Adaptive Cybersecurity Mechanisms for Climate-Resilient Agricultural IoT Systems

Ms. Mansi Dilip Shriwastav
Department of Computer Science, IT and Animation Deogiri College, Chh. Sambhajinagar-431005

Dr. Madhavi Satish Avhankar
Department of Computer Science Indira College of Commerce and Science, Pune, India.

DOI: 10.29322/IJSRP.16.02.2026.p17038
https://dx.doi.org/10.29322/IJSRP.16.02.2026.p17038

Paper Received Date: 9th January 2026
Paper Acceptance Date: 8th February 2026
Paper Publication Date: 12th February 2026

Abstract

The increasing deployment of Agricultural Internet of Things (Ag-IoT) systems is transforming food production and enabling climate-resilient farming practices. However, the growing reliance on interconnected sensing, automation, and cloud platforms significantly expands the attack surface, exposing agricultural operations to cyber threats that can disrupt critical processes, compromise data integrity, and undermine food security. This paper explores adaptive cybersecurity mechanisms designed to enhance the resilience of Ag-IoT ecosystems operating under climate-induced environmental and network constraints. The proposed approach integrates context-aware access control, federated threat learning, zero-trust architectures, and distributed ledger technologies to secure dataflows, device interactions, and supply-chain processes.

Experimental evaluations and simulated farm scenarios demonstrate improved attack detection, operational continuity, and system reliability during extreme weather events and adversarial conditions. The results suggest that adaptive cybersecurity strategies are essential for protecting next-generation digital agriculture and ensuring resilient, secure, and sustainable food systems in an era of accelerating climate variability.

Keywords:- Smart Agriculture, IoT, Ag-IoT, Cyber-attack, Adpative agro, Precision Farming,

1. Introduction

Climate change introduces major uncertainty to crop yield, resource management, and global food systems. Ag-IoT systems have emerged as key enablers of climate-resilient agriculture by enabling real-time monitoring of soil, weather, irrigation, and pest dynamics. Yet the digitalization of agriculture dramatically expands cybersecurity risk.

Modern Ag-IoT landscapes involve heterogeneous sensors, autonomous machinery, gateways, low-power wireless networks, cloud decision engines, and integration with supply-chain systems. Cyber intrusions may alter sensor readings, disrupt irrigation control, cause inventory fraud, or compromise safety-critical operations. Climate-driven network instability and extreme weather further exacerbate risk by degrading communication links and power availability, creating conditions where traditional fixed security policies are insufficient.

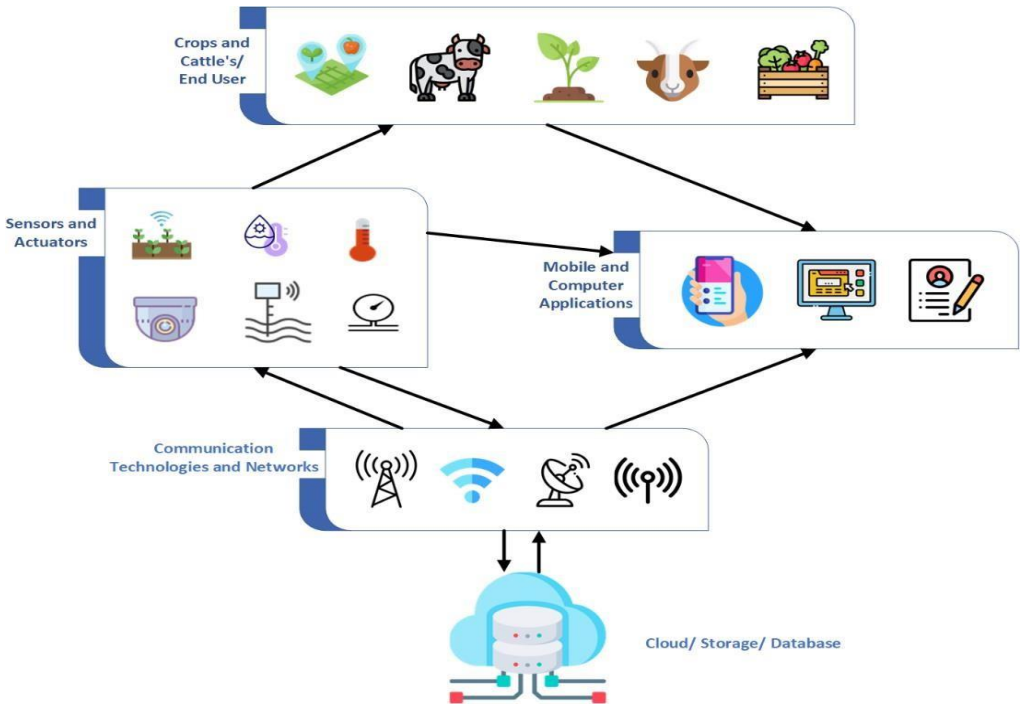

Fig:- Multilevel Diagram for smart agriculture[1]

Climate change poses significant challenges to agriculture, affecting crop yields, water availability, and overall food security. Traditional farming methods often fall short in adapting to these changes. However, the integration of Internet of Things (IoT) sensors into farming practices offers a promising solution. By enabling real-time monitoring and data- driven decision-making, IoT sensors facilitate the development of climate-resilient farming solutions. Smart agriculture refers to the use of advanced technologies, including IoT sensors, data analytics, and automation, to enhance farming practices. These technologies enable farmers to monitor and manage their crops and livestock more efficiently, leading to increased productivity and sustainability. IoT sensors play a crucial role in building climate-resilient farming solutions by providing accurate and timely data that helps farmers adapt to changing climatic conditions. A security mechanism is a method or technology that protects data and systems from unauthorized access, attacks, and other threats. Adaptive cybersecurity in climate-resilient agriculture involves using security systems that can dynamically adjust to emerging threats while protecting the digital technologies (e.g., Internet of Things (IoT), AI, automation) that help farms adapt to climate change. The goal is to ensure the reliability and integrity of systems that manage vital functions like irrigation, climate monitoring, and crop health. Adaptive security shifts from traditional, static defenses to a dynamic approach that continuously assesses risks and adjusts protective measures in real-time.

2. Research Elaborations

The convergence of smart agriculture, climate resilience, and cybersecurity has emerged as a multidisciplinary research area. Agricultural IoT (Ag-IoT) deployments increasingly rely on sensors, drones, autonomous machinery, digital platforms, and machine learning. Early research on agricultural IoT focused on enabling connectivity, sensing, and low- power mesh networking. Studies on precision irrigation, soil monitoring, and livestock tracking demonstrated efficiency gains, yet cybersecurity was largely neglected at the system design stage. Climate-resilient IoT research focuses on maintaining operational performance during environmental stress.

There are many characteristics in the proposed and existing use cases of IoT devices that make it critical to ensure their cybersecurity. These characteristics include IoT devices being part of people's homes, meaning compromised systems can be used to collect private or sensitive information, the IoT devices being critical cyber-physical systems that may cause harm in the real world and the increased power consumption of a compromised system, them being used in botnets. In order to improve the cybersecurity of IoT devices, it is paramount to understand their key characteristics and how they differ from other software systems and technologies [7].

Precision farming uses a number of technologies to maximize crop yields, including GPS systems, sensors and Big Data [9]. IoT can be interpreted as a network of intelligent, interconnected devices that are able to communicate with each other and produce relevant data about the world in which they operate [9].

3. Results or Finding

Adaptive security is defined as a security system that learns from the environment and reacts according to the situation and can handle threats with very little computation and 5. Discussion energy consumption. This security makes IoT systems more secure and reliable [1]. One of the primary cybersecurity challenges in IoT-driven farms is the lack of standardization in IoT

devices. The rapid development and deployment of various IoT devices by different manufacturers have led to a fragmented ecosystem with inconsistent security protocols [3]. Many devices lack uniform security standards, resulting in vulnerabilities that can be exploited by malicious actors. For instance, some devices may not encrypt data transmissions adequately or may use outdated encryption methods, making it easier for attackers to intercept and manipulate data [3]. The absence of standardized security measures complicates the integration of multiple devices into a cohesive and secure smart agriculture system. Weak authentication mechanisms are another significant vulnerability in IoT devices used in smart agriculture. Many IoT devices rely on default or easily guessable passwords, making them susceptible to unauthorized access. Additionally, some devices may not support multi-factor authentication (MFA), which adds an extra layer of security. Attackers can exploit these weaknesses to gain control over the devices, access sensitive data, or disrupt agricultural operations. For example, an attacker could potentially manipulate irrigation systems or livestock monitoring devices, leading to significant agricultural losses [3].

Cybersecurity Challenges in Ag-IoT

Primary threats include:

- Spoofing and tampering of sensor data :- In an IoT system (like in smart agriculture), sensors collect data such as soil moisture, temperature, humidity, etc. Spoofing and tampering are two types of cyberattacks that target this data[3]:

1. **Spoofing :-** means an attacker pretends to be a legitimate device and sends fake data to the system.
   Example:- A fake sensor sends false soil moisture readings that say the field is dry even when it isn't.
   Result:- The system may turn on irrigation unnecessarily, wasting water and energy.
2. **Tampering :-** means an attacker alters the real data while it is being transmitted or stored.
   Example: Real temperature data=30°C, Tampered data=42°C
   Result:- The farm control system may change greenhouse cooling settings incorrectly.

Distributed Denial of Service (DDoS) attacks on gateways

- Ransomware affecting farm management systems: Ransomware is a type of malicious software (malware) that locks or encrypts a computer system's files and demands payment (a ransom) to unlock them. When this type of attack targets farm management systems, it means hackers take control of digital tools that farmers use for: irrigation scheduling, crop planning and monitoring, machinery coordination (e.g., tractors, drones, sensors).
- Privacy leakage in livestock and farm analytics
- Firmware-level malware in embedded devices

Agricultural IoT Field Data

Used to simulate real climate-driven farming environments:

- soil moisture
- humidity/temperature
- irrigation parameters
- crop growth data
- meteorological/climate data

Attack Scenarios

As we are dealing with cyber security in smart farming there can be some attacks means Cyber Attack in IoT systems.In cyber security, you must define what your system is defending.

For agricultural IoT, realistic attack scenarios include:

Network-Layer Attacks

- DoS / DDoS on irrigation controllers
- Routing attacks on LoRaWAN, 5G, or satellite links
- Packet injection or replay attacks

Application/Protocol Attacks

- data tampering (e.g., altering soil moisture data)
- command spoofing (e.g., false irrigation commands)
- man-in-the-middle attacks

Device-Level Attacks

- sensor firmware manipulation
- botnet infections on edge nodes
- unauthorized actuator control

Traditional Machine Learning Algorithms

Traditional Machine Learning Algorithms which can be used in Adaptive Cybersecurity Mechanisms are:

- Classification Algorithm

- Clustering Algorithm
- Regression Algorithm

Cybersecurity Threats in Agriculture

As agriculture becomes increasingly digitized, it faces a growing array of cybersecurity threats that can disrupt operations, compromise data integrity, and jeopardize food security [4].

Malware and Ransomware

Malware and ransomware attacks are some of the most devastating cyber threats to smart farming systems. These attacks can encrypt essential data or lock farmers out of critical systems until a ransom is paid. The ransomware attack on New Cooperative in 2021 demonstrated how such incidents could paralyze agricultural operations, affecting grain distribution and raising fears of food shortages.

Broader impacts of ransomware:

- Operational shutdowns: Ransomware attacks often target peak operational periods, maximizing their disruptive potential.
- Financial losses: Beyond ransom payments, farms incur costs from downtime, system restoration, and potential reputational damage.

4. Conclusions

This study proposes an evaluation framework applied to IoT-based smart agriculture. Agricultural IoT environments operate under unique constraints, including harsh environmental conditions, power limitations, intermittent connectivity, and heterogeneous hardware ecosystems. These challenges necessitate cybersecurity solutions that are not only robust but inherently adaptive to changing climatic and operational contexts.

Adaptive cybersecurity mechanisms — such as context-aware policy reconfiguration, zero- trust architectures, federated threat learning, and blockchain-based data integrity — provide a promising pathway for safeguarding Ag-IoT infrastructures against evolving threats. By dynamically adjusting security strategies to real-time environmental signals and threat intelligence, these mechanisms enhance operational continuity, improve data reliability, and strengthen supply-chain trust during climate-induced disruptions.

Although the implementation of such adaptive systems introduces complexity and higher computational overhead, the long-term benefits outweigh the costs, particularly as climate volatility increases. Future research should focus on scalable governance models for shared threat intelligence, resilient communication architectures tailored for rural deployments, and secure hardware-software co-design for field devices. Overall, adaptive cybersecurity represents a critical enabler for ensuring that digital agriculture remains both productive and secure in the face of accelerating climate challenges.

References

1. Riaz, A. R., Gilani, S. M. M., Naseer, S., Alshmrany, S., Shafiq, M., & Choi, J. G. (2022). Applying adaptive security techniques for risk analysis of internet of things (IoT)-based smart agriculture. Sustainability, 14(17), 10964.
2. Chui, K. T., Gupta, B. B., Liu, J., Arya, V., Nedjah, N., Almomani, A., & Chaurasia, P. (2023). A survey of internet of things and cyber-physical systems: Standards, algorithms, applications, security, challenges, and future directions. Information, 14(7), 388.
3. 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.
4. Singh, I. P., Ahmad, M. M., & Sani, B. S. CYBERSECURITY IN AGRICULTURE: SAFEGUARDING SMART FARMS.
5. Carvalho, N., Adão, T., Morais, R., Costa, A. R., & Peres, E. (2025). Cybersecurity in Precision Agriculture: a short review and a practical status assessment over mySense IoT- based platform. Procedia Computer Science, 256, 255-266.
6. Balaji, S. R. A., Rao, S. P., & Ranganathan, P. (2023, October). Cybersecurity challenges and solutions in IoT-based precision farming systems. In 2023 IEEE 14th Annual Ubiquitous Computing, Electronics & Mobile Communication Conference (UEMCON) (pp. 237-246). IEEE.
7. Rauti, S., & Laato, S. (2024). Enhancing resilience in IoT cybersecurity: the roles of obfuscation and diversification techniques for improving the multilayered cybersecurity of IoT systems. Data & Policy, 6, e74.
8. Kumar, L., Ahlawat, P., Rajput, P., Navsare, R. I., & Singh, P. K. (2021). Internet of things (IOT) for smart precision farming and agricultural systems productivity: A review. IJEAST, 5, 141-146.
9. Karthiyayini, J., Jain, A., Prasad, K. S., Abedi, T. A. A. U., Prasanna, Y., & Murugesan, K. (2025, February). Flood Prediction and Adaptive Farming Solutions Using IoT, Machine Learning, and Remote Sensing for Climate-Resilient Agriculture. In 2025 International Conference on Intelligent Control, Computing and Communications (IC3) (pp. 777-782). IEEE.