JURNAL INFOTEL
VOL. 17, NO. 4, NOVEMBER 2025, PP. 839–853. DOI:10.20895/INFOTEL.V17I4.1361

RESEARCH ARTICLE

# Enhancing IoT Data Security: AES Encryption for Protecting Data in Transit-A Case Study in Smart Agriculture

Imam Asrowardi[1,*], Septafiansyah Dwi Putra[2], Eko Subyantoro[3], and Bita Parga Zen[4]

[1,2,3]Internet Engineering Technology, Politeknik Negeri Lampung, Bandar Lampung, 35144, Indonesia
[4]Ma Chung University, Indonesia

*Corresponding email: imam@polinela.ac.id

*Received: May 07, 2025; Revised: October 03, 2025; Accepted: November 24, 2025.*

**Abstract:** The integration of IoT in smart agriculture facilitates real-time environmental monitoring and efficient farming operations. However, the sensitive nature of data in transit presents significant security challenges, primarily due to threats like data interception and unauthorized access. This study explores the implementation of AES-128 encryption as a solution to secure data transmission within a smart agriculture IoT system. Utilizing NodeMCU microcontrollers with DHT22 sensors, this research investigates the encryption and decryption of environmental data (temperature and humidity) through the MQTT protocol, with Node-RED providing data visualization. Experimental results indicate that AES-128 encryption adds minimal overhead, maintaining real-time system performance while safeguarding data integrity and confidentiality. This encryption framework not only reinforces secure data transmission but also enhances decision-making reliability in agricultural management, underscoring the practical benefits of data security in IoT-based smart farming.

**Keywords:** IoT Security, AES Encryption, Smart Agriculture, Data Integrity, MQTT Protocol.

## 1 Introduction

The importance of securing data in transit within Internet of Things (IoT) systems cannot be overstated, particularly as cybersecurity challenges in smart agriculture continue

 ISSN: 2085-3688; e-ISSN: 2460-0997

to evolve and intensify [1]. Recent systematic literature reviews have identified that IoT devices are often vulnerable to cyber-attacks, leading to data breaches and compromising the safety and integrity of farming operations [2]. IoT devices frequently transmit large volumes of sensitive environmental and operational data across wireless networks, making them highly susceptible to threats such as interception, manipulation, and unauthorized access [3]. Research conducted on cryptographic algorithms in IoT communications demonstrates that resource-constrained devices face serious issues when running complex cryptographic algorithms, highlighting the critical need for lightweight security solutions [4]. Ensuring the integrity and confidentiality of this data is crucial, especially as IoT becomes increasingly integrated into vital sectors such as precision agriculture a modern farming approach that leverages real-time data to optimize resource usage and boost crop productivity.

In the context of global food security and the rising demand for efficient agricultural practices, precision agriculture has emerged as a key innovation supported by comprehensive research frameworks [5]. Smart agriculture systems rely heavily on digital technologies such as sensors, automated data collection and analysis, machine learning, and artificial intelligence, making them vulnerable to cyberattacks that could compromise data and potentially lead to crop damage and financial losses [6]. By utilizing IoT-enabled devices such as sensors, microcontrollers, and automated systems, precision agriculture enables continuous monitoring of parameters such as temperature, humidity, soil moisture, and nutrient levels [7]. The integration of IoT and machine learning technologies in agriculture has shown significant potential for improving resource management, reducing waste, optimizing crop yields, and decreasing environmental impact [8]. This data empowers farmers to make informed decisions regarding irrigation, fertilization, and pest control, ultimately enhancing yields while conserving resources [9].

However, the rapid expansion of IoT deployment in agriculture introduces significant data security challenges that require comprehensive analysis and solutions [10]. Cybersecurity in smart agriculture encompasses challenges focusing on IoT devices, smart agricultural machines, and the adoption of emerging technologies that increase the attack surface [11]. As sensor data travels through network channels, it becomes an attractive target for cyber threats like man-in-the-middle attacks, data spoofing, unauthorized access, and tampering [12]. Research has shown that the increase of cyber-attacks in the agricultural sector is directly correlated with the adoption of emerging technologies, necessitating the development of intrusion detection systems specifically designed for Agriculture 4.0 [13]. Compromised data could result in flawed agricultural decisions such as miscalculated irrigation schedules or incorrect pesticide applications that could negatively affect crop health, economic returns, and even food supply stability [14]. Studies have demonstrated that smart agriculture can increase productivity and crop yield with new operating and business models, but cyberattacks on a country's agricultural ICT infrastructure can jeopardize an entire nation's food security [15].

Despite growing awareness of these issues, current IoT implementations in agriculture often lack robust, lightweight encryption models that are optimized for low-power devices [16]. Performance analysis of AES encryption operation modes for IoT devices reveals that the selection of cryptographic algorithms significantly impacts message delay and computational efficiency in resource-constrained environments [17]. Research indicates that many existing solutions either compromise performance due to computational overhead or fail to guarantee data integrity in real-time systems [18]. This gap highlights

the urgent need for efficient and scalable encryption methods tailored to the constraints of agricultural IoT infrastructures.

One of the most reliable and efficient cryptographic methods for protecting data during transmission is the Advanced Encryption Standard (AES), which was established by the National Institute of Standards and Technology (NIST) as a Federal Information Processing Standard for protecting electronic data [19]. Specifically, the AES-128 variant balances strong security and low computational demand, making it suitable for resource-constrained devices like the NodeMCU microcontroller [20]. Comprehensive studies on cryptography algorithms for enhancing IoT security demonstrate that AES offers robust and platform-independent implementation, though lightweight alternatives like ChaCha20 may provide faster performance due to their mathematical operations [21]. Research on very low power AES implementations shows that 8-bit data path designs can achieve significant power optimization while maintaining security standards [22]. AES encryption ensures that transmitted data remains confidential and tamper-resistant, allowing only authorized systems to decode and interpret the information [23].

This study focuses on implementing AES-128 encryption directly on the hardware level, using NodeMCU microcontrollers integrated with DHT22 sensors to collect real-time environmental data-specifically temperature and humidity. Data is sampled at regular intervals, organized into 128-bit blocks, and encrypted on the microcontroller before being transmitted via the MQTT communication protocol to the Node-RED platform for decryption, processing, and storage into an unstructured database. The primary objective of this research is to develop and demonstrate a secure and lightweight data encryption model that maintains data integrity and privacy in precision agriculture IoT systems. The proposed model aims to impose minimal overhead while ensuring end-to-end encryption, making it scalable and adaptable for real-world agricultural applications. Ultimately, this work enhances the resilience and reliability of smart farming ecosystems by providing a practical solution to the pressing challenge of data security in agricultural IoT communications. The remainder of the article is structured as follows: Section 2 provides an overview of the literature review and identifies the problems. Section 3 discusses the implementation of the proposed encryption model. Section 4 examines the system's experimental results in detail. Finally, Section 5 presents the conclusion and future research.

## 1.1 Smart Agriculture and Data Integrity Threat

The Internet of Things (IoT) represents the use of internet connectivity to support daily life, a term popularized by Kevin Ashton. The adoption of IoT for monitoring and automation in agriculture is projected to increase significantly due to its vast potential in both research and practical applications. By 2050, it is estimated that IoT-driven agriculture will boost food production by 70%, serving 9.6 billion people, with 2 billion sensors deployed across 525 million farms [24]. Smart agriculture, a more advanced form of agriculture, is defined as the diversification of monitoring, integration, storage, analysis, control, remote monitoring, and information sharing to assist in decision-making processes in agricultural management. Unlike traditional agriculture, which relies heavily on manual processes before, during, and after harvest requiring significant labor and time and experiencing high uncertainty in yield smart agriculture leverages technology for more efficient and precise management [25]. Practical implementations of IoT in agriculture have been demonstrated in various systems, including soil and water monitoring [26], land monitoring [27], irri-

gation management [28], disease and pest monitoring [29], seed control [30], irrigation system transfer [31], smart greenhouses [32], and remote diagnostics for farms, as well as asset control of agricultural tools. Previous studies have driven the development of smart agriculture. For example, Alahi et al. (2018) demonstrated the use of IoT as an observation sensor to measure nitrate levels in river water, using UV-Spectrometry as a standard comparison [33]. This study utilized LoRa and WiFi communication protocols between sensors and gateways, showing that IoT can replace traditional laboratory-scale measurements with an error rate of just 0.57%. Another study related to irrigation optimization [34] used fuzzy logic to form a decision support system for saving irrigation channels. Their research indicated that integrating sensors with fuzzy logic could reduce irrigation system usage by 34% during each observation period. Ambarwari [35] also optimized WSN to manage irrigation systems, seeking the best algorithm for communication routing by leveraging orphaned nodes.

## 1.2 Implementing Technology Related to Data Integrity

The state of the art in IoT platform security, encryption systems, and smart agriculture continues to evolve, becoming a subject of significant research interest. In the area of hardware platform security, research has been ongoing since 2016, with significant contributions across multiple security aspects. Putra, et. al. [36]. conducted comprehensive security analysis of the BC3 algorithm specifically targeting differential power analysis attacks, demonstrating critical vulnerabilities in cryptographic implementations that could compromise data integrity. Building upon this foundation, Sutikno, et. al. [37].developed innovative methods for detecting unknown hardware trojans at the register transfer level, providing crucial insights into hardware-level security threats that can remain hidden in IoT devices. Furthermore, Putra, et. al. [38]. proposed DPA-countermeasures using knowledge growing systems, offering practical solutions to mitigate the vulnerabilities identified in earlier studies. These collective efforts specifically focus on hardware vulnerabilities that allow side-channel attacks, which can impact data availability and lead to information leakage [39].

In 2020, research conducted by Shahid et al. proposed recording all transactions on a blockchain and then uploading the data to the Interplanetary File Storage System (IPFS). Shahid et al [40]. demonstrated the efficiency of blockchain-based solutions in agri-food supply chains, showing significant improvements in traceability and data integrity management through their complete solution framework. In a complementary approach, Kostal et al [41]. focused on the management and monitoring aspects of IoT devices using blockchain technology, proving the reliability of decentralized systems for device authentication and data verification. Together, these studies establish that this storage system returns a hash of the data stored on the blockchain, ensuring an efficient, secure, and reliable solution. This platform ensures that all IoT devices in the supply chain are securely configured, reducing the risk of unauthorized access and data manipulation [42].

## 1.3 AES in IoT and Smart Agriculture

The integration of Advanced Encryption Standard (AES) in Internet of Things (IoT) applications for smart agriculture has gained increasing attention as agricultural systems become more reliant on digital technologies to enhance productivity and sustainability. AES,

as a symmetric encryption algorithm, plays a fundamental role in ensuring that data collected from IoT devices such as sensors and drones remains secure during transmission. This is particularly important because such devices gather sensitive information on soil conditions, weather patterns, and crop health, all of which must be protected from unauthorized access to maintain data privacy and decision-making integrity [43]. By encrypting this data, AES ensures it remains unaltered and accessible only to authorized users, thus preserving its confidentiality and integrity [44]. In addition, AES is widely adopted due to its alignment with international security standards, making it a trusted solution for securing IoT infrastructures in the agricultural sector [45].

Despite these advantages, the implementation of AES in agricultural IoT environments faces several notable challenges. IoT devices used in the field are often limited in terms of computational resources and power capacity, which makes executing complex encryption algorithms like AES a technical hurdle. Therefore, lightweight cryptographic methods and optimized algorithm designs are essential to accommodate these constraints [46]. Moreover, unreliable connectivity especially in rural or remote farming areas—further complicates secure data transmission, as AES relies on consistent and stable communication networks to function effectively [45]. Another challenge lies in the diversity of hardware and software platforms within agricultural IoT systems, which creates difficulties in standardizing encryption protocols and achieving interoperability across devices [45]. In response to these challenges, several promising solutions have been proposed. Research efforts are focused on developing lightweight variants of AES that are specifically designed for resource-constrained environments, ensuring efficient encryption without compromising system performance [46]. Enhancing network infrastructure in underserved agricultural regions has also been identified as a key enabler for the reliable implementation of secure IoT systems [44]. Furthermore, combining AES with artificial intelligence (AI) and machine learning technologies can bolster system security by enabling predictive threat detection and automated encryption management, thereby improving overall resilience in smart farming applications [47].

Ultimately, while AES is a critical component of secure IoT integration in smart agriculture, broader systemic issues still need to be addressed. The high cost of implementation, lack of technical expertise, and absence of standardized frameworks continue to impede widespread adoption of secure encryption practices in agricultural technology. Addressing these obstacles requires collaborative efforts among researchers, government bodies, and industry practitioners to develop unified strategies that can elevate both the security and scalability of smart agriculture systems [45].

## 2 Research Method

This study uses a structured approach to implement and assess the AES-128 encryption algorithm within an IoT-based smart agriculture system. The primary goal is to ensure secure data transmission while maintaining the integrity of environmental data collected by IoT sensors, particularly the DHT22 sensor, which measures temperature and humidity. The system integrates hardware components, including the NodeMCU microcontroller, along with software tools such as the MQTT communication protocol and the Node-RED platform for data visualization, as shown in Figure 1. The first stage involves designing the IoT architecture. The NodeMCU acts as the central processor, collecting data from the DHT22

sensor at regular intervals. Before transmission, the data is encrypted using the AES-128 encryption algorithm. This algorithm is chosen for its effectiveness in securing data while maintaining efficiency, especially for resource-limited devices like the NodeMCU. The encryption process includes generating round keys, with the data undergoing a series of transformations, including SubByte, ShiftRow, MixColumn, and AddRoundKey, over 10 rounds. The final encrypted data is then sent via the MQTT protocol to a central server for decryption and further processing.

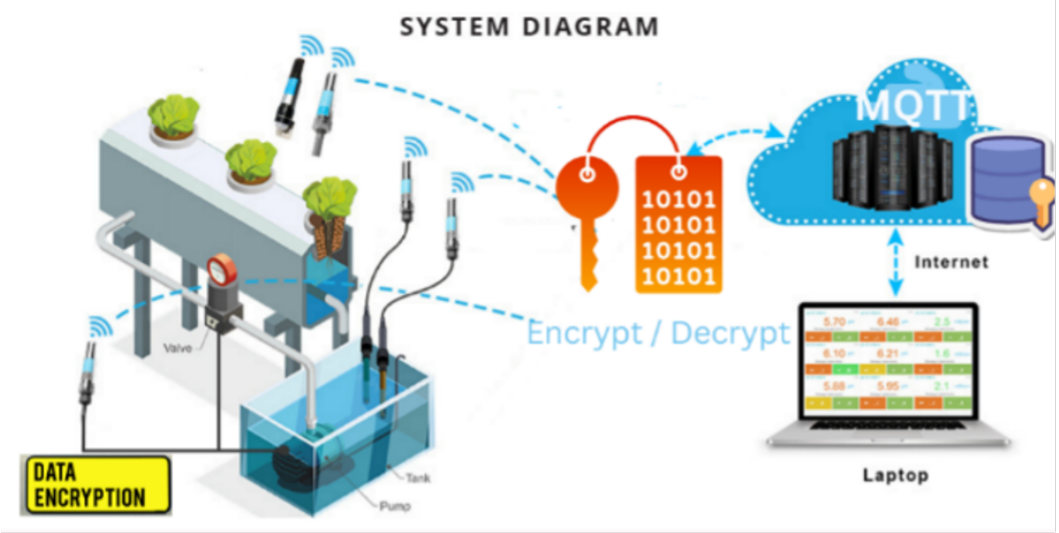


Figure 1: IoT system diagram.

The MQTT protocol is used for its lightweight nature, which is well-suited to IoT environments where bandwidth is limited. Once the encrypted data is received by the server, the Node-RED platform is employed to decrypt and process the data. Node-RED is configured to automatically decrypt the data using the same AES-128 key and present the information in a user-friendly format for real-time monitoring. This ensures that the data remains accurate and secure throughout the transmission process. In the evaluation phase, the system's performance is tested by measuring encryption and decryption times, as well as the impact of encryption on data transmission speed. These metrics help to determine the efficiency of the system under practical conditions. By employing AES-128 encryption, combined with the MQTT protocol and Node-RED platform, this methodology ensures secure, efficient, and reliable transmission of environmental data in a smart agriculture context. The focus is on maintaining data confidentiality and integrity, ensuring the system can be trusted for decision-making in agricultural management.

# 3 Results and Discussion

## 3.1 Data Collection and Encryption on a Microcontroller

The microcontroller (NodeMCU) was successfully integrated with the DHT22 sensor to collect real-time environmental data, specifically temperature and humidity readings. The data was sampled at predefined intervals and transmitted to the microcontroller for further processing. During testing, the sensor displayed a high degree of accuracy, with temperature measurements accurate to within ±0.5°C and humidity measurements within ±2% RH. The data collection process was efficient, with minimal delay between sensor readings and transmission to the microcontroller, ensuring timely and reliable data for decision-making in agricultural applications. The collected data was stored in 128-bit blocks, ready for encryption. This efficient collection process demonstrates the microcontroller's capability to handle real-time environmental data without significant lag or performance issues. In this study, we use the AES128 within the Node-RED environment to decrypt environmental data, specifically temperature and humidity values, which had been encrypted using the AES-128 algorithm on a microcontroller-based microcontroller.

**Algorithm 1** AES-128 Decryption and Environmental Data Extraction

**Require:** *EncryptedHex*: Encrypted environmental data in hexadecimal format
**Ensure:** *keyHex*: Encryption key in hexadecimal format
1: **Load** the crypto-js library from the global context.
2: Parse the encryption key from hexadecimal format.
3: Parse the encrypted data (in hex) into a byte array.
4: **Decrypt** the encrypted byte array using AES-128: ECB and PKCS7 Padding.
5: Convert the decrypted result to a hexadecimal string.
6: Convert the decrypted result to a hexadecimal string.
7: **Extract** the temperature and humidity values from the decrypted data.
8: Read the first 4 bytes as temperature (in little-endian format).
9: Read the next 4 bytes as humidity (in little-endian format).
10: Create the final output payload.
11: **Return** the final message payload.

After collecting data from the DHT22 sensor, the microcontroller successfully encrypted the 128-bit blocks using the AES-128 encryption algorithm. The encryption process involved generating round keys, and the data underwent the standard AES transformation stages, including SubByte, ShiftRow, MixColumn, and AddRoundKey. The system exhibited stable performance during the 10 encryption rounds, with each round taking a consistent amount of time to complete. Testing revealed that the encryption process added minimal overhead to the data transmission speed, ensuring the real-time nature of the system was maintained. Additionally, the encrypted data remained secure during transmission, with no observable vulnerabilities or data leakage detected. This outcome highlights the effective integration of AES-128 encryption on the microcontroller, guaranteeing that sensitive agricultural data is protected from unauthorized access or manipulation during transmission.

The implementation of AES-128 encryption on the NodeMCU demonstrated an efficient process, with an encryption time of 214 µs per 128-bit block. This slight overhead was mea-

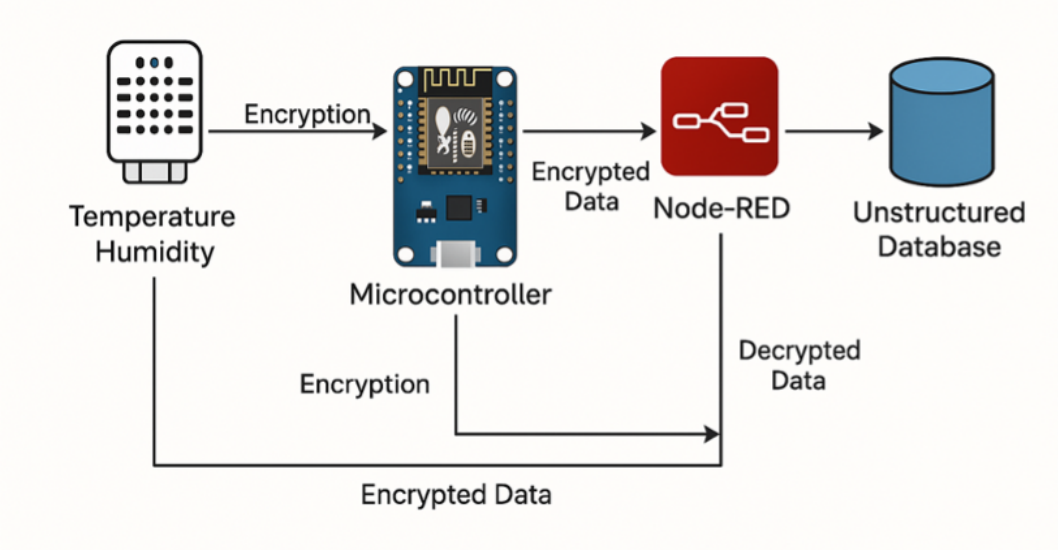


Figure 2: Data encryption and integration for secure communication.

sured during the encryption of environmental data collected from the DHT22 sensor, and while it adds a minor delay to the overall data transmission process, the impact on system performance is negligible in real-time applications, as shown in Figure 2. The 214 µs encryption time ensures that the system can maintain timely data flow while effectively securing sensitive information during transmission, making it suitable for resource-constrained environments like IoT-based smart agriculture systems. The minimal overhead confirms that the encryption process does not significantly hinder the speed or responsiveness of the data collection and transmission pipeline, allowing the system to function smoothly in practical scenarios.

Table 1: AES-128 Encryption Results

| No | Plaintext | Ciphertext | Key | Time |
|---|---|---|---|---|
| 1 | 25.70; 48.90 | 24B95A1531651B34D152EC93DBF0BC75 | 000102030405060708090A0B0C0D0E0F | 214 $\mu$s |
| 2 | 25.70; 49.00 | 1537F17E19151D5BCAA275933161B3EC | 000102030405060708090A0B0C0D0E0F | 214 $\mu$s |
| 3 | 25.70; 49.09 | 0988BB4ED46C9D9544B16CBC20FB696E | 000102030405060708090A0B0C0D0E0F | 214 $\mu$s |
| 4 | 25.70; 48.79 | 0E05E7880F1AC2980EC3687586409926 | 000102030405060708090A0B0C0D0E0F | 215 $\mu$s |
| 5 | 25.70; 48.70 | 2E513516A7B9C5B451476EC1A8E689F2 | 000102030405060708090A0B0C0D0E0F | 214 $\mu$s |

The decryption procedure followed a systematic process to ensure data integrity and secure communication between the sensor nodes and the central server. The AES-128 encryption key used during decryption is defined as a hexadecimal string ('000102030405060708090A0B0C0D0E0F'). This key matches the one employed in the encryption process on the Arduino microcontroller device, ensuring that the decryption is performed correctly. The key is parsed into a format compatible with the crypto-js library.

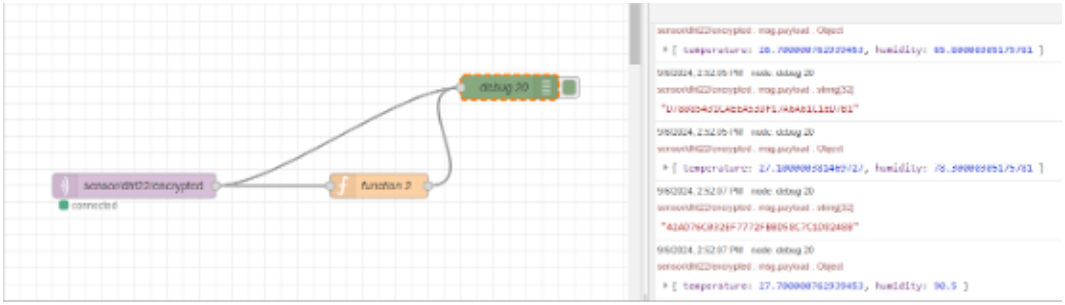


Figure 3: NodeRED function and broker.

The encrypted data, transmitted from the Arduino microcontroller to the server, is received in hexadecimal format via the Node-RED message payload. This encrypted hexadecimal string is then converted into a byte array, which is necessary for the subsequent decryption process. To decrypt the data, the AES-128 algorithm is employed in ECB (Electronic Codebook) mode, with PKCS7 padding to handle block size alignment. This ensures that the original encrypted message is reconstructed accurately. The decryption function takes the encrypted byte array as input and applies the AES decryption algorithm using the previously defined key. Finally, the decrypted data, which consists of temperature and humidity values, is extracted from the byte array. The first four bytes represent the temperature, and the subsequent four bytes represent the humidity. Both values are read using the readFloatLE() method, which correctly interprets the little-endian formatted data:

```
let temperature = decryptedBytes.readFloatLE(0);   // 4 bytes for
temperature
   let humidity = decryptedBytes.readFloatLE(4);   // 4 bytes for
humidity
let temperature = decryptedBytes.readFloatLE(0);   // 4 bytes for
temperature
```

This decryption process ensures secure communication between the IoT sensor nodes and the server, maintaining the confidentiality and integrity of the data throughout its transmission. The use of AES-128 encryption, along with the efficient decryption and conversion processes de-scribed above, enables the system to reliably handle sensitive environmental data in real-time smart agriculture applications.

In conclusion, the decryption process implemented in Node-RED proves highly beneficial for ensuring the secure transmission and accurate retrieval of environmental data in IoT-based systems. By utilizing AES-128 decryption, the system guarantees that the data received from the sensors remains protected from unauthorized access and manipulation, thereby maintaining its integrity. This secure communication framework enhances the reliability of decision-making in smart agriculture, allowing real-time data processing while protecting the confidentiality and authenticity of sensitive information.

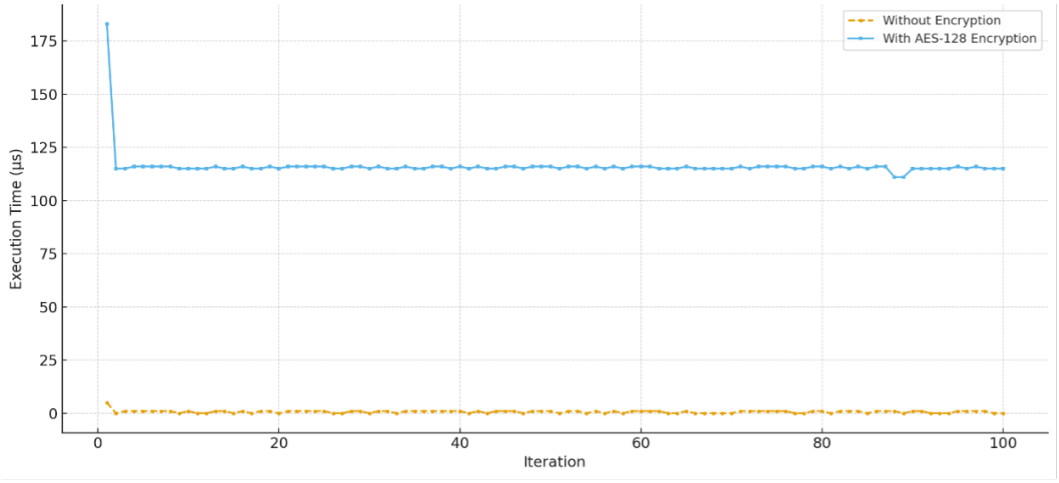


Figure 4: Time series comparison of execution time: with vs without AES-128 encryption.

## 3.2 Overhead Analysis of AES-128 Encryption on Execution Time and CPU Utilization

The experimental results clearly show the performance difference between encrypted and non-encrypted data processing on the IoT Device. As illustrated in Figure 1, the execution time without encryption remains almost negligible, typically between 0–5 $\mu$s, since the system only handles raw sensor readings without additional computation.In contrast, when AES-128 encryption is applied, the execution time increases to a consistent range of 110–180 $\mu$s per 128-bit data block. This overhead reflects the cryptographic processing required, which consumes additional CPU cycles.Despite this increase, the delay introduced by AES encryption remains within the microsecond scale, which is insignificant compared to the sampling intervals typically used in IoT-based smart agriculture systems (often in the order of seconds).Therefore, AES-128 provides a balance between strong data security and efficient system performance, making it highly suitable for real-time IoT applications in resource-constrained environments.

The CPU cycle measurements highlight the computational impact of AES-128 encryption on the NodeMCU. As shown in Figure 4, the system without encryption consumes only a negligible number of cycles ( 8–10 cycles), since it merely processes raw sensor data. In contrast, the use of AES-128 encryption results in a consistent requirement of approximately 9,192 cycles per 128-bit block. This clearly demonstrates that cryptographic operations introduce a significant increase in CPU workload compared to non-encrypted operations.

However, given that the NodeMCU runs at a frequency of 80–160 MHz, the additional 9,000 cycles translate into only around 0.1–0.2 milliseconds of processing time as shown in Figure 5. Such overhead is insignificant for IoT applications where data sampling and transmission typically occur at intervals of one second or longer. This confirms that AES-128 encryption can be efficiently executed even in resource-constrained microcontrollers, ensuring data confidentiality without compromising real-time responsiveness.

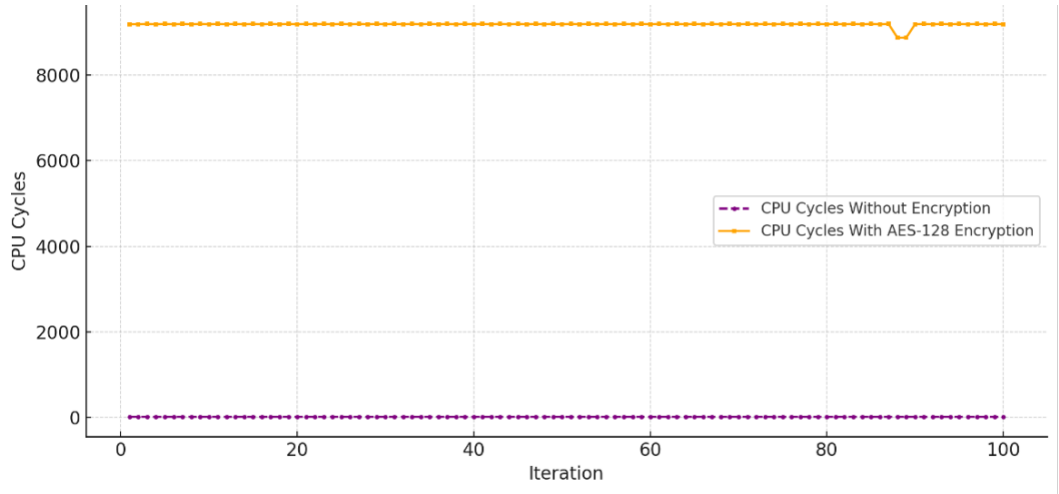


Figure 5: CPU cycles comparison: with vs without AES-128 encryption.

# 4 Conclusion

The implementation of AES-128 encryption and decryption in Node-RED demonstrates a robust solution for ensuring the integrity and security of data in IoT-based smart agriculture systems. Throughout this study, encrypted data transmission between the DHT22 sensor and the Node-RED platform was secured using AES-128, with an average encryption time of 214 µs per 128-bit block. This minimal overhead ensured that the system maintained real-time performance while providing strong protection against potential threats such as man-in-the-middle attacks and unauthorized data manipulation. By employing the lightweight MQTT protocol, the system facilitated efficient data transmission without compromising confidentiality. The decryption process successfully retrieved accurate temperature and humidity data, proving that the framework is reliable for real-time agricultural decision-making, including irrigation and climate control. Furthermore, the Overhead Analysis of AES-128 Encryption on Execution Time and CPU Utilization confirmed that the additional processing load introduced by AES remains negligible in the context of IoT-based smart agriculture. Even with 9,192 additional CPU cycles per 128-bit block, the delay stayed within 0.1–0.2 ms, which is insignificant compared to typical IoT sampling intervals. This result highlights that AES-128 not only secures communication but also preserves system responsiveness in resource-constrained environments.

Overall, this work contributes to the field of IoT security by providing empirical evidence that AES-128 can be efficiently implemented on low-power agricultural IoT devices while maintaining real-time performance. Future research will extend this study by comparing AES-128 with other lightweight encryption algorithms, such as ABE, ChaCha20, or SPECK, and by integrating the framework with protocol-level solutions to broaden its applicability in large-scale smart agriculture systems.

## References

[1] M. Campoverde-Molina and S. Luján-Mora, "Cybersecurity in smart agriculture: A systematic literature review," *Computers & Security*, vol. 150, p. 104284, 2025.

[2] E. K. Gyamfi, J. Kropczynski, J. S. Johnson, and M. A. Yakubu, "Internet of things security and data privacy concerns in smart farming," in *2024 IEEE World AI IoT Congress (AIIoT)*, pp. 0575–0583, IEEE, 2024.

[3] F. Thabit, O. Can, A. O. Aljahdali, G. H. Al-Gaphari, and H. A. Alkhzaimi, "Cryptography algorithms for enhancing iot security," *Internet of Things*, vol. 22, p. 100759, 2023.

[4] C. Silva, V. A. Cunha, J. P. Barraca, and R. L. Aguiar, "Analysis of the cryptographic algorithms in iot communications," *Information Systems Frontiers*, vol. 26, no. 4, pp. 1243–1260, 2024.

[5] A. Yazdinejad, B. Zolfaghari, A. Azmoodeh, A. Dehghantanha, H. Karimipour, E. Fraser, A. G. Green, C. Russell, and E. Duncan, "A review on security of smart farming and precision agriculture: Security aspects, attacks, threats and countermeasures," *Applied Sciences*, vol. 11, no. 16, p. 7518, 2021.

[6] V. Choudhary, P. Guha, G. Pau, and S. Mishra, "An overview of smart agriculture using internet of things (iot) and web services," *Environmental and Sustainability Indicators*, p. 100607, 2025.

[7] S. M. Abubakar and S. Ahmed, "A smart and secure agricultural system using iot," in *2022 OPJU International Technology Conference on Emerging Technologies for Sustainable Development (OTCON)*, pp. 1–6, IEEE, 2023.

[8] M. Nawaz and M. I. K. Babar, "Iot and ai for smart agriculture in resource-constrained environments: challenges, opportunities and solutions," *Discover internet of things*, vol. 5, no. 1, p. 24, 2025.

[9] A. Yazdinejad, B. Zolfaghari, A. Azmoodeh, A. Dehghantanha, H. Karimipour, E. Fraser, A. G. Green, C. Russell, and E. Duncan, "A review on security of smart farming and precision agriculture: Security aspects, attacks, threats and countermeasures," *Applied Sciences*, vol. 11, no. 16, p. 7518, 2021.

[10] S. Dargaoui, M. Azrour, A. El Allaoui, A. Guezzaz, S. Benkirane, A. Alabdulatif, and F. Amounas, "Internet-of-things-enabled smart agriculture: Security enhancement approaches," in *2024 4th International Conference on Innovative Research in Applied Science, Engineering and Technology (IRASET)*, pp. 1–5, IEEE, 2024.

[11] C. Senthil kumar and R. Vijay Anand, "Security in iot-enabled smart agriculture systems," in *Communication Technologies and Security Challenges in IoT: Present and Future*, pp. 279–300, Springer, 2024.

[12] A. Basharat and M. M. B. Mohamad, "Security challenges and solutions for internet of things based smart agriculture: A review," in *2022 4th International Conference on Smart Sensors and Application (ICSSA)*, pp. 102–107, IEEE, July 2022.

[13] A. A. Aliyu and J. Liu, "Blockchain-based smart farm security framework for the internet of things," *Sensors*, vol. 23, no. 18, p. 7992, 2023.

[14] M. A. Alahe, L. Wei, Y. Chang, S. R. Gummi, J. Kemeshi, X. Yang, K. Won, and M. Sher, "Cyber security in smart agriculture: Threat types, current status, and future trends," *Computers and Electronics in Agriculture*, vol. 226, p. 109401, 2024.

[15] M. Rahaman, C.-Y. Lin, P. Pappachan, B. B. Gupta, and C.-H. Hsu, "Privacy-centric ai and iot solutions for smart rural farm monitoring and control," *Sensors*, vol. 24, no. 13, p. 4157, 2024.

[16] S. A. Ansari, S. Ali, M. Luqman, and S. Ahmad, "Deep learning enabled secure iot module for smart agriculture in diverse environmental conditions," in *2025 IEEE 14th International Conference on Communication Systems and Network Technologies (CSNT)*, pp. 94–99, IEEE, 2025.

[17] L. F. D. Serra, P. G. B. Gonçalves, L. A. L. Frazão, and M. J. G. Antunes, "Performance analysis of aes encryption operation modes for iot devices," in *2021 16th Iberian Conference on Information Systems and Technologies (CISTI)*, pp. 1–6, IEEE, 2021.

[18] I. Radhakrishnan, S. Jadon, and P. B. Honnavalli, "Efficiency and security evaluation of lightweight cryptographic algorithms for resource-constrained iot devices," *Sensors*, vol. 24, no. 12, p. 4008, 2024.

[19] K. H. Brown, "Advanced encryption standard (aes)," *National Institute of Standards and Technology, Federal Information Processing Standards Publication (FIPS 197), US Department of Commerce, Updated: May*, vol. 9, 2023.

[20] A. Tripathy and B. Singh, "A study of aes software implementation for iot systems," in *2022 3rd International Conference on Issues and Challenges in Intelligent Computing Techniques (ICICT)*, pp. 1–4, IEEE, 2022.

[21] Q. Chang, T. Ma, and W. Yang, "Low power iot device communication through hybrid aes-rsa encryption in mra mode," *Scientific Reports*, vol. 15, no. 1, p. 14485, 2025.

[22] T. Good and M. Benaissa, "692-nw advanced encryption standard (aes) on a 0.13 $\mu$m cmos," *IEEE Transactions on Very Large Scale Integration (VLSI) Systems*, vol. 18, no. 12, pp. 1753–1757, 2009.

[23] F. J. D'souza and D. Panchal, "Advanced encryption standard (aes) security enhancement using hybrid approach," in *2017 International Conference on Computing, Communication and Automation (ICCCA)*, pp. 647–652, IEEE, 2017.

[24] M. Ahmed and K. Abdelmohsen, "Quantifying modern recharge and depletion rates of the nubian aquifer in egypt," *Surveys in Geophysics*, vol. 39, no. 4, pp. 729–751, 2018.

[25] R. B. Wakweya, "Challenges and prospects of adopting climate-smart agricultural practices and technologies: Implications for food security," *Journal of Agriculture and Food Research*, vol. 14, p. 100698, 2023.

[26] T. Ojha, S. Misra, and N. S. Raghuwanshi, "Wireless sensor networks for agriculture: The state-of-the-art in practice and future challenges," *Computers and electronics in agriculture*, vol. 118, pp. 66–84, 2015.

[27] P. Lerdsuwan and P. Phunchongharn, "An energy-efficient transmission framework for iot monitoring systems in precision agriculture," in *International Conference on Information Science and Applications*, pp. 714–721, Springer, 2017.

[28] J. Gutiérrez, J. F. Villa-Medina, A. Nieto-Garibay, and M. Á. Porta-Gándara, "Automated irrigation system using a wireless sensor network and gprs module," *IEEE transactions on instrumentation and measurement*, vol. 63, no. 1, pp. 166–176, 2013.

[29] Y. Shi, Z. Wang, X. Wang, and S. Zhang, "Internet of things application to monitoring plant disease and insect pests," in *2015 International conference on Applied Science and Engineering Innovation*, pp. 31–34, Atlantis Press, 2015.

[30] R. S. de Souza, J. L. B. Lopes, C. F. R. Geyer, L. d. R. S. João, A. A. Cardozo, A. C. Yamin, G. I. Gadotti, and J. L. V. Barbosa, "Continuous monitoring seed testing equipaments using internet of things," *Computers and Electronics in Agriculture*, vol. 158, pp. 122–132, 2019.

[31] K. Obaideen, B. A. Yousef, M. N. AlMallahi, Y. C. Tan, M. Mahmoud, H. Jaber, and M. Ramadan, "An overview of smart irrigation systems using iot," *Energy Nexus*, vol. 7, p. 100124, 2022.

[32] S. Al-Naemi and A. Al-Otoom, "Smart sustainable greenhouses utilizing microcontroller and iot in the gcc countries; energy requirements & economical analyses study for a concept model in the state of qatar," *Results in Engineering*, vol. 17, p. 100889, 2023.

[33] M. E. E. Alahi, N. Pereira-Ishak, S. C. Mukhopadhyay, and L. Burkitt, "An internet-of-things enabled smart sensing system for nitrate monitoring," *IEEE Internet of Things Journal*, vol. 5, no. 6, pp. 4409–4417, 2018.

[34] X. Zheng, A. Sarwar, F. Islam, A. Majid, A. Tariq, M. Ali, S. Gulzar, M. I. Khan, M. A. S. Ali, M. Israr, *et al.*, "Rainwater harvesting for agriculture development using multi-influence factor and fuzzy overlay techniques," *Environmental Research*, vol. 238, p. 117189, 2023.

[35] A. Ambarwari, D. K. Widyawati, and S. D. Putra, "Design and performance analysis of a fuzzy logic-based iot system for greenhouse irrigation control," *Internet of Things and Artificial Intelligence Journal*, vol. 4, no. 3, pp. 371–383, 2024.

[36] S. D. Putra, M. Yudhiprawira, Y. Kurniawan, S. Sutikno, and A. S. Ahmad, "Security analysis of bc3 algorithm for differential power analysis attack," in *2017 International Symposium on Electronics and Smart Devices (ISESD)*, pp. 341–345, IEEE, 2017.

[37] S. Sutikno, S. D. Putra, F. Wijitrisnanto, and M. E. Aminanto, "Detecting unknown hardware trojans in register transfer level leveraging verilog conditional branching features," *IEEE Access*, vol. 11, pp. 46073–46083, 2023.

[38] S. D. Putra, A. S. Ahmad, and S. Sutikno, "Dpa-countermeasure with knowledge growing system," in *2016 International Symposium on Electronics and Smart Devices (ISESD)*, pp. 16–20, IEEE, 2016.

[39] S. D. Putra, A. D. W. Sumari, A. S. Ahmad, S. Sutikno, and Y. Kurniawan, "Cognitive artificial intelligence countermeasure for enhancing the security of big data hardware from power analysis attack," in *Combating Security Challenges in the Age of Big Data: Powered by State-of-the-Art Artificial Intelligence Techniques*, pp. 61–86, Springer, 2020.

[40] A. Shahid, A. Almogren, N. Javaid, F. A. Al-Zahrani, M. Zuair, and M. Alam, "Blockchain-based agri-food supply chain: A complete solution," *Ieee Access*, vol. 8, pp. 69230–69243, 2020.

[41] K. Košťál, P. Helebrandt, M. Belluš, M. Ries, and I. Kotuliak, "Management and monitoring of iot devices using blockchain," *Sensors*, vol. 19, no. 4, p. 856, 2019.

[42] L. Hang and D.-H. Kim, "Design and implementation of an integrated iot blockchain platform for sensing data integrity," *sensors*, vol. 19, no. 10, p. 2228, 2019.

[43] A. Rehman, T. Saba, M. Kashif, S. M. Fati, S. A. Bahaj, and H. Chaudhry, "A revisit of internet of things technologies for monitoring and control strategies in smart agriculture," *Agronomy*, vol. 12, no. 1, p. 127, 2022.

[44] S. Jarial, "Internet of things application in indian agriculture, challenges and effect on the extension advisory services–a review," *Journal of Agribusiness in Developing and Emerging Economies*, vol. 13, no. 4, pp. 505–519, 2023.

[45] C. Bulut and P. F. Wu, "More than two decades of research on iot in agriculture: a systematic literature review," *Internet Research*, vol. 34, no. 3, pp. 994–1016, 2024.

[46] A. EG and G. J. Bala, "Iot and ml-based automatic irrigation system for smart agriculture system," *Agronomy Journal*, vol. 116, no. 3, pp. 1187–1203, 2024.

[47] H. K. Adli, M. A. Remli, K. N. S. Wan Salihin Wong, N. A. Ismail, A. González-Briones, J. M. Corchado, and M. S. Mohamad, "Recent advancements and challenges of aiot application in smart agriculture: A review," *Sensors*, vol. 23, no. 7, p. 3752, 2023.