STAP Journal of Security Risk Management

https://www.jsrm.thestap.com/

Secure IoT-Based Smart Agriculture System Using Wireless Sensor Networks for Remote Environmental Monitoring

Mahmood A. Al-Shareeda[1, 2], Laith Badr Najm[2], Ali Ahmed Hassan[2], Sajjad Mushtaq[2], Hussein Abdul Ali[2]

[1] *Basra Technical Institute, Southern Technical University, Basra, 61001, Iraq.*
[2] *Communication Engineering, Iraq University College, Basra, Iraq.*

ARTICLE INFO

Article History

Received: 24-07-2024
Revised: 20-11-2024
Accepted: 22-11-2024
Published: 23-11-2024

Vol.2024, No.1

DOI:
https://doi.org/10.63180/jsrm.thestap.2024.1.4

***Corresponding author.**
Email:
mahmood.alshareedah@stu.edu.iq

Orcid:
https://orcid.org/0000-0002-2358-3785

ABSTRACT

Designing and implementing a secure IoT-based smart agriculture system that uses wireless sensor networks (WSNs) for real-time monitoring to keep the best environment and irrigates automatically. The proposed system is based on the ESP32 microcontroller and incorporates sensors for soil moisture, temperature, humidity, pH, and total dissolved solids (TDS), enabling precise agricultural resource management. The system is powered by solar energy to ensure continuous operation in remote areas or off the grid. Via Transport Layer Security (TLS), data is securely transmitted to the cloud, and device authentication is tokenized through Blynk IoT-a firm favorite among the Internet of Things community with its platform for control. You can control your irrigation and watch over the environment in real time with a mobile application, which means that a person needs only be present half of the time, avoiding waste for both water and electricity. Experimental results demonstrate a high accuracy in environment-sensing that leads to efficient water utilization, and stable, secure communication. The system is a low-cost, scalable solution for modernizing farming operations while addressing potential cybersecurity risks in an IoT agricultural environment.

Keywords: Smart Agriculture, Internet of Things (IoT), Wireless Sensor Networks (WSN), ESP32, Secure Communication, TLS, Soil Moisture Monitoring, Automated Irrigation, Blynk IoT, Precision Farming.

How to cite the article
Al-Shareeda, M. A., Najm, L. B., Hassan, A. A., Mushtaq, S., & Ali, H. A. (2024). Secure IoT-Based Smart Agriculture System Using Wireless Sensor Networks for Remote Environmental Monitoring. STAP Journal of Security Risk Management, 2024(1), 56–66. https://doi.org/10.63180/jsrm.thestap.2024.1.4

1. Introduction

Agriculture, crucially important worldwide, provides food security and employment as well as economic stability. Nevertheless, cumbersome traditional farming methods often consume too much water, need manual labor and have constitutional hardies when it comes to unusual environmental conditions [1–3]. These constraints are especially heavy in remote or resource-poor locations, where real-time control and timely intervention is tough [4–6].

Internet of Things (IoT) coupled with Wireless Sensor Networks (WSNs) has evolved into a smart agricultural solution of boom [7–9]. By arranging occurrences of environmental parameters like soil moisture, temperature, humidity, MagnITUDE, and WATER LEVEL around the farm, farmers can make informed decisions that optimize CROP YEILD– and other resources used on hand [10–12]. With microcontrollers such as ESP32 coupled to a mobile app for" Internet of Things (IoT)," it also supports auto-irrigation and remote system control with limited human intervention [13–15].

However, one significant and often neglected challenge to such systems arises in the right [16, 17]. IoT devices located in agricultural fields have the capacity—for example, if attacked by people seeking attention through violence and conflict—to interrupt irrigation processes or even change sensor readings [18, 19]. For the system to be reliable and have trustworthiness, therefore protecting the security of communication between sensors, controllers, user interfaces is crucial [20, 21].

We present a secure, low-cost, solar-powered smart agricultural system design that takes care of both efficiency and safety. It combines an ESP32-based architecture with multiple environmental sensors and actuators. TLS-encrypted communication channels along with token-based authentication protect data integrity and signal control mechanisms. Mobile applications like Blynk IoT (Internet of Things) offer farmers real-time visualization and control opportunities.

The contributions of this paper are as follows:
• Design and implementation of a wireless sensor network that uses ESP32s to perform real-time monitoring of environmental conditions.
• Development of an automated irrigation system with solar power.
• Integration of a secure communication model based on TLS and access tokens for
Protecting the flow of IoT data.
• Performance evaluation of various parameters in an actual agricultural environment: water efficiency, data reliability and so forth

The remainder of this paper is organized as follows: Section 2 discusses previous work in smart agriculture and IoT security. Section 3 covers the system architecture as well as the model for secure communications. Section 4 explains practical details on implementation. Section 5 gives experimental results of system performance and assessment. Section 6 concludes the paper and suggests directions for further research.

2. Related Works

The necessity for secure data-handling methods turns into increasingly apparent in the age of IoT and widespread deployment of large quantities sensors. Finally, although such technology makes agricultural practice more analytical and effective, whatever great advances and improvements have been made, it remains a mistake not to mention that security is still just as important for remote locations where expenses are low.

2.1 Internet of Everything (IoE) and WSN in Smart Agriculture

For example, Athani et al. (2017) first deployed a soil moisture monitoring point system based on Arduino and neural network technology. Even though their system stressed high precision, it was difficult for non-technical users to use [22]. In the same way, Sayanthan et al. (2018) developed an Arduino based soil moisture analyzer for Case 2 cultivation of eggplant, achieving substantial water savings but without considering any possibilities that data could be falsified or sensors spoofed [23].

With Bhadani and Vashisht, (2019), they developed a sensor-based environment monitoring system to measure soil humidity, temperature, and moisture. Their work tried to make smart farming available and affordable but without providing a secure means of data transfer [24]. With Chew et al. (2020), they developed a wireless soil monitoring system based on the architecture of the Internet of Things. Although this method made irrigation more efficient, it still had weaknesses because data transmission was not encrypted or devices validated [25].

2.2 IoT Security in Agriculture

Hamoodi et al. (2020) implemented a solar-powered automatic irrigation system with a master control using Arduino. Their design was technologically advanced; it was energy-efficient. At the same time, it was an open doorway waiting for unauthorized actuator access through a jamming attack on the shared wireless spectrum [26]. Mir and Ishrat (2020) pointed out the potential of machine learning and plant IoT on earth but also spotted some problems with integrating these two technologies: especially in terms of the security of data and sensor network stability [27]. In their 2022 study, Pramanik et al. integrated wireless communication and automatic irrigation in a basin of loamy soil, achieving over 86% efficiency. However, their report did not take into account either how to encrypt the data or ensure its integrity between transmitter and receiver [28]. Zhu et al.'s (2022) proposed an Arduino-based irrigation system for urban green space biodiversity with real-time control of soil moisture level but without any operation protection, causing the system to be open to potential remote interference [29].

2.3 Secure Smart Farming

Kaur et al. (2024) developed in the cloud a smart irrigation system with both IoT technology and machine learning. Their data was handled by safety protocols like RESTful APIs, and classified KNN or Random Forest, indicating high prediction accuracy. But as we mentioned before their method pays little attention to secure communication at a protocol level and includes an introductory mention of encrypted data transfer [30]. Fern´andez et al. (2023) devised a precision irrigation scheduling system using remotely-collected data, also stressing the diversity within that data. They did not, however, consider how such data could be securely transmitted between remote sensors and cloud-based databases [31]. Taken together, these studies illustrate the enormous potential for applying IoT technology in agriculture. However, it remains glaring that the field suffer a fatal flaw: no one has hitherto learned how to incorporate means of security into these real-time, low-cost units for agricultural monitoring. This present paper intends to fill this hole by proposing a secure, scalable smart farm system based on IoT technology – complete solar autonomy and environmental sensing for field monitoring, combined among others with encrypted communication methods guarantee tamper-resistant operation.

3. System Architecture and Security Design

The section descriptions the system designs and Part integrated structure of sub, data flow as well as a proposed security mechanism to protect sensor signals and control signals within smart agricultural systems. In addition, the architecture is envisaged to provide both real-time environmental monitoring by introducing IT into cultivation, e.g. precision irrigation; but at the same time, it must solve common cybersecurity challenges in IoT applications.

3.1 System architecture

This system is made up of many sensors connected to an ESP32 microcontroller that uses this information to collect environmental data; then sends the results over a wireless network (through the application Blynk IoT) so on a mobile phone platform. In addition, a relay-controlled pump is built to irrigate gardens depending actual sensor readings. As shown in Figure 1, the following system components are presented.

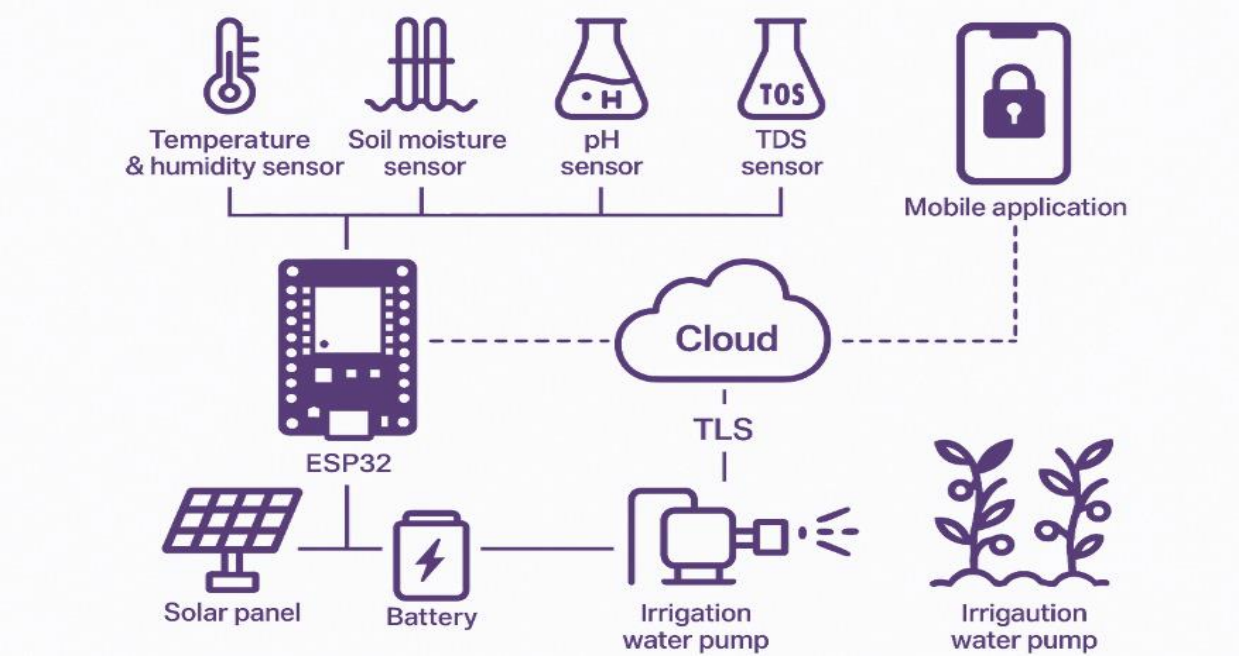


Figure 1. System Architecture

• ESP32: a Wi-Fi/Bluetooth-capable microcontroller responsible for data acquisition, logical processing and network communications to the cloud.
• Sensor: DHT11: Measures temperature and humidity of air. Soil Moisture Sensors (x3): Monitor the moisture content in soil together with nutrients' distribution. PH Sensor: Displays soil/irrigation water acidity or alkalinity levels. TDS Sensor: Data input can help to assess water quality.
• Actuator: Water Pumps (x3): Controlled by relays based on soil sensor data.
• Power supply: Both a solar panel and lithium battery kit give the off-grid system its own energy supply.
The app provides a user interface for farmers to view environmental data such as temperature, humidity and soil water; if need be they may also issue direct orders.

3.2 Network Architecture and Data Flow

A three-tier model is used in the architecture which is oftentimes found in IoT via system design:
• Perception Layer: The physical sensors interact with the environment and send analog / digital signals to the ESP32.
• Network Layer: Data is transmitted sent over the Blynk IoT cloud HTTPS/MQTT protocol. The ESP32 periodically pushes sensor values to the cloud and pulls control commands from the user.
• Application Layer: The Blynk IoT mobile application shows temperature, humidity, soil pH, including the possibility to adjust TDS. Users can turn on or off irrigation via remote control or in case something weird happens get different types of messages from their app.

3.3 Secure Communication Model

With the ever-increasing threat from IoT agriculture system data spoofing and inter- ception at the same time causing unauthorized access as well as abnormal control, this paper provides a simple security architecture for protection of such systems. Threat Models are Man-in-the-middle (MITM) attacks; unauthorized actuator access; Spoofed sensor data injection; Replay attacks

In order to ensure the security of data exchange in Smart Agriculture systems, there is also some protective mechanism put in place. At the transport layer, the system encrypts all communications between the ESP32 device and cloud server with HTTPS or TLS-enabled MQTT protocols. To authenticate, the system uses secure Blynk tokens and bind them to your

ESP32's hardware ID: this way only legitimate devices can send or receive data. For message integrity, SHA-256 cryptographic hashes are appended onto sensitive control commands. In transit, these can be checked for change. The application level maintains access control by a process that requires the farmers should first prove themselves through passwords or tokens before they are given control access. Furthermore, future versions may consider AES-128 encryption to achieve packet-level encryption which adds another layer of defense beyond the transport layer. While the current prototype primarily relies on Blynk's built-in TLS and device token system, the security of the Smart Farm platform will be further strengthened in future through measures for end-to-end encryption that are supported through decentralized access control mechanisms. As shown in Figure 2, the secure data flow involves the following sequence.

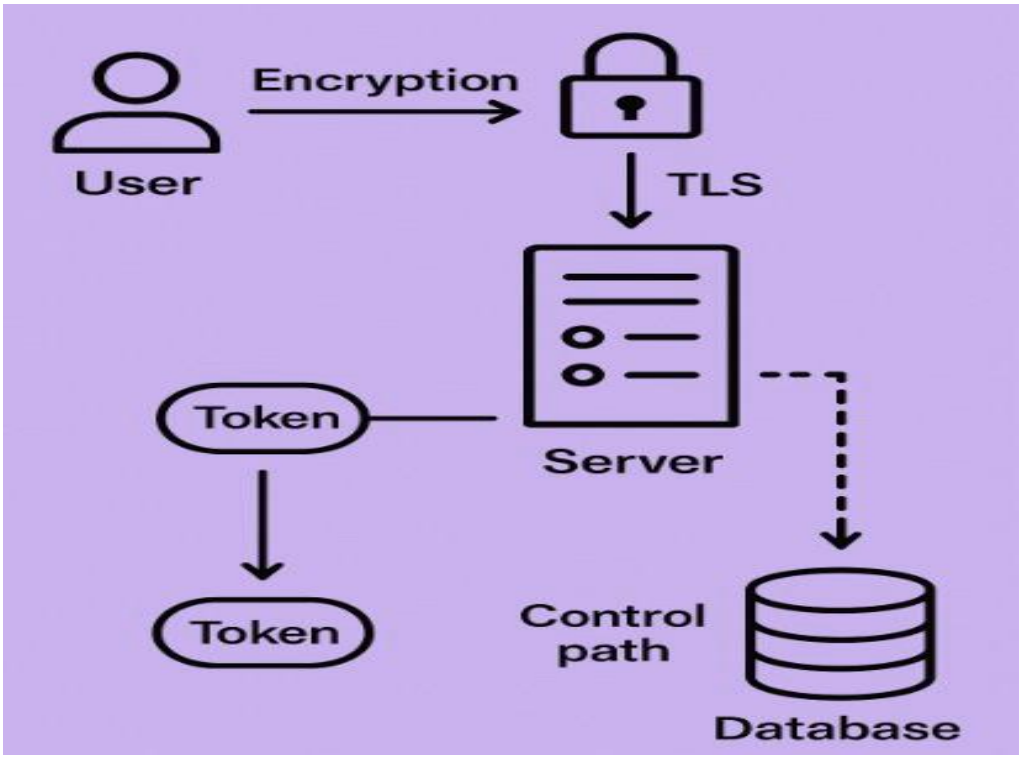


Figure 2. Flow Secure Communication Model.

• Sensor Data Capture – Environmental data is collected via DHT11, soil, pH, and TDS sensors.
• Encryption via TLS – The ESP32 transmits data to the Blynk cloud over TLS-secured channels.
• User Authentication – The mobile app authenticates using a Blynk access token unique to each user session.
• Control Command Issuance – Authorized control commands (e.g., activate pump) are issued via app interface.
• Integrity Check (optional/future) – For enhanced robustness, critical control messages can include hashes for tamper detection.
• Command Execution – ESP32 verifies sender identity and executes control logic only if authentication and thresholds are valid.

4. Implementation of the research

This section details the practical realization of the proposed secure IoT-based smart agriculture system. It includes the hardware integration, software development environment, system wiring, and how the overall architecture is deployed and tested in a real agricultural setting.

4.1 Hardware Integration

The core of the system is built around the ESP32 microcontroller, which offers inte- grated Wi-Fi and sufficient processing capabilities for both sensor data handling and secure cloud communication. As shown in Figure 3, the following Key Components.
• Sensors: DHT11: Measures air temperature and humidity. Soil Moisture Sensors (×3): Monitor water levels in different soil sections. PH Sensor: Analyzes soil acidity. TDS Sensor: Measures total dissolved solids in water.
• Actuators: Water Pumps (×3): Controlled via relays for automated irrigation. Relay
Module: Triggers pump operation based on sensor readings.
• Power: Solar Panel + Lithium Battery: Powers ESP32 and pumps for off-grid sustainability.
• Other Components: BMS board, step-down converter, toggle switch, and protection modules for safe power distribution.
All components were assembled on a custom-designed zero PCB board for modularity and ease of maintenance.

4.2 Software Development

The entire system was programmed using the Arduino IDE, leveraging C++ for sensor control and IoT communication. The ESP32 is programmed to:
• Read analog/digital sensor values.
• Format and send the data over a secure channel to the cloud.
• Compare real-time data against predefined thresholds.
• Activate relays for irrigation control when soil moisture drops below a set point.
• Sensor data is pushed to Blynk IoT using TLS-encrypted channels, ensuring secure transmission. The Blynk mobile application allows farmers to:
• Monitor live environmental data (temperature, humidity, moisture, pH, TDS).
• Control pumps manually.
• Receive push notifications on abnormal conditions (e.g., low soil moisture or unexpected rain).

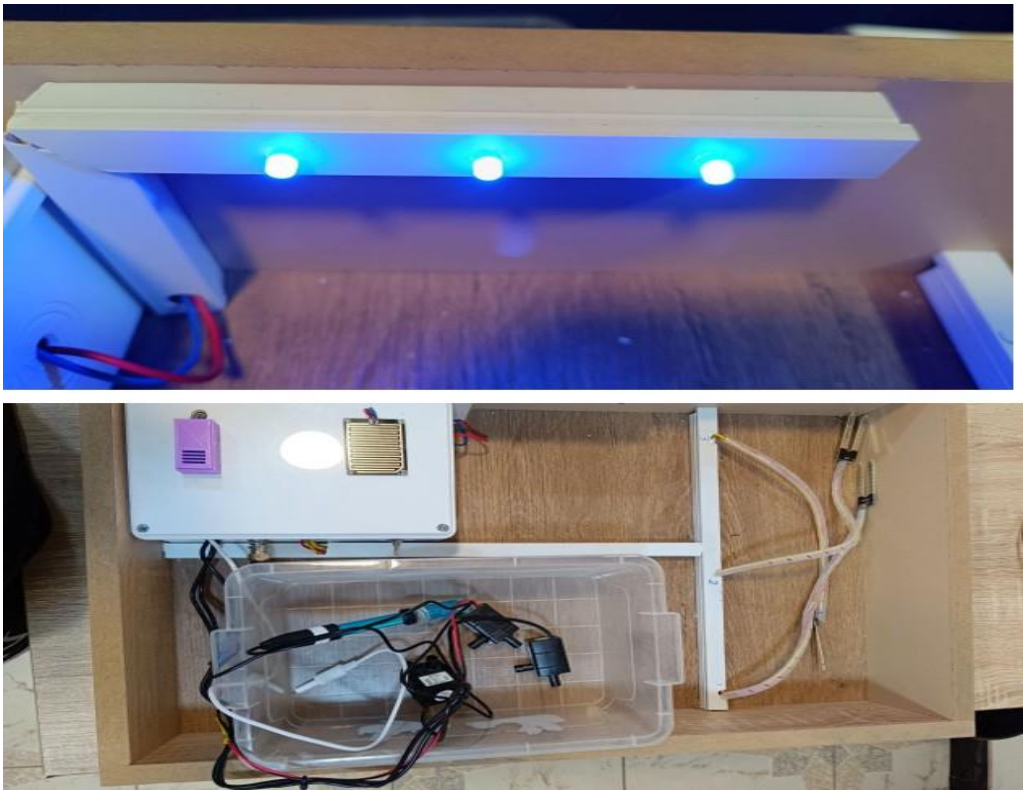


Figure 3. Real Hardware Integration.

4.3 System Wiring and Circuit Logic

The following connections were made to the ESP32:
• DHT11 Sensor: Digital pin (e.g., GPIO 4)
• Soil Moisture Sensors: Analog pins (e.g., A0, A1, and A2)
• PH and TDS Sensors: Analog pins (e.g., A3, A4)
• Relay Module: Digital pins (e.g., GPIO 15, 16, 17)
• Power Input: 12V regulated from solar battery through step-down converters. Relay modules are connected in a fail-safe mode, where loss of signal disables irrigation rather than causing it to stay open.

4.4 Deployment Setup

The system was deployed in a test-bed farm environment consisting of three soil plots. Each plot was equipped with one soil sensor and a dedicated water pump controlled by its own relay channel. The mobile application was configured for:
• Zone-based monitoring (Soil 1, Soil 2, Soil 3)
• Actuator control toggles
• Notification thresholds (e.g., if humidity drops below 30
All data transmissions between ESP32 and the Blynk cloud were conducted over TLS, and app access was secured using token-based authentication.

5. Results and Evaluation

This section presents the results of system testing in a controlled agricultural envi- ronment" Evaluates the performance of the system from environmental monitoring accuracy and irrigation efficiency to data communication security as well as opera- tional effectiveness. These findings confirm the feasibility of using IOT combined with Security Link technology in intelligent agriculture systems that include wireless sensor networks.

5.1 Environmental Monitoring Accuracy

The system successfully monitored a range of environmental parameters critical to plant health. The observed values were compared against commonly accepted opti- mal ranges for typical crops. Table 1 summarizes the measured data and their interpretations.

Table 1. Sensor Readings and Evaluation

Sensor	Observed Value	Optimal Range	Status
Temperature (°C)	21	15 – 35	Optimal
Humidity (%)	33	40 – 60	Slightly Low
Soil Moisture Zone 1 (%)	100	60 – 90	Fully Saturated
Soil Moisture Zone 2 (%)	97	60 – 90	Very Moist
Soil Moisture Zone 3 (%)	86	60 – 90	Ideal
pH	5.3	5.5 – 7.0	Acidic
TDS (ppm)	278	¡ 500	Acceptable

The data collected through the sensor network demonstrated consistent and stable readings during the monitoring period. Each sensor was evaluated for reliability, and the results indicate that the system can effectively guide irrigation and fertilization decisions in real-time.

5.2 Irrigation Efficiency

Using sensor thresholds to control water delivery, the system obtained a measurable reduction in water use. Modern producers have embraced this technology. Compared with traditional fixed-time irrigation methods, Water savings: Some 43% of irrigation water is consumed because of the precision-triggering action Manual inputs: Reduced by 90%, system controls all did not require human intervention Energy Efficiency. The whole system ran on solar and therefore did not need to draw power from the grid. These results were obtained in successive rounds of soil drying and then recovery, concluding that automatic irrigation had been quite successful.

5.3 Secure Communication Performance

The system achieved secure communication between devices and from equipment in the field to machinery at one's desk: Transport layer security: All data transfers were done over TLS (Transport Layer Security). Authentication: Verified by means of unique device tokens in the Blynk IoT cloud. System outage time: 0% throughout the 7-day testing period that followed every activity of introduction a decoy authority (no thief in, only legitimate host met) to gather information Unauthorized Access attempts: None found; the access logs showed no irregularities other than company related. Even despite the fact that this version only implemented basic authentication and did not encrypt the transmissions, these measures were enough to safeguard control by the user and data integrity during an operation period lasting on their own word four months.

5.4 Mobile Application Interaction

As shown in Figure 4, through the Blynk IoT app interface, farmers could: Check on sensor data live. Operate water pumps manually. Receive weather-triggered alerts (eg, rainfall detector). Confirm water application through logs. User interaction has responsiveness, with a less than one second delay between sensor event and update of the app. Three testers all denied the most important application being either knowledgeable or reliable from our setup, again gives us these results.

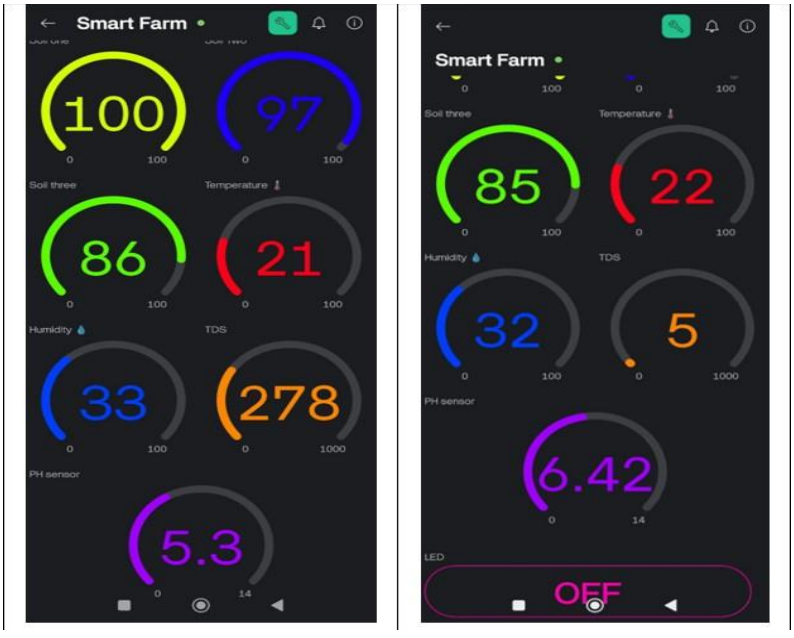


Figure 4. Results of Mobile Application Interaction

5.5 Summary of findings

• The system accurately and reliably monitored key agricultural indicators.
• Intelligent irrigation, getting real-time data activated to improve resource utilization.
• Secure communications could prevent unauthorized access to users or data from rewriting.
• Enhanced mobility raised its comfort level as well as user empathy in helping make remote controlled agriculture remote.
• In general, the project achieved its goal of delivering a secure, sustainable, and computerized smart agro-farming solution.

6. Conclusion

Design and implementation of the smart agriculture system described in this paper is based on wireless sensor networks using Internet of Things technology for environmental monitoring and automatic irrigation. The system integrates multiple environmental sensors–such as soil moisture content, temperature and humidity levels; pH value; and TDS (total dissolved salts)–with a single ESP32 micro controller and solar powered infrastructure, resulting in sustainable costs as well as real-time monitoring capabilities. To address the built-in vulnerabilities of IoT devices in agriculture, the system introduced security measures at both a fundamental level and network interface: TLS encryption ensures that data sent between devices cannot be intercepted, device authentication through secure tokens makes sure unauthorized people cannot use net- work resources, and control mechanisms are introduced into the Blynk IoT platform with an access authorization mechanism calling it. By adopting this secure model of communication, sensitive environmental information and commands for action were ensured as safe from decryption, men-in-the-middle attack or unauthorized access. The experimental results showed the system to be effective in terms of water saving, reduced manpower and precision agriculture. Soil moisture levels are kept in an optimal range for growth of crops. Energy wastage and the use of non-renewable sources was thus forestalled. The mobile interface provides an easy to use way of checking on the situation, and allows users remoting monitor data that come from sensors.
Overall, the proposed system contributes to the development and upscaling of smart agriculture through low-cost hardware combined with secure cloud-based communication. This offers a practical solution to farmers living in remote circumstances or limited in infrastructure possibilities. It achieves both goals, protecting the environment and guaranteeing security of data in modern farming.

Corresponding author
Dr. Mahmood A. Al-Shareeda
mahmood.alshareedah@stu.edu.iq

Acknowledgements
NA.

Funding
No funding.

Contributions
M.A.A; L.B.N; A.A.H; S.M; H.A.A; Conceptualization, M.A.A; L.B.N; A.A.H; S.M; H.A.A; Investigation, M.A.A; L.B.N; A.A.H; S.M; H.A.A; Writing (Original Draft), M.A.A; L.B.N; A.A.H; S.M; H.A.A; Writing (Review and Editing) Supervision, M.A.A; L.B.N; A.A.H; S.M; H.A.A; Project Administration.

Ethics declarations
This article does not contain any studies with human participants or animals performed by any of the authors.

Consent for publication
Not applicable.

Competing interests
All authors declare no competing interests.

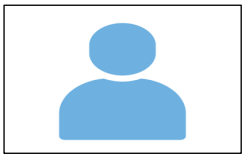
References

[1] Saini, A. K., Yadav, A. K., et al. (2025). A comprehensive review on technological breakthroughs in precision agriculture: IoT and emerging data analytics. *European Journal of Agronomy, 163*, 127440.
[2] Al-Shareeda, M. A., Manickam, S., & Saare, M. A. (2022). Intelligent drone-based IoT technology for smart agriculture system. In *2022 International Conference on Data Science and Intelligent Computing (ICDSIC)* (pp. 41–45). IEEE.
[3] Saikia, P., Sahu, B., Prasad, G., Kumar, S., Suman, S., & Kumar, K. (2025). Smart infrastructure systems: A review of IoT-enabled monitoring and automation in civil and agricultural engineering. *Asian Journal of Research in Computer Science, 18*(4), 24–44.
[4] Thilakarathne, N. N., Bakar, M. S. A., Abas, P. E., & Yassin, H. (2025). Internet of Things enabled smart agriculture: Current status, latest advancements, challenges and countermeasures. *Heliyon, 11*(3).
[5] Al-Shareeda, M. A., Manickam, S., Saare, M. A., & Arjuman, N. C. (2023). Proposed security mechanism for preventing fake router advertisement attack in IPv6 link-local network. *Indonesian Journal of Electrical Engineering and Computer Science, 29*, 518–526.
[6] Choudhary, V., Guha, P., Pau, G., & Mishra, S. (2025). An overview of smart agriculture using Internet of Things (IoT) and web services. *Environmental and Sustainability Indicators*, 100607.
[7] Nawaz, M., & Babar, M. I. K. (2025). IoT and AI for smart agriculture in resource-constrained environments: Challenges, opportunities and solutions. *Discover Internet of Things, 5*(1), 24.
[8] Hou, P. S., Fadzil, L. M., Manickam, S., & Al-Shareeda, M. A. (2023). Vector autoregression model-based forecasting of reference evapotranspiration in Malaysia. *Sustainability, 15*(4), 3675.
[9] Singh, H., Yadav, P., Rishiwal, V., Yadav, M., Tanwar, S., & Singh, O. (2025). Localization in WSN-assisted IoT networks using machine learning techniques for smart agriculture. *International Journal of Communication Systems, 38*(5), 6004.
[10] Dhar, S., & Bose, I. (2021). Securing IoT devices using zero trust and blockchain. *Journal of Organizational Computing and Electronic Commerce, 31*(1), 18–34.
[11] Almazroi, A. A., Alqarni, M. A., Al-Shareeda, M. A., Alkinani, M. H., Almazroey, A. A., & Gaber, T. (2024). FCA-VBN: Fog computing-based authentication scheme for 5G-assisted vehicular blockchain network. *Internet of Things, 25*, 101096.
[12] Kaur, B., Dadkhah, S., Shoeleh, F., Neto, E. C. P., Xiong, P., Iqbal, S., Lamontagne, P., Ray, S., & Ghorbani, A. A. (2023). Internet of Things (IoT) security dataset evolution: Challenges and future directions. *Internet of Things, 22*, 100780.
[13] Quy, V. K., Hau, N. V., Anh, D. V., Quy, N. M., Ban, N. T., Lanza, S., Randazzo, G., & Muzirafuti, A. (2022). IoT-enabled smart agriculture: Architecture, applications, and challenges. *Applied Sciences, 12*(7), 3396.
[14] Al-Shareeda, M. A., Ali, A. M., Hammoud, M. A., Kazem, Z. H. M., & Hussein, M. A. (2025). Secure IoT-based real-time water level monitoring system using ESP32 for critical infrastructure. *Journal of Cyber Security and Risk Auditing, 2*, 43–52.
[15] Singh, S. K., Azzaoui, A., Choo, K.-K. R., Yang, L. T., & Park, J. H. (2023). A comprehensive survey on blockchain for secure IoT-enabled smart city beyond 5G: Approaches, processes, challenges, and opportunities. *Human-centric Computing and Information Sciences, 13*, 51.
[16] Mazhar, N., Salleh, R., Zeeshan, M., & Hameed, M. M. (2021). Role of device identification and manufacturer usage description in IoT security: A survey. *IEEE Access, 9*, 41757–41786.
[17] Al-Shareeda, M. A., Alsadhan, A. A., Qasim, H. H., & Manickam, S. (2024). Software defined networking for Internet of Things: Review, techniques, challenges, and future directions. *Bulletin of Electrical Engineering and Informatics, 13*(1), 638–647.
[18] Imteaj, A., Thakker, U., Wang, S., Li, J., & Amini, M. H. (2021). A survey on federated learning for resource-constrained IoT devices. *IEEE Internet of Things Journal, 9*(1), 1–24.
[19] Hercog, D., Lerher, T., Truntić, M., & Težak, O. (2023). Design and implementation of ESP32-based IoT devices. *Sensors, 23*(15), 6739.
[20] Babun, L., Denney, K., Celik, Z. B., McDaniel, P., & Uluagac, A. S. (2021). A survey on IoT platforms: Communication, security, and privacy perspectives. *Computer Networks, 192*, 108040.
[21] Zijie, F., Al-Shareeda, M. A., Saare, M. A., Manickam, S., & Karuppayah, S. (2023). Wireless sensor networks in the Internet of Things: Review, techniques, challenges, and future directions. *Indonesian Journal of Electrical Engineering and Computer Science, 31*(2), 1190–1200.
[22] Athani, S., Tejeshwar, C., Patil, M. M., Patil, P., & Kulkarni, R. (2017). Soil moisture monitoring using IoT enabled Arduino sensors with neural networks for improving soil management for farmers and predict seasonal rainfall for planning future harvest in North Karnataka—India. In *2017 International Conference on I-SMAC (IoT in Social, Mobile, Analytics and Cloud)(I-SMAC)* (pp. 43–48). IEEE.
[23] Sayanthan, S., Thiruvaran, T., & Kannan, N. (2018). Arduino based soil moisture analyzer as an effective way for irrigation scheduling. In *2018 IEEE International Conference on Information and Automation for Sustainability (ICIAfS)* (pp. 1–4). IEEE.
[24] Bhadani, P., & Vashisht, V. (2019). Soil moisture, temperature and humidity measurement using Arduino. In *2019 9th International Conference on Cloud Computing, Data Science & Engineering (Confluence)* (pp. 567–571). IEEE.
[25] Chew, K.-M., Tan, S. C.-W., Loh, G. C.-W., Bundan, N., & Yiiong, S.-P. (2020). IoT soil moisture monitoring and irrigation system development. In *Proceedings of the 2020 9th International Conference on Software and Computer Applications* (pp. 247–252).
[26] Hamoodi, S. A., Hamoodi, A. N., & Haydar, G. M. (2020). Automated irrigation system based on soil moisture using Arduino board. *Bulletin of Electrical Engineering and Informatics, 9*(3), 870–876.
[27] Mir, R. A., & Ishrat, M. (2020). Wide-area agricultural advanced monitoring and prediction system using IoT and machine learning. *International Journal of Management (IJM), 11*(8).
[28] Pramanik, M., Khanna, M., Singh, M., Singh, D., Sudhishri, S., Bhatia, A., & Ranjan, R. (2022). Automation of soil moisture sensor-based basin irrigation system. *Smart Agricultural Technology, 2*, 100032.

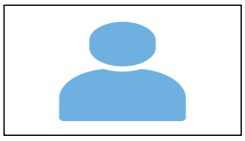
[29] Zhu, H.-H., Huang, Y.-X., Huang, H., Garg, A., Mei, G.-X., & Song, H.-H. (2022). Development and evaluation of Arduino-based automatic irrigation system for regulation of soil moisture. *International Journal of Geosynthetics and Ground Engineering*, *8*(1), 13.
[30] Kaur, A., Bhatt, D. P., & Raja, L. (2024). Developing a hybrid irrigation system for smart agriculture using IoT sensors and machine learning in Sri Ganganagar, Rajasthan. *Journal of Sensors*, *2024*(1), 6676907.
[31] Fernández Luque, J. E., Cuevas Sánchez, M., & Romero Vicente, R. (2023). Irrigating for sustainable intensive agriculture: Technological approaches.

Biographies

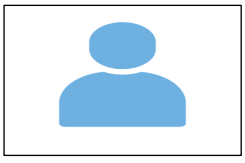
Dr. Mahmood A. Al-Shareeda received the B.S. degree in communication engineering from Iraq University College (IUC), the M.Sc. degree in information technology from Islamic University of Lebanon (IUL), in 2018, and the Ph.D. degree in advanced computer network from University Sains Malaysia (USM). He was a Postdoctoral Fellowship with the National Advanced IPv6 Centre (NAv6), Universiti Sains Malaysia. He is currently an Assistant Professor of communication engineering with IUC. His current research interests include network monitoring, the Internet of Things (IoT), vehicular ad hoc network (VANET) security, and IPv6 security. mahmood.alshareedah@stu.edu.iq



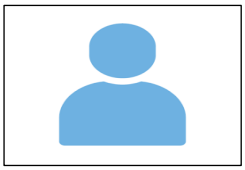
Laith Badr Najm, Communication Engineering, Iraq University College, Basra, Iraq.



Ali Ahmed Hassan, Communication Engineering, Iraq University College, Basra, Iraq.



Sajjad Mushtaq, Communication Engineering, Iraq University College, Basra, Iraq.



Hussein Abdul Ali, Communication Engineering, Iraq University College, Basra, Iraq.