Journal of
Network Security
https://journals.stmjournals.com/jons

ISSN: 2395-6739 (Online)
ISSN: 2321-8517 (Print)
Volume 14, Issue 1, 2026
January–April
DOI (Journal): 10.37591/JoNS

Review JoNS

Digital Agriculture Schemes in Kerala: Risk Analysis and Multi-Layered Security Framework

Sreekala K.M.[1,*], Thara Chakkingal[2]

Abstract

Kerala's agricultural sector is undergoing rapid digital transformation, driven by initiatives such as the e-Krishi platform and the growing adoption of Internet of Things (IoT)–enabled precision farming technologies. While these developments promise improved productivity, transparency, and data-driven decision-making, they also introduce significant cybersecurity and data governance challenges that cannot be overlooked. This paper critically examines the emerging security, privacy, and operational risks associated with the digitization of agricultural services in Kerala. Attention is given to the vulnerability of data integrity, the risks arising from low levels of digital literacy among farmers, and the often-underestimated threat of insider misuse within digital systems. Through a structured assessment, the study systematically identifies and ranks key security and operational threats that could undermine the reliability and trustworthiness of digital agriculture platforms. If dynamic agricultural data remains inadequately protected, or if farmers lack meaningful control over how their data is collected, shared, and used, the long-term growth of the sector may be compromised, and public trust significantly eroded. To address these concerns, the paper proposes a novel multi-layered security and data governance framework (M-LSF) tailored for resource-constrained environments. The framework integrates a strong policy foundation centered on farmer data sovereignty with practical, cost-effective technological safeguards. These include lightweight cryptographic mechanisms, role-based access controls, and artificial intelligence (AI)/machine learning (ML) driven anomaly detection to identify suspicious activities in real time. By combining governance principles with advanced yet scalable security controls, the M-LSF aims to safeguard farmer privacy, protect sensitive agricultural data, and strengthen institutional resilience, thereby enabling Kerala to pursue sustainable and trustworthy digital agriculture.

Keywords: Cybersecurity in AgTech, data governance, digital agriculture, farmer data sovereignty, IoT security, risk management

INTRODUCTION

The adoption of Agriculture 4.0, or smart farming, is driven by the worldwide requirement to boost food production to meet a growing world population, which calls for a fundamental change toward efficiency [1]. IoT, AI, and sensor technologies have been used in this technological revolution to maximize resource usage and boost productivity [2]. Kerala's strategy for this change started in 2006 with the e-Krishi project, which created an online platform that helped more than 10,000 small farmers by offering agricultural information and enabling online transactions, effectively resulting in better crop quality and reasonable prices [3]. IoT-driven operations for tasks such as soil testing and automated irrigation are part of the current state projects that have moved into high-tech farming [3].

***Author for Correspondence**
Sreekala K M
E-mail: kmsreekala@gmail.com

[1]Assistant Professor, Department of Management, Padmashree Institute of Management and Sciences, Bangalore, Karnataka, India
[2]Assistant Professor, Department of Management, Thakur Institute of Management Studies, Career Development and Research, Mumbai, Maharashtra, India

Received Date: December 22, 2025
Accepted Date: January 07, 2026
Published Date: February 20, 2026

Citation: Sreekala K M., Thara Chakkingal. Digital Agriculture Schemes in Kerala: Risk Analysis and Multi-Layered Security Framework. Journal of Network Security. 2026; 14(1): 23–30p.

Problem Statement and Research Gap

Although digital treatments have several advantages, such as improved monitoring and risk reduction [4], their general adoption rate in India's agricultural industry is still delayed because of intricate structural problems [5]. Agricultural data are extremely susceptible to cyber threats because of the increasing reliance on dynamic data streams from linked IoT devices in the field [6], endangering data integrity and overall system reliability. Because current research frequently offers generic AgTech security analyses, addressing this issue is crucial [7]. For regional e-governance systems such as e-Krishi, which must deal with highly localized sociotechnical concerns, including particular digital divides and possible integration challenges from legacy systems, a focused security and data governance architecture is necessary [8, 9].

Contribution and Report Structure

To fill the research gap, this report:

1. Identifies and ranks operational and cyber risks in Kerala's digital agriculture programs [10, 11].
2. The multi-layered security and data governance framework (M-LSF) deliberately blends institutional data governance approaches created for situations with limited resources and advanced technical protections [12].
3. Providing practical policy suggestions to ensure long-term system resilience and institutionalized farmer data sovereignty.

DIGITAL AGRICULTURE CHALLENGES AND OPERATIONAL RISK IN KERALA

Operational risks, which frequently serve as antecedents to or multipliers of technical cybersecurity vulnerabilities, are essential for the uptake and functionality of digital farm systems.

Adoption Challenges and Digital Complexity

The difficulty of gathering and combining data from various crops, temperature zones, and soil conditions under a single digital canopy complicates the implementation of digital agriculture solutions throughout India [5, 13]. Decision makers must develop effective ways to overcome intrinsic obstacles, including farmers' aversion to change and ignorance of the advantages of IoT technologies [14, 15]. The implementation process is made more difficult when underlying economic problems, including high farming expenses or low earnings, are not addressed [5].

Digital Divide and Human Factors

One major challenge in India is the poor digital literacy at the local level [6]. In Kerala, poor motivation and barriers to technology access diminish the self-assurance and independence of certain groups, including rural female farmers, when it comes to digital adoption [16]. This low literacy rate jeopardizes the foundation of sustainable development that these technologies are supposed to support [16]. This puts impoverished farmers at risk of financial exclusion [5].

An important cybersecurity risk multiplier is the low level of digital literacy. End users who lack the necessary skills to manage secure credentials or recognize phishing efforts have become the main attack vectors, making them more vulnerable to social engineering and enabling data loss [17]. Because Agriculture 5.0 systems require more human–machine interaction, this increasing human susceptibility is particularly pertinent [17]. As a result, researchers in the agricultural sector need to focus on rethinking tactics that are especially intended to raise farmers' levels of digital literacy [6].

The Vulnerability of Centralization and Scale

For effective management, the structural design of the e-Krishi project created a centralized, coordinated organizational structure from the state to the village level. Although historically beneficial, adding contemporary distributed IoT and cloud designs to this system increases the systemic risk. A single point of failure (SPOF) for the private information of more than 10,000 registered farmers is created by a breach at the cloud computing interface or central state-level node [18].

Adopting decentralized architectural controls, such as the honeycomb design (distributed storage and decentralized control), is necessary to offset the significant impact of any central breach owing to its intrinsic structural vulnerability. Insider threats from administrators, contractors, or e-Krishi employees also pose a continuous danger of data theft or sabotage due to the human–machine interactions involved [17].

CYBER RISK ANALYSIS AND THREAT PRIORITIZATION

Because of the complexity and difficult agricultural environment, digital agricultural systems are built on a multi-layered IoT architecture [19]. where weaknesses can be exploited unexpectedly [20].

Integrity and Trustworthiness—The Highest Priority

Data integrity is the highest priority security requirement because it is crucial for optimizing agricultural methods and informing policies [3].

Data Integrity Vulnerability

Changing dynamic sensor data, such as inputs of pH, humidity, or fertilizer solutions, might result in inaccurate automated judgments and seriously harm operations and crops [21]. The sector's total growth, financial viability, and sustainability may be impacted by a single fabricated data item, leading to incorrect conclusions [3]. To protect policy judgments, the framework must guarantee the security and integrity of data.

Trust Erosion and Resilience

Without mechanisms to ensure the transparency and integrity of crop environment data, distrust in data management persists, impeding the digital transformation process [22]. Therefore, the framework must prioritize solutions that ensure data resilience and non-repudiation, utilizing distributed storage and decentralized control (honeycomb architecture) alongside immutable ledgers, such as blockchain, which enhances trust by providing a tamper-proof record [22].

Systemic Threats Across Architecture Layers

Threats are distributed across the system's architecture:

Perception Layer Threats

The inherent limitations of resource-constrained IoT devices make the implementation of robust encryption challenging [4]. Attacks at this layer often target physical devices in the field or aim to spoof sensor readings, compromising the system functionality [20].

Network and Cloud Threats

The transfer of vast agricultural data to cloud storage exposes systems to various network threats, including specific HTTP attacks targeting cloud computing interfaces [18]. Availability risks such as denial of service (DoS) attacks on network gateways can disrupt real-time operations, affect supply chains, and drain device batteries [23].

Privacy and Big Data Challenges

Smart farming generates big data (characterized by volume, velocity, and variety), heightening concerns regarding the privacy of farmers and the potential unauthorized correlation of sensitive personal and land records [24, 25]. Data security, privacy, and storage are recognized bottlenecks that must be addressed using technical and governance solutions [6].

Risk Prioritization

Based on the potential impact and likelihood in the Kerala context (Table 1), risks were prioritized as follows:

MULTI-LAYERED SECURITY FRAMEWORK (M-LSF)

The M-LSF is designed as an integrated defense mechanism covering all architectural layers, addressing high-priority risks, and tailored specifically to the resource limitations of AgTech environments. Architecture employs a customized decentralized model that leverages edge devices (gateways) for processing and policy enforcement, thus mitigating the SPOF inherent in centralized e-governance systems [26].

Technical Layer Architecture and Deployment

The layered integration of security components depicts the deployment of lightweight cryptography at the perception layer, hybrid IDS/Policy Enforcement at the network/edge gateway, and blockchain/distributed ledger technology, along with honeycomb architecture at the application/cloud layer for data provenance and resilience [3].

Layer-Specific Technical Controls

Effective defense relies on the precise application of technical controls that are appropriate for each layer's constraints (Table 2).

Table 1. Prioritized security and operational risks in Kerala's digital agriculture.

Risk category	Specific threat/vulnerability	Consequence/impact	Priority level
Data integrity compromise	Sensor data manipulation/spoofing (IoT layer) leading to incorrect inputs (e.g., fertilizer, water)	Misinformed decisions, crop loss, resource wastage, regulatory failure, and loss of production efficiency [3].	High
Operational and trust	Digital divide and low digital literacy among end users/staff	System inaccessibility, exclusion of vulnerable groups, and increased human factor cyber vulnerability [6].	High
Data privacy (sovereignty)	Unauthorized data access, leakage, and correlation of farmer demographic/financial data by agribusinesses	Farmer exploitation, loss of data control, and market manipulation [27].	High
Insider threat	Compromise by administrative users, service providers, or central committee staff	Widespread data theft, intellectual property (IP) leakage, and system sabotage [17].	Medium
System availability	Distributed denial of service (DDoS) on network gateways or cloud interfaces	Halt of automated decision-making and remote operations, supply chain disruption [23].	Medium

Table 2. M-LSF technical controls mapped to IoT architecture layers.

IoT layer	Security requirement	Proposed technical control	Significance
Perception (devices)	Confidentiality, authentication, and low energy	Lightweight cryptography (e.g., LEA, EPCBC, Zorro) or group cellular automata (GCA)	Addresses the limitation of deploying robust encryption on energy-constrained IoT devices [12].
Network/edge (gateway)	Real-time anomaly/intrusion detection and policy enforcement	Hybrid ID utilizing BiGRU–LSTM/GRU/deep learning	Provides high detection accuracy (e.g., 97.5%) [11] for anomalies and HTTP threats [28] by analyzing sequential data at the edge, reducing critical latency [29].
Application/ cloud	Data integrity, resilience, and non-repudiation	Honeycomb architecture (distributed storage) and blockchain smart contracts	Combines decentralized control to prevent single points of failure with immutable ledgers to ensure data transparency and trust [22].
Human/access	Access control and insider threat mitigation	Preventive strategies grounded in human factor analysis (e.g., function allocation, task analysis) and robust authentication	Manages diverse insider types and safeguards critical information, including intellectual property (IP) [17].

ISSN: 2395-6739 (Online), ISSN: 2321-8517 (Print)

DATA GOVERNANCE FOR FARMER SOVEREIGNTY

To sustain reliability and trust in digital interventions, a comprehensive security framework must be underpinned by institutionalized data governance that prioritizes the rights and interests of farmers. Establishing robust and equitable data governance frameworks is essential for realizing the full potential of digital agriculture [30].

Institutionalizing Farmer Data Rights

The policy foundation of the M-LSF must establish farmer data sovereignty as its core principle [30]. This principle asserts the farmers' right to control their data, ensuring that they benefit equitably from the digitalization of their practices.

AI/ML-Driven Security Mechanisms

AI and ML are essential for handling the velocity and complexity of unstructured agricultural big data 30 and for creating adaptive security policies [31].

Advanced Anomaly and Threat Detection

The framework mandates edge-based intrusion detection systems utilizing deep learning techniques [30]. Specifically, ensembles like the bi-directional gated recurrent unit–long short-term memory (BiGRU–LSTM) model have demonstrated high precision (91.67%) and accuracy (92.67%) in threat identification in IoT-based smart farming datasets [28]. Similarly, Gated Recurrent Units (GRUs) achieve detection accuracies of up to 97.5% [11]. Deploying these models at the network edge minimizes latency, allowing the system to automatically detect anomalies and enabling timely intervention to prevent crop damage [29, 32].

Adaptive Security Policies

To secure communication among resource-constrained IoT devices, the M-LSF incorporates adaptive encryption mechanisms. Using deep Q-learning algorithms, the system can dynamically select the most suitable type of encryption based on the detected risk, device energy levels, and required time latency [31]. This context-aware approach results in significant resource optimization, reducing energy and latency usage by approximately 18.7% and 26.0%, respectively, compared with fixed encryption policies [33].

Farmer-Centric Governance Models

Farmer-centric models are critical for mitigating power imbalances in data ecosystems [30]. Data Cooperatives enable farmers to pool their data, allowing them to negotiate terms of use collectively with third parties. Data Trusts provide a mechanism in which a trusted third party or trustee manages the data on behalf of the farmers (beneficiaries), ensuring strict compliance with defined governance rules and enforcing against data misuse [30]. The adoption of these models fosters confidence and shifts the information paradigm in favor of farmers [34].

Legal and Regulatory Requirements

This transition necessitates the development of clear legal frameworks that recognize farmer data rights as fundamental [27]. India must implement robust data protection and sectoral regulatory frameworks and promote the adoption of international standards [35]. These frameworks must legally mandate transparency and accountability in the agricultural data ecosystem [27]. To ensure transparency and trustworthiness in e-governance systems, the implementation of blockchain platforms is emerging as a critical solution, mirroring its application in digital health infrastructure initiatives in India [36].

Mechanisms for Trust, Enforcement, and Capacity Building

Structural governance changes are necessary to mitigate the operational risks stemming from low farmer trust [22]. By granting farmers control and transparency, adoption rates and system viability are directly enhanced [34].

Enforcement and Data Separation

The governance structure must enforce the principle of strict separation between farmers' data streams to prevent unauthorized mixing or correlation of data across different sources [37]. In a Data Trust model, an independent board ensures strict compliance and enforcement of established rules [38]. For sensitive crop environment data, blockchain smart contracts ensure the integrity and provenance (origin and history of use) of the data, resolving distrust in centralized data management through transparent, immutable records [22].

Capacity Building

To ensure the successful implementation of user-centric data governance, investment is required in training and capacity building aimed at both practitioners and farmers [34]. This addresses the systemic issue of low digital literacy [6], empowering the farming community to meaningfully participate in the governance of their data [34].

CONCLUSION AND FUTURE DIRECTIONS

1. Kerala's digital agriculture environment necessitates an integrated security approach to address the high-impact risks of compromised data integrity, digital exclusion, threats to farmer data privacy, and inherent vulnerabilities resulting from centralized old systems.
2. The suggested multi-layered security framework (M-LSF) uses a hybrid approach to build resilience. Technically, it uses high-accuracy edge-based AI/ML intrusion detection systems (such as BiGRU–LSTM) and resource-efficient cryptographic constraints. To guarantee data integrity and non-repudiation, it uses a distributed honeycomb architecture and blockchain smart contracts. By requiring the creation of farmer data sovereignty and putting Data Trust models into place to boost farmers' confidence and maintain technological adoption, the M-LSF institutionally changes the paradigm of data control.

Three strategic areas should be the focus of future research:

1. Creating standardized training programs for digital literacy adapted to Kerala's unique linguistic and technological context to successfully close the digital divide.
2. To maximize resource usage in the field, operational benchmarking of sophisticated AI/ML security systems (such as BiGRU–LSTM ensembles) utilizes region-specific smart agricultural traffic statistics.
3. Examining the legal and regulatory frameworks needed to formally create and uphold farmer data rights and trusts within the larger Indian e-governance system.

REFERENCES

1. Gyamfi EK, ElSayed Z, Kropczynski J, Yakubu MA, Elsayed N. Agricultural 4.0 leveraging on technological solutions: Study for smart farming sector. 2024 IEEE 3rd International Conference on Computing and Machine Intelligence (ICMI), Mt Pleasant, MI, USA. 2024. p. 1–9. doi:10.1109/ICMI60790.2024.10585910.
2. Das M. National Bank for Agriculture and Rural Development (NABARD). Int J Res Rev. 2021;8(12):75–82. doi:10.52403/ijrr.20211211.
3. Vardhan R, Kumar R, Supraja P. Intelligent fortification of agricultural data integrity. 2024 2nd International Conference on Networking and Communications (ICNWC), Chennai, India. 2024. p. 1–8. doi:10.1109/ICNWC60771.2024.10537380.
4. Ahmed B, Shabbir H, Naqvi SR, Peng L. Smart agriculture: Current state, opportunities, and challenges. IEEE Access. 2024;12:144456–144478. doi:10.1109/ACCESS.2024.3471647.
5. Islam MH, Anam MZ, Hoque MR, Nishat M, Bari ABMM. Agriculture 4.0 adoption challenges in emerging economies: Implications for smart farming and sustainability. J Econ Technol. 2024;2:278–295. doi:10.1016/j.ject.2024.09.002.
6. Hota J, Verma VK. Challenges to adoption of digital agriculture in India. 2022 International Conference on Maintenance and Intelligent Asset Management (ICMIAM), Anand, India. 2022. p. 1–6. doi:10.1109/ICMIAM56779.2022.10147002.

7. Adewusi AO, Chikezie NR, Eyo-Udo NL. Cybersecurity in precision agriculture: Protecting data integrity and privacy. Int J Appl Res Soc Sci. 2023;5(10):693–708. doi:10.51594/ijarss.v5i10.1482.
8. Nodehi NR, Berisha F, Da Silva L, Pourzolfaghar Z, Helfert M. Integrating cybersecurity, data sovereignty and trustworthiness in agri-data sharing environments: A conceptual framework. 2024 Cyber Research Conference - Ireland (Cyber-RCI), Carlow, Ireland, 2024, pp. 1-8; 2024. p. 1–8. doi:10.1109/Cyber-RCI60769.2024.10939388.
9. Malhotra H, Bhargava R, Dave M. Challenges related to information security and its implications for evolving e-government structures: A comparative study between India and African countries. 2017 International Conference on Inventive Computing and Informatics (ICICI), Coimbatore, India. 2017. p. 30–35. doi:10.1109/ICICI.2017.8365370.
10. Hasan A, Hashem MMA. A lightweight cryptographic framework based on hybrid cellular automata for IoT applications. IEEE Access. 2024;12:192672–192688. doi:10.1109/ACCESS.2024.3519673.
11. 11Nagarajan S, Vijay S, Karthi S, Praveen R, Vijaya Babu KR, Naresh B. Enhancing IoT-based smart farming security with a hybrid GRU intrusion detection system. 2025 IEEE International Conference on Interdisciplinary Approaches in Technology and Management for Social Innovation (IATMSI), Gwalior, India. 2025. p. 1–6. doi:10.1109/IATMSI64286.2025.10985129.
12. Thakor VA, Razzaque MA, Khandaker MRA. Lightweight cryptography algorithms for resource-constrained IoT devices: A review, comparison and research opportunities. IEEE Access. 2021;9:28177–28193. doi:10.1109/ACCESS.2021.3052867.
13. Dargaoui S, Azrour M, El Allaoui A, Guezzaz A, Benkirane S, Alabdulatif A, Amounas F. IoT-driven smart agriculture: Security issues and authentication schemes classification. In: Mejdoub Y, Elamri A, editors. Proceeding of the International Conference on Connected Objects and Artificial Intelligence (COCIA 2024). Lecture Notes in Networks and Systems, vol. 1123. Cham: Springer; 2024. doi:10.1007/978-3-031-70411-6_10.
14. Kristen E, Kloibhofer R, Díaz VH, Castillejo P. Security assessment of agriculture IoT (AIoT) applications. Appl Sci. 2021;11(13):5841. doi:10.3390/app11135841.
15. Udisha O, Ambily Philomina IG. Bridging the digital divide: Empowering rural women farmers through mobile technology in Kerala. Sustainability. 2024;16(21):9188. doi:10.3390/su16219188.
16. Adewusi AO, Chikezie NR, Eyo-Udo NL. Cybersecurity in precision agriculture: Protecting data integrity and privacy. Int J Appl Res Soc Sci. 2023;5(10):693–708. doi:10.51594/ijarss.v5i10.1482.
17. Bissadu K, Hossain G, Velagala LP, Sonko S. Analyzing insider cyber threats and human factors within the framework of agriculture 5.0. 2024 12th International Symposium on Digital Forensics and Security (ISDFS), San Antonio, TX, USA. 2024. p. 1–5. doi:10.1109/ISDFS60797.2024.10527290.
18. Manwatkar AB, Deshmukh RK, Junnarkar AA, Kamble SJ, Kachare PK, Latkar SP. Securing Industry 4.0-based precision agriculture. 2024 IEEE 4th International Conference on ICT in Business Industry & Government (ICTBIG), Indore, India. 2024. p. 1–7. doi:10.1109/ICTBIG64922.2024.10911640.
19. Alahmadi AN, Rehman SU, Alhazmi HS, Glynn DG, Shoaib H, Solé P. Cyber-security threats and side-channel attacks for digital agriculture. Sensors. 2022;22:3520. doi:10.3390/s22093520.
20. Naseer A, Shmoon M, Shakeel T, Ur Rehman SU, Ahmad A, Gruhn V. A systematic literature review of the IoT in agriculture—Global adoption, innovations, security, and privacy challenges. IEEE Access. 2024;12:60986–61021. doi:10.1109/ACCESS.2024.3394617.
21. Abbasi M, Plaza-Hernandez M, Prieto J, Corchado JM. Security in the Internet of Things application layer: Requirements, threats, and solutions. IEEE Access. 2022;10:97197–97216. doi:10.1109/ACCESS.2022.3205351.
22. Jung N, Kang H, Li L, Choi W. Building a crop environmental data monitoring system using blockchain-based smart contracts. 2024 IEEE 13th Global Conference on Consumer Electronics (GCCE), Kitakyushu, Japan, 2024. p. 1340–1341. doi:10.1109/GCCE62371.2024.10760591.

23. Elbasi E, Mostafa N, AlArnaout Z, Zreikat AI, Cina E, Varghese G, Shdefat A, Topcu AE, Abdelbaki W, Mathew S, Zaki C. Artificial intelligence technology in the agricultural sector: A systematic literature review. IEEE Access. 2023;11:171–202. doi:10.1109/ACCESS.2022.3232485.
24. Bica I, Chifor BC, Arseni ȘC, Matei I. Multi-layer IoT security framework for ambient intelligence environments. Sensors. 2019;19(18):4038. doi:10.3390/s19184038.
25. Amiri-Zarandi M, Dara RA, Duncan E, Fraser EDG. Big data privacy in smart farming: A review. Sustainability. 2022;14(15):9120. doi:10.3390/su14159120.
26. von Lautz-Cauzanet E. e-Krishi: The online platform for small farmers (India). In: Zeng H, Xia W, Wang J, Wang R, editors. Approach of ICT in education for rural development: Good practices from developing countries. New Delhi: SAGE Publications; 2015. p. 342–366.
27. Gans Combe C, Camaréna S. Data sovereignty and valuation model for sustainable agriculture innovation and equity. npj Sustain Agric. 2025;3:61. doi:10.1038/s44264-025-00102-z.
28. Monisha PJ, Fallah MH, Meenakshi, Hemamalini M, Saranya NN. Threat detection for IoT-based smart farming systems based on bidirectional gated recurrent unit with long short-term memory. 2024 4th International Conference on Mobile Networks and Wireless Communications (ICMNWC), Tumkuru, India. 2024. p. 1–5. doi:10.1109/ICMNWC63764.2024.10872064.
29. Alanazi B, Alrashdi I. Anomaly detection in smart agriculture systems on network edge using deep learning technique. Sustain Mach Intell J. 2023;3. doi:10.61185/SMIJ.2023.33104.
30. Janssen SJC, Porter CH, Moore AD, Athanasiadis IN, Foster I, Jones JW, Antle JM. Towards a new generation of agricultural system data, models and knowledge products: Information and communication technology. Agric Syst. 2017;155:200–212. doi:10.1016/j.agsy.2016.09.017.
31. Sharma K, Shivandu SK. Integrating artificial intelligence and Internet of Things (IoT) for enhanced crop monitoring and management in precision agriculture. Sensors Int. 2024;5:100292. doi:10.1016/j.sintl.2024.100292.
32. Singhal G, Singh A. Probabilistic data structure in smart agriculture. 2023 Third International Conference on Secure Cyber Computing and Communication (ICSCCC), Jalandhar, India. 2023. p. 780–785. doi:10.1109/ICSCCC58608.2023.10176985.
33. Chakraborty S, Choudhury N, Kalita I. AI-based smart agriculture monitoring using ground-based and remotely sensed images. In: Panda SK, Mohapatra RK, Panda S, Balamurugan S, editors. The New Advanced Society: Artificial Intelligence and Industrial Internet of Things Paradigm. Hoboken (NJ): John Wiley & Sons; 2022. p. 191–221. doi:10.1002/9781119884392.ch9.
34. Demestichas K, Peppes N, Alexakis T, Adamopoulou E. Blockchain in agriculture traceability systems: A review. Appl Sci. 2020;10(12):4113. doi:10.3390/app10124113.
35. NITI Aayog. National Strategy for Artificial Intelligence. New Delhi: Government of India; 2018.
36. Kasyapa MS, Vanmathi C. A privacy protection mechanism for Indian health care data exchange using blockchain. 2023 Innovations in Power and Advanced Computing Technologies (i-PACT), Kuala Lumpur, Malaysia. 2023. p. 1–9. doi: 10.1109/i-PACT58649.2023.10434770.
37. Zafar O, González RS, Namazi M, Morales A, Ayday E. Empowering digital agriculture: A privacy-preserving framework for data sharing and collaborative research. [Preprint]. 2025. arXiv:2506.20872. doi:10.48550/arXiv.2506.20872.
38. Ada Lovelace Institute. Exploring Legal Mechanisms for Data Stewardship: Working Group Final Report. London: Ada Lovelace Institute; 2021. Available from: https://www.adalovelaceinstitute.org/report/legal-mechanisms-data-stewardship/

