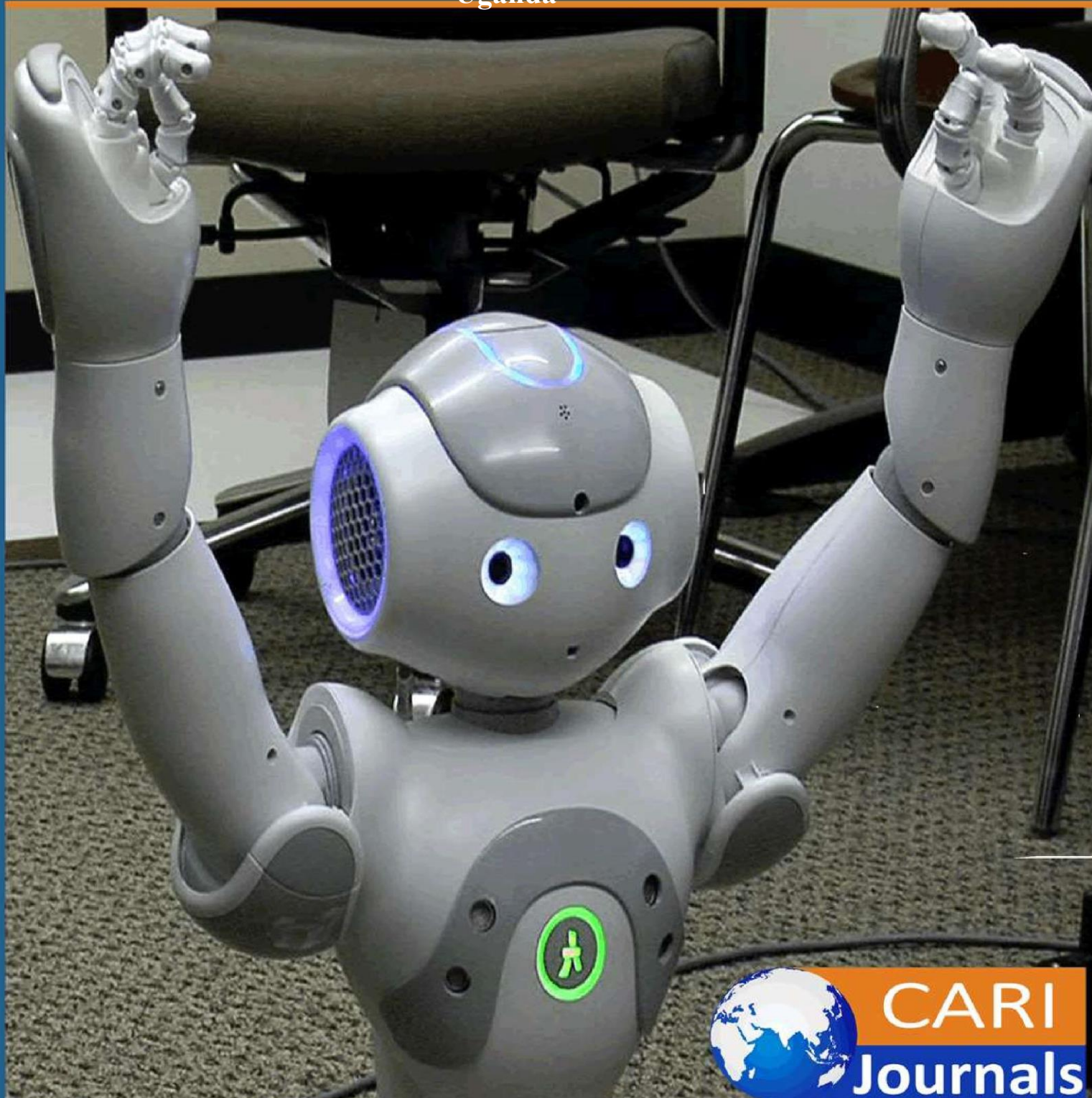
International Journal of
Computing and
Engineering
(IJCE)

A Structured Analytical Review of Cyber-Physical Systems and Edge Computing Architectures for Soil Health Monitoring in Uganda



CARI Journals

International Journal of Computing and Engineering

ISSN 2958-7425 (online)

Vol. 8, Issue No. 1, pp 78 - 92, 2026

www.carijournals.org

A Structured Analytical Review of Cyber-Physical Systems and Edge Computing Architectures for Soil Health Monitoring in Uganda: A Case Study of the Eastern Region Agricultural Sector

Opolot Francis[1*], Dr. Alunyu Andrew[1,2], Dr. Lukyamuzi Andrew[3,4], Dr. Angole Richard Okello[3,4]

[1]PhD candidate, Department of computer engineering & informatics, Busitema University

[2]Senior lecturer, Department of computer engineering and informatics, Lira University

[3]Senior lecturer, Faculty of science education, Busitema Nagongera Campus

[4]Senior lecturer, Department of information technology, Busitema University.

https://orcid.org/0000-0009-0000-4965

Accepted: 4th Jan, 2026, Received in Revised Form: 20th Jan, 2026, Published: 3rd Feb, 2026

Abstract

Purpose: This paper aims to analyze existing Cyber-Physical Systems (CPS) architectures for soil health monitoring and the integration of edge computing, with a focus on identifying security gaps that hinder reliable and trustworthy real-time agricultural intelligence in Uganda's Eastern Region.

Methodology: A structured systematic literature review was conducted on peer-reviewed publications published between 2020 and 2025. The review examined global and sub-Saharan African CPS-based soil health monitoring architectures, with particular attention to edge computing integration, security mechanisms, and architectural design patterns. Architectural, technological, and security dimensions were synthesized to identify recurring vulnerabilities and gaps relevant to Uganda's agricultural context.

Findings: The review reveals significant architectural fragmentation, inconsistent security implementations, and limited cross-layer protection across sensing, communication, edge, and application layers. Existing deployments remain vulnerable to sensor spoofing, physical tampering, insecure edge gateways, malware propagation, and compromised data transmission. While promising advancements exist such as ML-driven anomaly detection, federated learning, cryptographic safeguards, and IT/OT convergence these solutions are often applied in isolation rather than within holistic CPS-edge security frameworks.

Unique Contribution to Theory, Policy, and Practice: The study advances CPS and edge computing research by synthesizing fragmented architectural and security perspectives into a unified cross-layer analytical view. It provides evidence to support the development of secure smart agriculture and digital transformation policies in Uganda and similar contexts. The study outlines a conceptual direction for designing an integrated, secure CPS–edge architecture tailored to real-time soil health monitoring, supporting more resilient, trustworthy, and scalable agricultural decision-making systems.

Keywords: *Cyber-Physical Systems, Edge Computing, Soil Monitoring, IoT Security, Cross-Layer Security, Anomaly Detection, Uganda*

International Journal of Computing and Engineering
ISSN 2958-7425 (online)
Vol. 8, Issue No. 1, pp 78 - 92, 2026
www.carijournals.org

1. INTRODUCTION

Advances in digital agriculture have positioned Cyber-Physical Systems (CPS) and edge computing as transformative technologies for improving soil health monitoring, enabling farmers to make timely, data-driven decisions that enhance food security and sustainability. Globally, CPS integrates IoT sensors, embedded processors, real-time communication networks, cloud platforms, and intelligent automation to monitor dynamic agricultural environments and respond adaptively to soil changes (Liu et al., 2020), (Malik et al., 2020). Precision agriculture backed by CPS is becoming more popular in sub-Saharan Africa, as seen by the increased use of low-cost IoT sensors, remote monitoring systems, and agricultural decision-support platforms (Anosike et al., 2024). However, widespread adoption is constrained by architectural and security issues that are made worse by infrastructure limits, erratic connectivity, and regional environmental issues (Kansiime et al., 2022).

Strong soil health monitoring technologies are desperately needed in Uganda's Eastern Region, where agriculture continues to be the main source of income due to soil fertility loss, restricted access to real-time soil diagnostics, and inadequate digital infrastructure. Although CPS and edge computing provide a mechanism to increase agricultural output, there are many risks associated with their implementation, such as data manipulation, unsecured gateways, and assaults against cloud-integrated systems (Kariri, 2022), (Balasubramanian et al., 2025). The availability, confidentiality, and integrity of soil health data all essential for successful precision farming are jeopardized by these multi-layer security issues.

Although global studies demonstrate advanced CPS frameworks supported by distributed sensing, hierarchical edge-cloud architectures, and AI-enabled analytics (Akter et al., 2024) , (Latif et al., 2020), Coordinated cross-layer designs and integrated protections are missing from regional deployments. Without addressing the whole nature of CPS security, existing literature frequently isolates particular elements like IoT sensors, routing protocols, or ML-based anomaly detection. This work aims to fill this knowledge gap by analyzing current CPS and edge computing architectures for soil health monitoring and looking at the security issues they raise in the Ugandan setting.

This paper focuses on analysis of existing architectures of Cyber-Physical Systems (CPS) used for soil health monitoring globally and regionally, and examining how edge computing integrates into CPS architectures and to identify key associated security gaps, especially in contexts similar to Uganda’s Eastern agricultural region. The insights derived from these two objectives form the foundation for developing a future cross-layer security framework suitable for Uganda.

2. METHODOLOGY FOR LITERATURE REVIEW

The literature review adopted a systematic methodological approach designed to capture the most recent and relevant scholarly work on Cyber-Physical Systems (CPS), edge computing, and soil

health monitoring. To ensure rigor, the review focused exclusively on peer-reviewed publications produced between January 2020 and February 2025, a period that reflects significant global advancements in CPS design, distributed edge intelligence, and agricultural IoT innovation. The search process was framed around the need to consolidate fragmented knowledge across engineering, computer science, and agricultural technology disciplines while prioritizing empirical and architecture-focused studies.

The review process began with extensive searches across major academic databases known for high-quality publications in computing and agricultural systems research. These included IEEE Xplore, ACM Digital Library, Elsevier ScienceDirect, SpringerLink, Wiley Online Library, Taylor & Francis Online, and MDPI. Google Scholar was used selectively to capture additional highly-cited studies that occasionally fall outside subscription-based repositories. Each database was queried iteratively to ensure that no relevant publication was overlooked, particularly studies addressing CPS security, soil monitoring technologies, and edge-integrated architectures in resource-constrained settings. The use of multiple databases was essential because CPS-agriculture research is distributed across interdisciplinary venues, making single-source searches insufficient for a comprehensive review.

The search strategy used a carefully developed set of Boolean expressions intended to capture both broad and highly specific research themes. Terms such as *"Cyber-Physical Systems AND agriculture," "edge computing AND soil monitoring," "CPS architecture AND vulnerabilities," "IoT security AND smart farming,"* and *"machine learning anomaly detection AND agriculture"* were combined to maximize coverage. These keyword combinations were refined progressively based on initial search outcomes, enabling the identification of emerging areas such as federated learning, blockchain-enabled CPS, and cross-layer security models that appeared frequently in recent literature. The strategy allowed the review to capture both technological architectures and security-focused contributions, thereby addressing the dual objectives of the study.

Studies identified through database searches were then evaluated through a structured inclusion and exclusion process. Publications had to be peer-reviewed, published between 2020 and 2025, and directly advance knowledge of CPS architectures, edge computing frameworks, soil health monitoring systems, or security flaws in distributed sensing environments. Because they most closely matched the review's analytical objectives, articles that presented conceptual frameworks, experimental deployments, architecture models, or technical evaluations were given priority. On the other hand, studies that were unrelated to environmental or agricultural monitoring, lacked technical depth, or provided merely general commentary devoid of empirical or architectural contributions were disqualified. In order to avoid using out-of-date CPS models that do not accurately reflect current technical capabilities especially given the rapid expansion of IoT and edge intelligence over the past five years studies published before 2020 were excluded.

A precise collection of excellent publications was the result of this multi-phase selection procedure. After removing duplicates and screening titles for relevancy from a starting pool of 317 records, abstract and full-text evaluations were conducted. In the end, 58 papers met every requirement for inclusion and were included in the final synthesis. Soil sensor technologies, security models, edge analytics, CPS design, and smart agricultural applications were all evenly distributed throughout these investigations. Because of their variety, the review was able to look at the architectural underpinnings as well as the changing security issues related to multi-layer CPS-edge systems. The collected corpus of research offers a solid foundation for evaluating current architectural models and pinpointing crucial security flaws pertinent to the agricultural environment of Uganda's Eastern Region.

3. LITERATURE REVIEW

3.1. Analysis of Existing CPS Architectures for Soil Health Monitoring

The various CPS designs used in agriculture are highlighted in recent studies. These architectures are usually Organised as layered systems that include sensing, computation, communication, and cloud analytics. Soil moisture sensors, pH probes, nutrient detectors, and ambient sensors make up the basic sensing layer of most systems (Dinn et al., 2025),(Othaman et al., 2021). Through wireless protocols as LoRa WAN, ZigBee, NB-IoT, or 5G-enabled networks, these nodes gather and send granular soil data. A hierarchical design is used in many CPS systems, starting with the perception layer, moving on to the network and processing layers, and concluding with decision and actuation components (Mishra et al., 2022).

A notable trend in CPS architecture is the shift from centralized cloud-dependent designs to distributed edge-based models due to latency, bandwidth, and resilience considerations (El-Basioni et al., 2020), (Pengpeng et al., 2025). Studies demonstrate that real-time soil monitoring benefits from localized preprocessing at the edge, reducing communication overhead and improving responsiveness to soil condition changes (Chirkhare et al. 2022), (Kishor Syam et al., 2024). Furthermore, a number of systems use machine learning pipelines for irrigation control, nutrient prediction, and soil classification (Islam et al., 2023),(Srivastava et al., 2021).

Nevertheless, despite advancements worldwide, CPS systems used in low-resource areas have difficulties such as constrained processing power, unstable networks, and inadequate integration between sensing and analytics units (Ali et al., 2023), (Abdi et al., 2025). Deployments in Africa are still mostly pilot-level and concentrate on individual sensor devices without complete CPS orchestration (Chizema et al., 2024). Research shows that CPS adoption in actual agricultural settings is further weakened by inadequate multi-layer security integration (Kumar et al., 2020).

All things considered, current CPS designs offer useful technological underpinnings, but they lack unified security models that can safeguard the complete data flow from sensor to cloud.

3.2. Edge Computing Integration and Associated Security Gaps

By enabling real-time analytics, lowering dependency on remote cloud servers, and offering localized processing closer to sensors, edge computing improves CPS efficiency (Sathya et al., 2024), (Makondo et al., 2024) . Preliminary activities including data filtering, anomaly detection, packet validation, and model inference are frequently handled by edge nodes (Kim et al., 2021), (Babar et al., 2022). For soil monitoring situations where decisions made in real time impact soil conservation, fertilization, and irrigation, distributed intelligence is essential.

However, there are a lot of new attack surfaces when edge computing is included. According to studies, edge nodes are susceptible to insider threats, physical tampering, firmware alteration, malware injection, and unauthorized access (Zhukabayeva et al., 2025),(Manoj et al., 2023). Edge devices are especially vulnerable to sensor spoofing and device cloning since they operate in unsupervised, outside situations (Kim et al., 2023).

The integrity of soil data can be compromised by man-in-the-middle (MITM) attacks, eavesdropping, and replay attacks, which are made possible by insecure communication channels. Transmission security is still a key concern (Gupta et al., 2023), (Wang et al., 2024). Gaps in edge-to-cloud connectivity are especially risky in areas with weak cybersecurity regulations or low encryption use (Romaniuk et al., 2021).

By enabling decentralized model training without disclosing raw data, emerging techniques like federated learning have demonstrated potential in safeguarding dispersed CPS ecosystems (Ghimire et al., 2022), (Quan et al., 2025). Similarly, zero-trust network designs, blockchain-based integrity methods, and contemporary cryptographic protocols have been suggested to improve CPS-edge communication (Wang et al., 2025), However, due to budget limitations and a lack of technical know-how, these technologies are rarely used in agricultural installations throughout Uganda and most of Africa (Romaniuk et al., 2021), (Abiodun et al., 2021).

Evidence generally supports the necessity of CPS-edge designs for contemporary soil health monitoring, but they are nonetheless intrinsically insecure in the absence of a coordinated cross-layer security policy.

4. DISCUSSION

The examined literature shows that multi-layered cyber threats that take advantage of flaws in sensing devices, edge gateways, communication networks, and cloud platforms can affect CPS-edge systems installed in agricultural situations. Recent research on distributed sensing architectures, cyber-physical security, and precision agriculture between 2020 and 2025 has extensively documented these vulnerabilities (Liu et al., 2020),(Kagona, 2025). These vulnerabilities are further increased in the Eastern Region of Uganda because to fragmented installations, old firmware, unencrypted wireless connectivity, and inadequate infrastructure

maturity. These issues are similar to those reported in low-resource agricultural CPS deployments (Alyahya et al., 2022).

4.1 CPS–Edge System Attacks

Sensors, actuators, embedded microcontrollers, communication modules, cloud analytics, and other heterogeneous components are integrated into a coordinated operational loop by CPS-edge systems. Adversaries can alter agronomic intelligence or interfere with decision-making processes by taking advantage of the increased attack surface created by this linkage of the physical and cyber realms (Han et al., 2020), (Yazdinejad et al., 2021a). Low-cost soil sensors are susceptible to sensor spoofing and physical manipulation at the data-source layer because they frequently lack secure boot procedures and tamper-resistant hardware (Kasarapu et al., 2024), (Tirumala Rao et al., 2024). By injecting false signals, spoofing attacks enable attackers to confuse automated irrigation or fertilization systems and skew measures of soil moisture, pH, or nutrients (Alyas et al., 2025).

Numerous attacks that target edge gateways at the edge processing layer have been reported in the literature. These include malware delivered by vulnerable firmware updates, default passwords, compromised lightweight Linux distributions, and poor cryptographic setups (Chathoth et al., 2025),(Arinze et al. 2024). Any vulnerability at this tier can result in systematic misclassification or suppression of warnings because edge nodes do local analytics and machine learning inference, which is consistent with agricultural CPS security incidents seen worldwide (Laaroussi et al., 2021), (Almohri et al., 2020).

Attacks utilizing Wi-Fi, LoRa WAN, ZigBee, NB-IoT, and BLE protocols can still compromise the communication layer. Man-in-the-Middle (MITM) manipulations, packet injection, eavesdropping, and replay attacks are common in agricultural IoT deployments, according to recent empirical investigations (Aldhyani et al., 2023),(Abdulkarim et al., 2023). According to cybersecurity evaluations of distributed sensing networks, many rural deployments rely on unencrypted MQTT or CoAP channels, which greatly increases sensitivity to message tampering (Ali et al., 2024), (Alwaheidi et al., 2022).

Adversaries are increasingly using ransomware, account breach attacks, and Distributed Denial-of-Service (DDoS) on the cloud layer to target centralized analytics systems (Parween et al., 2021),(Adhikary et al., 2025). Data poisoning, unauthorized access, and ransomware-induced operational downtime are among the most detrimental concerns for CPS infrastructures, according to recent assessments on agricultural cloud security (Alyahya et al., 2022),(Xu et al., 2020). This is consistent with research showing that cross-layer, comprehensive security is needed for agricultural CPS systems instead of discrete patching techniques (Adewusi et al., 2022), (Liu et al., 2022).

4.2 Types of Cyber Attacks against CPS

4.2.1 Sensor Spoofing and Data Manipulation Attacks

Falsified digital or physical signals are used in sensor spoofing attacks to trick sensing systems. Research on environmental and soil monitoring reveals that enemies can alter data by using uncalibrated sensors, electromagnetic interference, or unprotected ADC interfaces (Alaeiyan et al., 2020), (Ataguba et al., 2024). In systems without anomaly detection or digital signatures, data modification assaults can happen during acquisition, preprocessing, or aggregation and frequently evade detection (Husnain et al., 2022).

4.2.2 Malware, Ransomware, and Firmware Attacks

CPS implementations are seriously threatened by ransomware and malware. Studies conducted between 2020 and 2025 show that supply-chain breaches, USB vectors, and insecure firmware updates are all contributing to the spread of malware (Paris et al., 2023),(Malik et al., 2020). According to recent cybersecurity event studies, ransomware attacks against agricultural CPS have led to data encryption, loss of operational control, and prolonged monitoring network outages (Yazdinejad et al., 2021), (Adewusi et al., 2022).

4.2.3 Man-in-the-Middle (MITM) Attacks

MITM attacks take advantage of misconfigured communication protocols and unprotected wireless channels. MQTT and CoAP are frequently shown to be high-risk protocols when used without TLS or certificate validation in scientific studies of IoT-based agricultural networks, (Hussain et al., 2022). MITM attacks compromise system integrity throughout field-to-cloud data flows by enabling packet interception, alteration, and replay (Dehury et al., 2024), (Hashemi et al., 2021).

4.2.4 Denial-of-Service (DoS) and Distributed Denial-of-Service (DDoS) Attacks

DoS/DDoS attacks interfere with real-time monitoring by flooding edge gateways, cloud APIs, or farm management platforms with excessive traffic. Numerous studies show that botnets like Mirai variants and agricultural IoT-specific malware strains are rapidly targeting CPS domains, particularly those in agriculture (Bhat et al., 2021), (Levshun et al., 2021).

4.2.5 Physical Layer and Environmental Attacks

Cutting connections, moving sensors, depleting batteries, and harming solar power infrastructure are examples of physical attacks. Wireless signals used for soil monitoring are disrupted by environmental interference threats such RF jamming and electromagnetic noise (Al-Dulaimi et al.,), (Adhikary et al., 2025). Distributed rural networks with little physical security are especially vulnerable to these threats. (Liu et al., 2025).

International Journal of Computing and Engineering
ISSN 2958-7425 (online)
Vol. 8, Issue No. 1, pp 78 - 92, 2026
www.carijournals.org

4.2.6 Supply-Chain and Third-Party Component Attacks

CPS systems mostly depend on imported parts, such as radio modules, microcontrollers, and sensors, which are frequently purchased from suppliers with differing quality control requirements. According to recent audits of IoT hardware ecosystems, supply-chain hacks may incorporate pre-installed malware, backdoors, or hacked firmware (Liu et al., 2022), (Ul Haq et al., 2023).

Table 1. Summary of CPS Attack Types and Their Effects

Attack Type	Primary Target Layer	Effect on Soil CPS	Representative Studies (2020–2025)
Sensor Spoofing	Source/Sensor Layer	False soil readings, misleading analytics	(Khan et al., 2021; Kim et al., 2023)
Firmware Tampering	Edge Gateway	Unauthorized control, altered preprocessing	(Ul Haq et al., 2023), (Xu et al., 2020), (Adewusi et al., 2022)
Malware Injection	Edge/Cloud	Data corruption, system hijacking	(Al-Dulaimi et al.), (Liu et al., 2022)
MITM Attacks	Communication Layer	Packet alteration, replay, data leaks	(Kondu et al., 2025), (Husnain et al., 2022)
DDoS Attacks	Edge/Cloud	Service disruption, data loss	(Al-Dulaimi et al.,), (Hussain et al., 2022)
Ransomware	Cloud Layer	Locked databases, halted dashboards	(Humayun et al., 2021), (Adewusi et al., 2022),
Replay Attacks	Communication Layer	Incorrect automation decisions	(Chen et al., 2022), (Ataguba et al., 2024)
Node Capture / Physical Tampering	Sensor Layer	Key theft, false node deployment	(Sadik et al., 2021.), (Panoff et al., 2021)

5. Conclusion

The review concludes that while CPS and edge computing offer transformative potential for soil health monitoring, current architectures fall short of providing the robust, secure, and scalable systems required for reliable agricultural decision-making. There are still serious flaws in the sensing, edge processing, data transmission, and cloud integration layers. A coordinated cross-layer security strategy designed for resource-constrained agricultural areas like Eastern Uganda is needed to address them. In order to improve CPS resilience in practical deployments, future research should concentrate on creating integrated frameworks that incorporate cryptography, IT/OT convergence, federated learning, and ML-based security intelligence.

References

Abdi, A. H., Mohamed, A. A., & Sheikh, S. N. (2025). Navigating Paths to Food Security in East Africa: Strengthening Rural Development Amid Climate Shocks, Political Instability, and Rising Food Prices. *Frontiers in Political Science*, *7*, 1636407.

Abdulkarim, O. M., Adebayo, O. S., Aliyu, H. O., & Olalere, M. (2023). *Cloud Data Security Audit Report Techniques Using Bat Inspired Algorithm (CDSART-BA): A Review*.

Abiodun, O. I., Abiodun, E. O., Alawida, M., Alkhawaldeh, R. S., & Arshad, H. (2021). A review on the security of the internet of things: Challenges and solutions. *Wireless Personal Communications*, *119*(3), 2603–2637.

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.

Adhikary, D., Plusquellic, J., & Tsiropoulou, E. E. (2025). Jamming Attacks Detection and Ejection in Over the Air Computation Concentrated Solar Power Systems. *IEEE Internet of Things Journal*.

Akter, T., Mahmud, T., Chakma, R., Datta, N., Hossain, M. S., & Andersson, K. (2024). Iot-based precision agriculture monitoring system: Enhancing agricultural efficiency. *2024 Second International Conference on Inventive Computing and Informatics (ICICI)*, 749–754.

Alaeiyan, M., Dehghantanha, A., Dargahi, T., Conti, M., & Parsa, S. (2020). A multilabel fuzzy relevance clustering system for malware attack attribution in the edge layer of cyber-physical networks. *ACM Transactions on Cyber-Physical Systems*, *4*(3), 1–22.

Aldhyani, T. H. H., & Alkahtani, H. (2023). Cyber security for detecting distributed denial of service attacks in agriculture 4.0: Deep learning model. *Mathematics*, *11*(1), 233.

Al-Dulaimi, R. T. A., & Türkben, A. K. (n.d.). *A Novel Hybrid Complex Multilayer Perceptron for Enhancing DDoS Attack Detection in Network Security*.

Ali, G., Mijwil, M. M., Buruga, B. A., Abotaleb, M., & Adamopoulos, I. (2024). A survey on artificial intelligence in cybersecurity for smart agriculture: state-of-the-art, cyber threats, artificial intelligence applications, and ethical concerns. *Mesopotamian Journal of Computer Science*, *2024*, 53–103.

Ali, N., Manjula, V. S., & Marega, F. (2023). *Impact of Digitization of Sustainable Agriculture in Uganda: A Case Study*.

Almohri, H. M. J., Watson, L. T., & Evans, D. (2020). An attack-resilient architecture for the Internet of Things. *IEEE Transactions on Information Forensics and Security*, *15*, 3940–3954.

Alwaheidi, M. K. S., & Islam, S. (2022). Data-driven threat analysis for ensuring security in cloud enabled systems. *Sensors*, *22*(15), 5726.

Alyahya, S., Khan, W. U., Ahmed, S., Marwat, S. N. K., & Habib, S. (2022). Cyber Secure Framework for Smart Agriculture: Robust and Tamper-Resistant Authentication Scheme for IoT Devices. *Electronics (Switzerland)*, *11*(6). doi: 10.3390/electronics11060963

Alyas, T., Abbas, S., Abbas, Q., Albouq, S., Niazi, M., & Khan, M. A. (2025). A Privacy-Preserving and Adversarially Robust Hybrid Deep-Quantum Model for CPS Security. *International Conference on Neural Computing for Advanced Applications*, 161–175.

Anosike, P. L., & Silas, U. (2024). A Roadmap for Intelligent Agriculture in Africa-A Case Study of Sub-Saharan Africa. *Ieomsociety. Org*.

Arinze, E. D., & Agwu, C. O. (2024). *Introduction to the Transformative Potential of the Internet of Things (IoT) in East Africa*.

Ataguba, H. E., Kokofi, C., Alade, O. O., & Babatunde, E. D. (2024). Integrating cybersecurity and ICT into climate-smart agriculture: a framework for resilient food systems. *Information Technologist*, *21*(2).

Babar, M., Jan, M. A., He, X., Tariq, M. U., Mastorakis, S., & Alturki, R. (2022). An optimized IoT-enabled big data analytics architecture for edge–cloud computing. *IEEE Internet of Things Journal*, *10*(5), 3995–4005.

Balasubramanian, P. N., & Shashank, M. A. Q. S. (2025). *Securing Low-Power Edge AI: A Vulnerability Analysis and Cybersecurity Framework for Resource-Constrained Devices*.

Bhat, S. A., Huang, N.-F., Sofi, I. B., & Sultan, M. (2021). Agriculture-food supply chain management based on blockchain and IoT: A narrative on enterprise blockchain interoperability. *Agriculture*, *12*(1), 40.

Chathoth, A. K., & Lee, S. (2025). PCAP-Backdoor: Backdoor Poisoning Generator for Network Traffic in CPS/IoT Environments. *ArXiv Preprint ArXiv:2501.15563*.

Chen, L., Tang, S., Balasubramanian, V., Xia, J., Zhou, F., & Fan, L. (2022). Physical-layer security based mobile edge computing for emerging cyber physical systems. *Computer Communications*, *194*, 180–188.

Chirkhare, G., Hablani, R., & Balamwar, S. (2022). Prediction of regional vegetation cover using spatial image features and semantic segmentation. *International Journal of Health Sciences*, *6*(S4), 5425–5435.

Chizema, T. R., Dlamini, P., Van Greunen, D., & Msomi, S. (2024). The Perceived Influence of Internet of Things on Precision Agriculture for Small-Scale Farming. *2024 IST-Africa Conference (IST-Africa)*, 1–10.

Dehury, M. K., Mohanta, B. K., & Chedup, S. (2024). Security issues and challenges in deploying a CPS using WSN. *Information Technology Security: Modern Trends and Challenges*, 25–46.

Dinn, C., Shakshuki, E., & Hassan, E. (2025). A Review of AIoT in Sustainable Agriculture: Advancing Soil Management with IoT Sensors. *Procedia Computer Science*, *265*, 366–373.

El-Basioni, B. M. M., & Abd El-Kader, S. M. (2020). Laying the foundations for an IoT reference architecture for agricultural application domain. *IEEE Access*, *8*, 190194–190230.

Ghimire, B., & Rawat, D. B. (2022). Recent advances on federated learning for cybersecurity and cybersecurity for federated learning for internet of things. *IEEE Internet of Things Journal*, *9*(11), 8229–8249.

Gupta, M., (Rav), M. G., & Yadav, A. K. (2023). *Future Connected Technologies*.

Han, K., Duan, Y., Jin, R., Ma, Z., Rong, H., & Cai, X. (2020). Open framework of gateway monitoring system for internet of things in edge computing. *2020 IEEE 39th International Performance Computing and Communications Conference (IPCCC)*, 1–5.

Hashemi, S., & Zarei, M. (2021). Internet of Things backdoors: Resource management issues, security challenges, and detection methods. *Transactions on Emerging Telecommunications Technologies*, *32*(2), e4142.

Humayed, A., Lin, J., Li, F., & Luo, B. (2017). Cyber-physical systems security—A survey. *IEEE Internet of Things Journal*, *4*(6), 1802–1831.

Humayun, M., Jhanjhi, N. Z., Alsayat, A., & Ponnusamy, V. (2021). Internet of things and ransomware: Evolution, mitigation and prevention. *Egyptian Informatics Journal*, *22*(1), 105–117.

Husnain, M., Hayat, K., Cambiaso, E., Fayyaz, U. U., Mongelli, M., Akram, H., Ghazanfar Abbas, S., & Shah, G. A. (2022). Preventing MQTT vulnerabilities using IoT-enabled intrusion detection system. *Sensors*, *22*(2), 567.

Hussain, A., Abughanam, N., Qadir, J., & Mohamed, A. (2022). Jamming detection in iot wireless networks: An edge-ai based approach. *Proceedings of the 12th International Conference on the Internet of Things*, 57–64.

Islam, M. R., Oliullah, K., Kabir, M. M., Alom, M., & Mridha, M. F. (2023). Machine learning enabled IoT system for soil nutrients monitoring and crop recommendation. *Journal of Agriculture and Food Research*, *14*, 100880.

Islam, S. N., Baig, Z., & Zeadally, S. (2019). Physical layer security for the smart grid: Vulnerabilities, threats, and countermeasures. *IEEE Transactions on Industrial Informatics*, *15*(12), 6522–6530.

Kagona, E. (2025). A Mixed-Methods Analysis of Policy, Legal, and Technical Barriers to the Adoption of AI and IoT-Driven Agricultural Solutions in the East African Community (EAC). *2025 IEEE/ACM Symposium on Software Engineering in the Global South (SEiGS)*, 7–14.

Kansiime, M. K., Mugambi, I., Rware, H., Alokit, C., Aliamo, C., Zhang, F., Latzko, J., Puyun, Y., Karanja, D., & Dannie, R. (2022). *Challenges and capacity gaps in smallholder access to digital extension and advisory services in Kenya and Uganda*.

Kariri, E. (2022). IoT powered agricultural cyber-physical system: Security issue assessment. *IETE Journal of Research*, 1–11.

Kasarapu, S., Shukla, S., & Dinakarrao, S. M. P. (2024). Optimizing Malware Detection in IoT Networks: Leveraging Resource-Aware Distributed Computing for Enhanced Security. *ArXiv Preprint ArXiv:2404.10012*.

Khan, S. Z., Mohsin, M., & Iqbal, W. (2021). On GPS spoofing of aerial platforms: a review of threats, challenges, methodologies, and future research directions. *PeerJ Computer Science*, *7*, e507.

Kim, C., Chang, S.-Y., Lee, D., Kim, J., Park, K., & Kim, J. (2023). Reliable detection of location spoofing and variation attacks. *IEEE Access*, *11*, 10813–10825.

Kim, J., & Lee, J. Y. (2021). Server-Edge dualized closed-loop data analytics system for cyber-physical system application. *Robotics and Computer-Integrated Manufacturing*, *67*, 102040.

Kondu, S. C. V., Ravikumar, G., & Mohan, S. N. (2025). CPS-DERMS: Cyber-Physical Security and Impact Analysis of DERMS Against MITM Attacks. *2025 IEEE Green Technologies Conference (GreenTech)*, 1–5.

Kishor Syam, S. K., & VA, B. (2024). An IoT-enabled real-time crop prediction system using soil fertility analysis. *Eng*, *5*(4), 2496–2510.

Kumar, C., Marston, S., & Sen, R. (2020). Cyber-physical systems (CPS) security: state of the art and research opportunities for information systems academics. *Communications of the Association for Information Systems*, *47*(1), 36.

Laaroussi, Z., & Novo, O. (2021). A performance analysis of the security communication in CoAP and MQTT. *2021 IEEE 18th Annual Consumer Communications & Networking Conference (CCNC)*, 1–6.

Latif, G., Alghazo, J., Maheswar, R., Vijayakumar, V., & Butt, M. (2020). Deep learning-based intelligence cognitive vision drone for automatic plant diseases identification and spraying. *Journal of Intelligent & Fuzzy Systems*, *39*(6), 8103–8114.

Levshun, D., Chechulin, A., & Kotenko, I. (2021). Design of secure microcontroller-based systems: application to mobile robots for perimeter monitoring. *Sensors*, *21*(24), 8451.

Liu, J., Du, Y., Yang, K., Wu, J., Wang, Y., Hu, X., Wang, Z., Liu, Y., Sun, P., & Boukerche, A. (2025). Edge-cloud collaborative computing on distributed intelligence and model optimization: A survey. *ArXiv Preprint ArXiv:2505.01821*.

Liu, R., Zhang, Y., Ge, Y., Hu, W., & Sha, B. (2020). Precision regulation model of water and fertilizer for alfalfa based on agriculture cyber-physical system. *IEEE Access*, *8*, 38501–38516.

Liu, X., Wu, Y., Yu, Q., Song, S., Liu, Y., Zhou, Q., & Zhuge, J. (2022). PG-VulNet: detect supply chain vulnerabilities in IoT devices using pseudo-code and graphs. *Proceedings of the 16th ACM/IEEE International Symposium on Empirical Software Engineering and Measurement*, 205–215.

Makondo, N., Kobo, H. I., Mathonsi, T. E., & Du Plessis, D. P. (2024). Implementing an efficient architecture for latency optimisation in smart farming. *IEEE Access*, *12*, 140502–140526.

Malik, A. W., Rahman, A. U., Qayyum, T., & Ravana, S. D. (2020). Leveraging fog computing for sustainable smart farming using distributed simulation. *IEEE Internet of Things Journal*, *7*(4), 3300–3309.

Malik, K. M., Javed, A., Malik, H., & Irtaza, A. (2020). A light-weight replay detection framework for voice controlled IoT devices. *IEEE Journal of Selected Topics in Signal Processing*, *14*(5), 982–996.

Manoj, T., Makkithaya, K., & Narendra, V. G. (2023). A trusted IoT data sharing and secure oracle-based access for agricultural production risk management. *Computers and Electronics in Agriculture*, *204*, 107544.

Mishra, A., & Ray, A. K. (2022). A novel layered architecture and modular design framework for next-gen cyber physical system. *2022 International Conference on Computer Communication and Informatics (ICCCI)*, 1–8.

Othaman, N. N. C., Isa, M. N. M., Hussin, R., Zakaria, S., & Isa, M. M. (2021). IoT based soil nutrient sensing system for agriculture application. *Int. J. Nanoelectron. Mater*, *14*, 279–288.

Panoff, M., Dutta, R. G., Hu, Y., Yang, K., & Jin, Y. (2021). On sensor security in the era of IoT and CPS. *SN Computer Science*, *2*(1), 51.

Paris, I. L. B. M., Habaebi, M. H., & Zyoud, A. M. (2023). Implementation of SSL/TLS security with MQTT protocol in IoT environment. *Wireless Personal Communications*, *132*(1), 163–182.

Parween, S., Hussain, S. Z., Hussain, M. A., & Pradesh, A. (2021). A survey on issues and possible solutions of cross-layer design in Internet of Things. *Int. J. Comput. Networks Appl*, *8*(4), 311.

Pengpeng, Y., Teng, F., Zhu, W., Shen, C., Chen, Z., & Song, J. (2025). Cloud–edge–device collaborative computing in smart agriculture: architectures, applications, and future perspectives. *Frontiers in Plant Science*, *16*, 1668545.

Pierce, F. J., & Elliott, T. V. (2008). Regional and on-farm wireless sensor networks for agricultural systems in Eastern Washington. *Computers and Electronics in Agriculture*, *61*(1), 32–43.

Piikki, K., Söderström, M., Eriksson, J., Muturi John, J., Ireri Muthee, P., Wetterlind, J., & Lund, E. (2016). Performance evaluation of proximal sensors for soil assessment in smallholder farms in Embu County, Kenya. *Sensors*, *16*(11), 1950.

Quan, M. K., Pathirana, P. N., Wijayasundara, M., Setunge, S., Nguyen, D. C., Brinton, C. G., Love, D. J., & Poor, H. V. (2025). Federated learning for cyber physical systems: a comprehensive survey. *IEEE Communications Surveys & Tutorials*.

Romaniuk, S. N., & Omona, D. A. (2021). Uganda's Cyber Security Capacities and Challenges. *Companion to Global Cyber-Security Strategy*, 573–632.

Sadik, M. , et al. (2021). (n.d.). • *Energy-efficient and secure communication for smart agriculture: Challenges and solutions. Sensors.*

Sathya, D., Thangamani, R., & Balaji, B. S. (2024). The revolution of edge computing in smart farming. In Intelligent Robots and Drones for Precision Agriculture (pp. 351–389). Springer.

Srivastava, P., Shukla, A., & Bansal, A. (2021). A comprehensive review on soil classification using deep learning and computer vision techniques. *Multimedia Tools and Applications*, *80*(10), 14887–14914.

Tirumala Rao, Mr. P., Balaka Anil, Siddhartha, G., Shyam, Y., & Pawan Rao, B. (2024). SMART FARMING DECISION SUPPORT SYSTEM FOR PRECISION AGRICULTURE. *Journal of Nonlinear Analysis and Optimization*, *15*(01), 1751–1758. doi: 10.36893/jnao.2024.v15101.1751-1758

Ul Haq, S., Singh, Y., Sharma, A., Gupta, R., & Gupta, D. (2023). A survey on IoT & embedded device firmware security: architecture, extraction techniques, and vulnerability analysis frameworks. *Discover Internet of Things*, *3*(1), 17.

Wang, X., Wu, Q., Zeng, H., Yang, X., Cui, H., Yi, X., Piran, M. J., Luo, M., & Que, Y. (2025). Blockchain-Empowered H-CPS Architecture for Smart Agriculture. *Advanced Science*, 2503102.

Wang, Y., & Yang, Y. (2024). A novel secure and energy-efficient routing method for the agricultural internet of things using whale optimization algorithm. *Journal of Cyber Security and Mobility*, *13*(4), 725–749.

Xu, J., Wei, L., Wu, W., Wang, A., Zhang, Y., & Zhou, F. (2020). Privacy-preserving data integrity verification by using lightweight streaming authenticated data structures for healthcare cyber–physical system. *Future Generation Computer Systems*, *108*, 1287–1296.

Yazdinejad, A., Zolfaghari, B., Azmoodeh, A., Dehghantanha, A., Karimipour, H., Fraser, E., Green, A. G., Russell, C., & Duncan, E. (2021a). A review on security of smart farming and precision agriculture: Security aspects, attacks, threats and countermeasures. *Applied Sciences*, *11*(16), 7518.

Zhukabayeva, T., Zholshiyeva, L., Karabayev, N., Khan, S., & Alnazzawi, N. (2025). Cybersecurity solutions for industrial internet of things–edge computing integration: Challenges, threats, and future directions. *Sensors*, *25*(1), 213.

©2026 by the Authors. This Article is an open access article distributed under the terms and conditions of the Creative Commons Attribution (CC BY) license (http://creativecommons.org/licenses/by/4.0/)