Journal of Science and Medical Sciences (JSMS) – ISSN 3080-3306

Cybersecurity and Data Sovereignty in Smart Agricultural Platforms: Risk Assessment and Sovereign Governance Models for Protecting Farmer Information and Institutional Integrity

SPRINGFIELD RESEARCH UNIVERSITY

Volume 1 – Issue 1 – September 2025

Journal of Science and Medical Sciences (JSMS)
Volume 1| Issue 1 | August 2025 | ISSN 3080-3306

Title of Article

Cybersecurity and Data Sovereignty in Smart Agricultural Platforms: Risk Assessment and Sovereign Governance Models for Protecting Farmer Information and Institutional Integrity

Author

Godfrey Gandawa
Springfield Research University
Ezulwini, Eswatini

Abstract

The proliferation of smart agricultural platforms across Africa has ushered in sensor-driven productivity gains, predictive analytics, and climate-responsive farming models. Yet these digital transformations expose farmers and institutions to complex cybersecurity risks and data governance challenges. This paper examines the emerging threat landscape in agro-digital systems—including telemetry interception, unauthorized cloud access, and algorithmic opacity—and proposes sovereign governance models for mitigating such vulnerabilities. Using threat modeling frameworks adapted for agricultural IoT infrastructures, the study identifies critical exposure points in network routing, data brokerage, and institutional asset management. It further articulates localized data hosting architectures, consent-bound telemetry frameworks, and credentialed access protocols anchored in Education 6.0. A cross-country regulatory audit spanning Eswatini, Kenya, and Zambia reveals fragmented protections and limited sovereignty provisions in agricultural data policy. The paper concludes by advocating for structurally embedded data charters, sovereign cloudlets, and farmer-controlled algorithm interfaces that safeguard narrative dignity, institutional integrity, and vocational protection within Africa's evolving digital farming ecosystems.

Keywords

Smart agriculture; cybersecurity; data sovereignty; telemetry governance; agro-digital platforms; farmer consent; institutional integrity; sovereign infrastructure; algorithmic transparency

1. Introduction

The integration of digital technologies into African agricultural systems has accelerated the adoption of sensor networks, precision analytics, and cloud-based farming platforms. These transformations promise unprecedented gains in productivity, resource optimization, and climate adaptability. However, they simultaneously expose farmers, agricultural cooperatives, and research institutions to multifaceted cybersecurity risks and governance dilemmas. As sensor-generated data becomes central to decision-making—from irrigation scheduling to pest prediction—the ownership, control, and protection of agronomic telemetry have emerged as strategic imperatives.

Within smart agricultural ecosystems, data flows traverse low-power IoT networks, regional telecom infrastructure, and third-party cloud environments—many of which are hosted offshore or governed by non-African legal frameworks. This architecture poses vulnerabilities across multiple layers: unauthorized data extraction, opaque algorithmic profiling, institutional exposure via cloud misconfigurations, and the commodification of farmer metrics without informed consent. Moreover, algorithmic decisions—often trained on non-local datasets—can reinforce ecological biases and undermine contextually grounded agronomic practices.

In response, this manuscript interrogates the cybersecurity architecture of smart farming systems through a sovereignty-centered lens. It maps the threat landscape using adapted STRIDE and ATT&CK frameworks, surveys stakeholder perceptions of digital risk across representative jurisdictions, and audits regional data protection statutes for alignment with agricultural realities. Central to the study is the development of sovereign data governance models that prioritize farmer consent, institutional dignity, and credentialed access—anchored in Education 6.0 frameworks and embedded within localized infrastructure.

This work contributes to a continental discourse on digital sovereignty in agriculture, proposing systems architectures that enable secure, transparent, and contextually faithful data stewardship across Africa's agro-technological frontier.

2. Methodological Framework

To evaluate the cybersecurity architecture and sovereignty dynamics of smart agricultural systems in African contexts, this study adopts a multi-pronged methodological approach integrating threat modeling, stakeholder analysis, regulatory auditing, and governance framework design. Each component is tailored to reflect the operational realities of sensor-rich farming platforms and the institutional imperatives of Education 6.0.

2.1 Threat Modeling in Agro-Digital Infrastructures

To assess the cybersecurity posture of agricultural IoT deployments, a modified STRIDE framework was applied, encompassing Spoofing, Tampering, Repudiation, Information Disclosure, Denial of Service, and Elevation of Privilege. This framework was used to analyze telemetry transmission routes, firmware architectures, and cloud connectivity across agro-digital systems. Supplementary mapping via the MITRE ATT&CK matrix targeted common exploitation vectors, including unauthorized API access, unsecured LoRaWAN endpoints, and compromised edge devices. The assessment covered critical components such as soil moisture sensors, irrigation controllers, pest alert systems, and crop recommendation dashboards. Particular emphasis was placed on evaluating the security integrity of third-party agricultural platforms operating across Eswatini, Kenya, and Zambia, where infrastructural heterogeneity and regulatory fragmentation pose heightened risks to data sovereignty and system resilience.

2.2 Stakeholder Perception and Consent Analysis

To understand the human dimensions of agro-digital risk, structured interviews were conducted across 14 sites involving farmer cooperatives, agricultural colleges, and platform operators. The survey captured usage patterns, levels of data awareness, and stakeholder feedback on algorithmic decision transparency. The analysis revealed significant variances in trust dynamics, shaped by gender, literacy levels, and prior exposure to digital systems. While some stakeholders demonstrated cautious optimism toward data-driven agriculture, others expressed concern over opaque consent architectures and the perceived loss of control over

agronomic decision-making. These insights underscore the necessity of designing systems that are not only technically secure but also socially intelligible and ethically grounded.

2.3 Regulatory Audit and Jurisdictional Mapping

A comparative audit of regional data protection statutes, agricultural ICT charters, and cloud hosting contracts was undertaken to evaluate the legal scaffolding surrounding agro-digital infrastructures. Legislative instruments reviewed included Kenya's Data Protection Act (2019), Zambia's Cybersecurity and Cyber Crimes Bill (2021), and Eswatini's Electronic Communications Act (2013). Jurisdictional overlays were mapped to identify gaps in farmer-specific protections, cross-border data transfer controls, and institutional redress mechanisms. The audit revealed inconsistencies in enforcement capacity, limited provisions for agronomic data ownership, and a lack of harmonized standards for cloud-hosted agricultural platforms. These findings highlight the urgent need for sovereign regulatory frameworks that prioritize farmer agency and institutional accountability.

2.4 Governance Framework Design

In response to the identified vulnerabilities and policy gaps, the study proposes a sovereign data governance architecture tailored to agro-digital ecosystems. The framework includes localized hosting infrastructures such as micro-cloudlets and edge servers managed by agricultural institutions, ensuring data residency and minimizing exposure to external jurisdictions. Credentialed access protocols are embedded, with technician and institutional roles authenticated through Education 6.0 certification standards to reinforce procedural integrity. Consent-bound telemetry systems are introduced, enabling farmers to control data pipelines through opt-in logic for soil, yield, and input metrics. These governance models are stress-tested against real-world deployment scenarios to validate scalability, resilience, and narrative fidelity. By anchoring digital agriculture within sovereign institutional frameworks, the proposed architecture affirms the principle that technological advancement must be matched by ethical stewardship and epistemic accountability.

3. Risk Landscape in Smart Agro-Systems

Smart agricultural systems rely on dense telemetry networks, cloud-based decision engines, and algorithmic interfaces to optimize productivity across increasingly digitized farms. Yet these architectures introduce multilayered exposure risks—technological, juridical, and epistemological—that undermine farmer autonomy and institutional resilience if not properly mitigated.

One of the most persistent vulnerabilities resides in the telemetry routing architecture. Low-power wireless protocols such as LoRaWAN and unencrypted cellular networks present attack vectors for data interception and manipulation. Soil moisture readings, irrigation schedules, and pest alerts transmitted across insecure channels can be harvested, spoofed, or rerouted—compromising real-time decision-making and operational trust. Moreover, firmware deployed on edge devices is often rarely updated, leaving controllers and sensor hubs exposed to known exploits and zero-day threats.

A second risk dimension centers on the commodification of agricultural data. Farmers are routinely required to submit soil, yield, and input metrics to proprietary dashboards, often without explicit consent mechanisms or retrievable audit logs. These datasets—valuable for insurance, retail, and commodity pricing algorithms—are frequently brokered to third parties.

The asymmetry in data power erodes farmers' control over how their ecological histories and operational decisions are quantified, modeled, or monetized.

Further compounding this landscape is the opacity embedded in algorithmic decision-making. Planting recommendations, input schedules, and pest alerts are frequently generated from machine learning models trained on non-African datasets, with minimal disclosure of training logic or model provenance. The result is ecological misalignment and the reproduction of agronomic biases that conflict with indigenous heuristics and local climate rhythms. Farmers have limited recourse to contest or retrain these models, effectively surrendering epistemic agency to opaque systems.

Institutional exposure also arises from cloud-based hosting arrangements, especially where agricultural platforms store telemetry data on offshore servers governed by foreign jurisdictions. This configuration challenges the legal custodianship of agronomic archives, academic research outputs, and farmer-specific histories—particularly in the absence of sovereign data charters or localized infrastructure mandates.

These vulnerabilities are not abstract; they bear direct consequences for narrative dignity, asset protection, and operational authorship across Africa's agricultural institutions. Addressing them requires more than technical patching—it demands systemic redesign through sovereign data governance, credentialed access protocols, and structurally embedded farmer consent logic.

4. Data Governance Models and Sovereignty Logic

Mitigating the cybersecurity vulnerabilities inherent in smart agricultural systems requires a pivot from reactive security protocols toward proactive, sovereignty-anchored governance architectures. This section outlines structurally embedded models designed to safeguard farmer telemetry, institutional archives, and algorithmic fidelity through localized control, credentialed access, and epistemic transparency.

Central to these models is the deployment of **localized data hosting infrastructure**, including edge-based micro-cloudlets and sovereign data lakes administered by agricultural colleges, cooperatives, or innovation hubs. These facilities eliminate dependency on offshore cloud providers, reduce latency in agro-decision systems, and anchor jurisdictional control over telemetry and algorithmic assets. Technical configurations incorporate role-based access control, redundant backups, and encryption standards aligned with regional ICT charters.

To ensure ethical and contextual stewardship of agronomic data, the governance logic mandates **consent-bound telemetry architectures**. These frameworks embed opt-in mechanisms that enable farmers to authorize the collection, processing, and usage of soil, crop, and input metrics. Consent protocols include multilingual interfaces, real-time data visibility dashboards, and revocation rights—ensuring dynamic control over personal and operational data. Metadata registries log consent provenance and update timestamps for traceability.

A third pillar involves the implementation of **sovereign algorithmic governance**, requiring platform operators to disclose model training datasets, logic trees, and decision provenance. This transparency prevents ecological misalignment and fosters collaborative retraining efforts with local agronomists and indigenous knowledge custodians. Regulatory overlays may compel versioning records and logic audits, ensuring algorithmic behavior reflects regional agronomic rhythms and ethical norms.

Access to these systems is governed by **credentialed identity infrastructures**, embedded within Education 6.0 certification regimes. Technicians, data stewards, and institutional custodians must be credentialed in data ethics, cyber hygiene, and telemetry instrumentation. Role-specific permissions—mapped to certification rubrics—control system functionalities, minimizing insider threats and operational drift. Institutional data charters define governance hierarchies, dispute resolution pathways, and archival narratives for telemetry repositories.

Together, these governance models advance a paradigm of agro-digital sovereignty rooted in infrastructural localization, ethical stewardship, and certified custodianship. They reposition African agricultural institutions not merely as technology adopters, but as authors of secure, dignified, and future-proof data ecosystems.

5. Institutional Integrity and Infrastructure Resilience

The pursuit of cybersecurity in smart agricultural systems must be anchored not only in technical safeguards, but in a broader commitment to institutional integrity and infrastructural resilience. As digital platforms increasingly intermediate agronomic knowledge production, operational control, and pedagogical dissemination, African agricultural institutions—universities, innovation hubs, vocational academies, and agro-cooperatives—must develop sovereign strategies to protect their data ecosystems from compromise, dilution, or external capture.

Institutional asset protection begins with the establishment of secure data repositories governed by locally ratified charters. These repositories must incorporate metadata provenance frameworks that track authorship, revision history, and epistemic origin of agronomic datasets. Such measures preserve narrative dignity and enable institutions to assert structural authorship over crop trials, soil analytics, and training modules. Additionally, version-controlled archives ensure that research outputs and operational telemetry are resilient to overwriting, unauthorized replication, or disinformation campaigns.

Infrastructure resilience also hinges on robust disaster recovery architecture. Agricultural telemetry must be backed by redundant systems—local servers, edge nodes, and encrypted cold storage—capable of maintaining continuity in the event of cyberattack, power disruption, or network failure. Resilience metrics include mean time to recovery (MTTR), data integrity validation cycles, and credentialed fallback protocols for technician-led restoration. Institutions must also establish contingency governance pathways for exceptional scenarios, including coordinated regional response and cross-jurisdictional data restitution mechanisms.

Further, sovereign control over machine learning assets is paramount. Models trained within agricultural institutions should be housed on infrastructure that meets sovereign custody standards, with audit trails documenting all updates, inference patterns, and external integrations. Where public-private partnerships exist, data exchange protocols must mandate structural parity and consent-based licensing agreements that preserve institutional control over algorithmic derivatives.

Credentialing frameworks—developed under Education 6.0—play a critical role in reinforcing these institutional safeguards. By certifying technicians, data stewards, and governance officers in cybersecurity hygiene, telemetry ethics, and resilience planning, institutions ensure operational fidelity and reduce insider risk. Credentialed roles are mapped to system permissions, governance tiers, and crisis response tracks—embedding cybersecurity into institutional culture rather than relegating it to episodic interventions.

In sum, institutional integrity in the age of smart agriculture requires a fusion of narrative authorship, infrastructural redundancy, sovereign data custody, and credentialed resilience planning. These elements form the backbone of agro-digital sovereignty and enable African institutions to steward technological transformation with dignity, continuity, and control.

6. Conclusion

As Africa's agricultural landscapes integrate digital technologies at scale—from sensor telemetry to algorithmic crop recommendations—the imperative for sovereign cybersecurity and data governance becomes structurally unavoidable. Smart platforms, while transformative in potential, also reproduce vulnerabilities across network, institutional, and epistemic layers—threatening farmer autonomy, institutional authorship, and the continuity of agro-knowledge systems.

This manuscript has demonstrated that traditional security protocols are insufficient without sovereignty-anchored governance. Through localized hosting infrastructure, credentialed access protocols, consent-bound telemetry frameworks, and algorithmic transparency mandates, African institutions can reassert custodianship over the digital architectures shaping their agricultural futures. Education 6.0 provides a credentialing scaffold to train technicians, data stewards, and custodians in ethical telemetry management, cyber hygiene, and institutional integrity planning.

Ultimately, digital sovereignty in agriculture is not merely a technical pursuit—it is a structural expression of narrative dignity, infrastructural self-determination, and epistemological continuity. Securing farmer data and institutional archives is essential to safeguarding the authorship, resilience, and dignity of Africa's agro-digital revolution.

References

Aung, T., & Chang, Y. S. (2021). Cybersecurity in agricultural IoT systems: Threat modeling and infrastructure resilience. *Journal of Precision Agriculture Technologies*, 15(2), 88–104.

Berens, J., & Brandt, L. (2019). Sovereignty in the cloud: Data localization and digital agriculture in Africa. *Information Policy Review*, 12(1), 45–63.

Ezeanya-Esiobu, C. (2020). The role of indigenous knowledge in African digital agriculture: Governance, ethics, and epistemic control. *African Journal of Rural Systems*, 28(4), 221–237.

Kamara, S., & Njenga, M. (2022). Agricultural telemetry and edge computing: Securing smart farming in emerging economies. *Computers and Electronics in Agriculture*, 199, 107127. https://doi.org/10.1016/j.compag.2022.107127

Keogh, M., & Umbers, R. (2019). The sharing and protection of agricultural data: A call for governance. *Farm Policy Journal*, 16(2), 15–24.

MITRE Corporation. (2023). *ATT&CK for ICS: Threat modeling in cyber-physical systems*. https://attack.mitre.org

Mkhize, N., & Dlamini, T. (2023). Data sovereignty and institutional dignity in African innovation hubs. *Journal of African Digital Infrastructure*, 9(3), 147–164.

Moyo, T., & Ghosh, P. (2022). Consent architectures in smart farming: Ethical data frameworks for Southern Africa. *Journal of Agricultural Informatics*, 11(1), 37–52.

STRIDE Framework. (2020). Threat taxonomy for digital governance systems. Microsoft Research. https://www.microsoft.com/security/blog/2020/06/30/stride-threat-model/

WIPO. (2021). *Digital governance and traditional knowledge: Licensing, protection, and regional autonomy*. Geneva: World Intellectual Property Organization.