SUNSHINE AGRICULTURE
e-Newsletter

ISSN (E): 2583 – 0821

Sun. Agri.:e- Newsletter, (2025) 5(9), 42-45

Article ID: 433

Cybersecurity Challenges in Digital Agricultural Extension

Manohar B. Dhadwad[1], Vishal Gulab Vairagar[2*]

[1]Assistant Professor, Department of Extension Education, MPKV Rahuri
[2]SMS Agri Extension KVK Solapur II Maharashtra

*Corresponding Author
Vishal Gulab Vairagar*

Available online at
www.sunshineagriculture.vitalbiotech.org

Article History
Received: 23.08.2025
Revised: 27.08.2025
Accepted: 1.09.2025

INTRODUCTION

The farming sector is changing in a paradigmatic way with the take-up of digital technologies. Precision farming, remote sensing, mobile tools, and data analytics are some of the tools that have transformed the way agricultural information is shared, making it possible for farmers to receive real-time information, expert opinion, and market information. Digital agricultural extension services have become a vital platform for improving productivity, sustainability, and resilience among farming communities.

But this rise in dependence on digital infrastructure has posed a new range of dangers cybersecurity threats. Farming systems are becoming more susceptible to data breaches, hacking, malware attacks, and privacy incursions. These dangers have the capability to interfere with information flows, compromise sensitive information, and erode confidence in digital platforms.

This article discusses the main cybersecurity issues of digital agricultural extension systems, their probable effects, and measures to counter these threats for guaranteeing secure, trustworthy, and efficient agricultural progress.

1. The Role of Digital Agricultural Extension

What is Digital Agricultural Extension?

Digital agricultural extension is the application of information and communication technologies (ICT) to offer farmers timely, precise, and site-specific information. Such platforms comprise mobile apps, websites, interactive voice services, decision support tools, and cloud-based advisory systems.

Source: https://www.sciencedirect.com

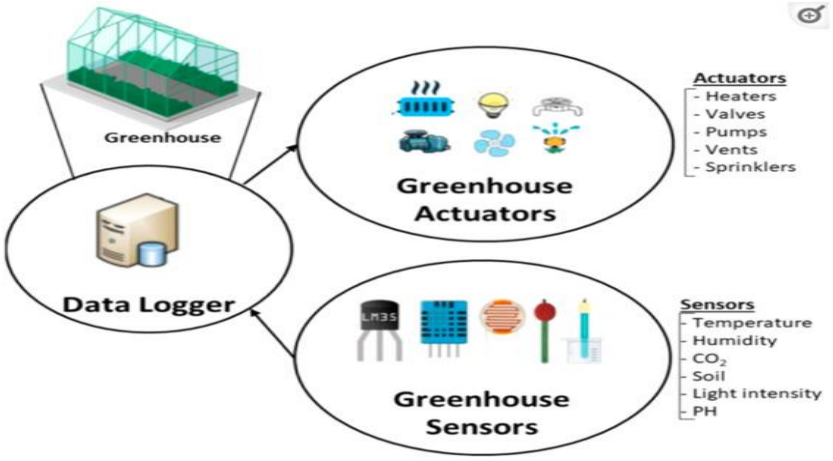
Advantages of Digital Agricultural Extension

- Improved access to information: Weather updates, pest control, soil conditions, and irrigation timetables.
- Market linkages: Timely prices and supply chain management.
- Capacity building and training: Webinars, agricultural knowledge-sharing platforms, and online tutorials.
- Sensors- and remote-data-enabled precision farming: Data-driven farming.

Why Cybersecurity Is Important

With the sector becoming digital, data flows intensify exponentially, and new actors (agri-businesses, farmers, tech providers, government bodies) share information through networks. This networked world is exposed to cyber-attacks that can interfere with operations, steal personal information, or tamper with agricultural systems.

2. Most Important Cybersecurity Challenges in Digital Agricultural Extension



Source: https://www.sciencedirect.com

1. Data Privacy and Confidentiality Risks

Digital platforms collect sensitive information such as farm location, crop patterns, financial data, and health-related records. Without proper safeguards, unauthorized access or data leaks can lead to identity theft, financial fraud, and exploitation by malicious actors.

2. Lack of Cybersecurity Awareness

Most farmers and extension personnel do not have sufficient knowledge of cybersecurity practices. This weakens them to phishing attacks, malware downloads, and social engineering schemes aimed at accessing devices and networks.

3. Poor Infrastructure and Funding

There is limited high-speed internet, stable power supply, and secure network in most rural areas. Cybersecurity systems need investment in hardware, software, and human capacity, which are usually low-priority items in agricultural budgets.

4. Third-Party Software Vulnerabilities

Online extension services are more dependent on third-party platforms and apps that are not up to cybersecurity requirements. Unsecured app vulnerabilities, plugin vulnerabilities, or operating system vulnerabilities are exploited to obtain unauthorized access.

5. Challenges to Device Security

Most farmers use smartphones or tablets with old operating systems, poor passwords, or insecure apps to access extension services. These are the soft targets for attackers planning to breach agriculture data.

6. Ransomware and Malware Threats

Ransomware infections have the capability to encrypt information, excluding farmers from important systems until a ransom is issued. In the same way, malware infections can damage files, intercept messages, and compromise network security.

7. Trust and Adoption Barriers

Cyber threats make farmers reluctant to embrace digital tools. Lack of confidence in data protection diminishes the capability of digital platforms and restricts the extension of agricultural extension services.

8. Regulatory Gaps and Policy Limitations

Most nations have inadequate holistic cyber security policies specifically for agricultural ecosystems. Inadequate standards and dispersed governance are the causes of weak data protection and incident response.

3. Consequences of Cybersecurity Incidents on Agriculture

Disruptions in Operations

Cyber attacks would interfere with farm operations through the incapacitation of irrigation systems, shutdown of advisory platforms, or corruption of data analytics tools. This would lead to loss of crops, decision-making delays, as well as added costs in production.

Financial Losses

Data breaches, identity fraud, and ransomware attacks can lead to significant financial losses for farmers and service providers. The expenses involved are data recovery, legal penalties, loss of reputation, and business disruption.

Compromised Food Security

If advisory services are hacked, incorrect suggestions regarding the application of pesticides, fertilizers, or irrigation schedules can result in low crop yields, wastage of resources, and food scarcity.

Erosion of Trust in Technology

Security breaches can generate distrust of electronic platforms, hindering uptake and innovation. Farmers might fall back on conventional practices, curtailing the impact of contemporary agricultural interventions.

4. Cybersecurity Solutions

1. Enhancing Data Protection Mechanisms

- Apply encryption protocols for data storage and data transmission.
- Apply secure authentication techniques like 2FA.
- Make privacy policies transparent and compliant with international data protection standards.

2. Farmer and Extension Worker Training Enhancement

- Conduct workshops and awareness campaigns on cyber hygiene practices.
- Offer step-by-step guides for identifying phishing emails and securing devices.
- Instruct farmers to update software from time to time and employ secure passwords.

3. Enhancing Infrastructure and Network Security

- Extend broadband internet coverage in rural areas.
- Invest in secure cloud platforms and data backup systems.
- Implement intrusion detection and prevention systems to scan network anomalies.

4. Fostering Collaboration and Policy Development

- Foster partnerships among government, private tech providers, and farmer organizations.
- Establish sector-specific cybersecurity guidelines and frameworks.
- Foster research on cybersecurity threats in agriculture and exchange best practices.

5. Establishing Trust Through Certification and Standards

- Establish cybersecurity certification programs for agricultural use and service providers.
- Promote adherence to data privacy laws and perform routine audits.
- Create grievance redressal processes for farmers impacted by cyberattacks.

6. Utilizing Emerging Technologies

- Employ blockchain for safe and traceable transactions of data.
- Utilize AI-enabled threat detection mechanisms to detect abnormal patterns.
- Investigate decentralized networks to minimize dependency on single points of failure.

5. Case Studies and Global Perspectives

Case Study 1 – Ransomware Attack on a Farming Cooperative

A regional farm cooperative in Europe was hit by a ransomware attack in 2022 that paralyzed its crop management system for a few days. Recovery entailed huge financial outlay and impacted supply chains in several regions.

Case Study 2 – Data Breach in Precision Farming Apps

A well-used farm tips app in Asia leaked thousands of farmers' location and personal information through poor encryption practices. The leak resulted in regulatory action and user distrust.

Global Initiatives

- FAO's Digital Agriculture Strategy prioritizes mainstreaming cybersecurity in rural extension services.
- EU's GDPR compliance has prompted technology vendors to use stringent data protection features in agriculture.
- Public-private partnerships in South America and Africa are centered on developing cybersecurity consciousness among smallholder farmers.

CONCLUSION

The agricultural future hinges on the extensive application of digital technology that lifts productivity, resilience, and sustainability. Cybersecurity threats, though, represent a major obstacle to these improvements, particularly in rural and disadvantaged areas. Cybersecurity challenges must be addressed with a systemic approach that converges technology, education, infrastructure, and policy. Equipping farmers with knowledge, tools, and resources to defend themselves against cyberattacks will build confidence in digital platforms and unlock the full potential of contemporary agricultural extension services. Cybersecurity investments are not only technical requirements—they are strategic facilitators for food security, rural development, and global economic stability. As agriculture becomes increasingly digital, data and system protection must be a top concern.

REFERENCES

Adewusi, A. O., Chiekezie, N. R., & Eyo-Udo, N. L. (2022). Securing smart agriculture: Cybersecurity challenges and solutions in IoT-driven farms. *World Journal of Advanced Research and Reviews*, *15*(03), 480-489.

Alahmadi, A. N., Rehman, S. U., Alhazmi, H. S., Glynn, D. G., Shoaib, H., & Solé, P. (2022). Cyber-security threats and side-channel attacks for digital agriculture. *Sensors*, *22*(9), 3520.

Barman, P., Nath, C., & Deka, P. (2024). Unleashing the Potential of Cyber Extension in Agriculture.

Botschner, J., Corley, C., Fraser, E. D., Kotak, R., McMahon, D., & Newman, L. (2024). Cybersecurity in Digital Agriculture: A National Security Risk?. In *(In) Security: Identifying the Invisible Disruptors of Security* (pp. 281-315). Cham: Springer Nature Switzerland.

Khatri, A., Lallawmkimi, M. C., Rana, P., Panigrahi, C. K., Minj, A., Koushal, S., & Ali, M. U. (2024). Integration of ICT in agricultural extension services: A review. *Journal of Experimental Agriculture International*, *46*(12), 394-410.