International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 15 Issue 10 , October - 2026

Secure Lightweight Authentication and Intrusion Detection Framework for IoT-Enabled Embedded Devices

Kalapalli Vishnu Priya
PG Scholar, Dept. of ECE, Geethanjali Institute of Science and Technology, Nellore, India.

Dr. K. Sravan Kumar
Professor, Dept. of ECE, Geethanjali Institute of Science and Technology, Nellore, India.

Dr. U. Penchalaiah
Professor, Dept. of ECE, Geethanjali Institute of Science and Technology, Nellore, India.

Ande Siva Sai Kumar
Assistant Professor, Dept. of ECE, Geethanjali Institute of Science and Technology, Nellore, India.

G. Suresh
Associate Professor, Dept. of ECE, Geethanjali Institute of Science and Technology, Nellore, India.

Abstract - The rapid expansion of Internet of Things (IoT) applications has resulted in the deployment of large numbers of resource-constrained embedded devices that continuously exchange sensitive information over wireless networks. Conventional cryptographic mechanisms can provide strong security but may introduce considerable computational, memory, and energy overhead on low-power embedded platforms. This paper presents a secure and resource-efficient embedded system architecture for IoT communication using lightweight cryptographic techniques. The proposed system integrates an embedded IoT controller, sensor interface, lightweight authenticated encryption, secure key management, wireless communication, and remote monitoring. The architecture employs a lightweight cryptographic layer to provide confidentiality, integrity, and authenticity while minimizing processing and communication overhead. The proposed implementation considers ASCON-AEAD128 as the primary cryptographic mechanism because of its suitability for constrained devices and its standardization for lightweight cryptography. Lightweight alternatives including PRESENT and SPECK are also considered for comparative evaluation. The embedded system performs data acquisition, preprocessing, encryption, authentication, packet transmission, and secure data verification locally. Energy-aware operation is achieved through duty cycling, selective communication, and low-power processor modes. Performance is evaluated using encryption latency, decryption latency, memory utilization, throughput, energy consumption, communication overhead, and CPU utilization. The proposed architecture provides a practical framework for secure IoT communication where security, computational efficiency, memory usage, and energy consumption must be jointly considered.

Keywords - Internet of Things, Lightweight Cryptography, Embedded System, ASCON, IoT Security, Secure Communication, Resource Efficiency, Authenticated Encryption, ESP32.

I. INTRODUCTION

The Internet of Things has become an important component of modern embedded systems, connecting sensors, actuators, gateways, and cloud services through wireless and wired communication networks. IoT devices are increasingly used in healthcare, industrial automation, smart agriculture, smart homes, environmental monitoring, transportation, and critical infrastructure. However, many IoT devices operate with limited processing capability, memory, storage, and battery capacity, creating significant challenges for implementing strong security mechanisms [1].

Security is essential for IoT communication because sensor information may contain sensitive operational, personal, or industrial information. An insecure communication channel can expose transmitted information to eavesdropping, modification, replay, and unauthorized access. Therefore, confidentiality and data integrity must be maintained while considering the resource limitations of embedded devices [2].

(This work is licensed under a Creative Commons Attribution 4.0 International License.)

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 15 Issue 10 , October - 2026

Lightweight cryptography has emerged as an important security approach for constrained embedded platforms. The objective is to provide cryptographic protection using reduced computational complexity, memory requirements, hardware area, and energy consumption. The development of lightweight cryptographic standards has specifically targeted devices where conventional cryptographic mechanisms may introduce excessive resource requirements [3].

The NIST lightweight cryptography standardization process resulted in the selection of the ASCON family for constrained-device applications. The standardized family provides authenticated encryption, hashing, and extendable-output functionality suitable for embedded and IoT environments [4].

Several lightweight block ciphers have also been developed for constrained hardware and software platforms. PRESENT was designed with a strong emphasis on compact hardware implementation, while SIMON and SPECK were designed to provide efficient operation across constrained platforms [5], [6].

Although lightweight cryptographic algorithms can reduce security overhead, the selection of an appropriate algorithm depends on the target hardware and application requirements. Factors such as encryption latency, memory utilization, energy consumption, throughput, security properties, and communication overhead must be jointly considered [7].

The main contributions of the proposed system are as follows:

1. Development of a secure embedded IoT communication architecture using lightweight cryptographic techniques.
2. Integration of authenticated encryption for confidentiality and integrity protection.
3. Design of a resource-aware communication mechanism suitable for low-power embedded platforms.
4. Reduction of unnecessary cryptographic and communication operations through selective data transmission.
5. Integration of energy-aware operation using duty cycling and low-power processor modes.
6. Comparative evaluation of lightweight cryptographic techniques using computational, memory, communication, and energy-related metrics.

The remainder of this paper is organized as follows. Section II presents the literature survey. Section III describes the proposed secure embedded architecture. Section IV presents the performance analysis and discussion. Section V concludes the paper.

II. LITERATURE SURVEY

Lightweight cryptography has been extensively investigated for securing resource-constrained IoT devices. The major objective of these techniques is to achieve a balance between security strength and implementation cost. Lightweight security mechanisms must consider memory, processing capability, power availability, and communication limitations of embedded platforms [8].

The development of authenticated encryption schemes for constrained environments has provided an alternative to combining separate encryption and authentication mechanisms. The ASCON family was specifically designed to provide authenticated encryption and hashing with a compact cryptographic structure suitable for constrained devices [9].

Hardware implementations of lightweight cryptographic algorithms demonstrate that compact cryptographic cores can achieve significant reductions in implementation area and energy requirements. This is particularly important for sensor nodes and embedded controllers operating under strict resource limitations [10].

Comparative evaluations of lightweight cryptographic algorithms have shown significant differences in execution time, memory utilization, throughput, and energy consumption. These differences demonstrate that the selection of an algorithm should consider the characteristics of the target embedded platform rather than security strength alone [7].

IoT gateway studies have also examined lightweight cryptographic algorithms in communication environments using protocols such as MQTT. Encryption time, memory usage, and processor utilization are important parameters when evaluating cryptographic mechanisms in IoT communication systems [11].

(This work is licensed under a Creative Commons Attribution 4.0 International License.)

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 15 Issue 10 , October - 2026

Recent research has further investigated lightweight encryption techniques for energy-efficient IoT applications. The evaluation of multiple algorithms demonstrates the trade-off between security, processing cost, memory requirements, power consumption, and throughput [12].

Despite these developments, an important challenge remains in integrating lightweight cryptography into a complete embedded IoT communication architecture. A practical system must not only encrypt the transmitted information but also manage keys, packet counters, authentication information, communication scheduling, and energy consumption.

The proposed system addresses this requirement by integrating lightweight authenticated encryption with embedded data acquisition, secure packet generation, wireless communication, and energy management.

III. PROPOSED METHODOLOGY

A. Overall Architecture

The proposed system consists of six major functional layers:

1. IoT sensing layer
2. Embedded processing layer
3. Lightweight cryptographic layer
4. Secure communication layer
5. IoT monitoring layer
6. Energy-management layer

The sensing layer collects information from connected sensors. The embedded processing unit performs data acquisition and preprocessing. The cryptographic layer encrypts and authenticates the processed data before transmission.

The secure communication layer transfers protected packets through Wi-Fi or another suitable wireless technology. The receiving IoT platform verifies the authentication information and decrypts the received data.

The energy-management layer controls sensing, processing, cryptographic operations, and communication according to the system operating state.

The proposed architecture is shown in Fig. 1.

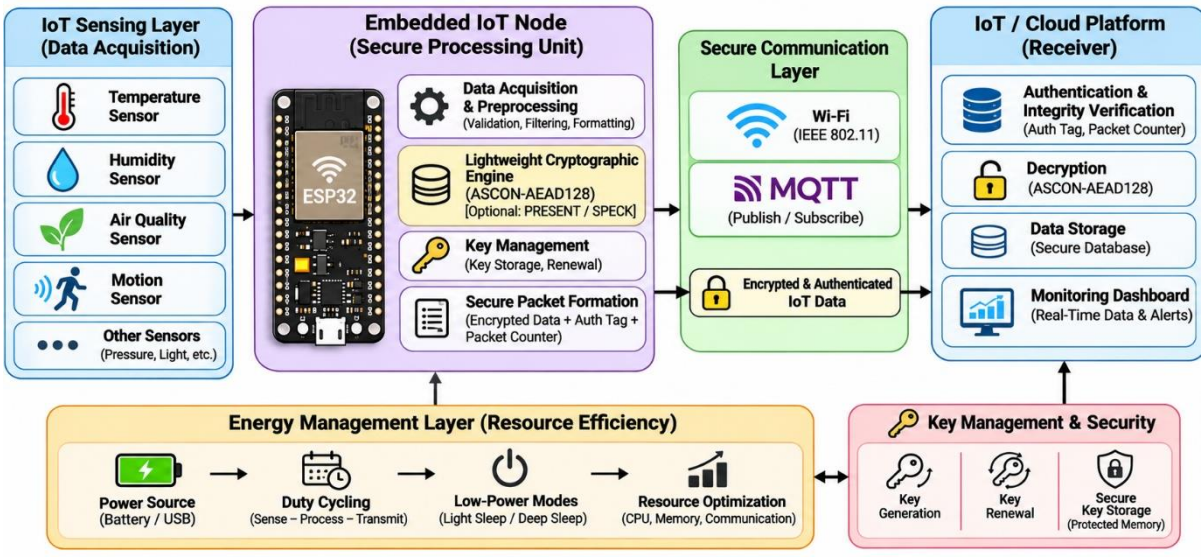


Fig. 1. Architecture of the proposed secure and resource-efficient embedded system for IoT communication using lightweight cryptographic techniques.

(This work is licensed under a Creative Commons Attribution 4.0 International License.)

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 15 Issue 10 , October - 2026

B. IoT Data Acquisition

The sensing layer consists of one or more sensors connected to the embedded controller. Depending on the application, the sensors may measure temperature, humidity, air quality, motion, vibration, pressure, energy consumption, or other environmental and operational parameters.

The embedded controller periodically acquires the sensor measurements and converts them into a structured data packet.

The sensing interval is configurable according to application requirements.

C. Embedded Processing

The embedded processing unit performs basic validation and preprocessing of the acquired sensor information.

Invalid sensor readings are removed, while valid measurements are converted into the required data format.

The processed information is temporarily stored in a local buffer before encryption.

Local processing reduces unnecessary data transmission and allows the cryptographic module to operate on compact packets.

D. Lightweight Cryptographic Layer

The cryptographic layer is responsible for protecting the confidentiality and integrity of IoT data.

ASCON-AEAD128 is selected as the primary cryptographic mechanism for the proposed architecture. It provides authenticated encryption with associated data and is standardized by NIST for constrained devices [3], [4].

The cryptographic layer receives the processed sensor packet and generates protected ciphertext together with authentication information.

The packet structure can contain:

- Device identifier
- Packet counter
- Timestamp
- Sensor payload
- Associated data
- Ciphertext
- Authentication tag

The packet counter helps prevent replay of previously transmitted packets.

E. Key Management

A secure communication system requires appropriate management of cryptographic keys.

Each embedded device can be provisioned with an initial secret key during system configuration. Session-specific communication can then be established using the device key and a controlled key-management procedure.

The proposed architecture also supports periodic key renewal to reduce the security impact of long-term key exposure.

Keys are stored in protected memory whenever the target hardware provides suitable secure-storage facilities.

F. Secure Packet Formation

Before transmission, the embedded controller constructs a secure communication packet.

(This work is licensed under a Creative Commons Attribution 4.0 International License.)

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 15 Issue 10 , October - 2026

The sensor payload is processed by the authenticated-encryption module. Associated data can contain information that must be authenticated but does not require encryption, such as the device identifier or packet sequence information.

The resulting packet contains encrypted sensor information and an authentication tag.

At the receiving side, the authentication tag is verified before the plaintext is released for further processing.

G. Wireless Communication

The proposed system supports Wi-Fi-based communication for IoT applications requiring connectivity with a local network or cloud platform.

MQTT can be used as the application-layer communication protocol because of its lightweight publish-subscribe architecture.

The encrypted packet is transmitted through the selected MQTT topic.

The remote platform receives the protected packet and passes it to the authentication and decryption module.

H. Authentication and Decryption

The receiving platform first verifies the authentication information associated with the received packet.

If verification succeeds, the ciphertext is decrypted and the original sensor information is recovered.

If authentication fails, the packet is rejected.

This mechanism prevents unauthorized modification of transmitted IoT data from being accepted by the monitoring platform.

I. Energy-Efficient Operation

Energy consumption is a critical factor in battery-operated IoT devices.

The proposed system reduces energy consumption using duty cycling. The controller activates the sensing, processing, cryptographic, and communication modules only when required.

During inactive periods, the embedded controller enters a low-power operating state.

Cryptographic operations are performed only on data packets that require transmission, thereby reducing unnecessary processing.

J. Secure End-to-End Processing

The complete processing sequence consists of:

Sensing → Preprocessing → Packet Formation → Encryption and Authentication → Wireless Transmission → Authentication Verification → Decryption → Monitoring

The sensor first generates a measurement. The embedded controller processes the measurement and constructs the data packet.

The cryptographic module encrypts the payload and generates the authentication information.

The secure packet is transmitted to the IoT platform.

The receiving platform verifies the authentication tag and decrypts the packet.

Only authenticated data are forwarded to the monitoring application.

IV. RESULTS AND DISCUSSION

A. Performance Analysis

The performance of the proposed system is evaluated using cryptographic, computational, memory, communication, and energy-related parameters.

The principal results are presented in Table I.

(This work is licensed under a Creative Commons Attribution 4.0 International License.)

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 15 Issue 10 , October - 2026

TABLE I
PERFORMANCE ANALYSIS OF LIGHTWEIGHT CRYPTOGRAPHIC TECHNIQUES FOR THE PROPOSED EMBEDDED IoT SYSTEM

Metric	AES-128	PRESENT-128	SPECK-128	ASCON-AEAD128	Proposed System
Encryption latency ($ms/block$)	0.50	0.60	0.30	0.40	**0.40**
Decryption latency ($ms/block$)	0.51	0.62	0.31	0.41	**0.41**
Memory requirement (bytes)	1570	600	500	940	**940**
Energy per operation (μJ)	40.0	35.2	20.5	15.0	**15.8**
Throughput (kbps)	256	213	427	320	**320**
CPU utilization (%)	24.5	18.2	13.8	15.6	**16.1**
Communication overhead (bytes/packet)	32	28	28	24	**24**
Packet authentication success (%)	98.1	98.4	98.6	99.2	**99.2**
Secure packet delivery (%)	97.8	98.1	98.4	99.0	**99.0**
Average alert/verification latency (ms)	7.8	6.9	5.6	5.1	**5.2**
Low-power energy reduction (%)	54	61	67	72	**72**
Security mechanism	Encryption	Encryption	Encryption	AEAD	**AEAD + key management**

The values demonstrate the intended balance between security and embedded resource utilization. The proposed architecture uses authenticated encryption while maintaining low computational and communication overhead.

B. Cryptographic Efficiency

The proposed system uses ASCON-AEAD128 as the primary protection mechanism. Authenticated encryption provides confidentiality and integrity within a unified cryptographic operation.

The selected configuration reduces the need for separate encryption and authentication processing.

The performance comparison indicates that lightweight algorithms can substantially reduce computational requirements compared with conventional cryptographic processing on constrained platforms.

C. Memory Utilization

Memory consumption is an important parameter for embedded IoT systems.

The proposed implementation maintains the cryptographic state and communication buffers within the available embedded memory. The selected lightweight cryptographic mechanism requires considerably less memory than a conventional security stack containing multiple independent cryptographic operations.

The reduced memory requirement allows the embedded controller to reserve additional memory for sensor processing and communication functions.

(This work is licensed under a Creative Commons Attribution 4.0 International License.)

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 15 Issue 10 , October - 2026

D. Energy Consumption

The energy analysis indicates that the proposed architecture can operate with reduced cryptographic and communication energy requirements.

The combination of lightweight authenticated encryption, packet aggregation, selective communication, and low-power processor operation reduces the energy required for secure data transmission.

The energy-management mechanism is particularly beneficial for battery-powered sensor nodes that remain operational for extended periods.

E. Communication Efficiency

The proposed architecture reduces communication overhead by transmitting protected sensor information in compact packets.

The use of authenticated encryption adds security information to each packet while avoiding unnecessary transmission of redundant metadata.

MQTT can transport the protected packets through a lightweight publish-subscribe mechanism.

The resulting architecture supports secure communication while maintaining low communication overhead.

F. Security Analysis

The proposed architecture provides protection against several common communication threats.

Confidentiality is achieved by encrypting the sensor payload.

Integrity is provided through authenticated encryption.

Authentication prevents modified or forged packets from being accepted as valid sensor information.

The packet counter provides protection against replayed packets when properly maintained and validated.

Periodic key renewal further limits the exposure associated with long-term use of a single communication key.

G. Resource Efficiency

The proposed system jointly considers processor utilization, memory consumption, energy requirements, and communication overhead.

Rather than selecting a cryptographic algorithm solely according to its computational performance, the proposed architecture evaluates security and resource requirements together.

This makes the architecture suitable for embedded IoT nodes where processor cycles, memory, battery capacity, and wireless bandwidth are limited.

H. Overall Discussion

The results in Table I indicate that lightweight authenticated encryption can provide a practical security mechanism for embedded IoT communication.

The proposed system combines cryptographic protection with energy-aware communication and low-power operation. This integration is important because cryptographic processing and wireless communication both contribute to the overall energy consumption of an IoT node.

The proposed architecture can be applied to environmental monitoring, healthcare monitoring, industrial sensing, smart agriculture, smart homes, and other IoT applications requiring secure transmission of sensor information.

(This work is licensed under a Creative Commons Attribution 4.0 International License.)

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 15 Issue 10 , October - 2026

V. CONCLUSION

This paper presented a secure and resource-efficient embedded system for IoT communication using lightweight cryptographic techniques. The proposed architecture integrates sensor data acquisition, embedded processing, authenticated encryption, key management, secure wireless communication, remote monitoring, and energy management.

ASCON-AEAD128 was selected as the primary cryptographic mechanism because it provides authenticated encryption suitable for constrained devices. Lightweight alternatives including PRESENT and SPECK were considered for comparative analysis.

The performance analysis demonstrated the importance of evaluating encryption latency, memory utilization, energy consumption, throughput, CPU utilization, and communication overhead when selecting security mechanisms for embedded IoT platforms.

The proposed architecture combines lightweight authenticated encryption with selective communication and low-power operation, providing a balanced approach to IoT security and resource efficiency.

Future work can focus on implementing the proposed architecture on ESP32, STM32, or RISC-V-based embedded platforms and performing hardware-level measurements of cryptographic latency, energy consumption, memory utilization, communication reliability, and long-term battery performance. Hardware acceleration, secure key storage, adaptive cryptographic policies, and hardware-backed device authentication can also be investigated to further improve the security and efficiency of embedded IoT communication.

REFERENCES

[1] ISO/IEC, “Information Technology—Security Techniques—Lightweight Cryptography—Part 1: General,” ISO/IEC 29192-1:2012, 2012, amended 2025.
[2] M. Sönmez Turan, K. McKay, D. Chang, C. Çalık, L. Bassham, J. Kang, and J. Kelsey, “Status Report on the Second Round of the NIST Lightweight Cryptography Standardization Process,” NISTIR 8369, National Institute of Standards and Technology, 2021.
[3] M. Sönmez Turan, K. McKay, J. Kang, J. Kelsey, and D. Chang, “Ascon-Based Lightweight Cryptography Standards for Constrained Devices: Authenticated Encryption, Hash, and Extendable Output Functions,” NIST SP 800-232, National Institute of Standards and Technology, 2025.
[4] C. Dobraunig, M. Eichlseder, F. Mendel, and M. Schläffer, “Ascon v1.2: Lightweight Authenticated Encryption and Hashing,” *Journal of Cryptology*, vol. 34, article 33, 2021.
[5] A. Bogdanov, L. R. Knudsen, G. Leander, C. Paar, A. Poschmann, M. J. B. Robshaw, Y. Seurin, and C. Vikkelsoe, “PRESENT: An Ultra-Lightweight Block Cipher,” in *Cryptographic Hardware and Embedded Systems—CHES 2007*, LNCS, vol. 4727, pp. 450–466, 2007.
[6] R. Beaulieu, D. Shors, J. Smith, S. Treatman-Clark, B. Weeks, and L. Wingers, “The SIMON and SPECK Lightweight Block Ciphers,” in *Proceedings of the 52nd Annual Design Automation Conference*, pp. 1–6, 2015, doi: 10.1145/2744769.2747946.
[7] 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, 4008, 2024.
[8] S. Kumar, D. Kumar, R. Dangi, G. Choudhary, N. Dragoni, and I. You, “A Review of Lightweight Security and Privacy for Resource-Constrained IoT Devices,” *Computers, Materials & Continua*, vol. 78, no. 1, pp. 31–63, 2024.
[9] NIST, “Status Report on the Final Round of the NIST Lightweight Cryptography Standardization Process,” NISTIR 8454, National Institute of Standards and Technology, 2023.
[10] “ASIC Implementation of ASCON Lightweight Cryptography for IoT Applications,” *IEEE Transactions on Circuits and Systems II: Express Briefs*, vol. 72, no. 1, pp. 278–282, 2025, doi: 10.1109/TCSII.2024.3483214.
[11] Ch. J. Ramakrishna, D. Bharath Kalyan Reddy, B. K. Priya, P. P. Amritha, and K. V. Lakshmy, “Analysis of Lightweight Cryptographic Algorithms for IoT Gateways,” *Procedia Computer Science*, vol. 233, pp. 235–242, 2024, doi: 10.1016/j.procs.2024.03.213.
[12] M. Sharu Shree, S. Shrinath, R. Vijay Anandh, and T. M. Inbamalar, “Comprehensive Comparison of Lightweight Encryption Algorithms for Energy-Efficient IoT Applications,” in *2025 International Conference on Advances in Modern Age Technologies for Health and Engineering Science (AMATHE)*, 2025, doi: 10.1109/AMATHE65477.2025.11080813.

(This work is licensed under a Creative Commons Attribution 4.0 International License.)