2-29-2024

Cybersecurity Challenges and Solutions in IoT-based Precision Farming System

Shree Ram Abayankar Balaji
shree.balaji@und.edu

Sriram Prabhakara Rao

Prakash Ranganathan
University of North Dakota, prakash.ranganathan@und.edu

Cybersecurity Challenges and Solutions in IoT-based Precision Farming Systems

Center for Cyber Security Research
College of Engineering & Mines
University of North Dakota

Introduction

- The adoption of technologies in agriculture, such as the Internet of Things (IoT), unmanned aerial vehicles (UAVs), and blockchain, has revolutionized farming activities.
- These advancements also bring a fair share of security challenges, including vulnerabilities that adversaries can exploit and compromise agricultural IoT networks.
- This may lead to compromised services and devices disrupting farming activities, causing losses to the farmers.

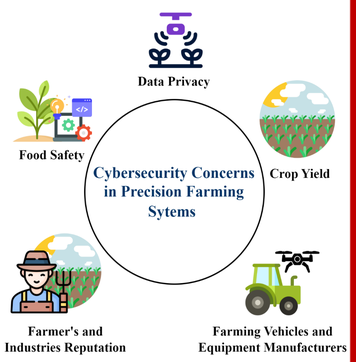

Figure 1: Illustration of Potential Impacts of Cyber Attacks in Precision Farming

Advancements

Technologies in Precision Farming

- It is critical to know the available technologies to help farmers understand how far we have come from traditional farming techniques.
- Precision farming technologies include but are not limited to supply chain networks, Global Positioning Systems (GPS), automated irrigation systems, guided UAVs, farming tractors, cloud services, databases, and forecast modules for monitoring and easing farming activities across large farms.
- Fig. 2 shows the technologies and their applications in precision farming. This section highlights the common technologies used in precision farming.

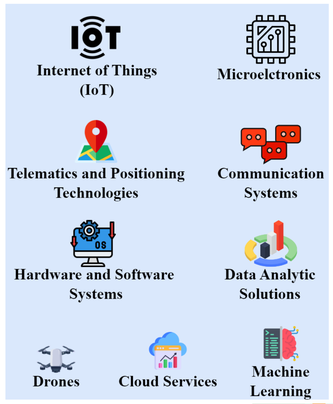

Figure 2: Evolving Technologies in Precision Farming

Figure 3: Beneficial Applications for Farmers through Evolving Technologies

Threats

Attacks on IoT-based Precision Farming

- Modern technologies also create a vulnerable space for attackers who are more than willing to inflict damage on their desired outcomes.
- Fig.3 depicts the vulnerable open attack areas in precision farming that adversaries can exploit.
- The outcomes can range from obtaining a ransom to release the compromised data, devices, and services to causing multiple losses for the farming community, creating a chain reaction in a collapsed supply chain and a nation's economy \cite{Hopkins_2023}.

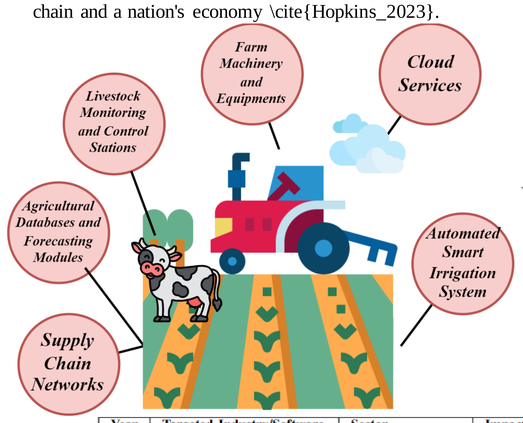

Figure 3: Attack Vulnerabilities in Precision Farming.

Year	Targeted Industry/Software	Sector	Impact and Economic Loss	Estimated Economic Loss
2023	Dole Plc, Ireland	Food Processing	Temporary shutdown of production plants in North America	$10.5M
2022	Hp Hood LLC, England	Diary Farming and Supply	Shortages of milk supply to schools in England due to the cyber attack	Not Publicly Disclosed
2021	JBS USA Holdings, Inc., USA	Meat Processing	Systems were taken offline, and a ransom of $11M was paid to the hackers in Bitcoin.	$11M
2021	Fort Dodge, Iowa-Based Grain Cooperative Inc., USA	Precision Farming	4-day outage disrupting grain operations, and a $5.9M Ransom was demanded	Not Publicly Disclosed
2020	Talman Software, Australia	Wool Trading	Buying and Trading System for trading wool was forced to take offline.	Not Publicly Disclosed
2020	Lion Diary & Drinks, Australia	Diary Farming and Drink Industry	Halted production and regular supply	$8M
2020	Jordan Valley Farm Irrigation Systems, Israel	Precision Farming	Pro-Palestine campaign and temporarily disabled irrigation system in Jordan Valley	Not Publicly Disclosed
2017	Mondelez International, Inc., USA	Food manufacturing	Over $100 million was spent on recovering from damages due to logistics software failure, inaccessible files and emails, and frozen company devices.	$100M

Table 1: Timeline of attacks on precision farming.

Vulnerabilities in Autonomous Vehicles

- Precision farming has seen many innovations, for example, John Deere's fully automated tractors at CES 2022 \cite{deereAutonomous}.
- Cybersecurity challenges in normal commuting vehicles may also be present in basic and autonomous farming vehicles, possessing a higher threat and damage when an adversary compromises.
- Fig. 4 depicts the vulnerable sensors, ECU, and software applications that can be exploited to compromise such autonomous farming vehicles used in a farming environment.

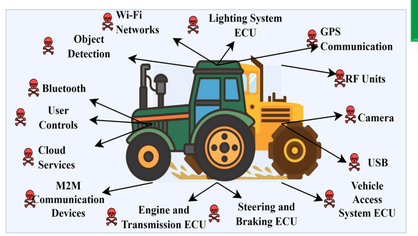

Figure 4: Vulnerable Farming Vehicles.

Attacks	Vulnerable component	Attack unit/Areas	Accessibility
Reverse engineering	Sensors, Heavy tractors Drones	Irrigation, Sprinkler	Physical layer
MITM attacks	Sensors, M2M communication devices	Irrigation, Ventilator	Network layer
Spoofing attacks	Wi-Fi router, GPS	Farm destruction	Network layer
DoS attack	Communication Gateway	Security Protocols, Databases	Network layer
Physical Tampering	Hardware, Cameras, Sensors, Heavy tractors, Drones	Production levels, Farm destruction	Physical layer
False Data injection	Sensors, Tractors, Drones, Communication Gateway	Access control	Network layer
RF Jamming	RF devices, GNSS	Network signals	Network layer
Password Cracking, Key Reinstallation attacks	Wi-Fi router	Monitoring Status and station control	Physical and Software layer
Side channel attacks	Sensors, GPS, Autonomous vehicle functions	Hardware units for data extraction	Physical layer
Cloud computing Attacks	ML algorithms, Cloud computing networks	Big Data, Forecasting modules	Network layer
Environmental attacks	All physical and remote systems	On device networks, Base stations	Physical and Network layer

Table 2: Attacks, Vulnerable Assets in Precision Farming Systems.

Security

Security Measures

- Precision farming requires specific measures and regular checks to ensure that IoT device and network security are uncompromised\cite{paloalto}.
- A security strategy is always necessary to protect the various endpoints present in the precision farming system.
- DLP policies, intrusion detection systems (IDS), and intrusion prevention systems (IPS) are used to monitor for possible data loss and intrusions in farming IoT networks.
- Fig. 5 shows the state of security practices in precision farming.

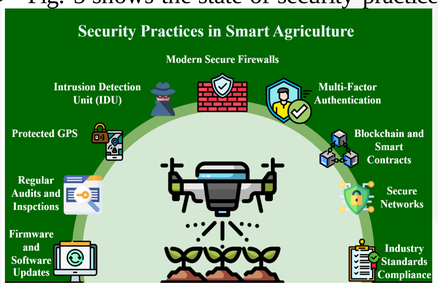

Figure 5: State of security practices in precision farming.

Secure IoT Lifecycle

- The IoT in the farming environment must be secured at various levels to prevent them from becoming compromised and posing a threat.
- Hardening the security of interconnected IoT devices requires different security methods, like intrusion detection systems and network traffic monitoring.
- Fig. 5 shows the overall security lifecycle for IoT devices installed on farms. Device inventories should be maintained for IoT assets installed across the farm.

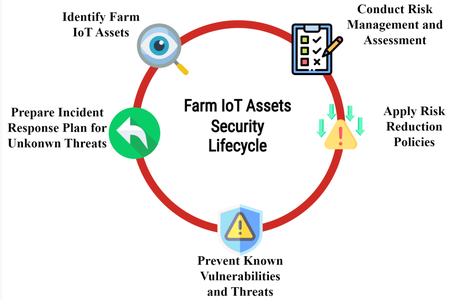

Figure 5: Secure IoT lifecycle

Conclusion

- This poster delves into the exciting world of precision farming, where technology empowers agricultural advancements.
- But with growth comes vulnerability, as interconnected devices and networks create pathways for cyber threats.
- The research is continued on evolving defenses against these modern-day agricultural pests, showcasing solutions like federated learning, blockchain, and zero-trust principles.

Author and Poster Design

Shree Ram Abayankar Balaji
Graduate Research Assistant,
School of Electrical Engineering and Computer Science,
shree.balaji@UND.edu

DATA, ENERGY, CYBER AND SYSTEMS
DECS
College of Engineering & Mines
University of North Dakota