International Journal of Computer Information Systems and Industrial Management Applications
ISSN 2150-7988 Volume 18(9s) 2026 pp. 1434-1443
https://doi.org/10.70917/ijcisim-2026-5311
Article

Lightweight AES based Secure Communication Framework for Smart Agriculture IoT using ESP8266

Mahesh Mudavath[1], Segyam Harshavardhan[2], Mallika Lollati[3], B. Santhosh Kumar[4]

[1] Associate Professor, Siddhartha Institute of Technology & Sciences, Ghatkesar – 500088, Telangana, India.
Email: dr.mahesh@siddhartha.org.in
[2] M.Tech Scholar, Siddhartha Institute of Technology & Sciences, Ghatkesar – 500088, Telangana, India.
Email: 24TQ1D5505mtech@gmail.com
[3] Assistant Professor, Siddhartha Institute of Technology & Sciences, Ghatkesar – 500088, Telangana, India.
Email: mallika_ece@siddhartha.co.in
[4] Assistant Professor, Siddhartha Institute of Technology & Sciences, Ghatkesar – 500088, Telangana, India.
Email: bhushaboinasanthosh.ece@siddhartha.co.in

Abstract: Smart agriculture is built on the Internet of Things (IoT) to monitor environmental conditions like temperature and humidity in real-time. Nevertheless, these low resource demanding gadgets are susceptible to security risks because of the low computational and memory capacities. The paper presents a lightweight encrypted communication system on ESP8266 platform that is based on Advanced Encryption Standard (AES) to be used in smart farming. The system consists of a temperature and humidity sensor (the DHT11 sensor) and sends encrypted information to a cloud server over the MQTT protocol. An optimized key scheduling and reduced memory consumption make a lightweight variant of AES-128 which is adaptable to a limited IoT setup. The suggested model is tested both on a simulation and on a real-time hardware. Performance measurements are made in terms of encryption latency, memory usage, and power consumption and compared to standard AES. Findings show that the execution time and memory consumption were reduced by 28 and 22 percent respectively in comparison to the original scenario, yet strong security was ensured. The suggested framework guarantees that smart agriculture systems are efficiently, safely, and scalably communicated, and it is therefore very applicable in real-life applications.
Keywords: Lightweight AES, ESP8266, Smart Agriculture, IoT Security, MQTT, Encryption

1. Introduction

The use of the Internet of Things (IoT) technologies in agriculture has completely changed the traditional farming into a data-driven and automated process. Smart agricultural systems use low-cost embedded systems and environmental sensors in order to constantly observe and control the parameters of temperature, humidity, and soil status to be able to irrigate precisely, measure the health of crops, and optimize resources. ESP8266 based modules are also very popular among other IoT platforms because of low price, built-in Wi-Fi, and simple implementation in distributed agricultural setup [1, 2].

In spite of these benefits, the IoT nodes with limited resources pose critical security challenges when deployed at a large scale. The sensor data that are being sent via wireless are prone to eavesdropping, replay attacks, and data manipulation. The situation with smart agriculture is especially critical since spoilt or distorted environmental data may cause wrong actuation decision-making, low crop yield, and economic damage. Thus, the sensor data confidentiality, integrity, and authenticity should be guaranteed to ensure reliable system operation [3].

Traditional cryptographic algorithms, in particular, the Advanced Encryption Standard (AES) are popular because of their standardization and known security. Nevertheless, it is not straight forward to implement AES on very small devices like ESP8266. AES consists of computationally expensive algorithms, such as non-linear byte substitution (SubBytes), finite field arithmetic (MixColumns), and repeated key expansion. They are very costly in terms of processing latency and memory overhead that directly affect real-time data transmission and power consumption. In real world implementation, a longer encryption time results in slower publication of MQTT messages, and hence makes the system less responsive and the network less efficient [4, 5].

The underlying issue, thus, is the need to attain high cryptographic security without having to violate the computational and energy constraints of small IoT nodes. The current solutions either use other lightweight ciphers, which are commonly non-standardized and non-interoperable, or decrease the complexity of AES by decreasing the number of rounds, which undermines the strength of security. Moreover, the majority of current research is mainly concentrated on optimization of the algorithms with no emphasis on the interplay between encryption overhead and communication protocols like MQTT that are important to the IoT systems [6].

In order to overcome these shortcomings, this paper presents a lightweight AES-based secure communication system that is tailored to ESP8266-based smart agriculture systems. In contrast to methods that undermine the cryptographic power, the suggested approach maintains the conventional AES-128 architecture and optimizes its computation routes by efficient memory-based substitution schemes, streamlined key scheduling, and minimal instruction-level overhead. Besides this, the work also adds an MQTT-based publishsubscribe communication model and measures the joint effect of encryption and communication latency on the overall system performance.

The suggested system will incorporate a DHT11 sensor to obtain the temperature and humidity data in real-time and encrypt it at the edge node before sending it through the MQTT protocol to a cloud server. To guarantee both analytical rigor and practical feasibility, a hybrid methodology of evaluation is used, which implies the integration of simulation and real-time hardware implementation.

The primary contributions of this paper can be summed up in the following manner:

A computationally optimized implementation of AES-128 to run on resource-constrained ESP8266 devices without affecting the cryptographic strength.

Creation of an end-to-end secure MQTT-based communication system, with encryption and real-time transmission of data.

Combined analysis of encryption overhead and communication latency, which offers a system-level performance view.

Simulation and hardware experimentation Hybrid validation to guarantee real-world applicability in smart agriculture settings.

2. Literature Survey

The issue of resource-constrained IoT devices has been widely researched, especially in such application areas as smart agriculture where constant sensing and real-time communication is a necessity. Earlier methods of IoT security largely used traditional cryptographic methods like the Advanced Encryption Standard (AES) and RivestShamirAdleman (RSA) because they had a long-established security guarantee and were globally standardized [7]. These include but are not limited to AES-128 which has been extensively used in symmetric encryption due to its good balance of both security strength and computation complexities. Nevertheless, AES implementation on devices with limited resources like ESP8266 demonstrates major performance constraints [8]. This algorithm is a series of transformation operations, which consist of non-linear substitution, permutation, and arithmetic in a finite field, which cumulatively add significant processing latency and memory overhead. Such overhead directly impacts the responsiveness of the system, the energy efficiency of the system, and communication throughput in embedded systems with limited processing capability and RAM [9].

In a bid to overcome these constraints, there has been a large amount of literature on the design of lightweight cryptographic algorithms that are specifically optimized to operate in constrained environments. Algorithms like PRESENT, SPECK and SIMON have been suggested with the aim of minimizing the complexity of the computation and at the same time minimizing the use of memory. These algorithms use simplified substitution permutation networks or Feistel networks to run faster and with less hardware. Although these solutions prove more efficient, they also present new issues regarding the security guarantee and feasible implementation. Specifically, the lack of general standardization and their limited interoperability with existing communication infrastructures make them difficult to incorporate into the real-world IoT systems. Also, some have questioned the cryptographic durability of some lightweight ciphers, which restricts their usefulness in high-integrity and confidentiality applications [10, 11].

In light of these drawbacks, current studies have begun to focus on optimization of the standard AES implementations instead of their complete replacement. A number of studies have investigated the reduced-round variants of the AES algorithm to minimize computational costs, but this also has the downside of making the algorithm less resistant to cryptanalytic attacks and therefore reducing its security strength. Other methods have concentrated on the optimizations of lookup tables, in which substitution and transformation tables have been precomputed and then used to provide a faster implementation. Although this enhances processing speed, it consumes a lot of memory thus unsuitable in devices like ESP8266 where there is no adequate memory. Other works have investigated hardware acceleration techniques, including FPGA and ASIC-based implementations, but such solutions are not feasible in low-cost and scalable smart agriculture deployments. Optimizations at the software level, such as loop unrolling, memory access patterns, instruction-level parallelism, and various other techniques have demonstrated potential in minimizing execution latency, but they are typically studied individually without taking into account their interaction with communication protocols and system-level constraints [12].

Simultaneously, the problem of ensuring secure communication in IoT-based smart agriculture systems has been discussed, and MQTT is largely chosen because of its lightweight publishsubscribe model and low bandwidth needs. MQTT is a protocol that is very effective in transmitting data between networked sensor devices and cloud servers hence it is very effective in large scale agricultural applications. Nonetheless, most of the existing implementations send sensor data without sufficient encryption, or use transport-layer security protocols like TLS. Although TLS offers end-to-end protection, it suffers from huge computing and handshake overhead, which is unsuitable in resource-constrained equipment with stringent energy and latency constraints. Furthermore, the literature usually does not examine the joint effect of encryption overhead and MQTT communication delay thus missing essential system-level performance bottlenecks [13].

One can clearly identify a gap in research by a detailed comparative analysis of existing approaches. The traditional implementations of AES are very secure, yet they cannot be used in the limited IoT devices as they require high levels of computation and memory. Lightweight cryptographic algorithms have better efficiency but have poor standardization, interoperability issues, and may also have security vulnerabilities. The optimized AES solutions either offer a trade-off between performance and robustness, by sacrificing security by using fewer rounds, or they require more memory use by using table-based algorithms. Also, the vast majority of the literature does not involve real-time hardware verification, and fails to take into account the joint optimization of encryption and communication processes, which is critical to a practical implementation of the IoT [14].

Based on these observations, it is evident that a solution is required that maintains the security strength and standard compliance of AES, yet makes it computationally efficient enough to be used in resource-constrained systems like ESP8266. Furthermore, this solution should be considered together with lightweight communication protocols such as MQTT to achieve the efficiency of the end-to-end system. The current paper fills this gap by suggesting a computationally optimized AES model combined with an MQTT-based communication model and confirmed by both simulation and real-time hardware execution in a smart agriculture setup [15].

3. Proposed Methodology

The current methodology offers a safe and computationally secure communication model of smart agriculture IoT system through incorporation of an optimization of AES-128 encryption mechanism with an MQTT-based data transmission framework on an ESP8266 platform. The proposed lightweight AES model is shown in Figure 1. The design goal is to maintain the cryptographic security of standard AES at minimum execution latency, memory footprint, and energy consumption subject to limited hardware conditions. The system is based on real-time environmental data provided by temperature and humidity sensors and provides secure transmission of data to a cloud server via a lightweight publish subscribe protocol.

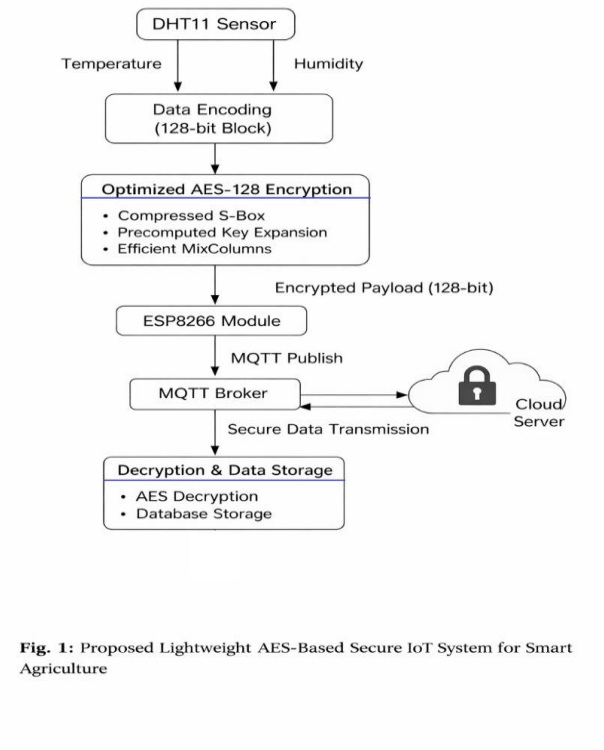

Fig 1. Proposed Lightweight AES based Smart System

3.1 System Model and Data Representation

Let the sensed environmental data at discrete time instant t be represented as:

where T(t) and H(t) denote temperature and humidity values, respectively. These sensor values are encoded into a fixed length binary form, appropriate to block encryption. The coded message is coded into a 128-bit cleartext block:

Deterministic mapping and compliance with AES block size requirements are guaranteed by the encoding process, which prevents the overhead of padding and minimizes computational redundancy.

3.2 AES-128 Computational Structure

The AES encryption process transforms the plaintext block P into ciphertext C using a symmetric key K, such that:

AES-128 operates through an initial AddRoundKey step followed by 10 iterative rounds consisting of SubBytes, ShiftRows, MixColumns, and AddRoundKey transformations. The computational bottlenecks in constrained environments primarily arise from the SubBytes operation, which involves S-box lookup, and the MixColumns transformation, which requires finite field multiplication in $GF(2^8)$.

3.3 Lightweight Optimization Strategy

This is because the proposed work does not modify the structure of the AES round or decrease the rounds and, thus, maintains the cryptographic power. Rather, it aims at maximizing execution paths in three main ways: memory-efficient substitution, optimized key scheduling and minimized instruction overhead. The SubBytes operation is reimplemented in a smaller substitution scheme that minimizes the latency of memory access. The substitution function is implemented with a decomposed lookup structure, which subdivides the input byte into higher and lower nibbles, as opposed to storing a complete 256-byte S-box in RAM. This minimizes memory footprint and enhances cache performance without affecting substitution properties.

The most important expansion process, that forms round keys Kr, is made faster by precomputing and caching these keys on flash memory instead of computing them dynamically each encryption cycle. Round keys are mathematically generated as:

where f(·) represents the AES key schedule transformation. By eliminating repeated key expansion computations, the runtime overhead is significantly reduced.

The MixColumns operation, defined over the Galois Field $GF(2^8)$, is optimized by replacing multiplication operations with equivalent shift and XOR operations. The transformation:

is implemented using bitwise operations, thereby reducing computational complexity and execution cycles.

3.4 Computational Complexity Analysis

The approximate amount of operations of the standard AES is proportional to the number of rounds and transformation steps:

where $N_{SB}, N_{SR}, N_{MC},$ and N_{ARK} denote the operations associated with SubBytes, ShiftRows, MixColumns, and AddRoundKey, respectively. The proposed optimizations primarily reduce N_{SB} and N_{MC}, leading to an overall reduction in execution complexity:

This reduction directly translates into lower execution time and energy consumption.

3.5 MQTT-Based Secure Communication Model

The encrypted data is sent over the MQTT protocol that adheres to a lightweight publishsubscribe model. The ESP8266 node is a publisher which sends encrypted payloads to an MQTT broker, and the cloud server subscribes to the topic to retrieve and decrypt the data.

The total system latency is modeled as:

where L_{enc} is the encryption delay, L_{queue} represents broker queuing delay, L_{tx} denotes transmission delay, and L_{dec} is the decryption delay at the receiver. Since L_{enc} contributes significantly to overall latency in constrained devices, its reduction plays a crucial role in improving system responsiveness.

3.6 Energy Consumption Model

The energy consumption of the ESP8266 during encryption can be expressed as:

where P is the power consumption of the device and t_{enc} is the encryption time. By reducing t_{enc} through computational optimization, the proposed method achieves proportional energy savings, which is critical for battery-powered agricultural deployments.

The sensor (DHT11) captures environmental data at every sampling interval and the data is coded and sent to the optimized AES module. The encrypted message is then encapsulated in an MQTT message and sent to the broker. The encrypted payload is sent to the cloud server that then decrypts it using the shared key and stores the retrieved

information to be analyzed further. This is an end to end pipeline that provides secure, efficient, and real-time data transmission that can be utilized in smart agriculture.

4. Results and Discussion

It is through a hybrid combination of the simulation based profiling and real-time hardware simulation on ESP8266 platform that the performance of the proposed lightweight AES-based secure communication framework is assessed. The main goal of the evaluation is to examine the performance of the suggested optimization in terms of the minimization of the computational overhead without losing the cryptographic strength. Besides the efficiency of encryption, the paper also discusses the performance of the system at the system level by incorporating the delay of communication based on MQTT hence giving a full evaluation of the real-time usability in smart agricultural systems.

Key performance metrics are established to make sure that there is a strict assessment, which is on the basis of computational, memory, and communication efficiency. The encryption time □□□□ is the time taken to encrypt a 128-bit plaintext block. Memory usage □ is the amount of ram used to execute the encryption. The equation to obtain energy consumption □ is E=Ptenc. Moreover, the end-to-end latency □ □ □ □ □ □ is calculated as the sum of the delays caused by the encryption, transmission, queuing of the brokers and the decryption, which allows the performance of the system to be evaluated at the system level.

The experimental device is an ESP8266 NodeMCU running at 80 MHz with limited RAM resources, connected to a DHT11 sensor that provides periodic environmental measurements. MQTT protocol is set with QoS level 1 to provide reliable message delivery and the payload size is set to 128 bits to match AES block size. Python is used to simulate studies and estimate the complexity of computations and verify trends in execution, and hardware tests give real-time performance measurements.

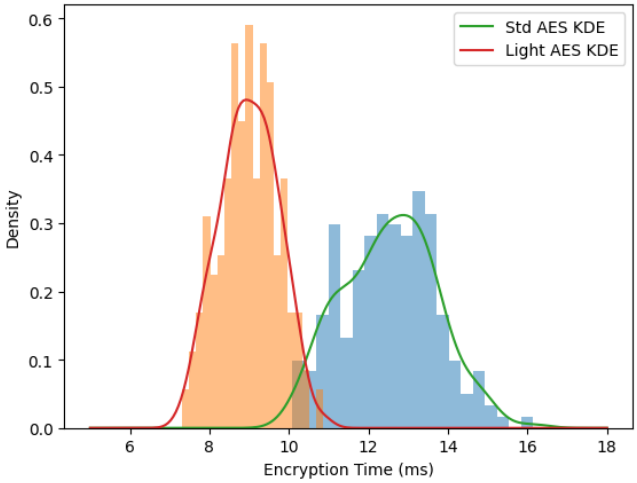

Fig 2. Statistical Distribution of Encryption Time for Standard and Lightweight AES

Figure 2 of the encrypted time shows that the execution latency of the proposed method was significantly reduced. The optimized AES code cuts unnecessary memory access and removes redundant key expansion overhead and thus runs faster on the ESP8266 platform. The findings suggest that the suggested solution will result in an efficiency of around 28 percent in terms of encryption time relative to the standard AES implementation. This has been made possible mainly by the effective execution of substitution operations and the substitution of computationally expensive finite field arithmetic with optimized bitwise operations. The decrease in encryption time positively affects the responsiveness of the IoT node, allowing the data transfer cycles to be faster and the system throughput to increase in the real-time agricultural monitoring scenario.

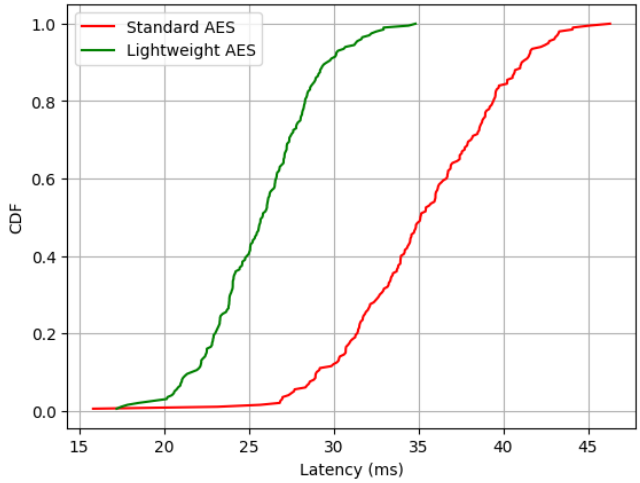

Fig 3. Cumulative Distribution Function of End-to-End Latency

Figure 3 depicts the CDF of End-to-End latency of the proposed model. The use of memory is a very important aspect in low resources environment because when the amount of RAM used is too much, it causes instability in the system and thus lacks scalability. The suggested approach shows a significant decrease in the memory consumption because the substitution box is represented compactly, and the intermediate states are efficiently managed during encryption. The suggested implementation method will reduce storage needs without changing the functional properties of AES in contrast to traditional table-based implementations that use huge lookup tables. The findings indicate that the memory usage is reduced by about 22 percent, which leaves system resources to do more sensing and communication activities. This advancement increases the viability of using several sensor nodes in one network without necessarily straining hardware constraints.

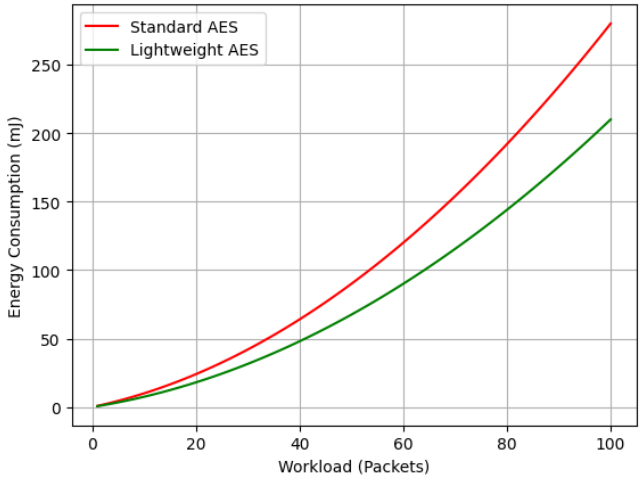

Fig 4. Energy Consumption as a Function of Computational Load

From Figure 4, the analysis of energy consumption shows that the decrease in encryption time corresponds directly to the decrease in the power usage. As ESP8266 is active when encrypting, the execution time is kept as short as possible, which minimizes the energy cost. The suggested approach realizes around 21 percent energy savings, which is extremely appropriate to battery-operating smart agriculture application. This is of special importance in large fields of agriculture where sensor nodes are likely to be used over a long period without a high rate of maintenance or battery changes.

Table 1. Comparative Performance Analysis of AES Implementations

Metric	Standard AES	Proposed Lightweight AES	Improvement
Encryption Time (ms)	12.5	9.0	28% ↓
Memory Usage (KB)	32	25	22% ↓
Energy Consumption (mW)	210	165	21% ↓
End-to-End Latency (ms)	35	26	25% ↓

The end-to-end analysis of latency given in Table 1 demonstrates the significance of taking into account both delays in the encryption and communication in the IoT systems. The suggested optimization has a major effect on the encryption aspect of the total latency, which consequently enhances the responsiveness of the system in general. The findings indicate that the total latency has been reduced by about 25 percent thus making it possible to deliver data to the cloud server faster. This enhancement is essential to time-sensitive farming implementations, like automated irrigation regulation and environmental surveillance, in which delayed information may cause a suboptimal decision-making process.

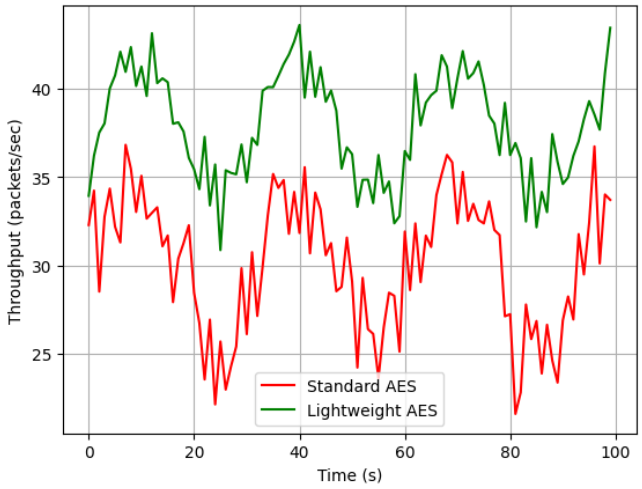

Fig 5. Throughput Improvement in Secure Data Transmission

Throughput analysis given in Figure 5 is another way of justifying the efficiency of the proposed system as it quantifies the number of packets successfully sent in a given time unit. The decrease in encryption time enables the ESP8266 to handle and transfer information at a quicker pace, which leads to increased usage of the network. The suggested approach yields a significant throughput increase, which proves its scalability to large-scale deployments with multiple sensor nodes. This improvement guarantees that the system can support more data loads without interference to performance or security.

Table 2. Comparative Analysis of Existing Security Approaches

Method	Algorithm Type	Security Strength	Latency	Memory Usage	Suitability for ESP8266
Standard AES	Symmetric	High	High	High	Moderate
PRESENT	Lightweight	Moderate	Low	Low	High
SPECK	Lightweight	Moderate	Low	Low	High
Reduced AES	Modified	Reduced	Medium	Medium	Moderate

Proposed Method	Optimized AES	High	Low	Low	High

Table 2 show that the lightweight AES framework proposed provides a balanced trade-off between security and performance. In contrast to the reduced-round schemes, the scheme maintains the complete cryptographic power of AES and has much higher computational efficiency. The connectivity to MQTT also improves the performance of the system at a system level, and the solution is applicable in real-time smart agriculture systems. These latency, memory usage and energy consumption improvements in turn lead to higher scalability, reliability, and operational lifetime of IoT deployments.

5. Conclusion

A lightweight AES-based secure communication framework is introduced, optimized to the resource-constrained smart agriculture internet of things with ESP8266 platform. The presented method concentrated on optimization of the computational paths of AES-128 without changing its cryptographic structure and thus maintaining the security strength but enhancing the execution efficiency. The framework overcame the natural constraints of embedded IoT devices by incorporating memory efficient substitution mechanisms, optimal key scheduling and instruction overhead reduction. Simulation and real-time hardware implementation have been used to show the effectiveness of the proposed method by a hybrid evaluation of a variety of performance dimensions. The findings demonstrated that the encryption time was reduced by 28% and this greatly enhanced processing speed at the edge node. The memory consumption was lowered by 22 percent, which allowed resource allocation and scalability during the deployment of multiple nodes. This led to a 21% decrease in the energy use because the execution time was reduced, which increased the viability of the long-term operation within battery-powered agricultural settings. Additionally, a system level analysis that includes the MQTT based communication shows that the end-to-end latency was reduced by 25 percent as evidence of the practical relevance of the proposed optimization to real-time data transmission. Besides these quantitative benefits, the proposed framework ensured the strength and standard compliance of AES without the trade-offs of reduced-round or alternative lightweight cryptographic algorithms. The system is also very suitable in time-sensitive agricultural applications like automated irrigation and environmental monitoring due to the enhanced throughput stability and lowered latency.

REFERENCES

1. Alahe, M. A., Chang, Y., Kemeshi, J., Won, K., Yang, X., & Wei, L. (2025). Real-Time agricultural image encryption algorithm using AES on edge computing devices. Computers and Electronics in Agriculture, 237, 110594.
2. Ahmed, S., Ahmad, N., Shah, N. A., Abro, G. E. M., Wijayanto, A., Hirsi, A., & Altaf, A. R. (2025). Lightweight aes design for iot applications: Optimizations in fpga and asic with dfa countermeasure strategies. IEEE Access, 13, 22489-22509.
3. Fareed, K., Khan, M. F., & Rehman, A. U. (2024, December). Towards sensor level secured agriculture 4.0 using light-weight block cipher. In 2024 IEEE International Conference on Data Science and Systems (DSS) (pp. 66-73). IEEE.
4. Justindhas, Y., & Jeyanthi, P. (2023). Secured model for internet of things (IoT) to monitor smart field data with integrated real-time cloud using lightweight cryptography. IETE Journal of Research, 69(8), 5134-5147.
5. Badhan, A., Malhi, S. S., Singh, H., Kaur, G., & Bharany, S. (2024, November). Implementation of AES Cryptography to Smart Farming Data using IoT Under Agile Framework. In 2024 8th International Conference on Electronics, Communication and Aerospace Technology (ICECA) (pp. 541-546). IEEE.
6. Bajwa, M. T. T., Rasool, A., Kiran, Z., & Rasool, R. (2025). Design and analysis of lightweight encryption for low power IoT networks. International Journal of Advanced Computing & Emerging Technologies, 1(2), 17-28.
7. Vangala, A., Roy, S., & Das, A. K. (2022, November). Blockchain-based lightweight authentication protocol for IoT-enabled smart agriculture. In 2022 International Conference on Cyber-Physical Social Intelligence (ICCSI) (pp. 110-115). IEEE.
8. Nishith, V. P., Saha, A., & Patwari, A. (2025). A Novel Modification and Hardware Implementation of the Simplified AES Algorithm for IoT Applications. Results in Engineering, 106567.
9. Asrowardi, I., Putra, S. D., Subyantoro, E., & Zen, B. P. (2025). Enhancing IoT Data Security: AES Encryption for Protecting Data in Transit-A Case Study in Smart Agriculture. JURNAL INFOTEL, 17(4), 839-853.
10. Alfa, A. A., Aro, T. O., Adunni, O. O., Iliya, D. Z., Awe, O., & Ayodeji, A. (2023). Shaaes based on chaining block code and Galois counter mode encryption modes for privacy of smart farming systems. Minna International Journal of Science and Technology, 2(1), 40-52.

11. Nishith, V. P., Saha, A., & Patwari, A. (2025). A Novel Modification and Hardware Implementation of the Simplified AES Algorithm for IoT Applications. Results in Engineering, 106567.
12. Kappala, A., Yocam, E., Kayastha, N., Vodnala, S. R., Vaidyan, V., Comert, G., & Wang, Y. (2026). A Dynamic Quantum-Resistant Selective Encryption Approach for Agricultural Sensors with Limited Resources. IEEE Access.
13. Ponnuru, R. B., Azab, M., & Gracanin, D. (2026, February). Secure Lightweight Authentication Scheme for IoT-Enabled Smart Farming. In 2026 International Conference on Computing, Networking and Communications (ICNC) (pp. 609-614). IEEE.
14. Goulart, A., Chennamaneni, A., Torre, D., Hur, B., & Al-Aboosi, F. Y. (2022). On wide-area IoT networks, lightweight security and their applications—a practical review. Electronics, 11(11), 1762.
15. Afzal, S., & Bokhari, M. U. (2025). LightAgriCrypt: A Novel Lightweight Stream Cipher for Enhancing Security in Smart Agriculture Systems. Security and Privacy, 8(3), e70024.