An Overview of Vulnerabilities in Smart Farming Systems

Teja Koduru

Introduction

According to the 2020 report of the United Nations Food and Agriculture Organization, the decades-long decrease in the prevalence of undernourishment (PoU) across the world has come to an end. In 2019, it was reported that globally, nearly 690 million people (8.9% of the world population) were undernourished. Between 2018 and 2019, the PoU increased by 0.3%, equivalent to 10 million people. [1] While a multitude of reasons are behind the rapid increase in PoU, it is agreed that human-caused climate change, world conflicts, increased urbanization, and lower global biodiversity are all major causes. As the world population expands to 9.4 billion in the coming decades, the problem of food production will be even more important [3].

Food production systems (FPSs) come in a variety of forms depending on their location. In developing countries, FPSs are fragmented into multiple interconnected systems and depend on smaller-scale farming operations (SSFOs). SSFOs are generally much less efficient than their larger counterparts. Addressing these inefficiencies is key to improving FPSs in developing regions. The most obvious solution is to integrate sophisticated modern agricultural practices into SSFOs; However, these practices are difficult to implement as a result of the low literacy rates of farmers in developing countries. [4] Another option is to integrate machines into farms, to automate several key processes. The combination of machines, sensors, and human oversight is known as smart farming.

Smart farming is a new type of agricultural management utilizing various techniques to increase farm yield. Smart farming may enable us to overcome challenges related to food production demands caused by a growing population. Technologies used in smart farms vary greatly, ranging from automated weather data collectors to Unmanned Aerial Vehicles (UAVs) designed to gather topological data or water crops [2]. Interconnected devices such as those on smart farms are collectively known as the Internet of Things (IoT). Within an IoT system, data from sensors actively change the conditions in which plants are grown, resulting in increased overall productivity. For instance, an IoT system might increase water distribution to plants in the event of a drought. Within the USA, the use of IoT devices in smart farms results, on average, in a 163 dollars/day per hectare increase in farm yield. In fact, this number could even be as high as 272 dollars depending on the type of crop [5].

While IoT devices used in smart farms are specialized for a variety of tasks, including watering crops and gathering environmental data, they are comparable to regular IoT devices in several areas. Previous studies have demonstrated vulnerabilities in IoT devices to cyberattacks (Distributed Denial of Service, Man in the Middle attacks, etc.) [6] Should these vulnerabilities be exploited, a smart farm stands to lose its entire crop, leading to widespread food shortage. Thus, addressing vulnerabilities in smart farming systems is of the utmost importance.

On April 9th, 2021, the Colonial Pipeline, which transports a significant percentage of fuel for the Eastern Coast of the United States, was involved in a ransomware attack. While the ransomware was eventually removed, the shutdown of the pipeline impacted millions of consumers across the US. A similar attack on smart farms could have an even more devastating impact, as the food shortage may lead to widespread famine. In Virginia, the agricultural industry has an economic impact of approximately 70 billion dollars and is responsible for 334,000 jobs. When combined with value-added industries (Which rely on agriculture), the agricultural industry makes up nearly 10% of the state's GDP. [7] Any disruption in the agricultural output of the state would cascade into millions of dollars worth of damage. In addition, thousands would lose their jobs leading to wide-scale unemployment. Virginia is currently building a network of smart farms through the SmartFarm Innovation Network project. As Virginia's agriculture begins to depend more heavily on smart farming, the poor cybersecurity protocols of these farms become more of a concern.

The aim of this literature review is to provide a brief but extensive overview of smart farming technology and potential cybersecurity vulnerabilities present in smart farms. In addition, this literature review will also suggest possible avenues to improve the security of smart farms. This document is organized as follows: Section 2 will provide a more in-depth overview of the types of IoT devices on smart farms. Section 3 will examine the potential security pitfalls present in these devices. Section 4 will provide techniques to mitigate these security risks. Finally, Section 5 will conclude the paper.

Section 2

The role of IoT and smart technology in the agricultural industry has steadily increased over the past few decades [8]. IoT-based agricultural systems are able to be more efficient than their traditional counterparts due to a variety of reasons. In most cases, this is due to smart sensors which relay information about soil and atmospheric conditions. However, IoT technology has many more applications within a smart farm. IoT devices are routinely used for rainfall monitoring, soil nutrition management, water management, pest infection management, and crop health monitoring [9].

Section 2.1 - Soil IoT

While IoT sensors on farms vary in their uses, a majority of sensors are used to measure soil conditions on the farm. Several companies offer IoT solutions that are used to identify key soil factors such as texture, water-holding capacity, and absorption rate. Knowing this information allows farmers to stop soil erosion, densification, salinization, acidification, and pollution, which can otherwise cause thousands of dollars in damages. AgroCeres, a company specializing in IoT solutions for the agricultural industry, has released a product known as Lab-In-A-Box. Lab-In-A-Box allows farmers to conduct hundreds of soil tests without formal training, miles away from a traditional farm. Farmers can then act on this information to improve their soil quality, resulting in a better harvest [10]. Monnit, another IoT company, provides wireless soil sensors able to connect to a central system. Data from Monnit sensors can be used in conjunction with smart pumps to actively change the amount of water given to plants based on soil moisture.

Section 2.2 - Weather IoT

The amount and timing of rainfall is arguably the most important factor affecting a farm's productivity. Fluctuations in weekly or monthly rainfall levels can have a drastic impact on agricultural productivity and revenue. Therefore, predicting future weather patterns using large datasets of previous weather patterns is key to improving farm efficiency [11]. Unmanned Aerial Vehicles (UAVs) are being used for a variety of reasons in smart farms. One particularly interesting application of UAVs is to collect weather data. After collection, the data is stored on cloud servers. Next, the data can be drawn from these servers and is used for a variety of purposes. Researchers in [12] proposed a method to create a genetic algorithm (GA) to predict future weather patterns based on old data. When new data is collected by UAVs, it is fed into the GA to determine if plants need water. A sensor system is also used to check the results of the GA. Should moisture levels fall below a critical threshold, smart pumps are used to provide additional water to plants.

Section 2.3 - Water IoT

Proper irrigation systems are an essential element in any farm. Improper distribution of water to plants, caused by a malfunctioning irrigation system, may lead to widespread crop failure. Global warming further contributes to this problem, by making water scarcer in certain regions. Therefore, identifying and solving problems in irrigation systems is of the utmost importance. IoT devices can be used to automate the process of irrigation, minimizing the risk of catastrophic failures. IoT irrigation systems come in several forms, from simple Arduino-based systems to those which implement AI technology [14]. However, in most systems, there are several key features. First, a power source is used to power the system. In most cases, this takes the form of a solar panel, but there are exceptions to this rule. Most notably, Arduino-based systems are normally powered by a combination of batteries and solar power [15]. Next, a central controller is used to obtain data regarding the environment. Should the data indicate that certain environmental variables do not fall within certain parameters, the central controller actively changes these variables through the use of smart pumps [16]. IoT systems are capable of independently performing this process multiple times a day, thereby reducing the risk of failures in irrigation systems normally caused by human error.

Section 2.4 - Pest IoT

The productivity of several key plant species necessary for humans, such as wheat, maize, and cotton, can be severely impacted by the presence of pests. One study found that the global potential loss of crops due to pests varied from roughly 50% in wheat to more than 80% in cotton [18]. A wide variety of pesticides are used to combat this problem. However, excessive use of pesticides can damage the local environment, aid in the development of pesticide-resistant crops, and lead to several health conditions in farmers [19]. While the use of IoT in regards to pest control is limited when compared to its other uses, several studies have created potential IoT systems to deal with pest infections. Researchers at the National Taiwan University designed an IoT-based system designed to identify pest insects throughout a farm. The resulting spatial-temporal information was then used to kill these pests [20]. Another study by the

Brazillian National Institute of Telecommunications expanded on this research by designing a trap that would both identify and exterminate pests. A computer vision algorithm was used to identify pests, based on images taken from an embedded system containing a camera, a GPS sensor, and motor actuators. Should the computer vision algorithm indicate that pests are present in the trap, the trap immediately kills them. [21] The potential of IoT systems in pest management is great. IoT systems may promise to reduce the amount of pesticide required to eliminate pests, thereby reducing risks to farmers while simultaneously saving large sums of money.

As shown above, IoT devices and systems are applied in a variety of forms throughout smart farms. While not all smart farms may contain all such devices, the presence of at least one of these systems greatly increases the farm's efficiency. However, one notable downside to intelligent IoT systems is their vulnerability to cyberattacks. Previous studies have demonstrated the ease with which bad actors are able to infiltrate IoT systems. As mentioned earlier, a malicious attack on a smart farm may have severe economic impacts due to the importance of the agricultural industry to statewide and nationwide GDP. Therefore, we will next examine the potential cybersecurity risks present in smart farm IoT systems.

Section 3

The rapid integration of IoT technology in various industries brings with it new risks in the form of novel security challenges. According to Tawalbeh et al. (2020), improper device updates, lack of efficient and robust security protocols, user unawareness, and famous active device monitoring are among the challenges that IoT is facing. These vulnerabilities are present in not only household IoT devices, but also in smart farming systems. Attacks that take advantage of these vulnerabilities may lead to serious disruptions in the farm environment, depending on which system is breached. Attacks on smart farming systems generally fall into one of two categories: Physical, where farm machinery is disrupted, or online, where farm data is modified or deleted. The following subsections will further elaborate on these vulnerabilities. We will also examine several case studies demonstrating the effects of a successful attack on IoT systems.

Section 3.1 - Physical Attacks

According to [23], the number of farm workers has steadily declined in the 20th century, while farm production has increased. The increased use of machinery is the cause of this discrepancy. Machinery is used for several purposes within a farm. Primary and secondary tilling of soil, harvesting, pest control, and erosion control are just some of the many applications of heavy machinery. Light machinery, on the other hand, primarily consists of drones, UAVs, and automated farm robots, and is primarily used for environmental data collection. Both heavy and light machinery can connect to IoT systems, although IoT-connected light machinery is more common.

Previous studies have demonstrated several methods used by bad actors to wirelessly take control of a drone. This concern is further exacerbated as tutorials on how to take control of a drone are available on numerous video-sharing platforms, including YouTube [24]. A study published in the Internet of Things journal [25] found that major vulnerabilities were present in a majority of light machinery products. A summary of several of these vulnerabilities, as stated in the study, is presented below.

1. Spoofing/ Data Interference
    a. Data streamed from a drone to a central controller can be intercepted and modified. Telemetry data, crucial to maintaining the correct flight profile of a drone, is normally unencrypted. Several experiments have demonstrated the ease with which this vulnerability can be exploited, giving bad actors full control of the drone [26][27].
2. Malware Infection
    a. Many UAVs contain software which allow pilots to fly them from various mobile platforms . This software can be used by bad actors to inject malware payloads into the UAVs memory or the ground station itself [28]. The malware used in such an attack may vary; However, in most situations, it enables bad actors to take full control of a UAV.

3. Prone to Wi-Fi Jamming

a. A specific type of Distributed Denial of Service (DDoS) attack called a deauthentication attack can be performed on a UAV. Next, a bad actor may jam the UAVs intended frequency and connect it to their own. Such an attack only requires a raspberry pi to execute.

Vulnerabilities present in light machinery are different from those present in heavy machinery. While less common, IoT-connected heavy machinery still has a multitude of vulnerabilities which can be exploited by bad actors. The types of heavy machinery varies greatly on a farm. A brief overview of the types of heavy machinery commonly found on a farm is below. The IoT capability of each machine is also listed.

Machine	**Purpose**	**IoT - Capability**
Tractor	● Provides power to perform several agricultural tasks ● Used to pull a variety of attachments depending on farm needs ● Examples include plowing the land, planting crops, and harvesting.	● In most cases, low ● Some companies, such as Hello Tractor, are developing IoT attachments for tractors.
Sprayer	● Used to distribute liquid solutions to plants. ● Can be used to water crops, although uncommon. ● Primary uses include fertilizer, pesticide, or herbicide application.	● High ● IoT pesticide sprayers have been proposed as a solution to overuse of pesticides [31]. ● These systems use solar power and are mostly autonomous.
Seeders	● Normally pulled by a tractor	● Medium

	● Used to evenly distribute seeds across a plot of land ● Beans, cotton, rice, wheat, and canola are all common crops that can be planted through the use of a seeder.	● Autonomous seeding robots have been proposed [32]; However, this technology is not mainstream. ● Several prototypes use Arduino boards as their central controllers, which are vulnerable to attacks.
Trailers	● Used to store crops during harvesting ● Normally towed by a tractor ● Can also be used to transport livestock long distances	● Medium ● Companies such as Convoy offer IoT solutions to monitor the conditions within a trailer ● These sensors track data such as temperature, speed, weight, etc. ● Intercepting and editing this data may have severe effects.
Slurry Tanks	● On farms, slurry is the combination of animal wastes with other organic matter, such as hay. ● Slurry is used as a rich fertilizer and has been shown to considerably increase farm yields [33]. ● Slurry tanks are used as storage to hold slurry. They can also be pulled by tractors during the application process.	● High ● IoT sensors can be placed within slurry tanks to gather key information, such as temperature, humidity, volume, and composition of the slurry. [34] ● If this data is changed, crops may die since the farmer may mistakenly add too much or the wrong type of slurry.
Center pivot	● Used to water crops and have been shown to use less water than traditional watering methods.	● High ● IoT solutions are being

irrigation systems	● Rotate around a fixed central point, hence the name ● Waters a circular region emanating from the center of the machine.	used to monitor center pivot irrigation systems. ● If data is modified in such a way that the irrigation system moves to an incorrect location or fails to dispense water, farms stand to lose thousands of crops.

General information gathered from [29], [30].

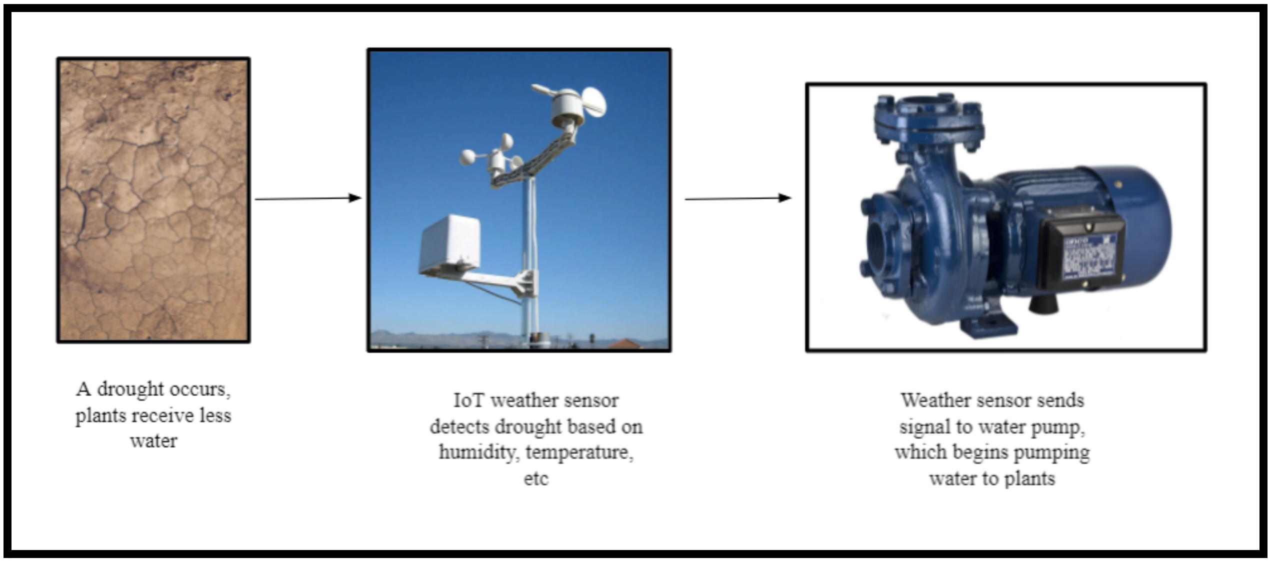
As shown above, IoT is being used to advance the capabilities of several types of heavy machinery used on farms. Notably, the machinery itself is not the target of the attack. The IoT systems used on the machinery to collect data is the primary attack vector. The consequences of a disruption of heavy machinery are varied:

- Crop failure due to more or less water applied than needed (See 6th entry in table)
- Crop failure due to improper application of fertilizer due to incorrect data provided by IoT sensors (See 5th entry in table)
- Crop/Livestock loss during transport (See 4th entry in table)
- Failure to plant crops properly should a farm use automated seeding robots (See 3rd entry in table)
- Crop failure as a result of improper pesticide/herbicide application (See 2nd entry in table)

The disruption of heavy machinery through cyberattacks can have a large impact on a farm’s productivity. However, it pales in comparison to a similar attack on online assets such as IoT sensor data.

Section 3.2 - Online Attacks

Smart farms rely heavily on data collected by intelligent, IoT-connected sensors. Environmental data collected from these sensors is used to dictate the actions of other IoT-connected devices, such as smart pumps or sprayers. The following diagram illustrates an example of this relationship:


A drought occurs, plants receive less water
IoT weather sensor detects drought based on humidity, temperature, etc
Weather sensor sends signal to water pump, which begins pumping water to plants

If the weather sensor, pump, or the data transferred between the devices is compromised, bad actors will have the capability of controlling the amount of water given to plants. The effects of such a compromise are disastrous: A bad actor may stop pumping water to plants while editing data to make it seem like plants are watered, leading to widespread crop failure within a matter of days. While this situation may be averted through human oversight, several smart farms proposals include little to none human supervision [[35], [36]].

Breaching an IoT system has been shown to be possible in a number of studies. While IoT devices designed for smart farms and IoT devices designed for private households have different uses, their vulnerabilities are similar. According to a paper by the Bulgarian Academy of Sciences [37] , an attack on an IoT system can be split into the following parts:

1. Reconnaissance - Attackers spend months researching their target, using multiple online sources. Attackers may not need to directly interact with the target during this phase.

2. Searching for Vulnerabilities - After reconnaissance yields enough data to satisfy the attackers, they move on to the second phase. This phase primarily consists of identifying vulnerabilities in the target system.

3. Attack - During this phase, attackers launch their attack based on target vulnerabilities identified in step 2. In several cases, a malicious payload is inserted into the target, allowing attackers to gain access to confidential data or giving them control of key systems. We provide an overview of various attack strategies below.
4. Achieve/Maintain access - Once attackers gain control of a system, they must also ensure that their access remains in place. To this end, they cover up evidence of a breach or attack other devices connected to the primary attack vector. The longer a breach is maintained, the more information that attackers can exfiltrate.

Attack strategies used by cybercriminals are ever changing. One research study [9] contains a detailed list of all major attack strategies used by cybercriminals to attack IoT criminals. Below is a summarized version of their findings, including only the most common attacks. However, we suggest visiting the source for more information if you are so inclined.

Target System	**Attack Type**	**Consequences**
Privacy	● Physical Attacks ● Masquerade Attack	● Attackers gain access to information about IoT systems and other devices on the smart farm.
Confidentiality	● Brute Force Attack ● Known Key Attack	● Confidentiality loss; Potentially sensitive information could be stolen and leaked.
Integrity	● Forgery Attack ● Trojan Horse Attack ● Man-In-The-Middle Attack (MITM)	● Information communicated between smart farm devices may not be trusted as it could have been modified by attackers.
Availability	● Denial of Service Attack	● IoT connected devices may stop functioning due to a high volume of requests, essentially shutting down the farm.
Authenticity	● Attacks against Authentication	● Information from the smart farm cannot be authenticated properly as attackers send fake data by mimicking authorized sources.

With the number of attacks possible on both physical and online assets of a smart farm, properly identifying vulnerabilities in IoT systems is crucial to maintaining security. In the next section, we will discuss possible avenues towards protecting key IoT systems on smart farms.

Section 4

We have identified several key cybersecurity vulnerabilities present in smart farming systems in section 3. However, even more important is the security measures needed to patch these vulnerabilities and ensure the security of IoT systems. To this end, a list of several of the more potent vulnerabilities and methods that can be used to fix them is presented below. The following chart is not an exhaustive list of all cybersecurity vulnerabilities in IoT systems. Rather, it will address the vulnerabilities presented in the previous chart (Within section 3). A more thorough analysis is presented in Appendix A.

Attack Type	Definition	Solutions	Source(s)
Cyber-Physical Attack	A cybersecurity breach which relinquishes control of physical systems , such as pumps, sensors, and other IoT devices, to attackers.	Cyber-Physical attacks refer to a wide variety of different cyberattacks. Therefore, the only way to prevent this type of attack is to build a network framework specifically designed to mitigate and respond to these attacks.	[38][39][40]

Masquerade Attack	A masquerade attack utilizes a fake identity to gain access to restricted information regarding a farm's operations. These attacks can be hard to identify since attackers act as a regular user.	Several methods are used to prevent masquerade attacks. Normal prevention methods include securing the authentication process in a system through various methods. More recent studies propose a machine learning approach to identifying attackers based on their pattern of movement through a file system.	[41][42]
Brute Force Attack	Brute force attacks attempt to break into a system by using a dictionary of common weak usernames and passwords. As most users use words in their passwords rather than completely random characters, this approach has a high chance of success.	As this attack is extremely common, many techniques exist to prevent it. The most simple is to lock out an account after a given number of login attempts. However, attackers can cause a denial of service by attempting to break into large amounts of accounts, thereby locking them out. A combination of several conditions, however, may indicate the presence of a brute force attack. See Appendix B for these conditions.	[43][44]
Trojan Horse Attack	The Trojan Horse attack, named after the famous Trojan Horse used during the Trojan	Trojan Horse attacks can appear as regular applications. However, applications which do	[45]

	War, conceals a malicious program within an authorized one. After a certain event, called the trigger, occurs in the system, the malicious program activates and proceeds to wreak havoc on the system.	not have a trusted status might harbor a Trojan Horse attack. Therefore, any suspicious applications without a trusted status should be removed. There exist several antivirus tools which are also able to identify and remove Trojan Horse programs within a system.	
Man-In-The-Middle Attack	Communication between two devices in a network is done through a data stream. If an attacker is able to intercept the data stream in the middle of transmission (Hence, man in the *middle*), they may be able to read or edit data transmitted between the devices.	Network Intrusion Prevention systems, a Communication Authenticity system, and a Static Network Configuration are all methods by which MITM attacks can be prevented. However, simply disabling or removing unnecessary network protocols can also limit the success of MITM attacks.	[46][47]
Denial of Service Attack	A Denial of Service attack (not to be confused with a Distributed Denial of Service attack) occurs when the capability of a system to respond to user requests is diminished or eliminated due to	The first step in dealing with such an attack is to identify it. Unavailability of a service or slow network performance are both signs of a DoS attack. To stop such an attack, an organization must maintain their antivirus and firewall	[48]

	a bad actor. While a DoS attack can occur on a variety of systems, it is most commonly performed on email, websites, or online accounts.	programs. Another option is to enroll in a DoS protection service, which is capable of identifying DoS attacks and only directing legitimate requests to the system.	

Section 5

This paper is intended to provide an overview of smart farming, IoT devices used on smart farms, and potential vulnerabilities present in these IoT systems. The findings presented in this paper demonstrate that while IoT solutions may lead to an immense increase in agricultural production, they come with severe security risks. Bad actors may be able to diminish or even destroy the food supply of a country by leveraging vulnerabilities in smart farming IoT systems.

IoT devices are not only present in agriculture. They play essential roles in a variety of industries, and can also be found in private residences. Several research studies have demonstrated the vulnerabilities in these IoT systems by breaking into them. However, as of yet, no similar study has been conducted to examine issues with smart farming IoT systems. Further research, therefore, is crucial to preventing cyberattacks on smart farming facilities. As the world population continues to increase, and as smart farming plays an ever increasing role in meeting food demands, identifying and addressing vulnerabilities in smart farming IoT systems becomes more important than ever.

Appendix A

The following chart expands on the vulnerabilities and solutions discussed in section 3 and 4. While these types of cyberattacks are not as common, knowing their effects and how to stop them is still valuable information to protect IoT systems.

Attack	Description	Solution	Source(s)
DDoS	Not to be confused with a denial of service (DoS) attack, a DDoS attack relies on several devices to carry out an attack. Therefore, it is both faster and harder to stop.	As DDoS attacks are extremely common, several methods exist which can be used to prevent such an attack. Most companies use preventive methods such as getting extra bandwidth to prevent a DDoS attack from happening in the first place. However, should an attack get past these outer defenses, rerouting connections to a backup server and contacting the ISP provider is the easiest way to stop the attack.	[49][50]
Spyware	Spyware allows attackers to monitor confidential data about a device or the network it connects to. Within a smart farm, this data may include instructions sent to several farm	One study found that information collected about IoT devices can easily be accessed by unauthorized individuals through the internet. Traffic shaping, and additional bandwidth	[51][52]

	IoT devices. Therefore, unauthorized access to this data is a major security risk.	were both found to be solutions to this problem	
Phishing	A phishing attack relies on a combination of social engineering and cybersecurity principles. Attackers imitate trusted individuals and send insecure messages to individuals. Normally, these messages contain a link which releases a virus. Should a user click on the link, attackers will soon have access to the entire network.	Education is the most effective way to deal with phishing attacks. Courses and training are both effective methods to educate employees about the dangers of phishing. If phishing links aren't clicked, then viruses will be unable to infect network devices.	[53][54]
Drive by Download	A Drive by Download attack occurs when a malicious program is downloaded to a user computer after visiting a website. It is one of the most common types of attacks used by bad actors due to the simplicity of the attack. If the user fails to notice the malware being downloaded onto their device, attackers may gain access to confidential information. They may also install	Web-filtering software is an effective tool to prevent Drive by Download attacks. It warns users when entering a potentially malicious site. In addition, ad blockers also help prevent these attacks as ads are commonly used as an attack vector. Finally, removing unnecessary software and using a firewall can both prevent Drive by Download attacks.	[55][56]

	keyloggers, ransomware, or other forms of malware on the device.		
Cross-site scripting	A cross-site scripting attack occurs when a vulnerable yet normally safe website is attacked by a bad actor. The bad actor inserts a malicious script into the website. Visitors to the website may interact with the malicious code and allow attackers to gain access to restricted files.	Cross-site scripting attacks can be mitigated by validating user input, ensuring that malicious data cannot enter the site. Sanitizing user input data can also be used for this purpose. However, the easiest way to prevent such an attack is to make the system itself more secure. This will prevent bad actors from inserting malicious code, blocking the attack at the source.	[57]
SQL Injection	An SQL injection attack interferes with requests that a system makes to a database. Attackers using SQL injection techniques can access or even modify user data, which can have disastrous consequences.	Vetting user input through input validation algorithms is the easiest way to address SQL injection attacks. Parameterized queries also help when dealing with such an attack.	[58][59]
Zero-Day Exploits	A Zero-Day Exploit is when attackers find vulnerabilities in recently released systems. Zero-Day Exploits are some of the most dangerous types of cybersecurity	Unfortunately, Zero-Day Exploits have no mainstream fixes. Several organizations utilize so-called “Bug Bounties”, where researchers are	[60]

	attacks given their nature. Since these attacks occur soon after a system is released to the public, security patches to solve potential vulnerabilities in the system are lacking. Therefore, attackers can steal confidential information before preventative measures can take place.	rewarded for finding vulnerabilities in a system and reporting them. Several anti-virus programs are also beginning to address Zero-Day Exploits by using machine learning algorithms to identify and counteract them.	
Rootkits	A rootkit attack provides attackers with a root-level access to a device and any other connected devices, while simultaneously remaining hidden from other users. They can also be used to deactivate antivirus and antimalware software. Finally, rootkits can also be used to launch other cyberattacks, such as a DoS attack.	A rootkit attack can only succeed if the user launches malicious software containing the rootkit. Therefore, scanning your system manually or through an anti-malware software can reveal attempts at a rootkit attack. Monitoring your network for unusual activity can also reveal such an attack.	[61][62][63]
Password Attack	A password attack occurs when an attacker attempts to access a system by cracking a user password. It is one of the simplest types of attacks available to bad actors.	In most cases, this type of attack does not rely on any software installed on the target system. Therefore, antivirus and anti-malware software programs will not offer much assistance. The simplest way to counter a password	[64][65]

		attack is to create a stronger password. Using a combination of upper and lower case letters, special characters, and numbers has been shown to be effective against these attacks. In addition, longer passwords are generally more secure than their shorter counterparts.	

Appendix B

According to the Open Web Application Security Project foundation [44], the presence of two or more of the following conditions may indicate that a brute force attack is being attempted:

- Many failed logins from the same IP address.
- Logins with multiple usernames from the same IP address.
- Logins for a single account coming from many different IP addresses.
- Excessive usage and bandwidth consumption from a single use.
- Failed login attempts from alphabetically sequential usernames or passwords.

- Logins with a referring URL of someone's mail or IRC client.
- Referring URLs that contain the username and password in the format <http://user:password@www.example.com/login.htm>.
- If protecting an adult website, referring URLs of known password-sharing sites
- Logins with suspicious passwords hackers commonly use, such as ownsyou (ownzyou), washere (wazhere), zealots, hacksyou, and the like.

[1] The State of Food Security and Nutrition in the World 2020. (2020). FAO, IFAD, UNICEF, WFP and WHO. https://doi.org/10.4060/ca9692en

[2] Virk, Ahmad & Noor, Mehmood Ali & Fiaz, Sajid & Hussain, Saddam & Hussain, Hafiz & Rehman, Muzammal & Ahsan, Muhammad & Ma, Wei. (2020). Smart Farming: An Overview. https://doi.org/10.1007/978-3-030-37794-6_10.

[3] United Nations, Department of Economic and Social Affairs, Population Division (2019). World Population Prospects 2019: Highlights. ST/ESA/SER.A/423.

[4] Lamuka P.O. (2014) Public Health Measures: Challenges of Developing Countries in Management of Food Safety. In: Motarjemi Y. (ed.) Encyclopedia of Food Safety, Volume 4, pp. 20-26. Waltham, MA: Academic Press.

[5] doi:10.3390/agronomy10020207

[6]Kholoud Y. Najmi, Mohammed A. AlZain, Mehedi Masud, N.Z. Jhanjhi, Jehad Al-Amri, Mohammed Baz,A survey on security threats and countermeasures in IoT to achieve users confidentiality and reliability, Materials Today: Proceedings, 2021, ISSN 2214-7853, https://doi.org/10.1016/j.matpr.2021.03.417.

[7] Virginia Department of Agriculture and Consumer Services. (n.d.). Agricultural facts and figures. Retrieved June 27, 2021, from https://www.vdacs.virginia.gov/markets-and-finance-agriculture-facts-and-figures.shtml

[8] doi:10.3390/electronics9020319

[9] Demestichas, K., Peppes, N., & Alexakis, T. (2020). Survey on Security Threats in Agricultural IoT and Smart Farming. Sensors (14248220), 20(22), 6458. https://doi.org/10.3390/s20226458

[10] Ayaz, Muhammad & Uddin, Ammad & Sharif, Zubair & Mansour, Ali & Aggoune, el-Hadi. (2019). Internet-of-Things (IoT)-Based Smart Agriculture: Toward Making the Fields Talk. IEEE Access. PP. 1-1. 10.1109/ACCESS.2019.2932609.

[11] Marcelo Torres, Richard Howitt, Lineu Rodrigues, Analyzing rainfall effects on agricultural income: Why timing matters, EconomiA, Volume 20, Issue 1, 2019, Pages 1-14, ISSN 1517-7580, https://doi.org/10.1016/j.econ.2019.03.006.

[12] Roy, S.K.; De, D. Genetic Algorithm based Internet of Precision Agricultural Things (IopaT) for Agriculture 4.0. Internet Things 2020, 100201. [CrossRef]

[13] Almalki, F.A.; Soufiene, B.O.; Alsamhi, S.H.; Sakli, H. A Low-Cost Platform for Environmental Smart Farming Monitoring System Based on IoT and UAVs. Sustainability 2021, 13, 5908. https://doi.org/10.3390/su13115908

[14] ; doi:10.3390/s20041042

[15] Babaa, Saleh & Ahmed, Muneer & Khan, Shahid Ali & Al-Jahdhami, John. (2020). Smart Irrigation System using Arduino with Solar Power. International Journal of Engineering Research and. V9. 10.17577/IJERTV9IS050088.

[16] Ratnadewi, Ratnadewi & Nurdiyanto, Heri & Najmurrokhman, Asep & Prabowo, Cipto & Idmayanti, R & Eteruddin, Hamzah & agus s, Castaka & Kurniasih, N & Siburian, H & Nababan, Darsono & Rahim, Robbi. (2018). Control and Notification Automatic Water Pump with Arduino and SMS Gateway. IOP Conference Series: Materials Science and Engineering. 407. 012160. 10.1088/1757-899X/407/1/012160.

[17] Aluthgama Acharige, Raneesha & Halgamuge, Malka & Wirasagoda, Hemika & Syed, Ali. (2019). Adoption of the Internet of Things (IoT) in Agriculture and Smart Farming towards Urban Greening: A Review. International Journal of Advanced Computer Science and Applications. 10. 11-28. 10.14569/IJACSA.2019.0100402.

[18] OERKE, E. (2006). Crop losses to pests. The Journal of Agricultural Science, 144(1), 31-43. doi:10.1017/S0021859605005708

[19] DOI: 10.1081/E-EPM-120009921

[20] Rustia, Dan Jeric & Lin, Ta-Te. (2017). An IoT-based Wireless Imaging and Sensor Node System for Remote Greenhouse Pest Monitoring. Chemical Engineering Transactions. 58. 10.3303/CET1758101.

[21] https://arxiv.org/ftp/arxiv/papers/2004/2004.04504.pdf

[22] doi:10.3390/app1012410

[23] Britannica, The Editors of Encyclopaedia. "Farm machinery". Encyclopedia Britannica, 14 Jan. 2020, https://www.britannica.com/technology/farm-machinery. Accessed 10 July 2021.

[24] S. Das, B. K. Mohanta and D. Jena, "IoT Commercial Drone and It's Privacy and Security Issues," 2020 International Conference on Computer Science, Engineering and Applications (ICCSEA), 2020, pp. 1-4, doi: 10.1109/ICCSEA49143.2020.9132958.

[25] Yaacoub, J. P., Noura, H., Salman, O., & Chehab, A. (2020). Security analysis of drones systems: Attacks, limitations, and recommendations. Internet of Things, 11, 100218. https://doi.org/10.1016/j.iot.2020.100218

[26] Kim S.J., Lim G.J., Cho J. Drone flight scheduling under uncertainty on battery duration and air temperature. Comput. Ind. Eng. 2018;117:291–302. [Google Scholar]

[27] Alwateer M., Loke S.W., Zuchowicz A. Drone services: issues in drones for location-based services from human-drone interaction to information processing. J. Locat. Based Serv. 2019;13(2):94–127. [Google Scholar]

[28] Kim A., Wampler B., Goppert J., Hwang I., Aldridge H. Infotech@ Aerospace 2012. 2012. Cyber Attack Vulnerabilities Analysis for Unmanned Aerial Vehicles; p. 2438. [Google Scholar]

[29] Leerburger, Benedict A. "Agricultural Machines." The Gale Encyclopedia of Science, edited by Katherine H. Nemeh and Jacqueline L. Longe, 6th ed., vol. 1, Gale, 2021, pp. 83-87. Gale In Context: Science, link.gale.com/apps/doc/CX8124400057/SCIC?u=tjhs_e&sid=bookmark-SCIC&xid=a42c364d. Accessed 12 July 2021.

[30] Rumsey, J. W., & O'Brien, M. (2021). Agricultural machinery. AccessScience. Retrieved July 12, 2021, from https://doi.org/10.1036/1097-8542.015600

[31] Amaresh A M, Anagha G Rao, Fenaaz Afreen, Moditha N, Syeda Arshiya, 2020, IOT Enabled Pesticide Sprayer withSecurity System by using Solar Energy, INTERNATIONAL JOURNAL OF ENGINEERING RESEARCH & TECHNOLOGY (IJERT) IETE – 2020 (Volume 8 – Issue 11),

[32] Kshirsagar, Pravin. (2020). IOT BASED SMART AGRICULTURE AND AUTOMATIC SEED SOWING ROBOT.

[33] You, L., Yu, S., Liu, H., Wang, C., Zhou, Z., Zhang, L., & Hu, D. (2019). Effects of biogas slurry fertilization on fruit economic traits and soil nutrients of Camellia oleifera Abel. PLOS ONE, 14(5), e0208289.

[34] https://www.scitepress.org/Papers/2019/77601/77601.pdf

[35] Ryu, Minwoo & Yun, Jaeseok & Miao, Ting & Ahn, Il-Yeup & Choi, Sungchan & Kim, Jaeho. (2015). Design and implementation of a connected farm for smart farming system. 1-4. 10.1109/ICSENS.2015.7370624.

[36]Budaev, D. & Lada, Aleksandr & Simonova, E. & Skobelev, Petr & Travin, V. & Yalovenko, O. & Voschuk, Georgy & Zhilyaev, Alexey. (2018). Conceptual design of smart farming solution for precise agriculture. International Journal of Design & Nature and Ecodynamics. 13. 307-314. 10.2495/DNE-V13-N3-307-314.

[37]https://www.researchgate.net/profile/Kristina-Dineva/publication/334735028_SECURITY_IN_IOT_SYSTEMS/links/5d6e2f0ba6fdcc547d75afc0/SECURITY-IN-IOT-SYSTEMS.pdf

[38] M. Gupta, M. Abdelsalam, S. Khorsandroo and S. Mittal, "Security and Privacy in Smart Farming: Challenges and Opportunities," in IEEE Access, vol. 8, pp. 34564-34584, 2020, doi: 10.1109/ACCESS.2020.2975142.

[39] M. A. Ferrag, L. Shu, X. Yang, A. Derhab and L. Maglaras, "Security and Privacy for Green IoT-Based Agriculture: Review, Blockchain Solutions, and Challenges," in IEEE Access, vol. 8, pp. 32031-32053, 2020, doi: 10.1109/ACCESS.2020.2973178.

[40] Yaacoub, J. A., Salman, O., Noura, H. N., Kaaniche, N., Chehab, A., & Malli, M. (2020). Cyber-physical systems security: Limitations, issues and future trends. Microprocessors and microsystems, 77, 103201. https://doi.org/10.1016/j.micpro.2020.103201

[41] Saljooghinejad H., Bhukya W.N. (2012) Layered Security Architecture for Masquerade Attack Detection. In: Cuppens-Boulahia N., Cuppens F., Garcia-Alfaro J. (eds) Data and Applications Security and Privacy XXVI. DBSec 2012. Lecture Notes in Computer Science, vol 7371. Springer, Berlin, Heidelberg. https://doi.org/10.1007/978-3-642-31540-4_19

[42] Ben Salem, M. (2012). Towards Effective Masquerade Attack Detection. (Doctoral dissertation, Columbia University).

[43] Wang A., Liang R., Liu X., Zhang Y., Chen K., Li J. (2017) An Inside Look at IoT Malware. In: Chen F., Luo Y. (eds) Industrial IoT Technologies and Applications. Industrial IoT 2017. Lecture Notes of the Institute for Computer Sciences, Social Informatics and Telecommunications Engineering, vol 202. Springer, Cham. https://doi.org/10.1007/978-3-319-60753-5_19

[44] https://owasp.org/www-community/controls/Blocking_Brute_Force_Attacks

[45]https://www.britannica.com/topic/information-system/Computer-crime-and-abuse

[46] https://csrc.nist.gov/glossary/term/man_in_the_middle_attack

[47] https://collaborate.mitre.org/attackics/index.php/Technique/T0830

[48] https://us-cert.cisa.gov/ncas/tips/ST04-015

[49] Yarımtepe, Oğuz & Dalkılıç, Gökhan & Ozcanhan, Mehmet. (2015). DDoS Prevention Techniques.

[50] Chakraborty, Sushmita & Kumar, Praveen & Sinha, Bhawna & Professor, Assistnat & Head,. (2019). A STUDY ON DDOS ATTACKS, DANGER AND ITS PREVENTION. 10.1729/Journal.20847.

[51] https://arxiv.org/ftp/arxiv/papers/2101/2101.05614.pdf

[52] arXiv:1708.05044

[53] https://www.consumer.ftc.gov/articles/how-recognize-and-avoid-phishing-scams

[54]https://www.occ.gov/topics/consumers-and-communities/consumer-protection/fraud-resources/phishing-attack-prevention.html

[55] A. K. Sood, & S. Zeadally (2016). Drive-By Download Attacks: A Comparative Study. IT Professional, 18(05), 18-25.

[56] Aldwairi, Monther & Hasan, Musaab & Balbahaith, Zayed. (2017). Detection of Drive-by Download Attacks Using Machine Learning Approach. International Journal of Information Security and Privacy. 11. 10.4018/IJISP.2017100102.

[57] https://doi.org/10.14569/IJACSA.2020.0110481

[58] Devi, Ruby & Venkatesan, R. & Koteeswaran, Raghuraman. (2016). A study on SQL injection techniques. International Journal of Pharmacy and Technology. 8. 22405-22415.

[59] Mohd Yunus, Mohd Amin & Brohan, Muhammad & Mohd Nawi, Nazri & Salwana, Ely & Najib, Nurhakimah & Liang, Chan. (2018). Review of SQL Injection : Problems and Prevention. JOIV : International Journal on Informatics Visualization. 2. 215. 10.30630/joiv.2.3-2.144.

[60] https://cybersecurity.osu.edu/cybersecurity-you/avoid-threats/what-zero-day-exploit

[61] https://scholar.afit.edu/cgi/viewcontent.cgi?article=4107&context=etd

[62] Arnold, Thomas & Yang, T.. (2011). Rootkit attacks and protection: a case study of teaching network security. Journal of Computing Sciences in Colleges. 26. 122-129.

[63] Liu, Leian & Yin, Zuanxing & Shen, Yuli & Lin, Haitao. (2012). Research and Design of Rootkit Detection Method. Physics Procedia. 33. 852-857. 10.1016/j.phpro.2012.05.145.

[64] Raza, Mudassar & Iqbal, Muhammad & Sharif, Muhammad & Haider, Waqas. (2012). A Survey of Password Attacks and Comparative Analysis on Methods for Secure Authentication. World Applied Sciences Journal. 19. 439-444. 10.5829/idosi.wasj.2012.19.04.1837.

[65] Rodwald, Przemysław. (2020). Attack on Students' Passwords, Findings and Recommendations. 10.1007/978-3-030-19501-4_42.