International Journal of Engineering and Information Systems (IJEAIS)
ISSN: 2643-640X
Vol. 5 Issue 6, June - 2021, Pages: 24-31

Smart Agriculture and Cybersecurity

Abeer Alshammari[1], Qamra Alharbi[1], Rawan Alonazi[1], Nora Aljomaih[1], Zainab Malik[2]

[1] Department of Computer Engineering, Prince Sattam Bin Abdulaziz University, Alkharj, Saudi Arabia
[2] Department of Electronics Engineering, Sudan university of science and technology, Khartoum, Sudan
E-mail: zienabmalik@gmail.com

***Abstract*—** *With the strife in cybersecurity and the staggering advances in Artificial Intelligence (AI), it is just normal that cybersecurity experts consider further utilizing learning techniques to help secure their organizations and improve the effectiveness of their security activity focuses. Due to the ever-expanding complexities in cybercrimes, there is a requirement for cybersecurity techniques to be more powerful and astute. This will make defense mechanisms and instruments to be capable of making real-time decisions for settling on ongoing choices that can adequately react to advanced attacks. To help this, the analysts and specialists should be acquainted with current strategies for guaranteeing cybersecurity. Specifically, the utilization of AI for fighting cybercrimes. In any case, there is an absence of outlines on AI techniques for battling cybercrime. It was observed that AI strategies have made remarkable contributions and commitments to fighting cybercrimes with a significant improvement in interruption identification frameworks. It was also observed that there is a decrease in computational multifaceted nature, model training times, and bogus alerts. AI technologies have a significant positive and challenging impact on cybersecurity in many fields. The purpose of this research is to highlight the strong overlap between AI and cybersecurity in smart agriculture field, also to explain the mechanism of AI, then clarify the relationship between cybersecurity and AI besides reviewing the challenges and risks facing smart agriculture.*

Keywords— cybersecurity; cyberattack; artificial intelligent (AI); smart agriculture.

1. INTRODUCTION

Agriculture is one of the important fields that positively effect on countries and recently, it has witnessed a development in several aspects, all of them concerns to solve the problems that reduce productivity like the time spent on farming and harvesting operations, the required labor and accuracy but with the rapid development in the world and the emergence of automation, it was essential for the field of agriculture to be a part of this growth. In the past years, various machines have appeared that assist in cultivation, irrigation and harvesting and with the initiation of AI and the Internet of Things (IoT), farms became fully automated. The irrigation is controlled depending on weather sensing and plant's need and the farm is fully monitored. This helped to reduce time and effort, increased productivity and enable the future production to be predicted through data collected. This means that the agriculture sector will rely more and more on smart information systems to improve operations and increase competitiveness and profit. Despite the enormous benefits gained from the use of technology, it can contain many risks, and the sector finds itself targeted like never, due to its modernity and most food and agricultural companies are still not investing in cybersecurity [1][2]. Hence, it is important to develop awareness in smart agriculture about the importance of cybersecurity and security and the challenges that arise from the extensive use of technology in the agricultural sector. In this paper, we discussed smart agriculture and the expected cybersecurity threats and how AI can improve cybersecurity beside presenting examples of smart agriculture structure. The remaining paper is organized as follows: Section 2 discusses some related work on smart agriculture. Section 3 reviews smart agriculture layers and security attacks. Section 4 presents comparison between different smart agriculture that using cybersecurity and analyze it. Finally, Section 5 concludes the work.

2. LEATREATURE REVIEW

In this section, we discuss the related work that uses AI and cybersecurity in agriculture field. K. Demestichas et. al presented a review on the current and potential threats in agricultural field and their effect on farm. Also, it presents different mitigation countermeasures against cybersecurity threats and attacks and finally it summarizes the most important keys that help the new method or system to success which is the ability to reduce cost, time, effort and risk and this can be done by AI algorithms to support a variety of conceptual models and security activities. Also, it suggests that farmers should be more aware about recent technology and how it can help to increase the productivity [3]. Similarly, the authors of [4] discussed security and privacy in smart farming, it outlines a multi layered architecture relevant to the smart agriculture domain and discusses the security, privacy issues and cyber-attack scenarios. It reviews different researches that discuss the using AI and machine learning in farms and it found that most of them have a limitation because of limited data, addressing security and privacy issue, not scalable, limited experiments, limited use cases. It suggests that there is a need to work and have more researches on access control security, data security,

network layer security and supply chain security. In [5] a systematic mapping of literature was done in AI for cybersecurity, it suggests that the application of AI in the Cybersecurity domain has been promising with detection and prevention system showing improvement. AI has facilitated a reduction in computational complexity and reduced model training times, the authors suggests that the opportunity can be found with doing combination with new AI algorithms because most of researchers have focused on fewer algorithms and as such newer algorithms are not popular. While in [1] the authors discuss different methods to adapt advanced security measures for cyberthreat prevention and mitigation. The potential implications of cyberthreats have been analyzed with real-world examples across different industries. It also compares between relevant researches in framework, machine learning and cyberattacks. It addresses the attack types by network layer in addition to the role of AI in cybersecurity as a new research area.
As shown, most of the previous works addressed the attacks and issues but there is a need to list them into groups depending on the cause of it and the solution needed. The suggested organization is to list the cyberattack issues into technical and non-technical issues. This division can ease the process of making an action and designing a suitable solution for smart agriculture system. The goal of this research is to presents cybersecurity threats that might be happen in smart agriculture, how AI can improve cybersecurity and to discuss smart agriculture issues and solutions from technical and non-technical lens.

3. SMART AGRICULTURE

Smart agriculture is the use of information and communications technology (ICT), Internet of Things technologies and data analysis to improve agriculture and its operations. The main purpose of smart agriculture is the need to monitor crops and environmental data related to soil testing, fertilization and irrigation. Smart agriculture generally relies on smart networks based on cyber-physical systems (CPS) that are controlled by the computer and the communication system allowing interaction with other devices, which are sensors, motors, processing control units and communication devices. For example, sensors can collect and transmit information such as soil moisture, fertilization, and weather fluctuations through a cellular wireless network to provide farmers real-time access to information and analyzes on their territory, Crops, livestock, logistics, machinery and then the operators can Perform pre-programmed work. This enables the smart agriculture to improve its operating performance through Analyze the collected data and act on it in ways that It can increase productivity or simplify operations [2]. Among the things that are controlled in smart agriculture are the following:

- Water management
- Fertigation
- Livestock safety and maturity monitoring
- Crop communication
- Drilling, seeding and spraying
- Crop monitoring
- Supply chain monitoring

All these things increase the possibility of threats due to the interconnected connections between devices and sensors.

3.1 Security Issues and Cyberattack Types in Smart Agriculture

- Data security and privacy
- Authorization and trust
- Authorization and secure communication
- Compliance and regulation

Cyberattacks in smart agriculture can be divided into four areas: Data attacks, networking and equipment attacks and supply chain attacks [4]. Fig. 1 explains examples of each attack.

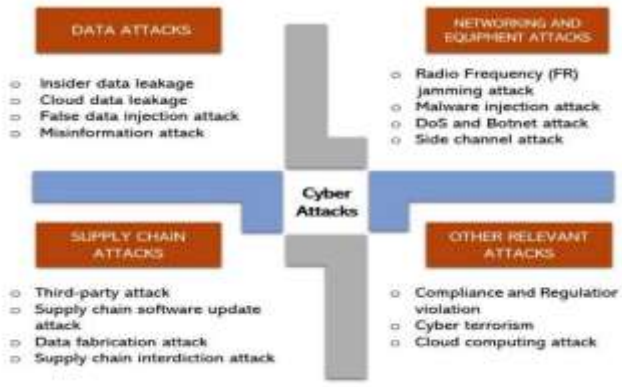

Fig.*1.* *Different cyberattack types*

The following table (Table I) is a review of several scientific papers on attacks in farms, their causes and suggested solutions.

Reference	Objectives/ research question	Attacks found	cyberattack causes	Counter measure used	Proposed solution	Suggested research area/ challenges
[3]	To review the security issues and threats and address effective mitigation strategies	-Physical Attack - Replay Attack -Attacks against Authentication -Malicious Code Attack	Multiple access points within users' homes and any other kind of application or space for hackers to exploit.	-Firmware Update Block -Unnecessary Ports -Encryption of Drives -Two-Factor Authentication	Apply Machine and Deep Learning application for cybersecurity in agriculture	When designing a new method or system it should be able to: (i) reduce costs; (ii) save time; (iii) increase trust; (iv) reduce risk. Stakeholders in agriculture should be willing to adopt new ways of working only when they are convinced that the newly proposed method or system is secure, safe and usable, increases productivity and brings added value.
[4]	To outlines a multi layered architecture relevant to the precision agriculture domain and discusses the security and privacy issues.	- Data attack -Network and equipment attack -Supply chain attack -Cloud computing attack -Cyber terrorism	Leakage of such information either through unauthorized access or by an insider can cause potential threats.	Software defined network (SDN)	Adapt SDN and other 5G related next generation communication technologies in smart farming to enable smart farms to get the most benefit out of complex machine learning and AI algorithms to automate network management of large number of devices and sensors.	Research challenges in: -Access control, trust and information sharing -Machine learning and AI in cybersecurity -Next generation network security -Trust way supply chain and compliance
[6]	To list possible threat scenarios for small farms' basic telecommunication infrastructure and the equipment and machinery connected to it.	-Consumer-grade equipment is not suitable for the physical farm environment and breaks easily -Network topology is not known to the farmer, so they	-Low general level of cybersecurity readiness in agricultural primary production. -Lack of farmer awareness of cybersecurity issues, lack of IT	Survey and field tour for six farms in Finland	-Increase the farmer awareness of cybersecurity -Map the farm network topology -Find expert support or IT technician to be responsible of network and devices check	-The paper results are limited to farms in Finland with the same specifications which means that any researcher should be careful when applying these results to other countries. -Only dairy farms are analyzed, and this open a research area

		are unable to maintain it or plan expansions -Malicious software protection is installed only on some of the devices leaving others vulnerable	technicians in farms. -The farm network is likely to be implemented without systematic design.			in other type of farms of mixed farms.

Table 1: Comparison Between Different Researches in, Cyberattack Causes, Types and Solutions

Table 1: Continued

Reference	Objectives/ research question	Attacks found	cyberattack causes	Counter measure used	Proposed solution	Suggested research area/ challenges
[7]	To develop a connected ecosystem which defines sensors and their communication among different entities.	-Data attacks -Network attack	-Large volumes of data generated by the sensors deployed in members farms. -Sharing or misusing data with an unauthorized entity or another member farm owner without permission	-	Proposed AI applications that add value to the smart farming co-op ecosystem in resources, security, mentoring and analysis.	Technologies must be resilient against cyber threats and call for the development of tailored security solutions.
[8]	To create a smart farming ontology and use it to develop an Attribute Based Access Control system.	-Man in the Middle attack -The Night Dragon attack	-False Data Injection which lead to data loss -Large connected devices, sensors	-	Create a smart farming ontology to encode farm specific sensors and interactions.	Develop the suggested smart farm design with the ability to cover and solve all the issues that list on the scenarios and might cause an attack.
[9]	To present simple and cost-effective smart farm architecture that uses a DoS cyber-attack to show the vulnerabilities in the system.	-Wi-Fi deauthentication Attack -Steps to a Denial-of-Service (DoS) Attack	-Non-reliable access point -Wifi -Weak password	MakerFocus ESP8266 Development Board and WiFiDeauth Monster	Implement a Wi-Fi DE authentication attack on the smart farm Wi-Fi network	-Expand on other attacks on smart farming infrastructure including evil twin access point and password cracking. -Extend these attacks to include protocols such as zigbee and bluetooth to launch attacks such as man-in-the-middle and replay.

[10]	To assist researchers and agriculturists to choose the most suitable and flexible security mechanisms for IoT deployment.	-Data attack -Authentication attack -Malware attack -Man in the middle attack	-No two authentication -Weak password -Weak network design	-Tamper-resistant hardware -Cryptography	Presents possible countermeasures against attacks on IoT devices in agriculture.	To focus on security issues in deployment of 5G communication technologies in IoT-based farming.

4. DISCUSSION AND ANALYSISI

The smart agriculture system is mainly consisting of sensors, actuators and data transport system. The collect data from the crop field to a control station for decision-making, operation and control according to the crop need. In every smart agriculture system, the layout design consists of different layers, Fig. 2 explains the four important layers in smart agriculture [11].

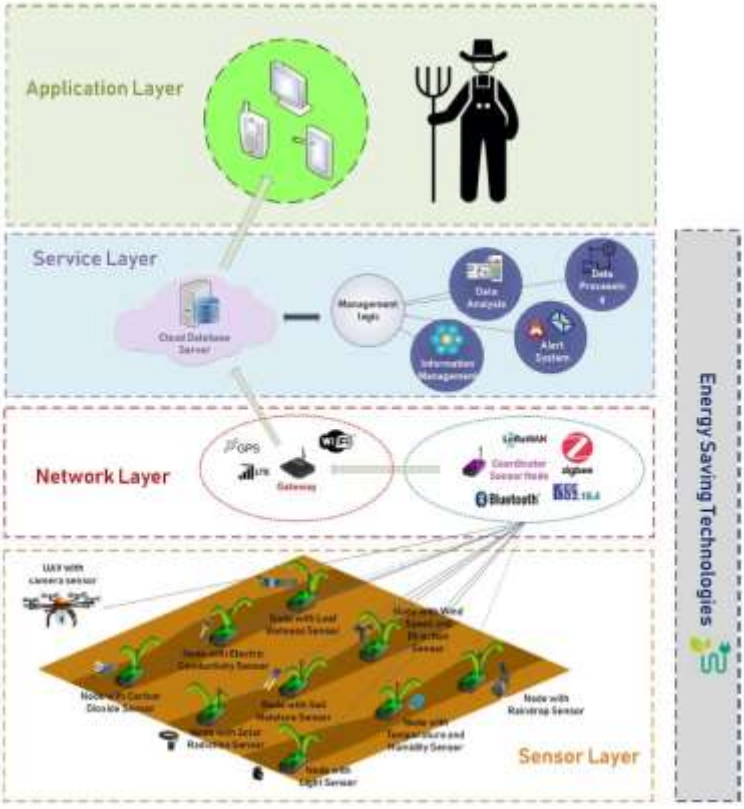

Fig.2. *Smart agriculture layers*

- Sensor layer contain all sensors and end nodes. The attack in this layer can be environmental (dust, water) or physical threat. This can affect on sensor reading which can response in false decision that can damage the crop.
- Network layer, it consists of all available communication technologies between the sensor and the Internet. In order to deploy effective crop and field management, the IoT platform uses wireless sensor networks (WSNs).
- Service layer, involving processing and analysis of the collected data.
- Application layer, providing the visualization of information of the sensor network.

As shown in Table I, several scientific papers related to cybersecurity in the field of agriculture were reviewed. The comparison was made in several aspects, the first of which is the aim of the research, the causes of the threats, the types of threats that were found and how they were measured, and then the proposed solutions, future actions or proposed areas of research.

With a comparison of the cyberattacks, we found that most of them revolve around data attacks, network attacks, supply chain attacks and cloud attacks. In addition to some of the attacks expected from hackers due to privacy issue. The reasons for these cyberattack were also presented and it was found that most of them are due to the poor design of the farm network or due to the neglect of the cybersecurity issue and the lack of IT technicians on the farm, which makes it vulnerable to tampering as well. Among the causes are weak passwords and weak WiFi networks security. From Table I, the attack causes can be divided into two types, technical causes and non-technical causes.

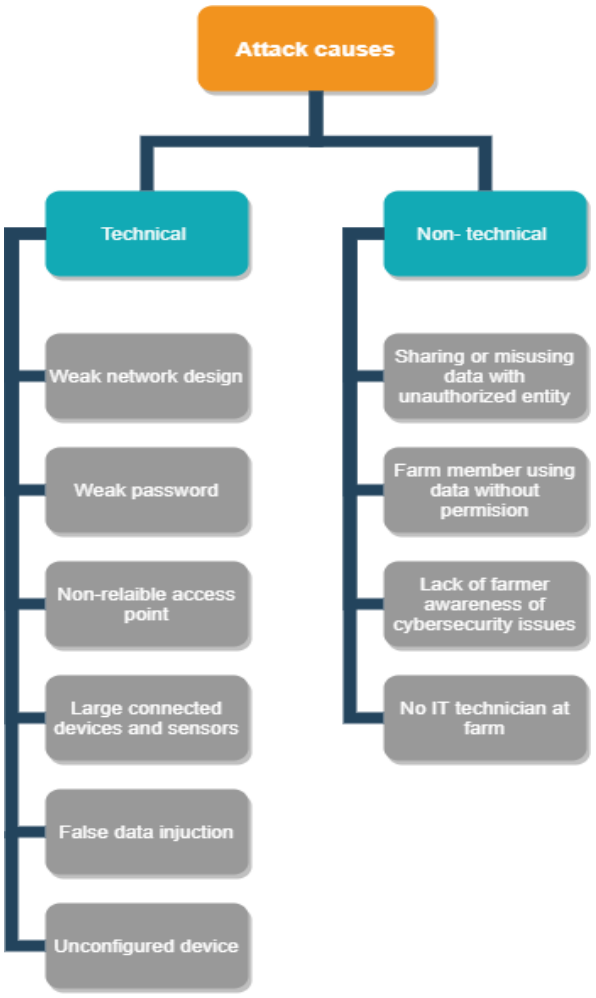

Fig. 3. *Common attack causes*

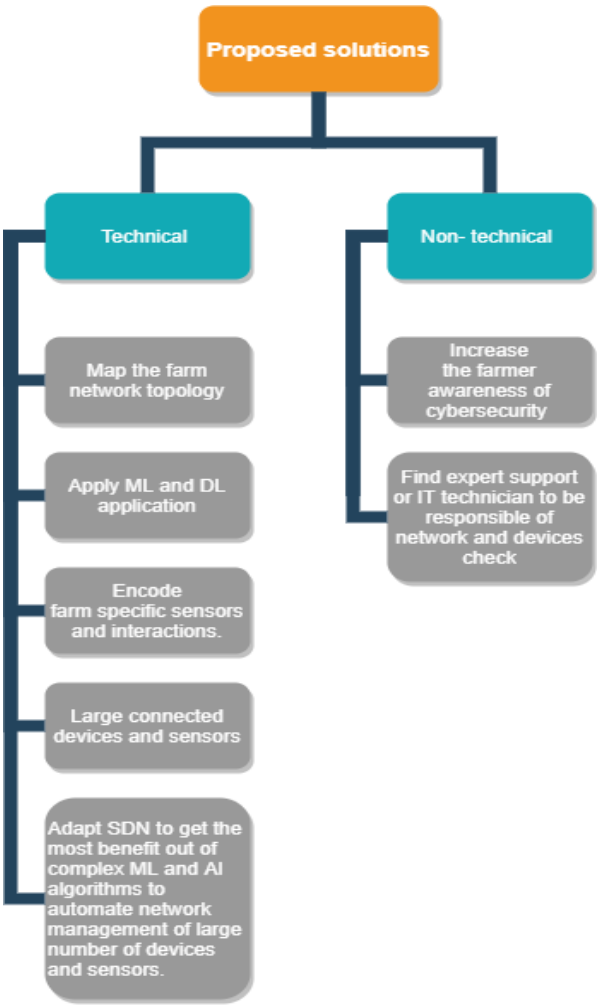

Fig. 4. *Common attack solutions*

As shown in Fig. 3, the non-technical attack causes concern with awareness or farmer information about cybersecurity beside IT technician to check the farm every period of time. The technical attack causes come from the primary design of farm network sometime the network design of large farm installed in a small farm which cause problems related to the unsuitability of the system with the farm size. Fig. 4 shows the solutions suggested, and it divided also into two types technical and non-technical.

The proposed solutions varied, but most of them are in the direction of integrating AI with cybersecurity, and how it can detect threats early before penetration, in addition to enhancing farmer's awareness of cybersecurity and its importance.

4.1 Cyberattack Effects on Smart Agriculture

Irrigation is one of the important processes in agriculture and has recently begun to pay attention to it within the goals of sustainable development. In smart agriculture, irrigation is controlled automatically, starting from placing sensors in the soil and then giving an

indication if the crop needs irrigation or not. Attacks on the system negatively affect crops because there are crops such as rice that need full water immersion, so if delivery is disrupted, this leads to large losses, and like that lettuce, it needs water in measured quantities. If it increases, decreases, or does not exist, this leads to the destruction of the entire crop and heavy losses as shown in Fig.5.

Fig.5. *Crop damage by water*

5. CONCLUSION

The aim of this research is to present several models of research on cybersecurity in smart agriculture and how AI can improve cybersecurity. Also, the importance of cybersecurity in smart agriculture and the types of threats that can arise were presented. Finally, a comparison was made between several models in terms of the causes and types of threats, and future suggestions from the perspective of technical and non-technical. It was found that most of the research recommend the integration of AI with cybersecurity and how it can be done by means of detecting threats before they affect the smart agriculture system. The reasons for the threats were also summarized, including poor information on cybersecurity by farmers and the seriousness of the threats that could occur, as well as the lack of permanent legalization on farms that increases the likelihood of being attacked.

6. REFERENCES

[1] S. Sadik, M. Ahmed, and L. F. Sikos, "Toward a Sustainable Cybersecurity Ecosystem," pp. 1–17, 2020, doi: 10.3390/computers9030074.

[2] L. Barreto and A. Amaral, "Smart Farming: Cyber Security Challenges," in 9th International Conference on Intelligent Systems 2018: Theory, Research and Innovation in Applications, IS 2018 - Proceedings, 2018, pp. 870–876, doi: 10.1109/IS.2018.8710531.

[3] K. Demestichas, N. Peppes and T. Alexakis, "Survey on Security Threats in Agricultural IoT and Smart Farming" Sensors, vol. 20, 2020, doi: 10.3390/s20226458.

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

[5] I. Wiafe, F. N. Koranteng, E. N. Obeng, N. Assyne, A. Wiafe, and S. R. Gulliver, "Artificial Intelligence for Cybersecurity: A Systematic Mapping of Literature," IEEE Access, vol. 8, pp. 146598–146612, 2020, doi: 10.1109/ACCESS.2020.3013145.

[6] J. Nikander, O. Manninen, and M. Laajalahti, "Requirements for cybersecurity in agricultural communication networks," Comput. Electron. Agric., vol. 179, no. September, p. 105776, 2020, doi: 10.1016/j.compag.2020.105776.

[7] S. S. L. Chukkapalli et al., "Ontologies and Artificial Intelligence Systems for the Cooperative Smart Farming Ecosystem," IEEE Access, vol. 8, pp. 164045–164064, 2020, doi: 10.1109/access.2020.3022763.

[8] S. S. L. Chukkapalli, A. Piplai, S. Mittal, M. Gupta, and A. Joshi, "A Smart-Farming Ontology for Attribute Based Access Control," Proc. - 2020 IEEE 6th Intl Conf. Big Data Secur. Cloud, BigDataSecurity 2020, 2020 IEEE Intl Conf. High Perform. Smart Comput. HPSC 2020 2020 IEEE Intl Conf. Intell. Data Secur. IDS 2020, pp. 29–34, 2020, doi: 10.1109/BigDataSecurity-HPSC-IDS49724.2020.00017.

[9] S. Sontowski et al., "Cyber Attacks on Smart Farming Infrastructure," 6th IEEE Int. Conf. Collab. Internet Comput. (IEEE CIC 2020), 2020.

[10] O. E. Oche, S. M. Nasir, and A. H. Muhammed, "Internet of Things-Based Agriculture: A Review of Security Threats and Countermeasures," Int. J. Sci. Res. Publ., vol. 10, no. 8, pp. 738–748, 2020, doi: 10.29322/ijsrp.10.08.2020.p10494.

[11] K. Bresniker, A. Gavrilovska, J. Holt, D. Milojicic, and T. Tran, "Grand challenge: Applying artificial intelligence and machine learning to cybersecurity," Computer (Long. Beach. Calif)., vol. 52, no. 12, pp. 45–52, 2019, doi: 10.1109/MC.2019.2942584.