming operation. [2].

Security is a highly-challenging aspect of SF [2,32,33] and PA [34–36] due to different properties of IoT devices including heterogeneity, mobility, and resource limitations. This exposes SF and PA to a broad range of cyber-threats.

Although the literature comes with several research reports focusing on security-related issues in SF and PA, to the best of our knowledge, there is no systematic review on these issues. A survey in this area, along with a future road map, can improve public awareness and pave the way for further research.

In this paper, we first discuss security aspects of SF and PA. Next, we review state-of-the-art attacks on SF and PA, and study the security aspect(s) violated by each of them. In reviewing literature for examples of specific attacks on SF and PA, we identify the general security violations of each. In many cases, these attacks are on IoT technologies that support SF and PA functions thus countermeasures suggested here focus on these identified threats, rather than on novel SF/PA specific mitigation techniques. According to our studies on security aspects and attacks, we present a taxonomy on cyber-attacks to SF and PA. Our taxonomy is based on the relation between attacks and the stages of Cyber-Kill Chain, which is a methodology for analyzing the chronology of complex cyber-attacks.

As a chosen class of threats for further study, we discuss the anatomy as well as the behavioral characteristics of Advanced Persistent Threats (APTs). Furthermore, we review risk mitigation strategies and countermeasures against cyber-threats to SF and PA. On the basis of the above discussions, we suggest some topics for future research on security of SF and PA.

The main contributions of this paper can be explained as follows.

- We itemize the security aspects of SF and PA and establish a map between attacks and security aspects.
- We use CKC [37] for the first time to present a systematic taxonomy on cyber-threats to SF and PA.
- We study the anatomy as well as the behavioral characteristics of APT.
- Finally, we develop a future road map to highlight some related emerging areas that still need to be studied in future research.

The rest of this paper is organized as follows: Section 2 presents a review on existing reviews to highlight our motivations for the work of this paper. We examine cyber-attacks on SF and PA in Section 3. CKC-Based taxonomy on security threats to SF and PA are presented in Section 4. Moreover, APTs are specifically studied in more detail in Section 5. We study threat mitigation strategies and countermeasures in Section 6. Section 7 presents the future road map and; Section 8 concludes the paper.

2. Existing Reviews

Many researchers have conducted reviews on different aspects of PA. Some of these surveys focus on the applications of AI-based techniques in PA [38–40], the design of sensors [41] and sensor networks [42–46] to support PA, the application of educational hardware such as Raspberry Pi [47] and technical aspects such as imaging techniques [48] and routing protocols [49,50]. More specifically, few researchers have reviewed the literature on threats to PA. For example, Boghossian et al. [51] have presented a review on vulnerabilities of PA as well as the related threats along with some limited threat mitigation strategies. Another review on cyber-security threats to PA has been reported by Window [34]. However, none of the aforementioned reviews on threats to SF come with a taxonomy or a future road map for further research in this area.

On the other hand, surveys on SF and related technologies have been of interest to several researchers in recent years [52,53]. Especially, the roles of IoT [54–56] and AI [57] in SF has received great attention. Moreover, security-related aspects of SF have appeared as

part of the subject in some surveys. As an example, one may refer to the research reported by Gupta et al. [2], wherein some challenges related to the security and privacy of SF have been studied, without presenting a taxonomy of threats. As another example, a review published by Barreto et al. [58] takes an empirical approach towards the identification of cyber-security challenges of SF. However, the most relevant works to the scope of this paper are those focusing on threats to SF. Among these works, we can mention the one reported by Demestichas et al. [3], which fails to develop a taxonomy or a future roadmap. Table 1 presents the characteristics of the existing surveys in the scope of SF and PA.

Table 1. Characteristics of the existing reviews in SF and PA.

Reviews	Objective & Contribution	Considering Technology
[2]	Study on security and privacy in SF ecosystems Elaborates on potential cyber-attack scenarios Open research challenges and future directions	IoT, Wireless Sensor Network (WSN), Blockchain, AI, Machine Learning (ML)
[3]	Study on security threats in SF and agricultural IoT Highlights the innovations, techniques, and threats in SF	IoT, Blockchain, AI, ML
[38]	Applying ML methods for PA Demonstrates the impact of ML in improving the quality of the product	IoT, AI, ML
[39]	Studies the data mining approaches for the management of PA Applying Fuzzy, DBSCAN, SVM, algorithms	AI, ML
[40]	Using AI algorithms for formulating yield prediction in PA Finding the best classification algorithm, bagging, in crops	AI, ML
[41]	Designing energy-saving sensors for PA Measures temperature, soil moisture, and humidity by sensors in SF	WSN
[42]	Study WSN methods in PA and SF Plant monitoring with the image processing using field-programmable gate array (FPGA)	WSN, FPGA
[43]	Presents the importance of PA over traditional agriculture techniques Applying WSN for obtaining parameters of land	IoT, WSN
[44]	Reviews WSN applications in SF and PA	IoT, WSN
[45]	Design WSNs and smart humidity sensors for PA Comparative review of research in the field of agriculture	WSN, Very large-scale integration (VLSI)
[46]	The review outlines the applications of WSNs in agriculture Provides a taxonomy of energy-efficient techniques for WSNs in agriculture Shows opportunities for processing IoT data	IoT, WSN
[47]	Considers Raspberry Pi as visual sensor nodes in PA Applying random forest and support vector machine classifiers to classify crops	WSN, AI, ML
[48]	Studies ranging and imaging techniques for PA Develops sensing techniques to provide information about crop growth Presents innovative sensing methods in pesticide management and crop monitoring	AI, ML
[49]	Studies Routing Protocols for WSN in PA Applies Ad-Hoc, MANET, VANET and WSN to facilitate control of PA	MANET, VANET, WSN
[50]	Studies energy efficient routing protocol for IoT Based PA	IoT, WSN
[52]	Review on SF with Zinc-Fortified sprouts Considers robotic solutions with AI in agricultural techniques	IoT, AI
[54]	Review on role of IoT in SF Discusses different tools, hardware, and software used in SF	IoT
[55]	Studies the IoT effect when implementing SF Highlights security issues in IoT in agriculture Presents open research issues and challenges in IoT agriculture	IoT, WSN, AI, ML
[56]	Review on IoT-based Multidisciplinary models for SF Considers Cyber-Physical systems role in PA Applies cloud computing technologies for better production of crops	IoT, WSN, Cloud computing
[57]	Explores the advantages of using deep learning in SF Provides a bibliography containing 120 papers in SF and PA	IoT, AI, ML
[58]	Studies cyber-security challenges in SF using an empirical methodology to highlight security threats in SF systems	IoT, ICT

3. Cyber-Attacks on SF and PA

As suggested by recent research works, the main security aspects of SF and PA can be outlined as follows.

- **Privacy** is required to keep a user from unauthorized access to other users' information. Some attacks such as Physical Attack, Replay Attack, Masquerade Attack can lead to the violation of privacy. Several research works have focused on the privacy of SF and PA [59–61].
- **Integrity:** guarantees information not to be changed during storage or transmission. Integrity of PA and SF has been part of the topic in several research projects [62].
- **Confidentiality** of SF and PA, which protects data against unauthorised access has been of interest to a few researchers [61,63].
- **Availability** guarantees the continuity of the provided services. Some recent research works have focused on the availability of SF and PA [64].
- **Non-Repudiation** keeps users from repudiating what they have done in the system. The importance of non-repudiation in SF and PA has received attention from a few researchers [65].
- **Trust:** makes it impossible for a user to spoof another identity. The literature in this area comes with a few research projects focusing on authenticity of SF and PA [65].

In the absence of proper provisions for security aspects discussed above, SF and PA may be exposed to a variety of attacks that may exploit these environments and related smart information systems or cause harm, stealth, unauthorized change, or destruction on them.

In the following, attacks on SF and PA are classified on the basis of their target components.

- **Attacks on Hardware:** Unknown or unprotected vulnerabilities of IoT and cyber-physical devices (as well as other hardware components) may be exploited by professional attackers using specialised tools [66]. As good examples for this kind of attacks, we may refer to side channel and Radio frequency (RF) jamming attacks, which can violate privacy, confidentiality, or authenticity when they hit poorly-designed IoT and cyber-physical systems [2,66–68].
 - **Side Channel Attack** [2,69] aims at gathering unauthorized information regarding the implementation detail of a system via monitoring physical parameters such as electrical current or voltage. Attacks of this type violate the confidentiality of the system.
 - **RF jamming** [2,68] attacks are caused by the open nature of wireless channels and the progress in designing jamming-resistant wireless networking systems. Attacks of this type violate the availability of the systems in the SF and PA area like a greenhouse.
- **Attacks on the Network and Related Equipment:** target the network or the connected devices. This category of attacks can be further categorized as follows.
 - **Denial of Service (DoS)** [70,71] prevents users or devices from their authorized access to a resource such as a node, a server, or a communication link/network. For example, *Radio Frequency (RF) Jamming* [2,72] overwhelms the RF spectrum used by a network aiming to deny communication services to the connected nodes.
 - **MITM (Man-In-The-Middle) Attacks** [2,67,72] transparently store and replay (or in some cases modify) data transmitted over a connection. These attacks may target the confidentiality or the integrity of the system.
 - **Botnets** [2,73,74] are groups of Internet-connected devices (remote sensors), each running one bot or more. Botnets can be used for many different purposes, including Distributed DoS (DDoS) attacks, information stealing, SPAM dissemination. They can be designed to violate availability, integrity, or trust.

- **Cloud Computing Attacks** [2] misuse cloud features such as self-provisioning, on-demand services and auto-scaling to take advantage of cloud resources. For instance, an infected virtual machine can quickly spread the infecting malware to other virtual machines via the cloud. These attacks may target non-repudiation, trust, or integrity.
- **Attacks on Data:** hit the data while being stored, transmitted, or processed in the system. This category of attacks can be divided into the following subcategories [75].
 - **Data Leakage** [2,76] refers to the illegal transmission of an organization's data by a source (a person or a device) within the organization to an unauthorized external destination. This kind of attack violates the confidentiality of the data.
 - **Ransomware** [37,72] encrypts files, partitions or entire storage devices, and keeps the key secret to make the owner [77] pay a ransom. These attacks violate the privacy, trust, and integrity.
 - **Cloud Data Leakage** [76,78] is the exposure of data related to the users of an organization or the provided services, which violates the privacy of users or parties.
 - **False Data Injection** [2,79] is a title for attacks that try to feed malicious information or control commands into the system. This kind of attack targets the integrity of the data.
 - **Misconfiguration** [2] is the action of configuring the SF or the PA reporting systems in a way that reflects invalid information regarding the managed farm, which can lead to costly, disruptive decisions and actions from the farmers. Misconfiguration attacks violate the integrity.
- **Attacks on Code (applications):**
 - **Software Update Attacks** [2] violate the integrity and the availability of the system via disrupting the update process of the installed software.
 - **Malware Injection** [2,72,80] refers to attacks that infect nodes and devices by malicious codes. This kind of attack violates integrity.
 - **Buffer overflow** [72,80] is a software coding error or vulnerability that hackers can exploit to gain unauthorized access to corporate systems. This kind of attack violates availability.
 - **Indirect Attacks (SQL Injection)** [2,81] use code injection techniques in order to mislead the database server to run malicious SQL codes injected into entry fields of the database. Indirect attacks violate trust.
- **Attacks on Support Chain:** are designed to hit different components of the support chain.
 - **Third Party Attacks** [2,80] occurs when an adversary infiltrates a system via an outside partner or provider who has access to the system and/or the data. Third party attacks can violate the confidentiality or the integrity of the system.
 - **Data Fabrication** [82] involves the creation of malicious data or processes misusing an access provided for another purpose. It can lead to the violation of the system's integrity.
- **Misuse Attacks:** include attacks that misuse SF and PA physical resources in order to conduct attacks on other entities such as people or institutes.
 - **Cyber-Terrorism** [2] may use IoT systems and cyber-physical devices to attack people or premises from afar. This can lead to the violation of trust in SF and PA systems.
 - **Invalidation and /compliance** [2,83] refers to disruptions in the certification process created by fabricated false data. These attacks target the integrity of the system.

Figure 2 demonstrates the above classification of attacks on SF and PA and maps each class of attacks to the related security aspects.

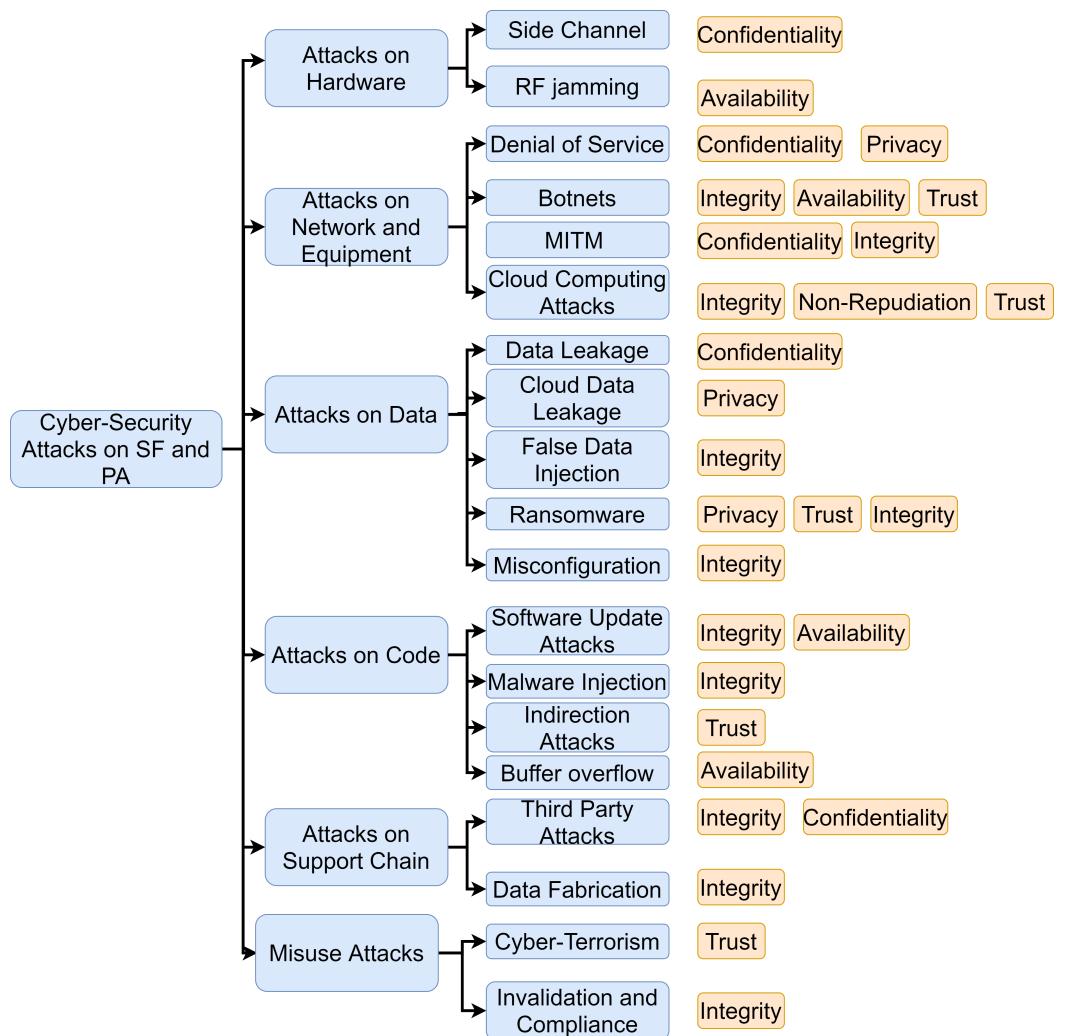


Figure 2. Classification of attacks on SF and PA.

4. CKC-Based Taxonomy on Security Threats to SF and PA

In this section, we present a CKC-based taxonomy for cyber-threats to SF and PA. Developed by Lockheed Martin [84], CKC decomposes the process of conducting a complex attack into seven stages. This decomposition improves the analyst's insight into an attack, and facilitates the study of adversarial strategies, approaches, and methods. The CKC stages of an attack are chained in a way that the whole attack scenario will fail if each of the adversaries fail to accomplish any individual stage. Our taxonomy provides a stage-by-stage operational understanding of every cyber-threat, which can be efficiently used to detect APT groups active in the area of SF and PA.

In the following, we first, introduce the CKC model in more detail, and then propose our CKC-based taxonomy.

4.1. CKC

As suggested by CKC model, a typical complex attack consists of the following stages.

1. **Reconnaissance**, where the attacker starts to identify and profile the victim via gathering as much information as possible. Any relevant information, such as email addresses, can be of interest in the reconnaissance stage. The primary goal of this stage is to discover the vulnerabilities of the victim. If properly accomplished, this stage can facilitate and accelerate a cyber-attack and make it difficult to detect via identifying the weak and strong points of the victim system. Moreover, the reconnaissance itself should not be suspicious to security mechanisms in the victim's system.

We can consider a passive and active approach for Reconnaissance. In the context of a cyberattack, passive Reconnaissance is known as footprinting. Active Reconnaissance is commonly referred to as scanning. An easy scan would be to ping every IP address owned by the destination network to see which ones went to real hosts. More sophisticated exploitation methods connect to every port number of the IP address to determine what services run on that host and which ports are open. In contrast to footprinting, scanning provides more specific information but is more intrusive. Additionally, the target may be alerted to a potential attack since scanning can trigger more abnormal connections, which must be avoided when scanning.

2. **Weaponization**, wherein the attacker designs and implements the *remote access malware (the weapon)* e.g., the backdoor, virus or worm tailored to the vulnerabilities of the victim (discovered in the reconnaissance phase).
3. **Delivery**, in which the attacker launches the remote access malware onto the victim (e.g., via a USB device, an e-mail attachment or a website).
4. **Exploitation**, which triggers the remote access malware. In this stage, the attacker utilizes the remote access malware to action on the victim and the related network in order to exploit vulnerability.
5. **Installation**, where the attacker tries to get permanent access to the victim via installing proper Command and Control (C2) servers.
6. **C2**, wherein the attacker communicates with the C2 server in order to control the victim.
7. **Action on Target**, where the attacker completes the attack scenario and achieves the final goal by compromising the victim.

The aforementioned stages are demonstrated in Figure 3. A point to note here is that not every attack goes through all of the above stages strictly and clearly. Moreover, some stages may not be observed, tracked, or reported. For example, the Reconnaissance stage is usually a secret stage, although the vulnerabilities identified in this stage may be reported later.

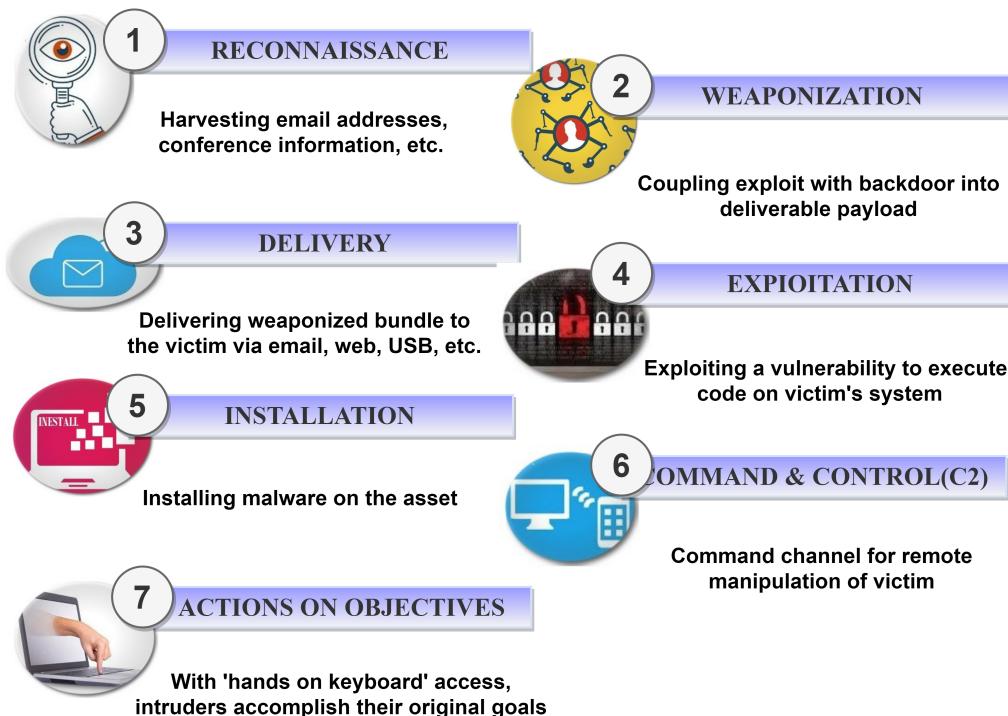


Figure 3. The stages of a typical cyber-attack according to CKC (Courtsey [85,86]).

4.2. The Taxonomy

The taxonomy presented in this subsection connects known SF and PA cyber-threats to CKC stages.

4.2.1. Threats Related to the Reconnaissance Stage

Our review demonstrates that many state-of-the-art cyber-attacks on SF focus on several layers of the multi-layered architecture to collect information in the reconnaissance stage [37]. Moreover, IoT hardware is of great interest in the reconnaissance stage for many attackers targeting SF [1,2] or PA [2,3] systems. Thus, most cyber-threats to SF and PA fall into one of the following two categories.

- **Threats to the IoT hardware:** Although IoT devices are commonly protected by software applications, they may be vulnerable to some hardware attacks such as default password attacks [2,87].
- **Threats to the multi-layer architecture:** These threats target different layers of the multi-layered architecture of Figure 1 as explained below.
 - **Physical Layer** [2,88,89]: where sensors and actuators spread over farms and greenhouses gather environmental data and transmit it through gateways or receive command and control messages via the gateways. This layer is threatened by a variety of attacks during the reconnaissance stage.
 - **Edge Layer:** SF and PA environments rely on the edge layer devices for their real-time or near real-time computations and services. In some scenarios, attackers may be able to shutdown the function of these devices, causing disruption, delay, customer dissatisfaction, and financial loss [2].
 - **Network Layer:** This layer resolves the heterogeneity of devices spread over farms and greenhouses. Moreover, this layer provides connectivity, which makes devices available to SF and PA. DoS attacks and botnets are commonly conducted in this layer [2,70,71].
 - **Cloud Layer:** This layer provides the virtualization for cloud services. Web attacks and application blocking attacks are examples of attacks on this layer [2,88].

4.2.2. Threats Related to the Weaponization Stage

Attacks on SF and PA use a variety of techniques to evade detection in the weaponization stage. Most of these techniques try to prevent the attack to be revealed by security mechanisms operating in IoT device level or in network level. Thus, we classify cyber-threats related to the weaponization stage as follows.

- **IoT Device Level Evasion:** It has been observed that defence in IoT device level mainly relies on anti-viruses and end-point security solutions embedded in or installed on devices, which detect well-known virus signatures or anomalies in behaviors. Well-designed attacks on SF and PA try to hide themselves from these mechanisms. As an example, one may refer to hollowing technique or heap spraying, which may successfully embed a malicious code inside an application even in the case the anti-virus includes the related signature [90–93].
- **Network Level Evasion:** Firewalls and Intrusion Detection/Prevention Systems (IDSs/IPSs) are the most common tools for in-network protection [94,95]. A key point to be reiterated here is that there is no completely secure solution, including firewalls and IDS/IPS. Although these tools can detect a malicious executable file, they may be unable to detect a malicious file attached to an email. Thus, they are not considered as completely-secure mechanisms in SF and PA. To evade these mechanisms, SF and PA attacks depend on a wide range of techniques, among which we can mention illegal use of well-known protocols (HTTPS, DNS, HTTP, etc.) [37] or ports (53, 80, 443, etc.) [37] as well as network spoofing [89].

4.2.3. Threats Related to the Delivery Stage

After the completion of the Weaponization stage, the adversary needs to find a way to penetrate directly or indirectly into the victim node(s) to deliver the malicious payload [96,97]. In direct penetration, the adversary personally delivers the exploit to the victim. Indirect penetration depends on a trusted third party to compromise the victim in a way that the adversary can deliver the exploit.

According to the above discussions, we can divide threats related to the delivery stage into the following categories.

- **Direct Penetration:** Malicious payloads are commonly delivered through the body or the attachments of an email [98,99], such as a fake software update or a spear-phishing link [37,100].
- **Indirect Penetration:** In the indirect penetration scenario, a communication protocol, a gateway or a web application may play the role of the trusted third party. Trusted third parties can help attackers gather information via TCP/UDP port scan, spoofing and sniffing, or launch a pre-designed backdoor [1,3].

4.2.4. Threats Related to the Exploitation Stage

Some state-of-the-art attacks on SF and PA exploit a vulnerability in the software or in the underlying Operating System (OS) to get the victim run their malicious code in the exploitation stage [37,101]. Others use SQL injection techniques for this purpose [37,102]. Accordingly, the cyber-threats related to the exploitation stage can be classified as follows.

- **Exploiting Software and OS Vulnerabilities:** Zero-day exploits are good examples for this kind of threat [103]. They are not detectable by common software vulnerability protection mechanisms. They exploit unknown software vulnerabilities for which no patch or fix is available. Moreover, viruses, worms, Trojan horses, and backdoors are common threats related to OS vulnerabilities in smart devices and consequently in SF and PA [104,105].
- **SQL injection:** In recent years, SQL injection has frequently hit data-driven applications using code injection techniques [37]. It can potentially hit SF and PA databases as well.

4.2.5. Threats Related to the Installation Stage

In the installation stage, a downloader can be fooled, codes can be injected into the memory, or unofficial applications may be installed to download malware such as rootkits and backdoors [37,106]. To this end, some attacks may exploit vulnerabilities in Operating Systems (OSs) used in IoT such as Android [107], Raspberry Pi [108], Symbian [109], or Android with Linux kernel [110]. This kind of attacks may take one or a combination of the following approaches to achieve the goal.

- Modifying registry keys [111]
- DLL Search Order Hijacking [112]
- DLL side loading [113]
- Startup Folder Modification [37]

Other attacks may exploit vulnerabilities in embedded software or firmware [114]. In this case, some of the following approaches may be taken by the attacker.

- Brute-forcing access [115]
- Buffer overflow Exploit [116]
- SMS Trojan viruses [117]
- Install unofficial Apps on mobile OS [117]

4.2.6. Threats Related to the C2 Stage

This stage is about how hackers control the victim system after completing the installation stage. This commonly happens via registering a C2 server [118]. Our studies highlight

two C2 mechanisms in attacks on SF and PA, the first of which depends on network protocols [2,88] and the second uses removable media [37,101]. Thus, we categorise threats related to the C2 stage as explained below.

- **C2s using Network Protocols:** Many common attacks on SF and PA use HTTP/HTTPS, ICMP, DNS, FTP, SMTP and other standard network protocols for their communications in the C2 stage [119,120]. For example, in many scenarios, when direct connection to an external mail server or an agriculture database server is not possible, hackers rely on backdoors that use protocols such as FTP or SMTP to penetrate into the server via sending files or emails [37,101]. Moreover, to bypass common network security mechanisms, hackers may perturb DNS packets, which makes the attack more difficult to trace [121].
- **C2s using Removable Media:** Given the features of removable media (such as USB storage), they are commonly used to bypass networks for the exfiltration of data. For example, when a disk is formatted for decreasing the size of a partition, hundreds of megabytes of data (including malicious files) can be stored at the last addresses of the disk without being lost [37].

4.2.7. Threats Related to the Action Stage

In the last stage, the adversary tries to finalize the attack and achieve the ultimate goal, which can be the exfiltration of data or damaging valuable resources, etc. In this stage, most attacks on SF and PA try to infect as many IoT devices as possible, and get access to the network and the infrastructure in order to compromise valuable targets such as edge devices, servers, etc. [2,37,122]. Moreover, attackers may try to get command line terminals such as WinExe or credentials management tools such as Mimikatz to access one computer through another using methods such as Pass the Hash (PtH) [123].

4.2.8. Threats Related to More than One Stage

Include attacks that create threats related to more than one CKC stage. In this category, we can refer to ransomware and similar attacks. Specifically, APTs cover almost all CKC stages. These attacks are individually studied in more detail in Section 5.

Figure 4 demonstrates our CKC-based taxonomy on cyber-threats to SF and PA according to the above discussions.

4.3. Case Study

In this section, we study the anatomy of the DoS attack against SF infrastructures reported by Sontowski et al. [124], and connect it to the stages of CKC.

4.3.1. The Target Environment

The target is an SF system based upon Microsoft FarmBeats 11 [125] connected to Microsoft Azure cloud. The SF system uses a Raspberry Pi, to which different kinds of sensors including ambient temperature, light, humidity, and soil moisture sensors are connected. In this system, IEEE 802.11 connects the Raspberry Pi to a Wi-Fi access point that provides cloud connection.

4.3.2. Anatomy of the Attack

On the basis of the details reported in [124], we can use the CKC methodology to study the attack as explained below.

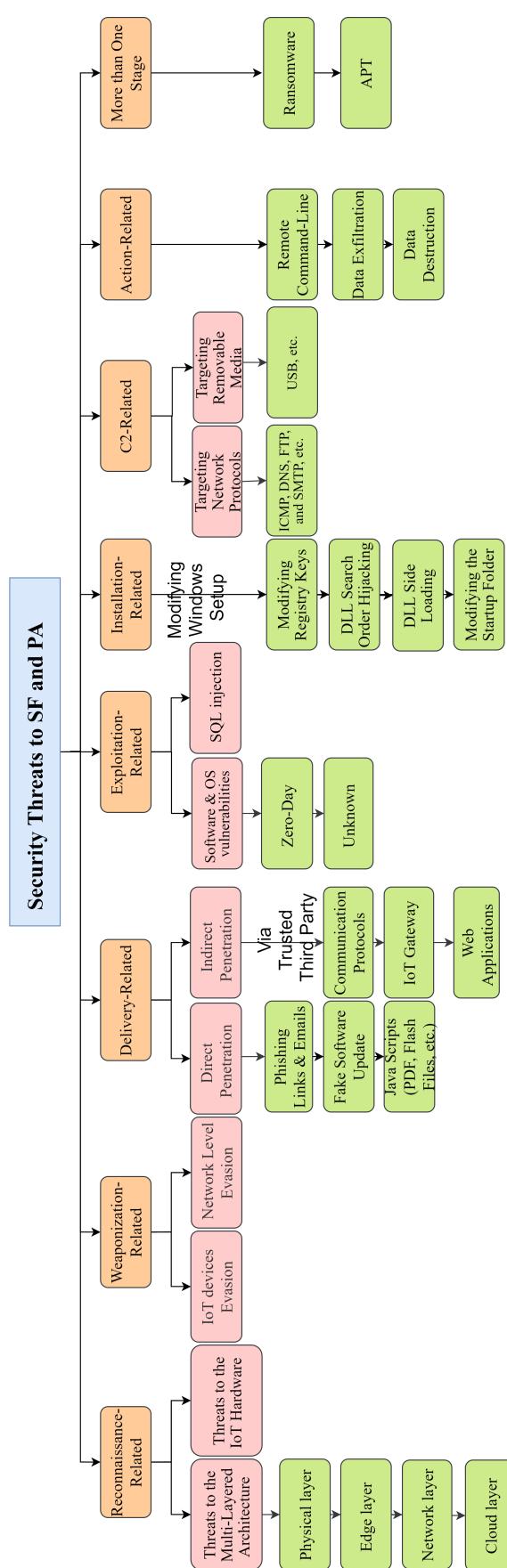


Figure 4. The CKC-based taxonomy on cyber-threats to SF and PA.

Reconnaissance:

In this stage, the attackers have studied the architecture and components of the victim's system and gathered the information mentioned in Section 4.3.1. Then they have used sniffing tools such as Wireshark in order to identify the address of the Raspberry Pi via tracking the sensor update packets it sends every few seconds/minutes. Moreover, they have identified the vulnerabilities in authentication and deauthentication mechanisms of IEEE 802.11, reported by Wright [126].

Weaponization:

In the Weaponization stage, the attackers have designed and implemented a Wi-Fi deauthentication tool capable of exploiting the vulnerabilities reported in [126] in order to disconnect the Raspberry Pi from the access point and consequently from the network and the cloud.

Delivery:

In this stage, the Wi-Fi deauther is installed on a MakerFocus ESP8266 Development Board, and imitates the Raspberry Pi via spoofing sensor update packets (using the address of the Raspberry Pi). Thereby, the deauthentication tool fools the access point because the access point perceives it as the Raspberry Pi.

Exploitation:

In this stage, the deauther fabricates and sends deauthentication notification packets to the access point (Spoofed as the Raspberry Pi). According to the IEEE 802.11 protocol, the access point is obliged to deauthenticate and disconnect the sender of these packets without the need for a new authentication. (In fact, this is the exploited vulnerability). This way, the Raspberry Pi is disconnected from the access point along with the sensors connected to it.

Installation:

The attack bypasses this phase, as it does not need any further installation after the deauther is delivered.

C2:

The attackers have designed a control panel software tool to control the deauther. This tool is installed on the MakerFocus ESP8266 Development Board along with the Raspberry Pi and plays the role of the C2 server.

Action on Target:

Since this attack is a DoS attack, the final goal is to disconnect the Raspberry Pi from the access point. Therefore, no further action is taken in this stage.

5. APTs in SF and PA

APT attacks create one of the most severe threats to SF and PA as they cover almost all CKC stages [37,101]. This severity motivates the discussions in this section, which are specifically focused on APTs as a chosen case for further study. In the rest of this section, we first introduce general APT attacks, and then go deeper into APT attacks on SF and PA. In addition to the anatomy of these attacks, we study some of their behavioral characteristics.

5.1. An Introduction to APT Attacks

APT generally refers to a threat where an adversary (or maybe a group of adversaries) are persistently connected to a network to identify and steal strategic data without being detected [127]. APTs usually target highly-strategic corporations, industries, or financial agencies as well as government institutes or national security and defence agencies, where top secret information is stored, transmitted, and processed. Information regarding military

and political plans, nuclear and aerospace technology, Intellectual Property (IP), etc. is of interest to APT groups [37,127,128]. Thus, it is pertinent to expect them to be interested in information regarding the agricultural sector as well.

APT attacks are different from other cyber-attacks in that they use personalized tools instead of more commonly used tools. Moreover, they take place over a longer period of time, which makes them more difficult to trace compared to other attacks. They utilise TTPs in a way that allows them to proceed covertly even in the presence of common IDSs or IPSs [37].

An APT attack is usually named after the researcher(s) who has (have) detected and systematically analyzed the attack. Among well-known APT attacks, one may refer to Sykipot[129], GhostNet [129], APT34 [129], APT28 [37], APT29 [37], APT30 [37], and APT37 [129].

Systematic APT attack detection and prevention methods typically depend on multi-faceted interaction between providers of security service providers and end users. Traffic monitoring, access control, and Whitelisting (monitoring and imitating access to the network from authorized domains) can be mentioned as commonly-used mechanisms used for this purpose [11,29].

5.2. APT Attacks on SF and PA

Most APT attacks on SF and PA try to gain hidden, persistent access to information regarding food chain and production network [4,129]. APT groups attempt to hit valuable targets such as greenhouses, livestock, and smart farms. To achieve their goals, APT groups depend on advanced techniques such as zero-day exploits, phishing attacks, and social engineering.

Among the consequences of ATP attacks in SF and PA, one may refer to the following.

- Theft of IP (patents, etc.)
- Stealth of critical data related to food chain, control, genetics, etc.
- Damage to important agricultural infrastructure (change to database entries or control parameters)

5.2.1. The Anatomy of an APT attack on SF or PA

A successful ATP attack on SF or PA is classically decomposed into the following three steps [130]. We map these steps to CKC stages.

1. Penetration (Infiltration):

This step can be mapped to the first three stages in CKC. Social engineering can be mentioned as a common reconnaissance technique used in this step [129]. This phase may involve vulnerability exploiting and malicious code uploading (SQL Injection). Penetration may lead to the installation of backdoors, which can provide the attacker with further access to the network.

This step is composed of the following phases.

- Testing the target for detection
- Deployment
- White noise attack
- Initial infiltration
- Outbound connection initiation

2. Further Access (Expansion):

This step may be mapped stages 4 through 6 in CKC. In this step, the attacker tries to gain longer access to the network or access to more strategic resources. The goal is getting control of critical functions and manipulating them to pave the way for the final step. This step is composed of the following phases. The following two functions can be run in this step.

- Expanding access and stealing credentials using phishing and similar techniques
- Broadening the presence

3. Information Stealth and Sabotage (Exploitation):

We can compare the final step to the last stage in CKC. In this step, APT groups may steal valuable information, shut down a strategic function, or cause damage to the system.

Critical business information regarding the production value or cultivation process of livestock or crops may be of interest to APT groups in this step. These kinds of information can be sold to a rival or used to undermine the production process. The stolen data may be stored somewhere inside the victim network for covert transportation in the future.

APT attacks commonly use white noise techniques (maybe in the form of a DDoS attack) to evade detection systems [131].

This step is typically composed of the following phases.

- White noise attack
- Extra data collection
- Covering tracks

Figure 5 demonstrates the anatomy of an APT attack.

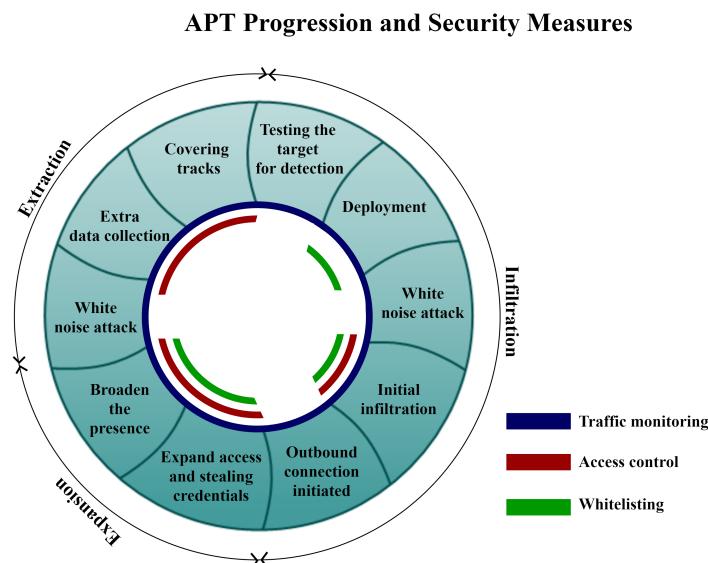


Figure 5. The anatomy of an APT attack.

5.3. Some Behavioral Characteristics of APT Attacks on SF or PA

In this subsection, we study some behavioral characteristics of APT attacks on SF and PA. In the following, we mention some symptoms that may be considered as warnings for an active APT attack.

- Unusual and suspicious activities in security and control systems (especially the high-level access systems)
- Widespread use of backdoor tools (Most of them can be detected by common IDSs.)
- Suspicious and unusual activities occurring in the databases
- Evidences for data and information stealth

6. Risk Mitigation Strategies and Countermeasure

Our discussions on attacks and threats related to SF and PA highlight the need for a study on related risk mitigation strategies and countermeasures for different IoT attacks and security threats in SF and PA, which can be considered as the important side of research in this area. Tables 2 and 3 summarize our studies in this regard.

While it is not necessarily feasible for every farmer to be an expert at technology and cyber-security threats in agriculture, there are some cyber-safe behaviours farmers

can perform to reduce the security risk. These include dynamic and secure passwords, frequently password changeover, data encryption, 2-factor user authentication, and updating software when prompted [132,133]. Avoidance of suspicious emails, links, and not saving personal or financial data on browsers and auto-fill features are recommended too [132,133]. Likewise, farmers should only make data-driven decisions when systems are demonstrably secure. Not only should farmers be wary of cyber-security threats, but it is imperative that the various stakeholders involved along the food production chain be cognizant of the risks. Farmers often are sharing data with trusted advisors, researchers, suppliers, and buyers - therefore, cyber-safe behaviours need to be encouraged throughout the data ecosystem.

Physical access controls and other physical behaviours can also reduce security risk. For instance, it is prudent to inspect and maintain devices regularly to prevent environmental and personal complications that could obscure security measures [133]. Creating back-ups of data helps reduce impact severity when data is stolen, and farmer access is denied. Protecting sensitive information, documents, and devices by placing them in secure spaces like locked cabinets, rooms, and off-site caches can also reduce security risk [133].

Blockchain technology has been applied to some architectures to ensure data privacy and security as well as addressing fault tolerance, access control, and third-party removal to tackle these challenges [3,134,135]. We summarize existing research on intensifying security issues and privacy in IoT and ICT usage in the agricultural sector. Table 3 outlines a list of countermeasures that can be taken versus security features threats and threats layer in a smart farming environment. In fact, understanding and considering them is a viable way to obtain security threat mitigation in SF and PA environments.

Table 2. Risk Mitigation Strategies for SF and PA.

Strategy	IoT Layer	Related Security Aspect
User Authentication [136–143]	Middleware	Privacy, Confidentiality, Authenticity
Secure Passwords [137–144]	Middleware	Privacy, Confidentiality, Authenticity
Device-Level Encryption [136–140,143,144]	Edge layer	Privacy, Integrity Middleware
Communication-Level Encryption (SSL/TLS) [65,137–144]	Access Gateway	Confidentiality, Integrity, Authenticity
Port Hardening [3,65,137,139–142]	Internet, Cloud	Privacy, Authenticity, Non-Repudiation
Remote Login Deactivation [137–143]	Internet, Cloud	Privacy, Authenticity, Non-Repudiation
Regular Firmware Update [3,138–142,144,145]	Application	Privacy, Confidentiality, Availability

Table 3. Attack Countermeasures for SF and PA.

Measure	IoT Layer	Related Security Aspect
Password Recovery Made Safe [65,137–141,144]	Middleware	Privacy, Confidentiality, Authenticity
Unauthorized Account Deactivation [138–140,142,144]	Edge layer	Privacy, Confidentiality, Authenticity
Periodic Device Evaluation [65,137,139–141,143,144]	Edge layer	Privacy, Availability

7. Future Roadmap

In this section, we discuss some open research challenges related to the security of SF and PA. While in this paper, we begin the first steps in creating novel SF/PA mitigation strategies by reviewing the literature, developing a taxonomy, and conducting a case study on APTs. Future research can build upon this through interdisciplinary research that draws on knowledge from farmers, SF tool developers, and computer scientists to test the mitigation techniques mentioned here and to develop more specific strategies to the SF and PA context. Listed below, these challenges can highlight a future road map for further research in this area.

- **Access Control from a Security Perspective:**
Dealing with hired labor and livestock, the owners of farms, greenhouses, etc. are traditionally concerned about access control. However, they need to adopt a security perspective for their property. Authentication, authorization, and accounting should be incorporated to prevent unauthorized access, which is the stepping stone in many severe attacks on SF and PA. Although the literature in this area comes with some relevant research reports [1–3,41,50], there is still opportunities for systematic research.
- **Data Protection:**
Given, the abilities of smart devices and IoT, enormous data acquisition, communication and processing is a well-known characteristic of SF and PA [1,2]. This raises the need for efficient data protection mechanisms, which has been of interest to a few researchers [1,2]. However, data protection can still be considered as an open research challenge in this area.
- **Network Infrastructure and Physical Layer Protection:**
The physical layer and the network infrastructure play critical roles in SF and PA. They are targeted by several attacks [3]. Although a few research projects have focused on this topic [4,9,81,135,136], research in this area still needs to be developed.
- **Education as Risk Reduction:** The social elements of reducing cyber-risks, such as education, has received relatively little attention by scholars [146]. Not only are farmers interested in education regarding security threats to their operations, but education is regarded as a vital tool for reducing security risk [132,147,148]. Future research opportunities exist in assessing what cyber-safe behaviours farmers currently utilize. From this, there can be investigation of what educational formats, content, and dispersion would be most effective and appreciated by these vital stakeholders.
- **Specific Secure Communication Protocols for SF and PA:**
In SF and PA, where sensors, actuators, drones, autonomous tractors and other smart devices are spread out in various locations, communication protocols are of critical importance. Although several network, Machine-to-Machine (M2M) and IoT protocols such as Bluetooth, NFC, WiFi, SSL, TCP, UDP and 6loWPA have been adopted from other technologies [3,121,149], there is still room for research on secure protocols specifically designed and standardized for SF and PA.

- **Secure Smart Devices:** Given the threats to smart devices used in SF and PA (studied in previous sections), security needs to be taken into consideration in design and implementation phases of these devices.
- **Secure AI Adoption:** In recent years, some researchers have been concerned about the application of AI in SF and PA [2,3]. Thus, the security threats to AI such as adversarial attacks [1,2] can motivate future research on secure AI in SF and PA. Informed by this taxonomy of cyber-threats, strengthening policy regarding cyber-security in PA is an important consideration for future research. Legal frameworks designed to protect private data and ensure privacy are key to addressing the challenge of cyber-security arising from new farming technologies [150]. Reviews on the social science of PA have highlighted that future research needs to address how policy-makers should respond to cyber-attacks on agri-food systems [151].

8. Conclusions

SF and PA have the potential to enhance global food security and reduce agriculture's impact on the environment, however to be able to realize this potential these technologies need to be protected from cyber-attacks. It's clear right now that there are plenty of cyber-attacks and security threats in this area. These attacks can impose serious disruptions to global markets and especially to the economies of developing nations that are heavily dependent on the agriculture industry. In this paper, we considered the security of SF and PA, which is a critical need in the field of smart farming. We highlighted important security aspects needed to be considered in SF and PA. We presented a survey on attacks that violate each of these security aspects. Accordingly, we introduced cyber-threats to SF and PA. It is a viable source to tackle existing security issues here. Our studies on SF and PA cyber-threats led to a systematic CKC-based taxonomy on these threats. Among the mentioned threats, we chose APTs for further studies. We studied the anatomy as well as behavioral characteristics of APTs. Moreover, we presented a survey on risk mitigation strategies and countermeasures against attacks on SF and PA. Lastly, we developed a future road map to pave the way for future research in this area.

Author Contributions: Authors contribution A.Y.: Conceptualization, Validation, Data curation, Writing—original draft, Writing—review & editing; B.Z.: Conceptualization, Methodology, Validation, Data curation, Writing—A.A. and A.D.: Methodology, Validation, Writing—original draft; H.K.: Conceptualization, Methodology, Writing—review & editing, Supervision; E.F., A.G.G., C.R. and E.D.: Conceptualization, Methodology, Writing—review & editing, Supervision. All authors have read and agreed to the published version of the manuscript.

Funding: This research is supported by Canada First Research Excellence Fund Food from Thought.

Institutional Review Board Statement: Not applicable.

Informed Consent Statement: Not applicable.

Data Availability Statement: Not applicable.

Conflicts of Interest: The authors declared that there is no conflict of interest in this study.

References

1. Roopaei, M.; Rad, P.; Choo, K.K.R. Cloud of things in smart agriculture: Intelligent irrigation monitoring by thermal imaging. *IEEE Cloud Comput.* **2017**, *4*, 10–15. [[CrossRef](#)]
2. Gupta, M.; Abdelsalam, M.; Khorsandrost, S.; Mittal, S. Security and privacy in smart farming: Challenges and opportunities. *IEEE Access* **2020**, *8*, 34564–34584. [[CrossRef](#)]
3. Demestichas, K.; Peppes, N.; Alexakis, T. Survey on Security Threats in Agricultural IoT and Smart Farming. *Sensors* **2020**, *20*, 6458. [[CrossRef](#)] [[PubMed](#)]
4. Lin, J.; Shen, Z.; Zhang, A.; Chai, Y. Blockchain and IoT based food traceability system. *Int. J. Inf. Technol.* **2018**, *24*, 1–16.
5. Gia, T.N.; Qingqing, L.; Queralta, J.P.; Zou, Z.; Tenhunen, H.; Westerlund, T. Edge AI in smart farming IoT: CNNs at the edge and fog computing with LoRa. In Proceedings of the IEEE AFRICON, Accra, Ghana, 25 September 2019.
6. Jahn, M.M.; Oemichen, W.L.; Treverton, G.F. *Cyber Risk and Security Implications in Smart Agriculture and Food Systems*; Technical Report; College of Agriculture and Life Sciences, University of Wisconsin: Madison, WI, USA, 2019.

7. Kasten, J. Blockchain on the Farm: A Systematic Literature Review. *J. Strateg. Innov. Sustain.* **2020**, *15*, 129–153.
8. Abuan, D.D.; Abad, A.C.; Lazaro, J.B., Jr.; Dadios, E.P. Security systems for remote farm. *J. Autom. Control Eng.* **2014**, *2*, 1–4. [[CrossRef](#)]
9. Vangala, A.; Sutrala, A.K.; Das, A.K.; Jo, M. Smart Contract-Based Blockchain-Envisioned Authentication Scheme for Smart Farming. *IEEE Internet Things J.* **2021**, *8*, 10792–10806. [[CrossRef](#)]
10. Sa, I.; Chen, Z.; Popović, M.; Khanna, R.; Liebisch, F.; Nieto, J.; Siegwart, R. weedNet: Dense Semantic Weed Classification Using Multispectral Images and MAV for Smart Farming. *IEEE Robot. Autom. Lett.* **2018**, *3*, 588–595. [[CrossRef](#)]
11. Su, J.; Yi, D.; Su, B.; Mi, Z.; Liu, C.; Hu, X.; Xu, X.; Guo, L.; Chen, W.H. Aerial Visual Perception in Smart Farming: Field Study of Wheat Yellow Rust Monitoring. *IEEE Trans. Ind. Inf.* **2021**, *17*, 2242–2249. [[CrossRef](#)]
12. Shadrin, D.; Menshchikov, A.; Somov, A.; Bornemann, G.; Hauslage, J.; Fedorov, M. Enabling Precision Agriculture Through Embedded Sensing With Artificial Intelligence. *IEEE Trans. Instrum. Meas.* **2020**, *69*, 4103–4113. [[CrossRef](#)]
13. Sambo, D.W.; Forster, A.; Yenke, B.O.; Sarr, I.; Gueye, B.; Dayang, P. Wireless Underground Sensor Networks Path Loss Model for Precision Agriculture (WUSN-PLM). *IEEE Sens. J.* **2020**, *20*, 5298–5313. [[CrossRef](#)]
14. Gigli, M.; Koo, S. Internet of things: Services and applications categorization. *Adv. Internet Things* **2011**, *1*, 27–31. [[CrossRef](#)]
15. Al-Fuqaha, A.; Guizani, M.; Mohammadi, M.; Aledhari, M.; Ayyash, M. Internet of things: A survey on enabling technologies, protocols, and applications. *IEEE Commun. Surv. Tutor.* **2015**, *17*, 2347–2376. [[CrossRef](#)]
16. Atzori, L.; Iera, A.; Morabito, G. The internet of things: A survey. *Comput. Netw.* **2010**, *54*, 2787–2805. [[CrossRef](#)]
17. Gubbi, J.; Buyya, R.; Marusic, S.; Palaniswami, M. Internet of Things (IoT): A vision, architectural elements, and future directions. *Future Gener. Comput. Syst.* **2013**, *29*, 1645–1660. [[CrossRef](#)]
18. Kamienski, C.; Soininen, J.P.; Taumberger, M.; Fernandes, S.; Toscano, A.; Cinotti, T.S.; Maia, R.F.; Neto, A.T. Swamp: An iot-based smart water management platform for precision irrigation in agriculture. In Proceedings of the Global Internet of Things Summit (GIoTS), Bilbao, Spain, 4–7 June 2018.
19. Hu, X.; Qian, S. IoT application system with crop growth models in facility agriculture. In Proceedings of the 6th International Conference on Computer Sciences and Convergence Information Technology (ICCIT), Seogwipo, Korea, 29 November 2011.
20. Stovces, M.; Vanvek, J.; Masner, J.; Pavlik, J. Internet of things (iot) in agriculture-selected aspects. *Agris On-line Pap. Econ. Inf.* **2016**, *8*, 8388.
21. Burton, L.; Dave, N.; Fernandez, R.; Jayachandran, K.; Bhansali, S. Smart gardening IoT soil sheets for real-time nutrient analysis. *J. Electr. Soc.* **2018**, *165*, B3156–B3162. [[CrossRef](#)]
22. Malik, A.W.; Rahman, A.U.; Qayyum, T.; Ravana, S.D. Leveraging Fog Computing for Sustainable Smart Farming Using Distributed Simulation. *IEEE Internet Things J.* **2020**, *7*, 3300–3309. [[CrossRef](#)]
23. Chukkapalli, S.S.L.; Mittal, S.; Gupta, M.; Abdelsalam, M.; Joshi, A.; Sandhu, R.; Joshi, K. Ontologies and Artificial Intelligence Systems for the Cooperative Smart Farming Ecosystem. *IEEE Access* **2020**, *8*, 164045–164064. [[CrossRef](#)]
24. Bacco, M.; Berton, A.; Gotta, A.; Caviglione, L. IEEE 802.15.4 Air-Ground UAV Communications in Smart Farming Scenarios. *IEEE Commun. Lett.* **2018**, *22*, 1910–1913. [[CrossRef](#)]
25. Chebrolu, N.; Läbe, T.; Stachniss, C. Robust Long-Term Registration of UAV Images of Crop Fields for Precision Agriculture. *IEEE Robot. Autom. Lett.* **2018**, *3*, 3097–3104. [[CrossRef](#)]
26. Bayrakdar, M.E. A Smart Insect Pest Detection Technique With Qualified Underground Wireless Sensor Nodes for Precision Agriculture. *IEEE Sens. J.* **2019**, *19*, 10892–10897. [[CrossRef](#)]
27. Huang, K.; Shu, L.; Li, K.; Yang, F.; Han, G.; Wang, X.; Pearson, S. Photovoltaic Agricultural Internet of Things Towards Realizing the Next Generation of Smart Farming. *IEEE Access* **2020**, *8*, 76300–76312. [[CrossRef](#)]
28. Verdouw, C.; Tekinerdogan, B.; Beulens, A.; Wolfert, S. Digital twins in smart farming. *Agric. Syst.* **2021**, *189*, 103046. [[CrossRef](#)]
29. Shabadi, L.S.; Biradar, H.B. Design and implementation of IOT based smart security and monitoring for connected smart farming. *Int. J. Comput. Appl.* **2018**, *179*, 1–4.
30. 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](#)]
31. Yazdinejad, A.; Parizi, R.M.; Dehghanianha, A.; Karimipour, H. Federated learning for drone authentication. *Ad Hoc Netw.* **2021**, *120*, 102574. [[CrossRef](#)]
32. Chae, C.J.; Cho, H.J. Enhanced secure device authentication algorithm in P2P-based smart farm system. *Peer-to-Peer Netw. Appl.* **2018**, *11*, 1230–1239. [[CrossRef](#)]
33. West, J. A prediction model framework for cyber-attacks to precision agriculture technologies. *J. Agric. Food Inf.* **2018**, *19*, 307–330. [[CrossRef](#)]
34. Window, M. Security in Precision Agriculture: Vulnerabilities and Risks of Agricultural Systems. Master’s Thesis, Department of Computer Science, Lulea University of Technology, Lulea, Sweden, 2019.
35. Grgic, K.; Zagar, D.; Krizanovic, V. Security in IPv6-based wireless sensor network—Precision agriculture example. In Proceedings of the 12th International Conference on Telecommunications, Zagreb, Croatia, 26 June 2013.
36. Chi, H.; Welch, S.; Vasserman, E.; Kalaimannan, E. A framework of cybersecurity approaches in precision agriculture. In Proceedings of the ICMLG2017 5th International Conference on Management Leadership and Governance, Johannesburg, South Africa, 16 March 2017.

37. Bahrami, P.N.; Dehghanianha, A.; Dargahi, T.; Parizi, R.M.; Choo, K.K.R.; Javadi, H.H. Cyber kill chain-based taxonomy of advanced persistent threat actors: Analogy of tactics, techniques, and procedures. *J. Inf. Process. Syst.* **2019**, *15*, 865–889.
38. Sharma, A.; Jain, A.; Gupta, P.; Chowdary, V. Machine Learning Applications for Precision Agriculture: A Comprehensive Review. *IEEE Access* **2020**, *9*, 4843–4873. [[CrossRef](#)]
39. Janrao, P.; Palivel, H. Management zone delineation in Precision agriculture using data mining: A review. In Proceedings of the International Conference on Innovations in Information, Embedded and Communication Systems (ICIIECS), Coimbatore, India, 19–20 March 2015.
40. Savla, A.; Israni, N.; Dhawan, P.; Mandholia, A.; Bhadada, H.; Bhardwaj, S. Survey of classification algorithms for formulating yield prediction accuracy in precision agriculture. In Proceedings of the International Conference on Innovations in Information, Embedded and Communication Systems (ICIIECS), Coimbatore, India, 19–20 March 2015.
41. Kumar, S.; Kumar, N.; Saini, R.K. Energy-Saving Sensors for Precision Agriculture in Wireless Sensor Network: A Review. In Proceedings of the Women Institute of Technology Conference on Electrical and Computer Engineering (WITCON ECE), Piscataway, NJ, USA, 22–23 November 2019.
42. Deepika, G.; Rajapirian, P. Wireless sensor network in precision agriculture: A survey. In Proceedings of the International Conference on Emerging Trends in Engineering, Technology and Science (ICETETS), Pudukkottai, India, 24–26 February 2016.
43. Goel, K.; Bindal, A.K. Wireless Sensor Network in Precision Agriculture: A Survey Report. In Proceedings of the Fifth International Conference on Parallel, Distributed and Grid Computing (PDGC), Solan, India, 20–22 December 2018.
44. Huerta, M.; Garcia, A.; Guillermo, J.C.; Martinez, R.C. Wireless Sensor Networks Applied to Precision Agriculture: A worldwide literature review with emphasis on Latin America. *IEEE Geosci. Remote Sens. Mag.* **2021**. [[CrossRef](#)]
45. Imam, S.A.; Choudhary, A.; Sachan, V.K. Design issues for wireless sensor networks and smart humidity sensors for precision agriculture: A review. In Proceedings of the International Conference on Soft Computing Techniques and Implementations (ICSCTI), Faridabad, India, 8–10 October 2015.
46. Jawad, H.M.; Nordin, R.; Gharghan, S.K.; Ismail, A.M.J.M. Energy-Efficient Wireless Sensor Networks for Precision Agriculture: A Review. *Sensors* **2017**, *17*, 1781. [[CrossRef](#)]
47. Kamath, R.; Balachandra, M.; Prabhu, S. Raspberry Pi as Visual Sensor Nodes in Precision Agriculture: A Study. *IEEE Access* **2019**, *7*, 45110–45122. [[CrossRef](#)]
48. Narvaez, F.Y.; Reina, G.; Torres-Torriti, M.; Kantor, G.; Cheein, F.A. A Survey of Ranging and Imaging Techniques for Precision Agriculture Phenotyping. *IEEE/ASME Trans. Mechatron.* **2017**, *22*, 2428–2439. [[CrossRef](#)]
49. Deroussi, A.; Alihamidi, I.; Charaf, L.A.; Madi, A.A.; Addaim, A. Routing Protocols for WSN: A Survey Precision Agriculture Case Study. In Proceedings of the IEEE 2nd International Conference on Electronics, Control, Optimization and Computer Science (ICECOCS), Kenitra, Morocco, 2–3 December 2020.
50. Lakshmi, T.A.; Hariharan, B.; Rekha, P. A Survey on Energy Efficient Routing Protocol for IoT Based Precision Agriculture. In Proceedings of the International Conference on Communication and Electronics Systems (ICCES), Coimbatore, India, 17–19 July 2019.
51. Boghossian, A.; Linsky, S.; Mutschler, P.; Ulicny, B.; Barrett, L.; Bethel, G.; Matson, M.; Strang, T.; Ramsdell, K.W.; Koehler, S. *Threats to Precision Agriculture*; Technical Report; United States Department of Homeland Security and Office of Intelligence and Analysis: Washington, DC, USA, 2018.
52. Ahmed, B.K.I.; Prakash, A.; Husna, M.S.; Prakash, A. A Review on Smart Farming with Zinc-Fortified Sprouts. In Proceedings of the Fourth World Conference on Smart Trends in Systems, Security and Sustainability (WorldS4), London, UK, 27 July 2020.
53. Sreedevi, T.R.; Kumar, M.S. Digital Twin in Smart Farming: A Categorical Literature Review and Exploring Possibilities in Hydroponics. In Proceedings of the Advanced Computing and Communication Technologies for High Performance Applications (ACCTHPA), Kerala, India, 2 July 2020.
54. Bhagat, M.; Kumar, D.; Kumar, D. Role of Internet of Things (IoT) in Smart Farming: A Brief Survey. In Proceedings of the 2019 Devices for Integrated Circuit (DevIC), Kalyani, India, 23 March 2019.
55. 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](#)]
56. Biradar, H.B.; Shabadi, L. Review on IOT based multidisciplinary models for smart farming. In Proceedings of the 2nd IEEE International Conference on Recent Trends in Electronics, Information & Communication Technology (RTEICT), Bangalore, India, 19 May 2017.
57. Ünal, Z. Smart Farming Becomes Even Smarter With Deep Learning—A Bibliographical Analysis. *IEEE Access* **2020**, *8*, 105587–105609. [[CrossRef](#)]
58. Barreto, L.; Amaral, A. Smart farming: Cyber security challenges. In Proceedings of the International Conference on Intelligent Systems (IS), Phuket, Thailand, 28 September 2018.
59. Idoje, G.; Dagiuklas, T.; Iqbal, M. Survey for smart farming technologies: Challenges and issues. *Comput. Electr. Eng.* **2021**, *92*, 107104. [[CrossRef](#)]
60. 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](#)]

61. Ametepe, A.F.X.; Ahouandjinou, S.A.R.; Ezin, E.C. Secure encryption by combining asymmetric and symmetric cryptographic method for data collection WSN in smart agriculture. In Proceedings of the IEEE International Smart Cities Conference (ISC2), Casablanca, Morocco, 19 October 2019.
62. Chamarajnagar, R.; Ashok, A. Integrity threat identification for distributed IoT in precision agriculture. In Proceedings of the 16th Annual IEEE International Conference on Sensing, Communication, and Networking (SECON), Boston, MA, USA, 10 June 2019.
63. Zhang, N.; Wu, R.; Yuan, S.; Yuan, C.; Chen, D. RAV: Relay aided vectorized secure transmission in physical layer security for Internet of Things under active attacks. *IEEE Internet Things J.* **2019**, *6*, 8496–8506. [CrossRef]
64. Bisogni, F.; Cavallini, S.; Di Trocchio, S. Cybersecurity at European level: The role of information availability. *Commun. Strateg.* **2011**, *81*, 105–124.
65. 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]
66. Xue, M.; Gu, C.; Liu, W.; Yu, S.; O'Neill, M. Ten years of hardware Trojans: A survey from the attacker's perspective. *IET Comput. Digit. Tech.* **2020**, *14*, 231–246. [CrossRef]
67. Alrajhi, A.M. A survey of Artificial Intelligence techniques for cybersecurity improvement. *Int. J. Cyber-Secur. Digit. Forensic* **2020**, *9*, 34–41. [CrossRef]
68. Jahromi, A.N.; Karimipour, H.; Dehghantanha, A.; Choo, K.K.R. Toward Detection and Attribution of Cyber-Attacks in IoT-enabled Cyber-physical Systems. *IEEE Internet Things J.* **2021**. [CrossRef]
69. Ukil, A.; Sen, J.; Koilakonda, S. Embedded security for Internet of Things. In Proceedings of the 2011 2nd National Conference on Emerging Trends and Applications in Computer Science, Shillong, India, 4 May 2011; pp. 1–6.
70. Kolias, C.; Kambourakis, G.; Stavrou, A.; Voas, J. DDoS in the IoT: Mirai and other botnets. *Computer* **2017**, *50*, 80–84. [CrossRef]
71. Antonakakis, M.; April, T.; Bailey, M.; Bernhard, M.; Bursztein, E.; Cochran, J.; Durumeric, Z.; Halderman, J.A.; Invernizzi, L.; Kallitsis, M.; et al. Understanding the mirai botnet. In Proceedings of the 26th USENIX Security Symposium, Vancouver, BC, Canada, 16 August 2017; pp. 1093–1110.
72. Ye, D.; Zhang, T.Y. Summation detector for false data-injection attack in cyber-physical systems. *IEEE Trans. Cybern.* **2019**, *50*, 2338–2345. [CrossRef] [PubMed]
73. Al Shorman, A.; Faris, H.; Aljarah, I. Unsupervised intelligent system based on one class support vector machine and Grey Wolf optimization for IoT botnet detection. *J. Ambient Intell. Humaniz. Comput.* **2020**, *11*, 2809–2825. [CrossRef]
74. What Is a Botnet Attack Work? Available online: <https://www.akamai.com/us/en/resources/what-is-a-botnet.jsp> (accessed on 5 December 2017).
75. Fard, S.M.H.; Karimimpour, H.; Dehghantanha, A.; Jahromi, A.N.; Srivastava, G. Ensemble sparse representation-based cyber threat hunting for security of smart cities. *Comput. Electr. Eng.* **2020**, *88*, 106825. [CrossRef]
76. Purohit, B.; Singh, P.P. Data leakage analysis on cloud computing. *Int. J. Eng. Res. Appl.* **2013**, *3*, 1311–1316.
77. Dovom, E.M.; Azmoodeh, A.; Dehghantanha, A.; Newton, D.E.; Parizi, R.M.; Karimipour, H. Fuzzy pattern tree for edge malware detection and categorization in IoT. *J. Syst. Arch.* **2019**, *97*, 1–7. [CrossRef]
78. Priebe, C.; Muthukumaran, D.; O'Keeffe, D.; Eyers, D.; Shand, B.; Kapitza, R.; Pietzuch, P. Cloudsafetynet: Detecting data leakage between cloud tenants. In Proceedings of the 6th edition of the ACM Workshop on Cloud Computing Security, New York, NY, USA, 7 November 2014; pp. 117–128.
79. Musleh, A.S.; Chen, G.; Dong, Z.Y. A survey on the detection algorithms for false data injection attacks in smart grids. *IEEE Transac. Smart Grid* **2019**, *11*, 2218–2234. [CrossRef]
80. Gruschka, N.; Jensen, M. Attack surfaces: A taxonomy for attacks on cloud services. In Proceedings of the 2010 IEEE 3rd International Conference on Cloud Computing, Miami, FL, USA, 5 July 2010; pp. 276–279.
81. Stoica, I.; Adkins, D.; Zhuang, S.; Shenker, S.; Surana, S. Internet indirection infrastructure. *IEEE/ACM Trans. Netw.* **2004**, *12*, 205–218. [CrossRef]
82. Khan, S.; Bagiwa, M.A.; Wahab, A.W.A.; Gani, A.; Abdelaziz, A. Understanding link fabrication attack in software defined network using formal methods. In Proceedings of the 2020 IEEE International Conference on Informatics, IoT, and Enabling Technologies (ICIoT), Doha, Qatar, 2 February 2020; pp. 555–562.
83. Cuker, B.E. Livestock and Poultry: Other Colonists Who Changed the Food System of the Chesapeake Bay. In *Diet for a Sustainable Ecosystem*; Springer: Berlin/Heidelberg, Germany, 2020; pp. 219–244.
84. The Cyber Kill Chain. Available online: <https://www.lockheedmartin.com/en-us/capabilities/cyber/cyber-kill-chain.html> (accessed on 5 March 2021).
85. Hutchins, E.M.; Cloppert, M.J.; Amin, R.M. Intelligence-driven computer network defense informed by analysis of adversary campaigns and intrusion kill chains. *Lead. Issues Inf. Warf. Secur. Res.* **2011**, *1*, 80.
86. Meyers, C.A.; Powers, S.; Faissol, D.M. *Taxonomies of Cyber Adversaries and Attacks: A Survey of Incidents and Approaches*; Technical Report; Lawrence Livermore National Laboratory (LLNL): Livermore, CA, USA, 2009.
87. Sidhu, S.; Mohd, B.J.; Hayajneh, T. Hardware security in IoT devices with emphasis on hardware Trojans. *J. Sens. Actuator Netw.* **2019**, *8*, 42. [CrossRef]
88. Vasisht, D.; Kapetanovic, Z.; Won, J.; Jin, X.; Chandra, R.; Sinha, S.; Kapoor, A.; Sudarshan, M.; Stratman, S. Farmbeats: An iot platform for data-driven agriculture. In Proceedings of the 14th USENIX Symposium on Networked Systems Design and Implementation, Boston, MA, USA, 27 March 2017.

89. Yazdinejadna, A.; Parizi, R.M.; Dehghantanha, A.; Khan, M.S. A kangaroo-based intrusion detection system on software-defined networks. *Comput. Netw.* **2021**, *184*, 107688. [[CrossRef](#)]
90. Lengyel, T.K.; Maresca, S.; Payne, B.D.; Webster, G.D.; Vogl, S.; Kiayias, A. Scalability, fidelity and stealth in the drakovuf dynamic malware analysis system. In Proceedings of the 30th Annual Computer Security Applications Conference, New York, NY, USA, 8 December 2014.
91. Lengyel, T.K. Malware Collection and Analysis via Hardware Virtualization. Ph.D. Thesis, University of Connecticut, Graduate School, Mansfield, CT, USA, 2015.
92. Process Hollowing. Available online: <http://www.autosectools.com/process-hollowing.pdf> (accessed on 4 March 2021).
93. HaddadPajouh, H.; Dehghantanha, A.; Parizi, R.M.; Aledhari, M.; Karimipour, H. A survey on internet of things security: Requirements, challenges, and solutions. *Internet Things* **2019**, *14*, 100129. [[CrossRef](#)]
94. Nissim, N.; Cohen, A.; Elovici, Y. Boosting the detection of malicious documents using designated active learning methods. In Proceedings of the 2015 IEEE 14th International Conference on Machine Learning and Applications (ICMLA), Miami, FL, USA, 9 December 2015.
95. Shafiq, M.Z.; Khayam, S.A.; Farooq, M. Embedded malware detection using markov n-grams. In Proceedings of the International Conference on Detection of Intrusions and Malware, and Vulnerability Assessment, Paris, France, 10 July 2008.
96. Sood, A.K.; Zeadally, S. A taxonomy of domain-generation algorithms. *IEEE Secur. Priv.* **2016**, *14*, 46–53. [[CrossRef](#)]
97. Karim, A.; Salleh, R.B.; Shiraz, M.; Shah, S.A.A.; Awan, I.; Anuar, N.B. Botnet detection techniques: Review, future trends, and issues. *J. Zhejiang Univ. Sci. C* **2014**, *15*, 943–983. [[CrossRef](#)]
98. Al-Taharwa, I.A.; Lee, H.M.; Jeng, A.B.; Wu, K.P.; Mao, C.H.; Wei, T.E.; Chen, S.M. Redjsod: A readable javascript obfuscation detector using semantic-based analysis. In Proceedings of the IEEE 11th International Conference on Trust, Security and Privacy in Computing and Communications, Liverpool, UK, 25 June 2012.
99. Cosovan, D.; Benchea, R.; Gavrilut, D. A practical guide for detecting the java script-based malware using hidden markov models and linear classifiers. In Proceedings of the 16th International Symposium on Symbolic and Numeric Algorithms for Scientific Computing, Timisoara, Romania, 22 September 2014.
100. Subrahmanian, V.; Ovelgonne, M.; Dumitras, T.; Prakash, B.A. *The Global Cyber-Vulnerability Report*; Springer: Berlin/Heidelberg, Germany, 2015.
101. Singh, V.K.; Govindarasu, M. Cyber Kill Chain-Based Hybrid Intrusion Detection System for Smart Grid. In *Wide Area Power Systems Stability, Protection, and Security*; Springer: Cham, Switzerland, 2021; pp. 571–599.
102. Yadav, T.; Rao, A.M. Technical aspects of cyber kill chain. In Proceedings of the International Symposium on Security in Computing and Communication, Kochi, India, 10 August 2015.
103. Ablon, L.; Bogart, A. *Zero Days, Thousands of Nights: The Life and Times of Zero-Day Vulnerabilities and Their Exploits*; Rand Corporation: Santa Monica, CA, USA, 2017.
104. Singh, J.; Sharmila, V.C. Detecting Trojan Attacks on Deep Neural Networks. In Proceedings of the 4th International Conference on Computer, Communication and Signal Processing (ICCCSP), Chennai, India, 28 September 2020.
105. Zhang, Z.; Jia, J.; Wang, B.; Gong, N.Z. Backdoor attacks to graph neural networks. *arXiv* **2020**, arXiv:2006.11165.
106. Operation Ephemeral Hydra: Ie Zero-Day Linked to Deputydog Uses Diskless Method. Available online: <https://www.fireeye.com/blog/threat-research/2013/11/operation-ephemeral-hydra-ie-zero-day-linked-to-deputydog-uses-diskless-method.html> (accessed on 5 March 2021).
107. Guri, M.; Poliak, Y.; Shapira, B.; Elovici, Y. JoKER: Trusted Detection of Kernel Rootkits in Android Devices via JTAG Interface. In Proceedings of the IEEE Trustcom/BigDataSE/ISPA, Helsinki, Finland, 20 August 2015.
108. Martin, E.D.; Kargaard, J.; Sutherland, I. Raspberry Pi Malware: An analysis of cyberattacks towards IoT devices. In Proceedings of the 10th IEEE International Conference on Dependable Systems, Services and Technologies, Leeds, UK, 5 June 2019.
109. Schmidt, A.D.; Clausen, J.H.; Camtepe, A.; Albayrak, S. Detecting symbian os malware through static function call analysis. In Proceedings of the IEEE International Conference on Malicious and Unwanted Software (MALWARE), Montreal, QC, Canada, 13 October 2009.
110. You, D.H.; Noh, B.N. Android platform based linux kernel rootkit. In Proceedings of the 6th International Conference on Malicious and Unwanted Software, Washington, DC, USA, 18 October 2011.
111. Park, W.H.; Park, K.C.; il Heo, K.; Kook, K.H. Agent Attacks Using a TTL Transformation of Windows Registry. In Proceedings of the International Conference on Information Science and Applications, Seoul, Korea, 10 April 2010.
112. Diogenes, Y.; Ozkaya, E. *Cybersecurity—Attack and Defense Strategies*; Packt Publishing: Birmingham, UK, 2018.
113. DLL Side-Loading Technique Used in the Recent Kaseya Ransomware Attack. Available online: <https://www.fortinet.com/blog/threat-research/dll-side-loading-technique-used-in-recent-kaseya-ransomware-attack> (accessed on 26 July 2021).
114. Hu, C. Backdoor detection in embedded system firmware without file system. *J. Commun.* **2013**, *34*, 140–145.
115. Vulnerable Embedded Systems, CVE-2019-17666. Available online: <https://nvd.nist.gov/vuln/detail/CVE-2019-17666> (accessed on 16 October 2019).
116. Park, C.S.; Lee, J.H.; Seo, S.C.; Kim, B.K. Assuring software security against buffer overflow attacks in embedded software development life cycle. In Proceedings of the 12th International Conference on Advanced Communication Technology (ICACT), Gangwon-Do, Korea, 7 February 2010.

117. Android Mobile Security Threats. Available online: <https://www.kaspersky.com/resource-center/threats/android-mobile-threats> (accessed on 10 December 2013).
118. Unit 42 Technical Analysis: Seaduke. Available online: <https://unit42.paloaltonetworks.com/unit-42-technical-analysis-seaduke/> (accessed on 5 March 2021)
119. Yazdinejad, A.; Bohlooli, A.; Jamshidi, K. P4 to SDNet: Automatic generation of an efficient protocol-independent packet parser on reconfigurable hardware. In Proceedings of the 8th International Conference on Computer and Knowledge Engineering (ICCKE), Mashhad, Iran, 25 October 2018.
120. Yazdinejad, A.; Kavei, S.; Razaghi Karizno, S. Increasing the Performance of Reactive Routing Protocol using the Load Balancing and Congestion Control Mechanism in MANET. *Comput. Knowl. Eng.* **2019**, *2*, 33–42.
121. Das, A.K.; Zeadally, S.; He, D. Taxonomy and analysis of security protocols for Internet of Things. *Future Gener. Comput. Syst.* **2018**, *89*, 110–125. [CrossRef]
122. Yazdinejad, A.; HaddadPajouh, H.; Dehghantanha, A.; Parizi, R.M.; Srivastava, G.; Chen, M.Y. Cryptocurrency malware hunting: A deep recurrent neural network approach. *Appl. Soft Comput.* **2020**, *96*, 106630. [CrossRef]
123. Microsoft Security Intelligence Report (Volume 19). Available online: https://download.microsoft.com/download/4/4/C/44CDEF0E-7924-4787-A56A-16261691ACE3/Microsoft_Security_Intelligence_Report_Volume_19_English.pdf (accessed on 5 March 2021).
124. Sontowski, S.; Gupta, M.; Chukkapalli, S.S.L.; Abdelsalam, M.; Mittal, S.; Joshi, A.; Sandhu, R. Cyber Attacks on Smart Farming Infrastructure. In Proceedings of the IEEE 6th International Conference on Collaboration and Internet Computing (CIC), Atlanta, GA, USA, 1 December 2020.
125. FarmBeats for Students. Available online: <https://education.microsoft.com/en-us/lesson/5d991297> (accessed on 27 July 2021).
126. Weaknesses in Wireless LAN Session Containment. Available online: http://i.cmpnet.com/nc/1612/graphics/SessionContainment_file.pdf (accessed on 27 July 2021).
127. Quintero-Bonilla, S.; Martín del Rey, A. A New Proposal on the Advanced Persistent Threat: A Survey. *Appl. Sci.* **2020**, *10*, 3874. [CrossRef]
128. Zulkefli, Z.; Singh, M.M. Sentient-based Access Control model: A mitigation technique for Advanced Persistent Threats in Smartphones. *J. Inf. Secur. Appl.* **2020**, *51*, 1–11. [CrossRef]
129. Hejase, H.J. Advanced Persistent ThreatS (APT): An Awareness Review. *J. Econ. Econ. Educ. Res.* **2020**, *21*, 1–8.
130. Advanced Persistent Threat (APT) Progression. Available online: <https://www.imperva.com/learn/application-security/apt-advanced-persistent-threat/> (accessed on 16 August 2021).
131. Cyber ThreatScape Report. Available online: https://www.accenture.com/_acnmedia/PDF-136/Accenture-2020-Cyber-Threatscape-Full-Report.pdf (accessed on 17 May 2021).
132. FBI Investigation. Smart Farming May Increase Cyber Targeting against US Food and Agriculture Sector. Available online: <https://info.publicintelligence.net/FBI-SmartFarmHacking.pdf> (accessed on 31 March 2016).
133. Wass, S.; Pourouri, S.; Ibbotson, G. Prediction of Cyber Attacks During Coronavirus Pandemic by Classification Techniques and Open Source Intelligence. In *Cybersecurity, Privacy and Freedom Protection in the Connected World*; Springer: Cham, Switzerland, 2021.
134. Yazdinejad, A.; Parizi, R.M.; Dehghantanha, A.; Choo, K.K.R. Blockchain-enabled authentication handover with efficient privacy protection in SDN-based 5G networks. *IEEE Trans. Netw. Sci. Eng.* **2019**, *8*, 1–12. [CrossRef]
135. Yazdinejad, A.; Parizi, R.M.; Dehghantanha, A.; Karimipour, H.; Srivastava, G.; Aledhari, M. Enabling Drones in the Internet of Things with Decentralized Blockchain-based Security. *IEEE Internet Things J.* **2020**, *8*, 6406–6415. [CrossRef]
136. Khanna, A.; Kaur, S. Evolution of Internet of Things (IoT) and its significant impact in the field of Precision Agriculture. *Comput. Electr. Agric.* **2019**, *157*, 218–231. [CrossRef]
137. Das, S.K.; Kant, K.; Zhang, N. *Handbook on Securing Cyber-Physical Critical Infrastructure*; Elsevier: Amsterdam, The Netherlands, 2012.
138. Zhang, H.; Wei, X.; Zou, T.; Li, Z.; Yang, G. Agriculture Big Data: Research status, challenges and countermeasures. In Proceedings of the International Conference on Computer and Computing Technologies in Agriculture, Beijing, China, 16 September 2014.
139. Daoliang, L. Internet of things and wisdom agriculture. *Agric. Eng.* **2012**, *2*, 1–6.
140. Butun, I.; Österberg, P.; Song, H. Security of the Internet of Things: Vulnerabilities, attacks, and countermeasures. *IEEE Commun. Surv. Tutor.* **2019**, *22*, 616–644. [CrossRef]
141. Ghadeer, H. Cybersecurity issues in Internet of Things and countermeasures. In Proceedings of the IEEE International Conference on Industrial Internet (ICII), Bellevue, WA, USA, 21 October 2018.
142. Pfleeger, C.P.; Pfleeger, S.L. *Analyzing Computer Security: A Threat/Vulnerability/Countermeasure Approach*, 1st ed.; Pearson: London, UK, 18 August 2011.
143. Whitacre, P. *Authenticity, Integrity, and Security in a Digital World: Proceedings of a Workshop—In Brief*; National Academies Press: Washington, DC, USA, 2019.
144. Mentsiev, A.U.; Magomaev, T.R. Security threats of NB-IoT and countermeasures. In Proceedings of the IOP Conference Series: Materials Science and Engineering, London, UK, 1 May 2020.
145. Mekala, M.S.; Viswanathan, P. A Survey: Smart agriculture IoT with cloud computing. In Proceedings of the International Conference on Microelectronic Devices, Circuits and Systems (ICMDCS), Vellore, India, 10 August 2017.

146. Bronson, K.; Knezevic, I. Big Data in food and agriculture. *Big Data Soc.* **2016**, *3*. [[CrossRef](#)]
147. Geil, A.; Sagers, G.; Spaulding, A.D.; Wolf, J.R. Cyber Security on the Farm: An Assessment of Cyber Security Practices in the United States Agricultural Industry. *Int. Food Agribus. Manag. Rev.* **2018**, *21*, 317–334. [[CrossRef](#)]
148. Homeland Security. Threats to Precision Agriculture. Public-Private Analytic Exchange Program. Available online: https://www.dhs.gov/sites/default/files/publications/2018%20AEP_Threats_to_Precision_Agriculture.pdf (accessed on 26 July 2018).
149. Yazdinejad, A.; Parizi, R.M.; Srivastava, G.; Dehghanianha, A. Making Sense of Blockchain for AI Deepfakes Technology. In Proceedings of the 2020 IEEE Globecom Workshops, Taipei, Taiwan, 7 December 2020; pp. 1–6.
150. Trendov, N.M.; Varas, S.; Zeng, M. Digital technologies in agriculture and rural areas: Status report. *Digit. Technol. Agric. Rural Areas* **2019**, *3*, 152.
151. Klerkx, L.; Jakku, E.; Labarthe, P. A review of social science on digital agriculture, smart farming and agriculture 4.0: New contributions and a future research agenda. *NJAS Wageningen J. Life Sci.* **2019**, *90*, 100315. [[CrossRef](#)]