Evaluating Cyber Threats and Mitigation Techniques for Smart Farming Technologies

Jessica Stevens- Montana State University
Mentors: Dr. Clemente Izurieta & Yvette Hastings

Introduction

Smart farming (SF) technologies, such as automated irrigation systems, GPS-guided equipment, and livestock monitoring technologies, have revolutionized agriculture, improving the efficiency, sustainability, and productivity of farming practices. However, these technologies have introduced significant cybersecurity vulnerabilities, resulting in ransomware attacks and data breaches. Cyberattacks on these systems have substantial financial losses, with major agricultural companies experiencing millions of dollars in damages due to operational shutdowns and data theft. Additionally, these attacks have disrupted food production and supply chains, leaving the world population at risk of contaminated food sources and increased food insecurity.

Due to a lack of cybersecurity awareness among farmers and limited industry-specific protective measures, the risks of cyberattacks have increased. This study presents a detailed analysis of cyber threats in agriculture, visualizing at-risk technologies and computer processes. Additionally, this study presents mitigation strategies, such as enhanced cybersecurity training, multi-factor authentication, and government-supported security initiatives, which have proven effective in reducing threats. The results of this study emphasize the urgent need for cybersecurity integration within the sector to safeguard food security and economic stability.

Research Method[1,2,4,5]

A literature review was conducted using the search string ‘Smart Farming Cyber Mitigation techniques on Google Scholar. I then ensured the paper related to the topic of Smart Farming by applying inclusion criteria.

Inclusion criteria:

- Is the paper about agriculture smart equipment not manual
- Does the paper have multiple authors
- Was it published between 2018-2025
- Is the paper’s topic directly related to Smart Farming mitigation techniques.

After the inclusion criteria was met, Google Scholar returned approximately 23000 papers. I randomly selected 25 papers and read their abstracts. Five of the 25 papers were determined applicable and useful to this study and are used to synthesize vulnerable attack points and countermeasure information.

Results

Findings from my comprehensive literature show that cyberattacks in smart farming most frequently exploit network vulnerabilities and data integrity issues. In this section, I showcase the main vulnerable attack points - such as network infiltration and misuse of support chains. I also highlight physical countermeasures including secure storage, regular maintenance, and the use of blockchain for enhanced data protection.

Vulnerable Attack Points (Fig. 1)[2]

- **Hardware** - violate privacy, confidentiality, or authenticity when they hit cyber-physical systems
- **Network** - target the connected devices
- **Data/Code** - hit data being stores or transmitted while violating the integrity of the software system
- **Support Chain** -hit different components of the support chain
- **Misuse** - attacks on physical resources on other entities

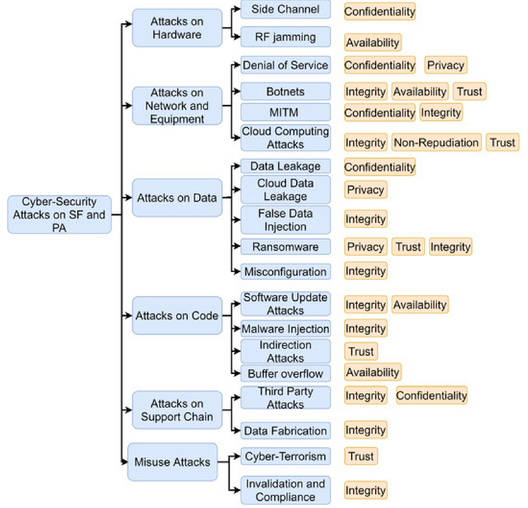

Fig. 1: Cyber-security attack tree. Image from: https://ieeexplore.ieee.org/abstract/document/9319032

Physical Countermeasures[2,3]

Physical access controls and other physical behaviors can reduce security risk. It is necessary to inspect and maintain devices regularly to prevent environmental and personal complications that could obscure security measures. 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 liked locked cabinets and rooms can also reduce security risk. Some architectures have applied blockchain technology to ensure data privacy and security as well as addressing fault tolerance, access control, and third-party removal to tackle these challenges. Understanding and considering them is a viable way to obtain security threat mitigation in SF and PA environments.

Conclusion[1,4,5]

It is clear there are many cyberattacks and security threats in SF that can cause serious disruptions to the markets and economies of many nations, especially those that are heavily dependent on the agriculture industry. The possibility of agricultural attacks has created an unstable and uncertain environment in the agriculture sector. This is because the agriculture sector is an attractive target for hackers and adversaries due to its relative ease of access compared to other sectors. Therefore, it is imperative researchers realize the potential these technologies need to be protected from cyber-attacks. 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. Security is a critical need in the field of SF. My studies on SF cyber-threats led to a systematic CKC-based taxonomy on these threats.

The information extracted from this literature review highlights the importance of future work in the SF domain. The four main areas of focus are:

- Designing safe and secure architecture, systems, and methods with resource-constrained smart devices in SF
- Enriching the SF taxonomy with in-depth analyses of the tactics, techniques, and procedures of various emerging advanced persistent threat actors, as well as incorporating network protection frameworks into the taxonomy
- Introduce machine-to-machine authorization devices between SF devices
- Use of deep learning and machine learning to identify and extract relevant technical metrics and other characteristics

Acknowledgements

This work is supported by funding for the VICEROY Northwest Institute for Cybersecurity Education and Research (CySER) provided by The Office of the Undersecretary of Defense for Research and Engineering, in collaboration with the Air Force Research Laboratory and Griffiss Institute.

References

[1] Adewusi, N. a. O., Chiekezie, N. N. R., & Eyo-Udo, N. N. L. (2022). The role of AI in enhancing cybersecurity for smart farms. *World Journal of Advanced Research and Reviews*, *15*(3), 501–512. https://doi.org/10.30574/wjarr.2022.15.3.0889

[2] *Cyber attacks on smart farming infrastructure*. (2020, December 1). IEEE Conference Publication | IEEE Xplore. https://ieeexplore.ieee.org/abstract/document/9319032

[3] *Cybersecurity for smart farming: Socio-Cultural context matters*. (2020, December 1). IEEE Journals & Magazine | IEEE Xplore. https://ieeexplore.ieee.org/abstract/document/9288982

[4] Mahlous, A. R. (2024). Security Analysis in Smart Agriculture: Insights from a Cyber-Physical System Application. *Computers, Materials & Continua/Computers, Materials & Continua (Print)*, *79*(3), 4781–4803. https://doi.org/10.32604/cmc.2024.050821

[5] *Smart farming: cyber security challenges*. (2018, September 1). IEEE Conference Publication | IEEE Xplore. https://ieeexplore.ieee.org/abstract/document/8710531