IJARSCT
International Journal of Advanced Research in Science, Communication and Technology
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
ISSN: 2581-9429
Volume 6, Issue 2, August 2026
Impact Factor: 8.2

A Review of Energy-Efficient Encryption Techniques for Secure Data Transmission in IoT Networks

Bavdhankar Pravin Bhanudas[1] and Dr. Nikhil Janardan Rathod[2]
[1]Research Scholar, Department of Electronics & Communication Engineering
[2]Associate Professor, Department of Electronics & Communication Engineering
Vikrant University, Gwalior, M.P, India

Abstract : *The Internet of Things connects sensors, actuators, embedded controllers, gateways and cloud services to support continuous data collection and automated decision-making. These devices frequently operate with limited battery capacity, processing power, memory and communication bandwidth. Encryption is essential for protecting data confidentiality, while authenticated encryption also provides integrity and source authenticity; however, cryptographic operations can increase energy use, latency, code size and packet overhead. This review examines energy-efficient encryption approaches for secure data transmission in resource-constrained IoT networks.*

Keywords: Internet of Things, Lightweight Cryptography, Energy Efficiency, Authenticated Encryption.

I. INTRODUCTION

The Internet of Things has become a foundational component of smart homes, healthcare monitoring, industrial automation, smart agriculture, transportation and urban infrastructure. IoT deployments combine large numbers of heterogeneous devices that continuously exchange telemetry, control commands and event notifications. Many endpoints are small battery-powered sensors or embedded controllers with modest processors, limited RAM and flash memory, and low-bandwidth wireless links. Their operating environment creates a distinctive security challenge: devices must protect sensitive information while preserving battery life and meeting real-time communication requirements.

Encryption is a central control for preventing unauthorized parties from reading transmitted data. Yet confidentiality alone is not sufficient. An attacker may alter a sensor reading, inject a false command, replay an old message or impersonate a device. Secure transmission therefore requires authenticated encryption, sound key establishment, freshness protection and secure implementation. Authenticated Encryption with Associated Data combines confidentiality and integrity protection while allowing selected packet headers to remain visible but authenticated. For constrained devices, a compact AEAD implementation can reduce the need to combine separate encryption and message-authentication operations.

Traditional cryptographic algorithms remain valuable, but their suitability depends on the hardware and workload. AES can be efficient on microcontrollers that provide dedicated AES instructions or accelerators, while software-only implementations may impose a different energy and latency profile. Stream ciphers such as ChaCha20 can perform well on processors without AES acceleration, although their suitability must be assessed alongside authentication and nonce management. ECC supports public-key authentication and key agreement with smaller keys than traditional RSA at comparable security levels, but public-key operations are usually more expensive than symmetric encryption. Lightweight designs such as Ascon were developed to address constrained environments, and NIST published SP 800-

IJARSCT
International Journal of Advanced Research in Science, Communication and Technology
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
ISSN: 2581-9429 Volume 6, Issue 2, August 2026 Impact Factor: 8.2

232 in August 2025 to standardize Ascon-based authenticated encryption, hashing and extendable-output functions (Turan 2025).

REVIEW METHODOLOGY

This paper uses a structured literature-review approach. The source set was assembled around peer-reviewed review articles, cryptographic design papers, standards publications and Internet Engineering Task Force (IETF) protocol specifications relevant to constrained IoT environments. Search concepts included "IoT lightweight cryptography," "energy-efficient encryption," "authenticated encryption," "Ascon," "AES," "ChaCha20," "ECC," "constrained devices," "OSCORE" and "IoT energy consumption." The literature base emphasizes publications from 2019–2026 while retaining foundational specifications where necessary.

Studies and standards were considered relevant when they addressed at least one of the following: (a) cryptographic algorithms intended for constrained hardware; (b) measured or discussed energy, execution time, memory, throughput or communication overhead; (c) authentication or key establishment for IoT; or (d) protocol integration for end-to-end protection. Material unrelated to IoT or lacking a clear connection to encryption or secure communication was not used in the synthesis. The review is qualitative and comparative rather than a statistical meta-analysis.

A methodological limitation should be stated clearly: this document is a structured narrative synthesis of identifiable literature and standards, not a registered PRISMA review with a fully reproducible multi-database search log, independent duplicate screening, or a formal risk-of-bias assessment. Accordingly, it does not claim a comprehensive count of all eligible papers or calculate pooled energy-effect estimates. Quantitative values are not invented where studies use different processors, clock rates, voltage levels, payload sizes and test conditions. The comparative tables therefore summarize functional characteristics and evaluation considerations rather than presenting non-comparable numerical rankings.

1. Analytical Framework

The reviewed techniques are compared across five dimensions: security capability, computational cost, memory footprint, communication overhead and energy behavior. Energy is treated as a system property. A useful conceptual model is:

E_total = E_crypto + E_radio + E_key + E_idle + E_retransmission

Here, E_crypto represents encryption and authentication energy; E_radio represents the energy required to transmit and receive packets; E_key represents key generation, exchange and renewal; E_idle represents listening and standby consumption; and E_retransmission represents additional energy caused by packet loss or protocol retries. This model is conceptual and is intended to prevent the common mistake of equating lower CPU execution time with lower total device energy.

ENERGY-EFFICIENT ENCRYPTION TECHNIQUES

1. Lightweight Authenticated Encryption: Ascon

Ascon is a family of permutation-based cryptographic algorithms designed for authenticated encryption and hashing in constrained environments. The Ascon design provides confidentiality and authenticity in one AEAD operation and was evaluated for implementation across both constrained platforms and general-purpose processors (Dobraunig 2021). NIST SP 800-232, finalized in August 2025, specifies Ascon-AEAD128, Ascon-Hash256, Ascon-XOF128 and Ascon-CXOF128 for constrained-device applications (Turan 2025). This standardization is significant because it provides a stable specification for developers and procurement teams.

Ascon is particularly relevant where compact software or hardware implementations are required and AES acceleration is absent or inefficient. Its AEAD interface allows packet metadata, such as protocol identifiers or sequence context, to be authenticated as associated data without encrypting it. However, the label "lightweight" does not guarantee the lowest energy on every platform. Implementations must follow the standardized parameters, use unique nonces as required, verify tags before accepting plaintext, and be benchmarked on the target microcontroller.

IJARSCT
International Journal of Advanced Research in Science, Communication and Technology
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
ISSN: 2581-9429
Volume 6, Issue 2, August 2026
Impact Factor: 8.2

2. Advanced Encryption Standard

AES is a widely deployed symmetric block cipher with extensive analysis, implementation experience and hardware support. In IoT devices equipped with AES acceleration, AES-based AEAD modes can provide strong security with low processing cost. AES-GCM is a commonly specified authenticated-encryption mode, but it requires careful nonce uniqueness and correct tag handling. On small processors without acceleration, software AES may require more cycles and code or data memory than expected. The practical conclusion is not that AES is unsuitable, but that its energy profile is hardware-dependent.

3. Stream Ciphers: ChaCha20-Poly1305 and Related Designs

ChaCha20-Poly1305 combines a stream cipher with a one-time authenticator to provide authenticated encryption. It is attractive on processors where software arithmetic is efficient but dedicated AES hardware is unavailable. Its performance can be competitive for larger payloads, although results depend on the processor architecture, implementation and packet size. XChaCha20 extends the nonce construction to support a larger nonce space in applications that need it; protocol and library specifications must be followed precisely.

Stream ciphers require strict nonce discipline. Reusing a nonce with the same key can expose plaintext relationships and compromise authentication. In low-power networks, packet counters, boot behavior, key rotation and counter persistence therefore become security-critical. ChaCha20-Poly1305 should be evaluated as a complete AEAD construction rather than treating ChaCha20 encryption as sufficient protection.

4. Elliptic-Curve Cryptography for Authentication and Key Establishment

ECC provides public-key capabilities such as digital signatures and key agreement with relatively compact key and message sizes compared with traditional RSA configurations. It is therefore useful for device identity, mutual authentication, provisioning and establishment of symmetric session keys. However, ECC operations are generally more computationally demanding than symmetric encryption. Performing a public-key operation for every sensor packet would usually be inefficient. A better design performs authentication and key establishment infrequently, then uses a symmetric AEAD cipher for routine data transmission.

This hybrid pattern separates two functions: ECC establishes or authenticates the session, while a symmetric cipher protects the high-volume data stream. Its overall efficiency depends on session duration, reconnection frequency, certificate or credential format, curve choice, implementation and the cost of storing keys. Secure random-number generation and key lifecycle management remain essential.

5. Lightweight Block Ciphers and Other Constructions

Research has examined lightweight block ciphers such as PRESENT, SIMON and SPECK for devices with severe hardware constraints. These designs can offer compact hardware implementations, but algorithm selection must consider the current cryptanalytic record, standardization status, implementation assurance and the exact security profile. A small gate count or low code size does not by itself establish adequate security. Some lightweight ciphers are better viewed as research candidates or specialized components than as default replacements for standardized AEAD.

Hash functions, message authentication codes and key-derivation functions also contribute to secure transmission. Their costs should be assessed as part of the complete protocol. A design that uses separate encryption and authentication primitives may require additional code, memory and processing compared with an integrated AEAD construction, although the outcome is implementation-dependent.

Table 1. Overview of encryption and cryptographic approaches for IoT

Technique	Primary role	Potential efficiency advantage	Main limitation / caution
Ascon-AEAD128	Authenticated encryption	Designed for constrained devices; integrated confidentiality and integrity	Benchmark on target hardware; follow standardized nonce and tag requirements
AES-based AEAD	Authenticated encryption	Very efficient where AES hardware acceleration exists; broad ecosystem support	Software-only performance varies; nonce uniqueness is critical

IJARSCT
International Journal of Advanced Research in Science, Communication and Technology
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
ISSN: 2581-9429 Volume 6, Issue 2, August 2026 Impact Factor: 8.2

ChaCha20-Poly1305	Authenticated encryption	Can perform well in software on processors without AES acceleration	Nonce reuse is dangerous; implementation and payload affect energy
ECC (e.g., ECDH/ECDSA)	Key agreement and authentication	Compact public-key material relative to traditional RSA options	Public-key operations are costlier than symmetric packet encryption
PRESENT / SIMON / SPECK	Lightweight block-cipher research and specialized use	Potentially compact hardware/software implementations	Security assurance, standardization and mode selection require scrutiny
Hybrid ECC + AEAD	Session establishment plus data protection	Expensive public-key work is amortized across many data packets	Key lifecycle, session duration and reconnection overhead matter

COMPARATIVE ANALYSIS OF ENERGY AND PERFORMANCE

The reviewed literature consistently treats execution time, memory usage, energy consumption and throughput as important indicators of lightweight cryptographic performance. Recent systematic reviews emphasize that results vary by algorithm family and platform, and that real-device validation remains a key concern (Ansari & Ali, 2025). A comparative experiment on the Nordic Thingy:53 evaluated Ascon and several stream-cipher candidates under Bluetooth mesh and bulk-transfer scenarios, demonstrating that algorithm performance changes with workload and payload size (Sorescu 2025). These findings support workload-specific selection rather than a universal ranking.

For a meaningful comparison, energy should be measured at the device supply or a calibrated power monitor, not inferred solely from instruction counts. Researchers should report average and peak current, voltage, elapsed time and energy per successfully delivered authenticated byte or message. The radio should be included because wireless transmission may dominate the total energy budget. Measurements should distinguish encryption-only energy from the complete secure communication cycle, including key exchange, packet transmission, acknowledgement, retransmission and sleep transitions.

Table 2. Recommended evaluation metrics and interpretation

Metric	What it measures	Why it matters	Reporting recommendation
Energy per message (J/message)	Energy consumed to protect and process a message	Directly relates to battery lifetime	Report payload size, voltage, hardware and whether radio is included
Energy per delivered byte (J/byte)	Energy normalized by successfully delivered data	Enables workload-oriented comparison	Count authenticated, successfully delivered payload bytes
Execution time / latency	Time for encryption, authentication or key exchange	Important for real-time and duty-cycled devices	Separate primitive time from end-to-end delay
RAM and flash footprint	Peak memory and program storage	Determines feasibility on constrained MCUs	Report compiler, optimization flags and library version
Throughput	Data processed per unit time	Useful for gateways and high-rate sensors	Report payload size and test mode
Packet expansion	Extra bytes due to tags, nonce, headers and metadata	Can increase radio energy and fragmentation	Report total wire size, not only cipher output
Security robustness	Resistance to known cryptanalytic and	Efficiency is irrelevant if security is inadequate	Document security level, nonce policy and side-channel assumptions

IJARSCT
International Journal of Advanced Research in Science, Communication and Technology
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
ISSN: 2581-9429
Volume 6, Issue 2, August 2026
Impact Factor: 8.2

	implementation attacks		

DISCUSSION

Three broad conclusions emerge from the literature. First, lightweight authenticated encryption is more useful as a complete security service than encryption-only primitives because it protects confidentiality and detects tampering within a single construction. Ascon's formal standardization in NIST SP 800-232 provides a contemporary, interoperable option for constrained devices. Second, AES and ChaCha20 remain strong candidates where the implementation matches the processor architecture. Hardware acceleration can reverse assumptions based on software-only comparisons; consequently, algorithm choice should follow target-device measurement rather than general claims that one cipher is always faster.

Third, hybrid cryptography is a practical architecture for heterogeneous IoT systems. Public-key techniques are valuable for identity, provisioning and session establishment, while symmetric AEAD is better suited to repeated data packets. This approach reduces the frequency of expensive public-key operations and supports scalable communication. However, it introduces operational requirements: secure provisioning, key rotation, device revocation, counter persistence, randomness, recovery after reboot and protection of long-term credentials.

The energy cost of communication deserves equal attention. A cipher that saves a small amount of CPU energy but expands packets enough to trigger fragmentation may increase total energy. Conversely, a slightly more expensive cryptographic operation may reduce retransmissions or enable a shorter secure exchange. The best optimization target is therefore energy per successfully authenticated and delivered message over the intended network, not merely cycles per block.

II. CONCLUSION

Energy-efficient encryption is essential for secure and sustainable IoT communication, but efficiency must be evaluated across the complete device and network lifecycle. The reviewed evidence supports authenticated encryption as the preferred foundation for protecting transmitted data. Ascon-AEAD128 is a significant standardized option for constrained devices following the publication of NIST SP 800-232 in 2025. AES-based AEAD remains attractive when hardware acceleration is available, while ChaCha20-Poly1305 can be effective on processors optimized for software operations. ECC is best used for authentication and key establishment, with symmetric AEAD protecting routine data packets. Protocol mechanisms such as OSCORE help apply end-to-end security to constrained application communication.

No algorithm is optimal for every IoT device. The appropriate solution depends on hardware, workload, network conditions, packet overhead, security requirements and key-management design. Future research should prioritize reproducible hardware-based measurements, total energy per delivered message, robust implementation security, interoperable key management and post-quantum readiness. A system-level approach that combines standardized lightweight AEAD, efficient session establishment and careful protocol engineering offers the most promising route to secure data transmission with sustainable energy consumption.

REFERENCES

1. Ansari, S. A., & Ali, S. (2025). A systematic review of lightweight cryptographic schemes for security and privacy in IoT. *Discover Computing*, 28, Article 266.
2. Dobraunig, C., Eichlseder, M., Mendel, F., & Schläffer, M. (2021). Ascon v1.2: Lightweight authenticated encryption and hashing. *Journal of Cryptology*, 34, Article 33.
3. Gușiță, B., Anton, A. A., Stângaciu, C. S., Stănescu, D., Găină, L. I., & Micea, M. V. (2025). Securing IoT edge: A survey on lightweight cryptography, anonymous routing and communication protocol enhancements. *International Journal of Information Security*, 24(3), Article 149.

IJARSCT
International Journal of Advanced Research in Science, Communication and Technology
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
ISSN: 2581-9429
Volume 6, Issue 2, August 2026
Impact Factor: 8.2

4. NIST. (2007). Recommendation for block cipher modes of operation: Galois/Counter Mode (GCM) and GMAC (NIST Special Publication 800-38D). *National Institute of Standards and Technology*.
5. Selander, G., Mattsson, J., Palombini, F., & Seitz, L. (2019). Object security for constrained RESTful environments (RFC 8613). *Internet Engineering Task Force*.
6. Sarker, K. U. (2025). A systematic review on lightweight security algorithms for a sustainable IoT infrastructure. *Discover Internet of Things*, 5, Article 47.
7. Shelby, Z., Hartke, K., & Bormann, C. (2014). The constrained application protocol (CoAP) (RFC 7252). *Internet Engineering Task Force*.
8. Silva, C., Tenório, N., & Bernardino, J. (2025). Lightweight encryption algorithms for IoT. *Computers*, 14(12), Article 505.
9. Sorescu, T.-G., Chiriac, V.-M., Stoica, M.-A., Comsa, C.-R., Soroaga, I.-G., & Contac, A. (2025). Comparative performance analysis of lightweight cryptographic algorithms on resource-constrained IoT platforms. *Sensors*, 25(18), Article 5887.
10. Turan, M. S., McKay, K., Kang, J., Kelsey, J., & Chang, D. (2025). Ascon-based lightweight cryptography standards for constrained devices: Authenticated encryption, hash, and extendable output functions (NIST Special Publication 800-232). *National Institute of Standards and Technology*.