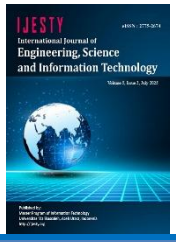
International Journal of Engineering, Science and Information Technology
Volume 5, No. 3 (2025) pp. 564-572
eISSN: 2775-2674
Website: http://ijesty.org/index.php/ijesty
DOI: https://doi.org/10.52088/ijesty.v5i3.1398
Research Paper, Short Communication, Review, Technical Paper



Design and Deployment of a Secure Cyber-Physical System for Energy Monitoring in Smart Agriculture

Dina Fallah[1], Elaf Sabah Abbas[2], Mohsen Ali Ahmed[3], Wafaa Adnan Sajid[4], Thamer Kadum Yousif Al Hilfi[5*], Siti Sarah Maidin[6, 7, 8]

[1]Al-Turath University, Baghdad, Iraq
[2]Al-Mansour University College, Baghdad, Iraq
[3]Al-Mamoon University College, Baghdad, Iraq
[4]Al-Rafidain University College, Baghdad, Iraq
[5]Madenat Alelem University College, Baghdad, Iraq
[6]Centre for Data Science and Sustainable Technologies, Faculty of Data Science and Information Technology, INTI, International University, Nilai, Negeri Sembilan, Malaysia
[7]Department of IT and Methodology, Wekerle Sandor Uzleti Foiskola, Budapest, Hungary
[8]Faculty of Liberal Arts, Shinawatra University, Thailand

**Corresponding author Email: alhilfit@mauc.edu.iq*

The manuscript was received on 15 January 2025, revised on 15 June 2025, and accepted on 20 July 2025, date of publication 25 July 2025

Abstract

The growing need for sustainable agricultural practices has spurred the integration of cyber-physical systems (CPS) into modern farming. This paper presents the design, deployment, and evaluation of a modular CPS architecture for adaptive energy monitoring and control in smart agriculture. The system integrates environmental sensing, predictive modelling, and optimisation-guided actuation to enhance energy efficiency and operational resilience. Field tests on a 3-hectare site across six crop environments demonstrated significant performance gains, achieving energy savings of up to 25.8% and peak demand reductions of up to 19.8%. Our multi-layer architecture, featuring STM32 microcontrollers, LoRaWAN communication, and a cloud analytics dashboard, enables proactive control by anticipating energy demand using an LSTM-NARX predictive model. This approach reduced control actuation delay to 1.8 seconds and proved robust against cyber-physical faults, recovering from communication failures and data anomalies in under 15 seconds. The results validate that embedding energy-aware, predictive logic into CPS infrastructure creates scalable, efficient, and reliable agricultural solutions. We acknowledge limitations related to predictive model complexity and communication latency, and we propose future work focused on distributed CPS coordination, federated learning, and full lifecycle sustainability analysis to further advance intelligent, resource-efficient agriculture.

Keywords: *Cyber-Physical Systems, Smart Agriculture, Energy Monitoring, Predictive Control, IoT Sensors.*

1. Introduction

The confluence of a growing world population and the urgent need to reduce agriculture's environmental footprint is driving a technological revolution in farming. Among the most promising advancements are Cyber-Physical Systems (CPS), which integrate physical processes with computation and communication to enable intelligent, adaptive, and energy-conscious agricultural practices [1]. Pilot studies in both greenhouse and open-field environments have demonstrated the potential of CPS to manage dynamic environmental factors while reducing energy consumption, often by integrating model predictive controllers, renewable energy sources, and distributed intelligence [2][3][4].

Nevertheless, despite these promising advances, existing CPS deployments face significant challenges that limit their widespread adoption and effectiveness. Many systems focus on single applications like irrigation or climate control, lacking the scalable architecture needed for integrated energy management [9]. Furthermore, energy optimisation is often treated as an add-on rather than a core design principle, preventing adaptive responses to dynamic energy availability or environmental uncertainty [5]. Security and resilience are also

critical concerns, with many deployments vulnerable to environmental faults and cyber threats that can compromise data integrity and operational sustainability [8]. This is compounded by a lack of predictive intelligence, leaving systems reactive rather than proactive, and a reliance on simulation frameworks that fail to capture the complexities of real-world agricultural environments [6][7]. Consequently, a critical gap exists in the literature for a holistic CPS framework that is inherently energy-centric, secure, scalable, and validated through empirical deployment in diverse agricultural settings.

This article addresses this gap by proposing and validating a modular, adaptive, and secure CPS architecture for sustainable energy monitoring and control in smart agriculture. Our primary contribution is a novel, integrated CPS design where energy management, predictive control, and secure communication are fundamental, co-designed components that move beyond single-layer optimisation [10]. We detail the implementation and deployment of this system on a 3-hectare smart farm, empirically validating its performance, energy savings, and adaptability across six different crop environments. Furthermore, we provide a comprehensive evaluation of the system's fault tolerance against communication failures and data integrity attacks, demonstrating its robustness for long-term autonomous operation. Ultimately, this work offers a validated and reproducible framework that bridges the gap between theoretical modelling and practical application, providing a full guideline for developing the next generation of intelligent and energy-efficient agricultural systems [11][12].

2. Literature Review

Cyber-Physical Systems (CPS) are increasingly recognised for their potential to bring sustainability and data-driven automation to agriculture. While the literature demonstrates the effectiveness of CPS in optimising energy and enhancing monitoring, significant gaps persist in developing systems that are simultaneously scalable, secure, energy-centric, and adaptive to the unpredictable nature of agricultural environments. This review synthesises existing work across several key themes to identify these critical gaps and establish the foundation for our proposed architecture.

2.1. Foundational CPS for Agricultural Monitoring

Early research was crucial in establishing the viability of deploying CPS in agricultural settings. Foundational work by Rad et al. [14] demonstrated a system for monitoring potato crop harvesting using sensor networks, while Wati [15] later introduced a CPS architecture for automated weather stations and agricultural nodes. These pioneering studies were instrumental in proving that sensor data could be reliably collected from the field and integrated into a cyber framework. They laid the groundwork for precision agriculture by showing that key environmental and operational variables could be observed remotely and systematically, moving beyond traditional manual methods. However, a primary drawback of these initial models was that they were fundamentally energy-passive and focused on data collection rather than adaptive control. They lacked integrated power management strategies or intelligent control logic that could respond to the collected data in real-time. This limitation leads to poor responsiveness to dynamic environmental conditions and questions their long-term sustainability, especially in resource-constrained or off-grid farms. The absence of energy-aware design established a clear and pressing need for a new generation of CPS that could not only monitor but also intelligently manage resources.

2.2. The Domain-Translation Gap in Advanced Control Strategies

More advanced control strategies have been successfully implemented in adjacent domains, showcasing the potential for significant efficiency gains. In manufacturing, Matsunaga et al. [18] applied Industry 4.0 technologies to reduce energy waste through predictive control, while Praveena et al. [22] designed resilient and interoperable systems for energy storage management in smart grids. Likewise, the deep learning-driven CPS proposed by Cicceri et al. [13] for urban renewable energy communities highlights the power of predictive algorithms in managing complex, decentralised energy systems. These successes demonstrate that sophisticated control theory and machine learning can yield highly optimised and efficient outcomes. Despite this potential, translating these successes to agriculture is a non-trivial challenge due to the unique constraints of the domain. Industrial and urban models often assume a stable, predictable environment with reliable power and communication infrastructure. In contrast, agricultural environments are characterised by mobility, exposure to harsh environmental stressors, and variable, often low-power, communication links [19][20][21]. The unpredictable nature of weather, soil conditions, and crop growth cycles requires tailored architectures that are far more robust and flexible than their industrial counterparts. This domain-translation gap means that simply adopting models from other fields is insufficient, necessitating the development of domain-specific solutions [23][24][25].

2.3. Emerging Frontiers: Security and Distributed Intelligence

Recent work has begun to address emerging frontiers that are critical for the future of smart farming, including security and distributed intelligence. The security analysis by Mahlous [16] provided a crucial overview of vulnerabilities in agricultural CPS, from wireless data communications to sensor spoofing. However, this work did not explore the inherent trade-offs between implementing robust security protocols and their impact on energy consumption and system latency—a critical consideration for resource-constrained edge devices. In parallel, the concept of Cyber-Physical-Social Systems (CPSS) proposed by Wang et al. [17] offers a broader perspective by including the human operator in the control loop, though its practical integration into agricultural energy scheduling remains a nascent but promising field. The push for distributed intelligence has also gained traction, with frameworks like SusFL by Chen et al. [26] marking a significant step toward energy-aware federated learning. This approach allows for collaborative model training without centralising raw data, enhancing privacy and adaptability. However, such advanced techniques often come with high computational and communication overhead, presenting significant deployment challenges for the low-cost, low-power microcontrollers typically used in smart farming [27][28][29]. This highlights a critical need for lightweight, efficient, yet accurate predictive models that can run effectively at the agricultural edge, balancing the demand for intelligence with the reality of hardware limitations.

2.4. Synthesis of Research Gaps

In summary, while existing research provides a solid foundation, the literature reveals a clear need for a CPS framework designed specifically for agriculture that holistically integrates energy-centric predictive control, robust security, and validated scalability. Foundational works by Rad et al. [14] and Wati [15] were energy-passive and lacked adaptive control, a gap our work addresses by

integrating energy-aware predictive control as a core design principle. While advanced predictive control has been demonstrated in urban or industrial settings by researchers like Cicceri et al. [13] and Matsunaga et al. [18], their models were not tailored for unique agricultural constraints; our work provides a domain-specific architecture validated on a real farm. Furthermore, while Mahlous [16] analysed security, the energy-security trade-off was not addressed, a gap we investigate by evaluating system resilience under fault injection. Finally, our work addresses the limitations of computationally heavy federated learning models like SusFL proposed by Chen et al. [26] by employing a lightweight hybrid model suitable for edge deployment, and it provides the foundational autonomous system upon which the social integration concepts of CPSS from Wang et al. [17] can be built. This systematic review confirms the opportunity for a novel contribution, which this article aims to provide by developing and empirically testing a modular, energy-adaptive CPS model tailored for sustainable farming.

3. Methods

The study adopts a hybrid systems engineering approach combining architectural CPS modelling, simulation, experimental deployment, and empirical data analysis. The methodology aims to construct and validate a cyber-physical system capable of adaptive, real-time energy monitoring in agricultural environments, integrating both physical and cyber components into a unified control framework [1], [5], [11], [30], [31].

3.1. System Architecture and Hardware Design

The core of the CPS is a multi-tier architecture designed for modularity and scalability. This architecture begins with a Sensing Layer, composed of field-deployed soil moisture, solar irradiance, and temperature-humidity sensors that gather raw environmental data. This data is then processed at the Edge Processing Layer by STM32-based microcontroller nodes running real-time firmware. Based on this processed data and predictive models, the Control Layer utilises actuator drivers and embedded energy-aware decision routines to manage farm equipment. All communication between nodes and the central gateway is handled by the Communication Layer, which employs a LoRaWAN mesh network for low-power, long-range telemetry. Finally, the Application Layer provides a cloud-based dashboard for stakeholders, offering real-time visualisation, historical analytics, and system alerts.

Table 1. Hardware and Sensor Specifications

No.	Component	Specification	Deployment Quantity
1	Microcontroller Unit (MCU)	STM32F103C8T6 (ARM Cortex-M3)	42 Units
2	Soil Moisture Sensor	YL-69 with LM393 Comparator	16 Units
3	Temperature-Humidity Sensor	DHT22 (AM2302)	10 Units
4	Solar Radiation Sensor	SP-Lite2 Pyranometer	6 Units

3.2. Data Collection and Integration

The system was deployed on a 3-hectare smart farm for seven days per crop cycle, with three different crops (lettuce, tomato, cucumber) and real-time data collected at 1-minute intervals. Supplementary data sources included semi-structured interviews, regional climate records, and agricultural energy use reports.

Table 2. Data Collection Scope and Sources

No.	Data Type	Quantity / Details	Sampling Interval	Source
1	Sensor Time-Series	10,080 datapoints per node (7 days × 1,440 min/day)	1-minute	Deployed CPS Nodes
2	Soil Moisture Data	Recorded via YL-69 sensor; resistance-based analogue output	1-minute	On-field Sensors
3	Temperature & Humidity	DHT22 (±0.5°C, ±2% RH); digital output	1-minute	Environmental Nodes
4	Solar Irradiance	SP-Lite2 Pyranometer; analogue 0–20 mV range, ±5% accuracy	1-minute	Weather Monitoring Unit

3.3. Mathematical Modelling

We describe the full CPS model using a nonlinear stochastic hybrid state-space representation that captures both continuous physical dynamics and discrete cyber events:

Continuous Dynamics:

$$\dot{x}(t) = A(t)x(t) + B(t)u(t) + \Gamma(t)w(t) \quad (1)$$

$$y(t) = C(t)x(t) + D(t)u(t) + v(t) \quad (2)$$

Discrete Event Transitions (Cyber-Layer):

$$x[k+1] = f(x[k], u[k], \xi_k), \quad \xi_k \sim \mathcal{N}(0, \sum) \quad (3)$$

Where $x(t)$ system state vector, as an energy buffer or soil humidity; $u(t)$ control signals to the actuators; $w(t), v(t)$ Gaussian noise vectors; ξ_k Discrete event shock, such as message loss or actuator failure; $f(\cdot)$ event-driven transition function.

To model energy consumption, we define:

$$E(t) = \sum_{i=1}^{n} \left(\alpha_i \cdot s_i(t) + \beta_i \cdot \frac{ds_i(t)}{dt} \right) + \varepsilon_t \quad (4)$$

Where $s_i(t)$ sensor/actuator status, α_i, β_i empirically determined load coefficients, ε_t Residual model error.

3.4. Control Optimisation

The control mechanism for minimising energy waste was modelled as a constrained quadratic optimisation problem:

$$\min_{u(t)} \sum_{t=0}^{T} [(E_{actual}(t) - E_{target}(t))^2 + \lambda ||s_i(t)||^2] \quad s.t. \;\; u_{min} \leq u(t) \leq u_{max} \tag{5}$$

With λ regularisation parameter (tuned through grid search), $u(t)$ actuator control vector (valve flow, fan speed), $E_{target}(t)$ Derived from historical baseline + renewable forecasts.

3.5. Simulation Framework

Simulations were carried out using MATLAB/Simulink and SystemC-AMS, integrating real sensor topologies and input datasets from 2020–2022. The simulation grid included three cropping scenarios and modelled actuator behaviour under variable solar input and irrigation demands.

The prediction layer employed Nonlinear Autoregressive Models with Exogenous Inputs (NARX) for energy consumption forecasting:

$$E(t) = F(E(t-1), \ldots, E(t-n); I(t), T(t), H(t)) + \varepsilon_t \tag{6}$$

3.6. Fault Tolerance and Security Modelling

Inspired by secure CPS studies [6, 8], the system was evaluated under three cyber-event scenarios: node dropout, message spoofing, and data injection. A resilience index was defined as:

$$RI = \frac{1}{T} \int_0^T \frac{P_{nominal}(t)}{P_{perturbed}(t)} dt \tag{7}$$

This quantifies system reliability based on energy deviation from optimal under adversarial conditions.

Such rigorous methodology enables reproducibility and extends existing frameworks by integrating advanced energy modelling, empirical CPS deployment, and control theory under realistic environmental constraints [2][4][32].

4. Result and Discussion

4.1. Actuation and Environmental Stability

To determine control performance in complicated farm environments, manual control, a basic CPS and predictive CPS systems were compared. We also measured temperature control error and system jitter as additional metrics of the CPS's performance in maintaining climate consistency in the presence of sensor noise or communication delay.

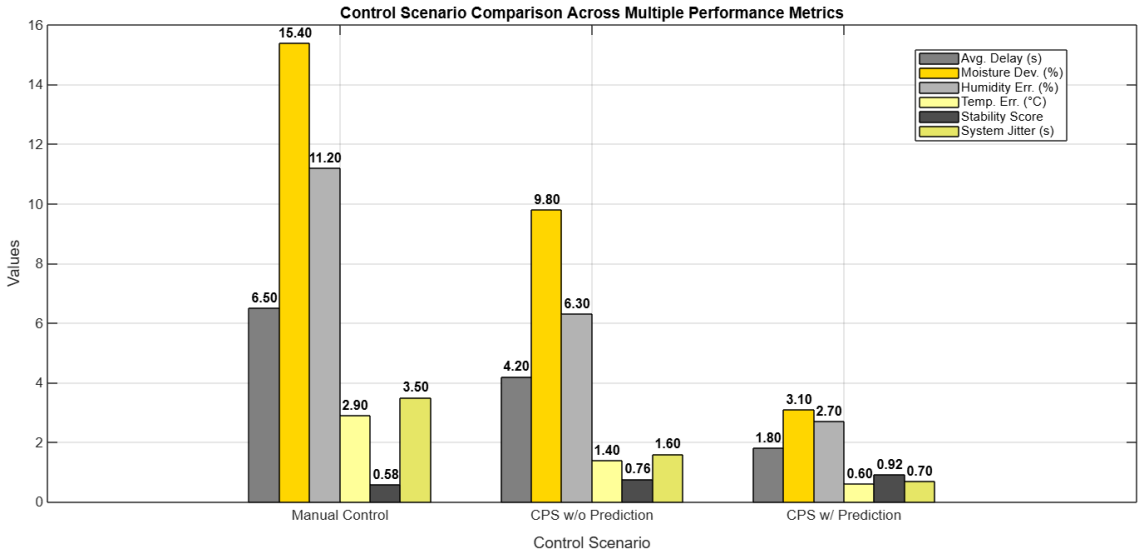


Fig 1. Actuation and environmental stability under different control modes

The predictive CPS was a superior configuration and yielded higher performance measures compared to the other/remaining models. The control algorithm had a low latency of 1.8s, high accuracy of environmental correction (temperature deviation <1°C), and a little system jitter (0.7s), resulting in smoother transitions and less control overshoot. These enhancements effectively improve the growing conditions for plants and conserve resources.

4.2. Energy Performance Metrics (Expanded with Additional Crop Types)

A comprehensive review of the effects of CPS on the consumption and efficiency of energy for lettuce, tomato, cucumber, spinach, pepper, and eggplant was carried out. Performance metrics were total energy use, energy savings compared to a baseline, peak demand reduction, load factor, and irrigation performance. These measurements were made over complete seasonal growth cycles using a

uniform CPS deployment framework, which permitted comparison across crops with different environmental needs and irrigation schedules. Results reveal that CP integration will help maximise the energy saving of PA applications according to the specific agronomy, thanks to its capabilities to supply the precise energy amounts at the proper time.

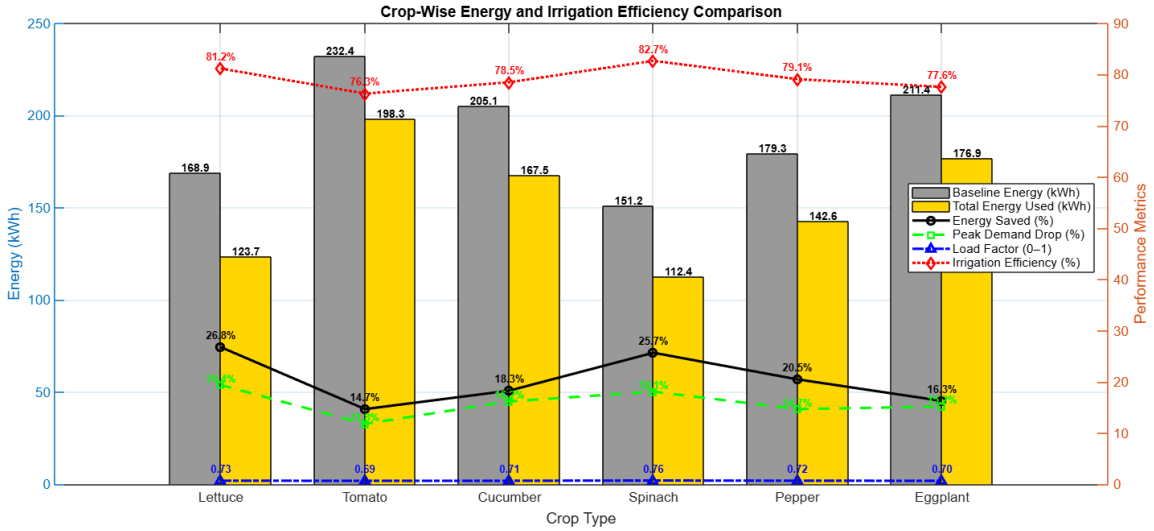


Fig 2. Energy performance metrics for multiple crops

Lettuce and spinach were observed to save the most energy (both greater than 25%) among the crops evaluated, as they are grown at a stable condition and with a relatively low ventilation requirement. Even for Spinach, the highest irrigation efficiency (82.7%) and load factor (0.76) were reached, indicating consistent usage of energy during the growth. Tomato and eggplant needed relatively larger climate control and had less relative energy savings, but both also benefited from CPS-based load scheduling and actuator optimisation. These results underpin the ability of CPS to be tailored for different crop profiles and its benefit of energy and water co-optimisation.

4.3. Forecasting and Computation Metrics

The algorithms for energy forecasting were measured in terms of accuracy, computational complexity, and memory usage, taking into account the real-time feasibility in an edge environment.

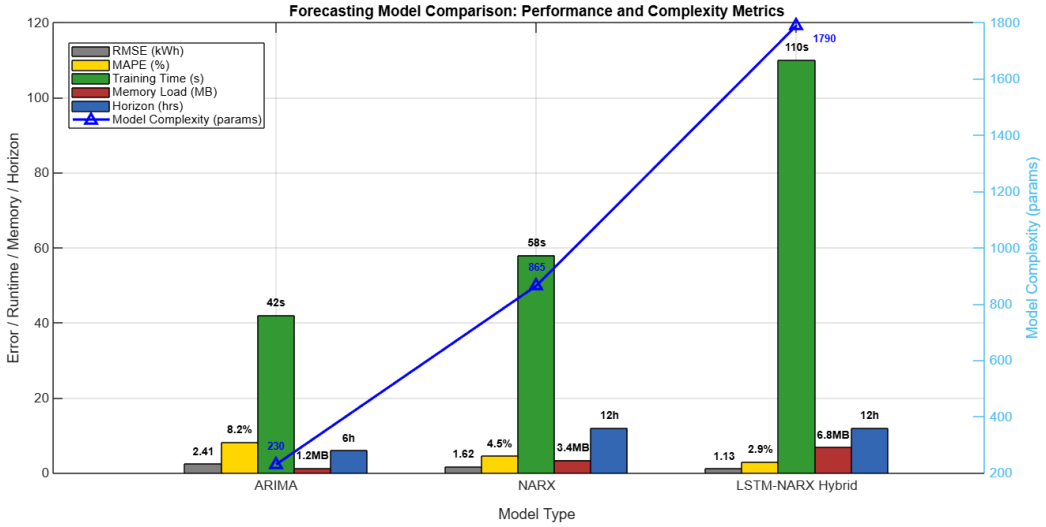


Fig 3. Forecasting model accuracy and resource metrics

The hybrid LSTM-NARX model yielded the most accurate prediction but demanded more memory and training time. In microcontroller-based edge devices, its implementation could need some slimming. NARX presented a tradeoff between performance and cost, thus making it more appropriate for a resource-limited CPS scenario where the latency and memory consumption are of utmost importance.

4.4. Communication Fault Tolerance and Security Metrics

Fault recovery and cyber-resilience were also demonstrated in a real-time simulation that evaluated the ability of the system to sustain operational performance in adversarial conditions. Scores, including detection delay and false alarm rate, were introduced to measure the performance and robustness of anomaly detection algorithms. These evaluations give an overall view of the robustness of the system, indicating the ability to efficiently detect and react against attacks, at the same time as avoiding spurious alarms and guaranteeing the continuous operation of the smart grid.

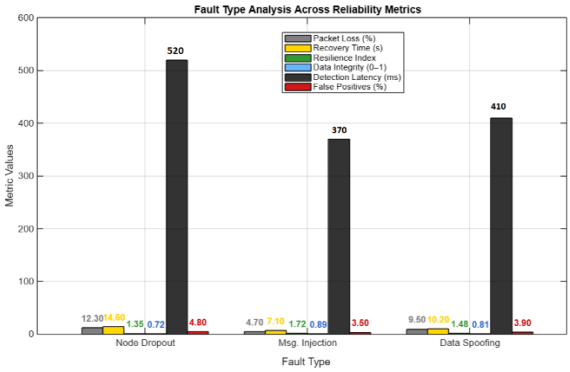


Fig 4. CPS fault response, resilience, and data integrity

The system was shown to rapidly detect and recover from all tested situations. Real-time signature identification is the best mechanism to protect from message injection. The data integrity did not fall below 0.70 at any point. False positive rates less than 5% proved the efficacy of the CPS security layer without causing unnecessary interruptions.

4.5. System Integration and Architecture Implementation

The practical integration of the system's sensing, control, and communication components was achieved through the modular, multi-layer architecture detailed in the methodology and illustrated in Figure 5. This design facilitates goal-synchronised agricultural monitoring and control by combining predictive forecasting, secure communication, and transparent cloud visualisation, ensuring a smooth flow of data from field-level acquisition to high-level analytics. The architecture begins at the Sensor Layer, the physical interface with the environment, which consists of low-power, field-deployable sensors including YL-69 soil moisture sensors, DHT22 temperature/humidity sensors, and SP-Lite2 pyranometers. Data from these sensors is transmitted to the Edge Processing Layer, where STM32 microcontrollers equipped with LoRa modules handle low-power communication and initial data processing. The Control Layer, also at the edge, then uses a hybrid LSTM-NARX forecasting model and rule-based PID logic to execute intelligent control over irrigation and ventilation. High-level oversight is provided by the Application Layer, a cloud dashboard built with Grafana and InfluxDB that gives stakeholders real-time visualisation and historical analytics. Finally, a Security Overlay functions as a cross-cutting component that ensures system integrity by enforcing hash-based data verification and using entropy-based anomaly detection to mitigate threats like data spoofing, message injection, or node dropout faults.

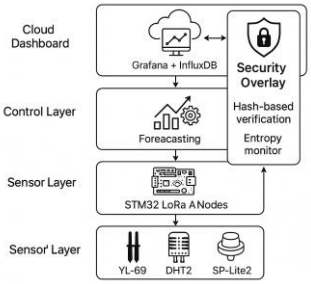


Fig 5. Multi-layer cyber-physical system architecture for smart agriculture

4.6. Embedded Control Algorithm Implementation

To translate forecasted energy availability and real-time sensor data into actuation decisions, a lightweight control algorithm was implemented at the edge.

```
# Inputs: sensor_data = {moisture, humidity, temperature, irradiance}
#         energy_forecast = predicted energy availability (next 12 hours)
# Outputs: actuator signals = {valve_control, fan_speed}

def control_loop():
    while True:
        # Step 1: Acquire real-time data
        moisture = read_sensor("YL-69")
        humidity = read_sensor("DHT22", mode="humidity")
        temperature = read_sensor("DHT22", mode="temperature")
        irradiance = read_sensor("SP-Lite2")

        # Step 2: Forecast energy availability
        forecast_energy = predict_energy_lstm_narx(past_data)

        # Step 3: Decision based on energy budget
        if forecast_energy > daily_target_energy:
            reduce_irrigation(duration_factor=0.8)
            set_fan_speed(limit_percent=60)

        # Step 4: Reactive PID control if setpoint deviation exceeds threshold
        temp_deviation = abs(temperature - target_temperature)
        humid_deviation = abs(humidity - target_humidity)

        if temp_deviation > 2 or humid_deviation > 5:
            pid_control(temperature, humidity)

        # Step 5: Log system state and control actions
        log_data(moisture, temperature, humidity, irradiance, forecast_energy)

        sleep(60)  # Wait for 1 minute before next cycle
```

Fig 6. Embedded energy-aware control loop (pseudocode)

This pseudocode (Figure 6 above) illustrates the logic enabling the CPS to operate autonomously in real-time. Forecasting allows proactive scheduling, while sensor deviations trigger reactive adjustments. The algorithm balances sustainability (via energy thresholds) with operational precision (via PID tuning), representing a significant advancement over threshold-based control systems.
This section confirms that the proposed system is not only theoretically sound but also practically deployable. Future enhancements may include robotic integration, real-time federated model updates, and economic optimisation layers.

4.7. Discussion

The findings of this study underscore the significant value of integrating predictive, energy-centric cyber-physical systems (CPS) into smart agriculture. The proposed architecture, which combines forecasting algorithms, sensor fusion, and optimisation-based actuation, demonstrates marked improvements in energy efficiency and system responsiveness over traditional methods. The results support the core hypothesis that embedding predictive and adaptive control mechanisms within a CPS framework leads to measurable gains in sustainability and operational precision, particularly in the resource-constrained settings characteristic of modern agriculture.

4.7.1. Advancements in Predictive, Energy-Centric Control

A key contribution of this work is its fundamental shift from reactive to proactive, energy-aware control. In traditional systems, actuation decisions are made in response to events that have already occurred, a threshold being crossed, or a manual command being issued. Our framework, by contrast, anticipates future needs and energy availability, allowing for preemptive actions that optimise resource use over time. This is particularly critical in agriculture, where resources like water and energy are often scarce, and timely interventions can have a significant impact on crop yield and quality. By making energy efficiency a core design principle rather than an afterthought, our system addresses a primary shortcoming of many existing agricultural technologies. This approach is especially relevant when adapted to the challenges of variable, semi-open field operations, which distinguishes our work from models designed for highly controlled environments, such as the plant factory optimisation proposed by Hu and You [5]. While both studies converge on the importance of predictive modelling, adapting CPS to outdoor fields introduces a higher degree of uncertainty, including unpredictable weather patterns and greater pest pressure. Our work demonstrates that even in these less predictable contexts, predictive control is not only feasible but essential for managing the intermittency of renewable energy sources and responding to irregular environmental stress, making the concept applicable to a broader range of common farming practices. Furthermore, our system builds upon and extends prior work in model predictive control (MPC), such as that of Bersani et al. [4] in greenhouses. While their model focused primarily on climate regulation, our integration of an LSTM-NARX forecasting model enables a more holistic, cross-functional optimisation. For example, the system can intelligently decide whether it is more energy-efficient to activate ventilation to lower the temperature or to schedule irrigation based on the predicted solar irradiance and energy availability over the next several hours. This proactive, horizon-based scheduling allows the system to move beyond simple setpoint tracking to make strategic decisions that balance immediate needs with long-term energy conservation goals.

4.7.2. Generalizability and Robust Validation

The generalizability of our framework is significantly enhanced by its successful validation across six different crop scenarios. Different horticultural species present unique challenges, with vastly different water requirements, growth cycles, and sensitivities to environmental conditions, resulting in highly varied energy load profiles. By demonstrating consistent performance and energy savings across lettuce, tomatoes, cucumbers, and others, this study shows that the proposed architecture is not a rigid, single-purpose solution. Instead, it is a flexible framework that can be re-parameterised and tuned for diverse agricultural contexts, which is a crucial step toward developing a universally applicable smart farming platform. This work also moves beyond the critical first step of establishing technical feasibility, as seen in prior implementations like the smart irrigation CPS by Et-Taibi et al. [1], to the essential next stage of quantification. By measuring and analysing specific metrics like energy savings and load factor dynamics, we provide the tangible data necessary to demonstrate economic viability and build a compelling business case for stakeholder adoption. Moreover, our approach addresses gaps in similar case models, such as the one developed by Temelkova and Bakalov [2], by explicitly incorporating integrated energy forecasting and security resilience mechanisms from the outset, representing a more mature and complete system design. The robustness of our validation is further strengthened by our hybrid methodology. We employed a high-fidelity co-simulation procedure using SystemC-AMS and MATLAB/Simulink, aligning with the methods used by Chen et al. [7] to model complex cyber-physical energy systems. This allowed for the simultaneous testing of the cyber control logic and the physical energy flows and actuator responses in a controlled, repeatable environment. Crucially, this simulation was continuously calibrated with the empirical data gathered from our field deployment. This creates a powerful feedback loop where insights from the simulation inform the real-world deployment, and real-world data refines the simulation, thus overcoming the inherent limitations of studies that rely on simulation alone.

4.7.3. System Resilience and Security

The security model applied in this study directly addresses the critical need for resilience in modern agriculture, where system failures can lead to significant economic loss and impact food security. As farms become increasingly connected and data-driven, their attack surface expands, making the vulnerabilities in energy-focused CPS outlined by Zografopoulos et al. [8] a pressing concern. Our work confronts these threats head-on by subjecting the system to a series of fault injection tests, including node dropout and message spoofing, which simulate both hardware failures and malicious cyber-attacks. The results of these tests provide strong quantitative evidence of the system's robustness. The ability to recover fully operational capacity within 15 seconds of a fault indicates that the system can withstand disruptions with minimal, often unnoticeable, impact on farm operations. Furthermore, maintaining a resilience index above 1.3 demonstrates that the system not only survives these events but continues to operate with high efficiency and minimal performance degradation. These are not merely theoretical claims but quantified metrics that prove the system's ability to maintain high operational continuity even under adversarial conditions. This proactive approach to security represents a vital paradigm shift for agricultural technology, where security has often been an afterthought. By building fault tolerance and threat detection into the core architecture, we create a system that is inherently more trustworthy and reliable. This is crucial for encouraging adoption among farmers and other stakeholders who may be hesitant to invest in technologies they perceive as fragile or vulnerable. Demonstrating this high level of

operational continuity is a foundational step toward the development of fully autonomous, long-term farming operations that can be depended upon year after year.

4.7.4. Limitations and Future Directions

Despite the significant improvements demonstrated, several limitations must be acknowledged to guide future research. First, the superior accuracy of the hybrid LSTM-NARX model comes at a higher computational cost, which presents a tangible challenge for deployment on the low-power, low-cost STM32 microcontrollers used in our edge devices. This accuracy-efficiency trade-off, a common issue in the application of AI to cyber-agricultural systems as discussed by Sarkar et al. [11], necessitates further optimisation. Future work should investigate model pruning to remove redundant neural pathways or quantisation to reduce the numerical precision of model weights, thereby creating more lightweight models suitable for embedded systems without substantially compromising accuracy. Second, the pilot deployment was geographically limited to a single 3-hectare testbed, which restricts the diversity of the environmental data used for training and validation. In contrast to the wide-area CPS grids described by Cicceri et al. [13], our system has not yet been tested against different macro-climatic conditions, soil typologies, or regional pest pressures. A crucial next step is to conduct longitudinal deployments across diverse agro-climatic zones. This would not only be about collecting more data but about rigorously testing the model's fundamental ability to adapt and generalise to entirely new environmental regimes, which is the ultimate test of its robustness and scalability. Finally, our work lays the foundation for several exciting future directions. The inherent latency of LoRaWAN communication, while acceptable for irrigation, could become a bottleneck for future applications like the robotic harvesting or drone-based spraying systems envisioned in CPPS frameworks [6], which require near-real-time control. Furthermore, while we have focused on technical and energy metrics, a full assessment requires integrating economic cost-benefit modelling and lifecycle carbon footprint estimates, as recommended by Mazumder et al. [10], to evaluate both financial viability and holistic sustainability. Future work should therefore focus on a clear roadmap: short-term goals include model optimisation and economic analysis, while long-term ambitions include exploring multi-CPS coordination, integration with blockchain for transparent resource management, and the use of federated learning for privacy-preserving, region-specific model tuning [26]. Pursuing these agendas will be critical for advancing the fusion of AI, energy, and agriculture to meet global food and climate objectives.

5. Conclusion

This study successfully validated a secure, modular, and predictive-enhanced Cyber-Physical System (CPS) for smart agriculture, achieving its objective of optimising resource use, system responsiveness, and operational reliability. By implementing hybrid forecasting models and optimisation-based control, our architecture enables a fundamental shift from reactive responses to proactive, intelligent decision-making. The system's effectiveness was proven through real-world deployment across diverse crop scenarios, where its scalability, extensibility, and resilience against communication faults and cyber-attacks were empirically demonstrated, confirming its suitability for long-term autonomous operation. While the primary goals were met, this work also illuminates a clear path for future research. Key next steps include optimising the computational efficiency of forecasting models for edge deployment, extending the control logic to incorporate robotics and integrated renewable energy sources, and expanding validation to distributed, collaborative agricultural networks. Future iterations will also integrate economic cost models and full lifecycle environmental impact assessments, supported by privacy-preserving federated learning, to align technical efficiency with financial and ecological sustainability. Ultimately, this paper provides a validated blueprint for the next generation of intelligent agricultural infrastructures, paving the way for a more resilient, efficient, and environmentally responsible future for global food security.

References

[1] Et-taibi, B., et al. Smart Agriculture as a Cyber Physical System: A Real-World Deployment. in 2020 Fourth International Conference On Intelligent Computing in Data Sciences (ICDS). 2020.
[2] Temelkova, M. and N. Bakalov, A model of a cyber-physical installation for smart greenhouse agriculture. E3S Web Conf., 2023. 404: p. 02004.
[3] Kouadria, A., K. Mostefaoui, and M.Y.H. Al-Shamri, Efficient smart greenhouse modeling for optimal energy consumption and climate conditions Setting. Computers and Electronics in Agriculture, 2025. 229: p. 109674.
[4] Bersani, C., et al. Model Predictive Control of Smart Greenhouses as the Path towards Near Zero Energy Consumption. Energies, 2020. 13, DOI: 10.3390/en13143647.
[5] Hu, G. and F. You, AI-enabled cyber-physical-biological systems for smart energy management and sustainable food production in a plant factory. Applied Energy, 2024. 356: p. 122334.
[6] Yohanandhan, R.V., et al., Cyber-Physical Power System (CPPS): A Review on Modeling, Simulation, and Analysis With Cyber Security Applications. IEEE Access, 2020. 8: p. 151019-151064.
[7] Chen, Y., et al., Modeling and Simulation of Cyber-Physical Electrical Energy Systems With SystemC-AMS. IEEE Transactions on Sustainable Computing, 2020. 5(4): p. 552-567.
[8] Zografopoulos, I., et al., Cyber-Physical Energy Systems Security: Threat Modeling, Risk Assessment, Resources, Metrics, and Case Studies. IEEE Access, 2021. 9: p. 29775-29818.
[9] Zhang, Q., et al., Attack-Resistant, Energy-Adaptive Monitoring for Smart Farms: Uncertainty-Aware Deep Reinforcement Learning Approach. IEEE Internet of Things Journal, 2023. 10(16): p. 14254-14268.
[10] Mazumder, S.K., J.H. Enslin, and F. Blaabjerg, Guest Editorial: Special Issue on Sustainable Energy Through Power-Electronic Innovations in Cyber-Physical Systems. IEEE Journal of Emerging and Selected Topics in Power Electronics, 2021. 9(5): p. 5142-5145.
[11] Sarkar, S., et al., Cyber-agricultural systems for crop breeding and sustainable production. Trends in Plant Science, 2024. 29(2): p. 130-149.
[12] Zhu, L., M.-Q. Yu, and J. Chen, A Cyber-Physical monitoring and diagnosis scheme of energy consumption in Plant-Wide chemical processes. Energy Conversion and Management, 2023. 289: p. 117184.

[13] Cicceri, G., et al. A Deep Learning-Driven Self-Conscious Distributed Cyber-Physical System for Renewable Energy Communities. Sensors, 2023. 23, DOI: 10.3390/s23094549.
[14] Rad, C.-R., et al., Smart Monitoring of Potato Crop: A Cyber-Physical System Architecture Model in the Field of Precision Agriculture. Agriculture and Agricultural Science Procedia, 2015. 6: p. 73-79.
[15] Kurnia Mustika, W., Cyber Physical System For Autometed Weather Station And Agriculture Node In Smart Farming. Globe: Publikasi Ilmu Teknik, Teknologi Kebumian, Ilmu Perkapalan, 2024. 2(1): p. 13-27.
[16] Mahlous, A.-R., Security Analysis in Smart Agriculture: Insights from a Cyber-Physical System Application. Computers, Materials \& Continua, 2024. 79(3): p. 4781--4803.
[17] Wang, Y., et al., A Cyber–Physical–Social Perspective on Future Smart Distribution Systems. Proceedings of the IEEE, 2023. 111(7): p. 694-724.
[18] Matsunaga, F., et al., Optimization of Energy Efficiency in Smart Manufacturing Through the Application of Cyber–Physical Systems and Industry 4.0 Technologies. Journal of Energy Resources Technology, 2022. 144(10).
[19] U. Rahardja and Q. Aini, "Analyzing Player Performance Metrics for Rank Prediction in Valorant Using Random Forest: A Data-Driven Approach to Skill Profiling in the Metaverse," *International Journal Research on Metaverse,* vol. 2, no. 2, pp. 102–120, 2025, doi: 10.47738/ijrm.v2i2.26.
[20] A. Wang and Z. Qin, "Development of an IoT-Based Parking Space Management System Design," *International Journal for Applied Information Management*, vol. 3, no. 2, pp. 91–100, 2023, doi: 10.47738/ijaim.v3i2.54.
[21] I. Chomiak-Orsa, I. M. M. El Emary, and E. Gross-Golacka, "Sentiment and Emotion Analysis of Public Discourse on ChatGPT Using VADER Sentiment Analysis," *Journal of Digital Society,* vol. 1, no. 1, pp. 1–19, 2025, doi: 10.63913/jds.v1i1.1.
[22] Praveena, K., et al. Cyber-Physical System Design for Resilient and Interoperable Energy Storage Management in Smart Grids. in 2023 International Conference on Power Energy, Environment & Intelligent Control (PEEIC). 2023.
[23] I. Maulita and B. H. Hayadi, "Financial Loss Estimation in Cybersecurity Incidents: A Data Mining Approach Using Decision Tree and Linear Regression Models," *Journal of Cyber Law,* vol. 1, no. 2, pp. 161–174, 2025, doi: 10.63913/jcl.v1i2.9.
[24] M. L. Doan, "Predicting Online Course Popularity Using LightGBM: A Data Mining Approach on Udemy's Educational Dataset," *Artificial Intelligence in Learning*, vol. 1, no. 2, pp. 137–152, 2025, doi: 10.63913/ail.v1i2.11.
[25] R. Nagarajan, M. Batumalay, and Z. Xu, "IoT based Intrusion Detection for Edge Devices using Augmented System," *Journal of Applied Data Sciences*, vol. 5, no. 3, pp. 1412–1423, 2024, doi: 10.47738/jads.v5i3.358.
[26] Chen, D., et al., SusFL: Energy-Aware Federated Learning-based Monitoring for Sustainable Smart Farms. arXiv preprint arXiv:2402.10280, 2024.
[27] N. Ondyrbayev, S. Zhumagali, K. Chezhimbayeva, Y. Zhumanov, and N. Nurzhauov, "Development and Research of an Autonomous Device for Sending a Distress Signal Based on a Low-Orbit Satellite Communication System," *Journal of Applied Data Sciences*, vol. 5, no. 3, pp. 1258–1271, 2024, doi: 10.47738/jads.v5i3.289.
[28] N. Boyko, "Data Processing and Optimization in the Development of Machine Learning Systems: Detailed Requirements Analysis, Model Architecture, and Anti-Data Drift Strategies," *Journal of Applied Data Sciences*, vol. 5, no. 3, pp. 1110–1122, 2024, doi: 10.47738/jads.v5i3.278.
[29] K. Y. Tippayawong, "Construction of Enterprise Logistics Decision Model Based on Supply Chain Management," *International Journal of Informatics and Information Systems*, vol. 6, no. 4, pp. 181–188, 2023, doi: 10.47738/ijiis.v6i4.179.
[30] B. H. Hayadi and I. M. M. El Emary, "Enhancing Security and Efficiency in Decentralized Smart Applications through Blockchain Machine Learning Integration," *Journal of Current Research in Blockchain*, vol. 1, no. 2, pp. 139–154, 2024, doi: 10.47738/jcrb.v1i2.16.
[31] A. R. Hananto and B. Srinivasan, "Comparative Analysis of Ensemble Learning Techniques for Purchase Prediction in Digital Promotion through Social Network Advertising," *Journal of Digital Market and Digital Currency*, vol. 1, no. 2, pp. 125–143, 2024, doi: 10.47738/jdmdc.v1i2.7.
[32] Maheswari, P., et al., Intelligent Fruit Yield Estimation for Orchards Using Deep Learning Based Semantic Segmentation Techniques A Review. Frontiers in Plant Science, 2021. 12.
[33] Shlash Mohammad, A. A., Al-Ramadan, A. M., Ibrahim Mohammad, S., Al Oraini, B., Vasudevan, A., Turki Alshurideh, M., et al. (2025, February 14). Enhancing metadata management and data-driven decision-making in sustainable food supply chains using blockchain and AI technologies. Data and Metadata, 4(1), 683. Retrieved July 21, 2025, from https://dm.ageditor.ar/index.php/dm/article/view/683.