Cyber-Security Threats And Side-Channel Attacks For Digital Agriculture

Dr.S.Manju[1], Praveen Kumar. V[2]
[1]Associate Professor, Dept of Computer Application (MCA)
[2]Dept of Computer Application (MCA)
[1, 2] PSG College of Arts & Science, Coimbatore, Tamil Nadu, India.

Abstract- *The Numerous labor-intensive jobs have been moved into the digital sector thanks to the development of intelligent low-power devices and pervasive Internet access. The agriculture sector has had to adapt to the digital transformation due to the lack of skilled labor and the rising food demand. Crops, plants, the environment, water, soil moisture, and illnesses are all monitored using sophisticated sensors and systems. The switch to digital agriculture would increase the quantity and quality of food available to the world's expanding population. In contrast to other publications that have been published, this research highlights the security risks and holes in digital agriculture. It also offers a thorough analysis of side-channel attacks (SCA) unique to digital agriculture that haven't been looked into before. The report also covers the unresolved issues in research.*

Keywords- side-channel attacks, vulnerability analysis, power analysis attack, security threats, cryptography, digital agriculture, smart agriculture, smart farming.

I. INTRODUCTION

In the past century, there has been a rapid growth in the human population. A rough estimate that by 2100, it will reach its high of 10.9 billion. The improvement in the quality and quantity of the world's food supply is largely attributable to technological advancements in genetic engineering over the five decades. Genetic engineering aids in creating seeds and plants that require less water and energy to flourish. In order to meet the demands of an expanding population, more water and nutrients must be produced. Digital The next technical advancement for the sustainable production of food in is agriculture. The industry of agriculture. Countries, like Saudi Arabia, are battling desertification Four million lemon trees that are part of the Saudi Vision 2030's "Green Initiative" hundreds of trees that rely on recycled water for irrigation are being planted.

Cyberattacks may affect anything from a vertical farm's heating and ventilation system to a drone used to spray crops, so digital agriculture is not immune. Recent cyber-attacks have made headlines all around the world, including those on the Florida water system, Lion (an Australian beverage corporation with businesses in dairy and drinks), wool broker software, and JBS, the largest meatpacker in the world. Due to supply, labor, and cost issues, this has brought to light the weaknesses of digital agriculture and the potentially severe consequences for the general populace.

Recently, researchers have focused their attention to side-channel attacks (SCAs) on traditional computer networks, mainly exploring cryptographic information leakage. To the best of the authors' knowledge, there is no work dedicated to side-channel attacks on digital agriculture or smart farming. SCAs on the Internet of Things (IoT) are the subject of the closest study . The discussion of side-channel risks, attacks, and their effects on digital agriculture will be presented in this study piece for the first time. We want to start a discussion in this largely uncharted area.

These are the contributions made by this paper:

- We assessed the body of research on cyberthreats to digital agriculture critically.
- Specific information about SCA threats to digital agriculture is provided, along with their effects.
- In this article, we go over open difficulties associated to digital agriculture that are both technical and non-technical, as well as cyberthreats.

The rest of the essay is structured as follows: The various uses of digital agriculture are defined in Section 2. Section 3 discusses dangers to digital agriculture. The review of side-channel assaults, their various subtypes, and risks in Section 4 includes instances from digital agriculture. The difficulties of the research are covered in Section 5, and the conclusions are covered in Section 6.

II. DIGITAL AGRICULTURE

Humans depend on agriculture for their survival since it not only produces food but also creates jobs. The agricultural industry needs to be modernized due to the rising demand for sustainable food production, a skills gap, and the efficient use

of finite environmental resources. The practice of using various digital devices to monitor, evaluate, and manage environmental factors that could have an impact on the production of food (crops, fruit, etc.) is known as digital agriculture (DigAg), sometimes known as smart agriculture/farming. Environmental factors may include soil quality, water utilization, moisture content, plant and crop diseases, climate, pests, pollination, dietary needs, and irrigation system. It is possible to use digital tools like smartphones, different sensors, global positioning systems (GPS), robotics, and drones to collect important data, analyze it, and take wise decisions to boost food production with less human resources and invention.

1. Layer 1 is a sensing layer that contains various sensors to keep an eye on the plants or other environmental elements, such as the soil or the weather. For various applications and use cases, different sensors would be used. These sensors are usually low-cost, have limited computing and battery power, are placed in the field, and are mostly left alone in dangerous situations. The same layer may include actuator capabilities to carry out a particular task, such as controlling water flow or spraying with drones.
2. The gateway layer, or layer 2, is where gateways act as a bridge between the Internet and sensors. Typically, sensors are connected using wireless communication. Zigbee, WiFi, Bluetooth, NB-IoT, Sigfox, LoRa, 5G, or satellite communication may be employed, depending on the needs of the application. Switches and access points, which serve as forwarding devices, are included.
3. The storage or processing layer is Layer 3. One option is to employ a cloud or internal data storage system.
4. The application layer, or layer 4, is where all users can view or manage sensors. The data is used to derive useful insights, and then an informed action is taken. A farmer, an agroscientist, a broker, a trader, a representative of the government, or a company could be the end-user.

Figure 1 shows an overview of digital agriculture and its various components. Broadly, it can be split into four separate layers.

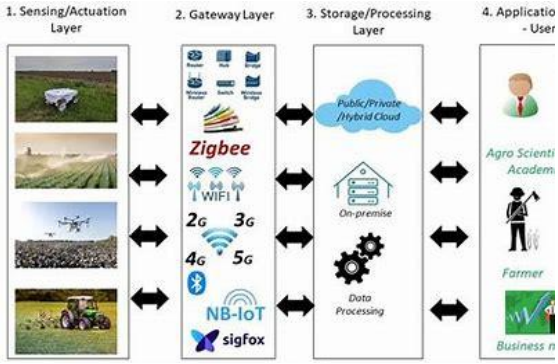

Figure 1 shows an overview of digital agriculture and its various components. Broadly, it can be split into four separate layers andan overview of digital agriculture and its various applications.

2.1.APPLICATION—INTELLIGENTMACHINERY IN AGRICULTURE

An intelligent agricultural machine may operate the machinery with the least amount of human intervention by using sensors and computer logic to control and operate the machinery. Small cultivation plots can be created from a vast agricultural acreage. With little manual or semi-autonomous resources, it is challenging to attain maximum output due to variations in the soil, moisture, correct seed planting, and land level. For instance, real-time analysis of the soil and moisture content and exact application of fertilizer or other chemicals according to requirement take time in a manual operation and depend on the competent farmer. The talent gap is filled by an intelligent machine that operates almost constantly. It could be used for various kinds of agricultural operations, including sowing seeds along streams, harvesting, applying fertilizer, checking on the health of the crops, and leveling and plowing the ground. A completely automated system should be intelligent enough to locate itself precisely, establish a route, have a safety system, and start monitoring, analyzing, and acting on cultivation-related data.

III. THREATS TO DIGITAL AGRICULTURE

As indicated in Section 2, many technologies are combined into one product to carry out particular agricultural activities. An irrigation system, as an illustration, includes intelligent sensors and actuators, software, conventional networking hardware, and human interaction. Cybercriminals can breach one or more components of the agricultural application by taking advantage of flaws in the sophisticated systems that are frequently outsourced from many vendors and created for a variety of environments and applications. While some of the vulnerabilities are unique to digital agriculture, others are comparable to threats in traditional computer or IoT

networks. Threats that have not been specifically investigated for DigAg are discussed in the following subsections.

3.1. RESEARCH AND INTELLECTUAL PROPERTY

Years of collaboration between academics, researchers, students, industry partners, funding agencies, and the government in the field of agriculture result in new ways to increase crop output and quality in a variety of conditions. This research and intellectual property (IP), which support the national economy and the life of the populace, are of great interest to malicious users and state actors. Insider threats, social engineering, technology flaws or misconfiguration, data leakage, and insider threats are all potential sources of IP threats.

3.2. PERSONALLY IDENTIFIABLE INFORMATION

DigAg systems are expensive and frequently used for extended periods of time. Over the course of their existence, many users, including technicians, farmers, tradespeople, service providers, etc., access them. When these users use the system, their personally identifiable information (PII) may be hacked and then utilized for identity theft.

3.3. INTERNET OF THINGS, ROBOTICS, AND AERIAL SYSTEMS

Digital agriculture is enabled through the Internet of Things, robotics, drones, and aerial systems. Remote controls are used to operate sensors and agricultural robots. Sensors, actuators, and robots that have been compromised may no longer function normally or, in the worst case scenario, may be employed in agricultural terrorism. Heavy tractors or drones can be used to commit crimes, destroy property, transport illegal products, or launch direct physical attacks against a target. Wireless communication flaws and GPS spoofing can both be used to launch damaging assaults.

THREATS	DESCRIPTION
Cyber attacks	Malicious activities targeted at digital agriculture systems, such as hacking or data breaches
Side-Channel attacks	Attacks that exploit information leaked through unintended channels, potentially compromising security.
Vulnerability analysis	Idenrifying weakness in digital agriculture systems that can be exploited by attackers.
Power Analysis	Analyzing power consumption to extract sensitive information from digital agriculture devices.
Security threats	Various risks to the security and integrity of digital agriculture systems and data.
Cryptography	The study of techniques used to secure information and communication in digital agriculture.

IV. SIDE-CHANNEL ATTACKS

Devices and communication channels make up a communication system. By only using secret credentials to access devices and encrypting the communication route, reasonable security can be attained. Side-channel attacks include obtaining information from data leaks that occur during communication or system access. The covert channel, which is used to communicate covertly to evade middle-of-the-conversation listeners or exfiltrate information, is a concept similar to the side-channel. The internal workings and operation of the targeted device can be used as the source of valuable sensitive information by side-channel and covert assaults, which take advantage of the physical characteristics of the hardware, software, or transmission media.

Kocher showed in 1996 that the complete secret key could be retrieved using timing information from the cryptographic implementation. Numerous side-channel attempts to bypass encryption and retrieve confidential credentials have been identified as a result of the growth of smart devices, IoT, sensors, and lax cryptographic implementation on hardware. Physical and functional side-channel assaults are distinguished by type. Based on a measurable amount that is a by-product of the implementation, the physical categorization is made. Examples include power output, electromagnetic emission, clock timing, user interaction, auditory, optical, and thermal signals, as well as network inference (wired/wireless). The functional type is based on how the computing system operates internally and how it implements internal functional functionality. The implementation of memory, CPU/GPU architecture, and the implementation/coding of cryptography in software and firmware are a few examples.

V. RESEARCH CHALLENGES AND FUTURE DIRECTIONS

To quickly seize the market, the majority of new technology goods are developed and commercialized. The customization of many equipment and sensors is primarily focused on operation in a harsh, uncontrolled outside environment, even when they are not built specifically for DigAg applications. Device security is given little consideration. Security is frequently given the lowest priority, similar to how other technologies are, as opposed to being integrated into the design process. Some of the unresolved problems—which are still in the early stages of research—are covered in this section.

5.1. INTRUSION DETECTION AND PREVENTION SYSTEM

In the past, massive data networks have been the focus of intrusion detection and prevention system (IDS/IPS) development. Different needs, such as low-rate sensor data, sparse observation and attenuation, unattended deployment, and remote control, are needed for digital agriculture. For digital agriculture, new intrusion detection/prevention algorithms should be created. IDS/IPS datasets are not yet accessible for DigAg applications. Traditional IoT-smart home datasets [55] or computer networks [56] are the two types of existing datasets. The development of such algorithms and systems would be aided by theexistence of an open-source dataset centered on agriculture. AI algorithms are useful while creating IDS/IPS systems. Blockchain technology and AI at the edge of computers would also be beneficial in reducing some of the current assaults. Deploying edge-based IDS systems will need a lot of work.

5.2. PRIVACY PRESERVING SCHEMES

Users could overlook the fact that the majority of the data in the DigAg are related to field work. DigAg privacy-preserving techniques are a developing field. To safeguard the data from the malevolent user in all aspects, including data privacy, data analytics, data utility, and overall system efficiency, new privacy-preserving strategiesmust be created specifically for digital agriculture. The use of new privacy-preserving techniques would reduce PII, commercially sensitive data, and IP theft.

5.3. VULNERABLITIES AND THREAT ANALYSIS

For varied applications, there are different DigAg devices and IT requirements. One particular approach incorporates hardware and software from various vendors, expanding the attack surface. Before connecting the devices, a comprehensive vulnerability and threat analysis should be carried out, taking into account side-channel assaults, which are challenging to analyze and often not addressed in cyber-security frameworks. Each hardware system should be examined in light of how it is used and potential dangers, whether they are software- or hardware-related.

VI. CONCLUSION

In order to boost crop productivity while using less resources, new applications and technological advancements are made possible by the digitalisation of agriculture. The majority of currently available technology is updated and networked to offer creative answers to the long-standing agriculture challenge. This post included a general threat analysis of our DigAg model's four layers. The implications of threats like IP and PII that are ignored by DigAg and side-channel assaults were thoroughly examined. Finally, future directions and open research problems were discussed. Instead of waiting until the very end, the research challenges should be tackled early oninthe development and deployment process. If not, it would cost a lot of money to fix them.

REFERENCES

[1] Desa, U. United Nations, Department of Economic and Social Affairs, Population Division. In World Population Prospects;United Nations: New York, NY, USA, 2019; Available online: https://population.un.org/wpp/Publications/Files/WPP2019_10KeyFindings.pdf (accessed on 15 January 2022).

[2] Basso, B.; Antle, J. Digital agriculture to design sustainable agricultural systems. Nat. Sustain. 2020, 3, 254–256. [CrossRef]

[3] Mathews, L. Florida Water Plant Hackers Exploited Old Software and Poor Password Habits.2021.Availableonline:https://www.forbes.com/sites/leemathews/2021/02/15/florida-water-plant-hackers-exploited-old-software-and-poorpasswordhabits/?sh=78dd125c334e(accessed on 19 December 2021).

[4] Musotto, R.; Naser, M. Ransomware Attack on Sheep Farmers Shows There's No Room for Woolly Thinking in Cyber Security.2020. Availableonline: https://theconversation.com/ransomware-attack-on-sheep-farmers-shows-theres-no-room-forwoollythinking-in-cyber-security-132882 (accessed on 19 December 2021).

[5] Seselja, E. Cyber Attack Shuts Down Global Meat Processing Giant JBS. 2021. Available online: https://www.abc.net.au/news/2021-05-31/cyber-attack-

shuts-down-global-meat-processing-giant-jbs/100178310 (accessed on 19 December 2021).

[6] Nikander, J.; Manninen, O.; Laajalahti, M. Requirements for cyber-security in agricultural communication networks. Comput.Electron. Agric. 2020, 179, 105776. [CrossRef]

[7] Zahidi, S. The Global Risks Report 2022, 17th Edition. 2018. Available online: https://www3.weforum.org/docs/WEF_The_Global_Risks_Report_2022.pdf (accessed on 19 January 2022).

[8] Nakhodchi, S.; Dehghantanha, A.; Karimipour, H. Privacy and Security in Smart and Precision Farming: A Bibliometric Analysis.

[9] In Handbook of Big Data Privacy; Springer: Cham, Switzerland, 2020. [CrossRef]

[10] Kristen, E.; Kloibhofer, R.; Díaz, V.H.; Castillejo, P. Security Assessment of Agriculture IoT (AIoT) Applications. Appl. Sci. 2021,11, 5841. [CrossRef]

[11] Haas, R.; Hoffmann, C. Cyber Threats and Cyber Risks in Smart Farming; VDI Verlag: Düsseldorf, Germany, 2020. [CrossRef]

[12] Demestichas, K.; Peppes, N.; Alexakis, T. Survey on Security Threats in Agricultural IoT and Smart Farming. Sensors 2020, 20, 6458. [CrossRef]

[13] Rosline, G.J.; Rani, P.; Rajesh, D.G. Comprehensive Analysis on Security Threats Prevalent in IoT-Based Smart Farming Systems. In Ubiquitous Intelligent Systems; Springer: Singapore, 2022. [CrossRef]

[14] Tudosa, I.; Picariello, F.; Balestrieri, E.; Vito, L.D.; Lamonaca, F. Hardware Security in IoT era: The Role of Measurements and Instrumentation. In Proceedings of the 2nd Workshop on Metrology for Industry 4.0 and IoT MetroInd4.0&IoT 2019, Naples, Italy, 4–6 June 2019; pp. 285–290. [CrossRef]

[15] Randolph, M.; Diehl, W. Power Side-Channel Attack Analysis: A Review of 20 Years of Study for the Layman. Cryptography 2020, 4, 15. [CrossRef]

[16] Devi, M.; Majumder, A. Side-Channel Attack in Internet of Things: A Survey. In Applications of Internet of Things; Springer: Singapore, 2021. [CrossRef]

[17] Schimmelpfennig, D. Farm Profits and Adoption of Precision Agriculture; Technical Report ERR-217; U.S. Department of Agriculture, Economic Research Services: Washington, DC, USA, 2016.

[18] Hedley, C.; Yule, I. A method for spatial prediction of daily soil water status for precise irrigation scheduling. Agric. Water Manag. 2009, 96, 1737–1745. [CrossRef]

[19] Salam, A. A path loss model for through the soil wireless communications in digital agriculture. In Proceedings of the 2019 IEEE International Symposium on Antennas and Propagation (IEEE APS), Atlanta, GA, USA, 7–12 July 2019.