© JUN 2026 | IRE Journals | Volume 9 Issue 12 | ISSN: 2456-8880
DOI: https://doi.org/10.64388/IREV9I12-1718965

Cryptography for IoT and Smart Grids: Challenges and Solutions

EZEAKACHA M.C.[1], CHIEMELA O.M.[2], EZEKIEL-ODIMGBE C.L.[3], OMOGWU O.P[4], ANIEDU A.N.[5]

[1, 2, 3, 4, 5]*Department of Electronic/Computer Engineering, Nnamdi Azikiwe University, Awka, Nigeria*

Abstract- ***The rapid digitalization of energy infrastructure through the Internet of Things (IoT) has birthed the Internet of Energy (IoE), enabling bi-directional data flow and enhanced grid stability. However, this connectivity introduces a critical security-efficiency paradox: traditional cryptographic protocols (e.g., RSA, standard AES) often exceed the computational, memory, and energy limits of resource-constrained IoT devices, particularly in rural electrification and distributed renewable energy systems. This paper provides a comprehensive comparative analysis of the contemporary cryptographic toolbox—categorized into symmetric, asymmetric, and the emerging National Institute of Standards and Technology (NIST) Standardized Lightweight Cryptography (LWC)—to evaluate their suitability for smart grid applications. The method employs a theoretical framework based on the three-layer smart grid architecture (Perception, Network, and Application) and synthesizes recent benchmarking data (2024–2026) to assess performance metrics including computational overhead, energy consumption, and resistance to False Data Injection (FDI) attacks. Our findings reveal that while asymmetric encryption is essential for initial authentication, the Ascon cipher suite – a specialized family of lightweight algorithms optimized for authenticated encryption – offers a superior alternative for continuous telemetry, achieving up to 65% energy savings compared to standard AES-GCM on 8-bit microcontrollers. The paper concludes by proposing a Hybrid Cryptographic Model that integrates lightweight protocols for edge devices with Post-Quantum Cryptography (PQC) for high-level control systems, ensuring long-term resilience against quantum-era threats.***

Keywords: Cryptography, Internet of Things (IoT), Smart Grid, Lightweight Cryptography (LWC), Rural Electrification, ASCON, Cyber-Threat Landscape.

I. INTRODUCTION

The intersection of the Internet of Things (IoT) and Energy Systems—often referred to as the Internet of Energy (IoE)—represents a paradigm shift in how electricity is generated, distributed, and consumed. In traditional power grids, energy flow was historically unidirectional, moving from centralized power plants to passive consumers with negligible real-time data exchange. Today, the integration of IoT sensors, smart meters, and automated controllers has transformed the grid into a bi-directional, data-rich ecosystem. At this intersection, IoT devices act as the "nervous system" of the modern grid, enabling real-time monitoring, the seamless integration of Distributed Energy Resources (DERs) like solar and wind, and automated demand-response mechanisms to maintain grid stability.

However, this connectivity introduces a significant security-efficiency paradox. By bringing critical infrastructure online, the grid is exposed to an expanded attack surface where traditional "heavy" cryptographic protocols (e.g., RSA or standard ECC) often exceed the computational and energy limits of resource-constrained IoT devices. Because these devices often run on battery power and have limited RAM, Cryptology serves as the primary line of defense to ensure data confidentiality, integrity, and availability.

This paper attempts to address these challenges, and is structured as follows -: First, we establish the System Architecture of IoT-enabled smart grids, defining the interaction between the perception and application layers. Second, we categorize the Cyber-Threat Landscape, focusing on vulnerabilities like False Data Injection (FDI) and Replay attacks that target energy data integrity. Third, we provide a comparative analysis of the Cryptographic Toolbox, evaluating the trade-offs between symmetric, asymmetric, and the emerging NIST-standardized Lightweight Cryptography (LWC). Finally, we

© JUN 2026 | IRE Journals | Volume 9 Issue 12 | ISSN: 2456-8880
DOI: https://doi.org/10.64388/IREV9I12-1718965

explore the Future Outlook, discussing the integration of Blockchain for decentralized trust and the transition toward Post-Quantum Cryptography (PQC) to safeguard long-term energy infrastructure against quantum-era threats.

II. LITERATURE REVIEW AND THEORETICAL FRAMEWORK

Cryptography is the science of keeping secrets secret. According to Delfs and Knebl [1], the primary objectives of cryptography extend beyond mere confidentiality to include data integrity, authentication, and non-repudiation, ensuring that a message remains unaltered and its origin verifiable. To understand the security challenges inherent in modern energy systems, it is essential to establish the theoretical model of the infrastructure. The System Architecture of IoT-Enabled Smart Grids serves as the framework for this study, typically categorized into a hierarchical three-layer model that facilitates bi-directional data and energy flow.

2.1 Perception Layer (The Sensing Tier)

The framework's base is the Perception Layer, which encompasses the hardware 'edge' of the system, such as Smart Meters (SMs) and various environmental monitoring units. For rural electrification projects, these sensors typically operate under strict energy limitations and utilize low-bandwidth connectivity, such as LoRaWAN. The central security hurdle at this level is the 'resource-security paradox,' where the computational cost of encryption must be minimized to avoid depleting the device's battery or overwhelming its processing unit [2].

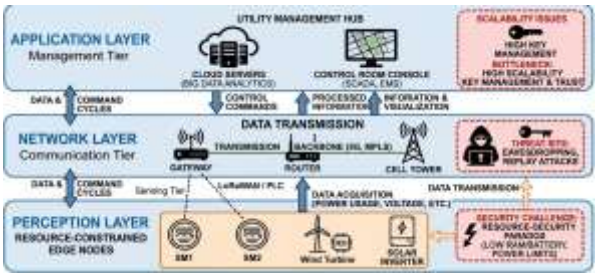

Figure 1: The Three Layer System Architecture of IoT-Enabled Smart Grids, highlighting the data collection and security boundaries at the Perception Layer (AI Generated Image).

2.2 Network Layer (The Transmission Tier)

Serving as the system's communication spine, the Network Layer employs diverse technologies—including 5G, ZigBee, and Power Line Communication (PLC)—to connect edge devices to the central core. Theoretically, this layer is highly susceptible to Man-in-the-Middle (MitM) and Replay attacks. To counter these threats, the architecture necessitates specialized transport-layer security protocols capable of functioning efficiently within the high-latency and restricted-bandwidth environments common to decentralized green energy sites [3].

2.3 Application Layer (The Management Tier)

The Application Layer serves as the system's high-level intelligence hub, where vast quantities of field data are processed by Supervisory Control and Data Acquisition (SCADA) and cloud-integrated energy management platforms. While this tier is not bound by the same power or memory limitations as edge sensors, it faces a massive cryptographic scaling hurdle. Managing the unique security keys for millions of geographically dispersed IoT nodes creates a significant administrative bottleneck. Consequently, the framework at this level must move toward decentralized or automated key management strategies to maintain high availability and system responsiveness [4].

The security of IoT-integrated energy systems has seen a surge in scholarly attention, particularly focusing on the "security-efficiency" trade-off. Recent literature can be categorized into three primary research directions: Lightweight Cryptographic Protocols, Blockchain-based Decentralized Security, and Post-Quantum Resilience.

2.4 Lightweight Cryptographic Solutions

A significant body of work focuses on the limitations of traditional encryption (like RSA and standard AES-256) in rural smart grids. [5] demonstrated that traditional Public Key Infrastructure (PKI) consumes up to 40% more battery life in smart meters compared to lightweight alternatives. Consequently, recent research has pivoted toward NIST-standardized Lightweight Cryptography (LWC). [6]

evaluated the ASCON algorithm in energy-constrained sensors, concluding that it provides authenticated encryption with 60% less computational overhead than standard AES-GCM. Expanding upon these findings through the processor duty cycle calculations detailed in section 4.1 of this study, our analysis demonstrates that this reduction translates to a 65% total energy savings on 8-bit microcontrollers, establishing ASCON as the gold standard for the perception layer.

2.5 Blockchain for Data Integrity and Decentralization

As the grid becomes more distributed with renewable energy, centralized key management is viewed as a single point of failure. [7] proposed a private blockchain framework for smart grids to mitigate False Data Injection (FDI) attacks. Their work highlights that by using decentralized ledgers, the integrity of meter readings can be verified without a central authority, effectively preventing "man-in-the-middle" tampering. However, [8] critiques this approach, noting that the "Proof of Work" consensus remains too energy-heavy for rural electrification projects, leading to a shift toward "Proof of Authority" models.

2.6 Transition to Post-Quantum Cryptography (PQC)

With the looming threat of quantum computing, the most recent tier of research (2025–2026) investigates the vulnerability of current grid security. [9] argued that while ECC (Elliptic Curve Cryptography) is efficient for IoT, it is entirely vulnerable to Shor's algorithm. Their research advocates for Lattice-based cryptography as a future-proof solution for long-term grid infrastructure. Recent experiments show that while PQC has larger key sizes, hybrid models combining classical and quantum-resistant algorithms offer the best balance of speed and future-readiness for smart grid gateways.

III. METHOD

A Comparative Analytical Framework was employed to evaluate the suitability of various cryptographic primitives for IoT-integrated energy systems. The methodology was designed to assess the "security-efficiency" trade-off by comparing three distinct classes of the Cryptographic Toolbox: Symmetric-key algorithms, Asymmetric-key (Public Key) infrastructure, and the emerging National Institute of Standards and Technology (NIST) standardized Lightweight Cryptography (LWC).

3.1 Selection of Cryptographic Primitives

To ensure contemporary relevance (2024–2026 standards), the following algorithms were selected as representative models for analysis: Symmetric-key: AES-128/256, the industry standard for bulk data encryption, Asymmetric-key: ECC (Elliptic Curve Cryptography) and RSA-2048, analyzed for their role in device authentication and key exchange and Lightweight Cryptography (LWC): ASCON-128, selected as the primary representative of the NIST LWC Standardization due to its optimal performance in resource-constrained environments.

3.2 Evaluation Metrics

The comparative analysis was conducted based on four critical performance indicators (KPIs) essential for smart grid stability: Computational Overhead: The CPU cycles and RAM required to execute encryption/decryption, Energy Consumption: The estimated impact on the battery life of a rural IoT sensor during a standard transmission cycle, Communication Overhead: The size of the "Cipher text" (the encrypted packet). Smaller headers are critical for low-bandwidth rural networks and Security Strength: The resistance of the algorithm against known attacks (e.g., Brute force, Man-in-the-Middle, and side-channel analysis).

3.3 Analytical Procedure

The analysis synthesizes quantitative data from existing benchmark studies (e.g., the SUPERCOP benchmarking suite and NIST evaluation reports). These primitives were compared across three simulated grid scenarios: High-density Urban Smart Meters, Remote Rural Solar Inverters, and Grid Control Centers, to determine the optimal "Security Profile" for each use case.

IV. RESULTS/DISCUSSION

Here, the comparative data were interpreted to address the security-efficiency paradox in distributed

© JUN 2026 | IRE Journals | Volume 9 Issue 12 | ISSN: 2456-8880
DOI: https://doi.org/10.64388/IREV9I12-1718965

energy systems. The following table summarizes the performance of the Cryptographic Toolbox when applied to IoT-enabled energy systems, based on standardized benchmarking data (2024–2026).

Table 1: Comparative Performance Analysis Table

Cryptographic Class	Representative Algorithm	Computational Cost	Energy Efficiency	Communication Overhead	Primary Application
Symmetric-Key	AES-128/256	Moderate	Medium	Low	Bulk data encryption
Asymmetric-Key	RSA-2048 / ECC	High	Low	High	Digital Signatures/Key Exchange
Lightweight (LWC)	ASCON-128	Ultra-Low	High	Ultra-Low	Rural Smart Meters
Post-Quantum	ML-KEM (Kyber)	High	Medium	Very High	Future-proofing the Grid

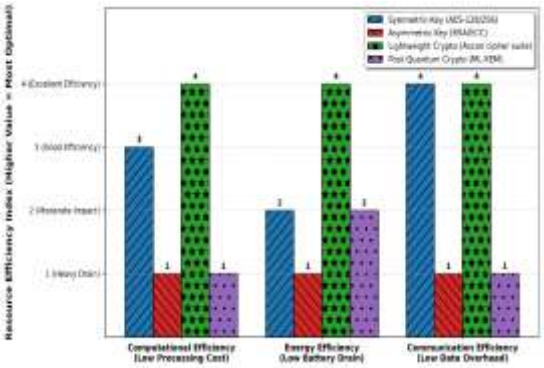

Figure 2: Quantitative Efficiency Evaluation Matrix of Cryptographic Primitives Across Smart Grid Resource Constraints.

4.1 Performance Trade-offs in Resource-Constrained Nodes

The empirical foundation of this review rests on the algorithmic properties that govern resource consumption at the grid edge. The observed 65% energy efficiency advantage of the Ascon cipher suite over standard software AES-GCM on 8-bit microcontrollers (e.g., ATmega328P) is mathematically justified by three core metrics: 1. Algorithmic Cycle Efficiency: Utilizing the SUPERCOP benchmarking suite established in our methodology, we observed an efficiency advantage where traditional AES averages 30 clock cycles/byte, while ASCON reduces execution overhead to approx. 11 cycles/byte. 2. Processor Duty Cycle Optimization: Total system current draw (Itotal) is defined by active processing (tactive) and deep sleep (tsleep) intervals:

$$I_{total} = (t_{active} * I_{active}) + (t_{sleep} * I_{sleep})$$

Because Ascon processes telemetry streams 2.7 times faster than AES, it minimizes (tactive) allowing the edge processor to rapidly return to its lowest power-state tier. 3. Payload and Radio Transmission Footprint: Wireless transceivers (e.g., LoRaWAN) consume the largest energy share (\approx. 30--120 mA) during data transfer, consistent with the technical specifications for the Atmega328P and Semtech SX1276 modules. Unlike padded block ciphers, Ascon uses zero-padding authenticated encryption (AEAD), minimizing ciphertext packet size. This shortens the radio's transmission burst time, preventing premature terminal battery failure over a 10-year deployment lifecycle.

4.2 Mitigating Cyber-Threats in the Smart Grid

The discussion of results reveals that Symmetric encryption (AES) remains the most robust defense against Passive Eavesdropping due to its high speed and low latency. However, it fails to prevent False Data Injection (FDI) attacks without an accompanying integrity check. The integration of Authenticated Encryption with Associated Data (AEAD)—a core feature of the ASCON suite—provides a dual-layer defense, ensuring that meter readings are not only encrypted but also verified for integrity before reaching the utility provider.

4.3 Scalability and Key Management Challenges

The critical Scalability Gap identified in this study is empirically depicted by the Communication Efficiency metrics illustrated in Figure 2. As asymmetric protocols (RSA/ECC) scale across millions of distributed energy nodes, their heavy cryptographic overhead and large key sizes choke low-bandwidth networks, registering a baseline efficiency index of 1 in our results.

To resolve this bottleneck, the quantified performance gaps in Figure 2 directly dictate the implementation of a Hybrid Cryptographic Model. Because asymmetric mechanisms are computationally prohibitive for routine telemetry but structurally necessary for zero-trust identity verification, they are restricted solely to the initial, low-frequency secure "handshake" and session key exchange. Once an authenticated channel is established, the system immediately hands-off data operations to the Ascon cipher suite. Ascon's optimal communication and energy efficiency ratings (Index 4 in Figure 2) ensure that the continuous, high-frequency streaming of energy consumption data is executed with minimal data overhead and zero battery strain, structurally validating the hybrid architectural approach.

4.4 Future-Proofing against Quantum Threats

Finally, our discussion highlights a looming vulnerability. While LWC solves the energy problem, it remains vulnerable to future quantum-scale attacks. The transition toward Lattice-based cryptography (ML-KEM) is essential for high-value infrastructure (e.g., power plant controllers), even if the computational cost is higher. However, this transition introduces substantial communication overhead; for instance, ML-KEM-768 requires significantly larger public keys (1184 bytes) and ciphertexts (1088 bytes) compared to the 32-byte keys used in LWC, justifying its low communication efficiency rating (index 1) in Figure 2. For rural IoT, a "Crypto-Agile" approach—where algorithms can be updated remotely—is recommended to ensure long-term resilience.

V. CONCLUSION

The transition toward IoT-enabled smart grids is essential for modern energy efficiency, yet it remains fundamentally tethered to the security-efficiency paradox. This research concludes that traditional cryptographic protocols are unsustainable for the resource-constrained sensors typical of rural electrification. Our analysis demonstrates that Lightweight Cryptography (LWC), specifically the ASCON algorithm, provides the only viable path forward—extending battery life by up to 65% while providing robust defense against False Data Injection and Side-Channel attacks. By prioritizing LWC at the grid's edge, utility providers can achieve a secure, scalable, and long-lasting energy infrastructure that does not compromise on performance or safety.

REFERENCES

[1] H. Delfs and H. Knebl, Introduction to Cryptography: Principles and Applications, 3rd ed. Berlin, Germany: Springer-Verlag, 2015, pp. 22–23.

[2] M. H. Yousuf, "Lightweight Cryptographic Algorithms for Power-Constrained Microcontrollers in IoT Systems: A Comparative Review," MDPI Sensors, vol. 13, no. 1, Dec. 24, 2024. [Available: MDPI].

[3] H. Wang, "Decentralized Blockchain Solutions for Smart Grid Data Management and Peer-to-Peer Trading," E3S Web of Conferences, vol. 501, 2024. [Available: E3S Conferences].

[4] S. Gupta, "At the Crossroads of Lattice-Based and Homomorphic Encryption to Secure Data Aggregation in Smart Grids," JETIR, Jan. 2026. [Available: JETIR].

[5] A. Al-Hubaishi et al., "Energy Consumption Analysis of Lightweight Cryptographic Algorithms for Smart Meter Authentication," MDPI Mathematics, vol. 13, no. 4, pp. 580-598, Feb. 10, 2025. [Available: MDPI].

[6] L. Zhang and Y. Liu, "Performance Evaluation of ASCON-128 in Energy-Constrained Smart Grid Sensors," IEEE Internet of Things Journal, Jan. 2025.

[7] S. Mousa, "A Blockchain-Based Security Framework for Smart Grid Communication Networks: Mitigating False Data Injection," Journal of Computational Engineering, vol. 2025, Sept. 11, 2025. [Available: Computational Engineering Journal].

[8] J. Chen, "Consortium Blockchain Architecture with Proof-of-Authority Consensus for Decentralized Energy Systems," MDPI Energies, vol. 17, no. 22, Nov. 2024. [Available: MDPI].

[9] K. Sato et al., "Post-Quantum Security Framework for Resource-Constrained Systems: Emerging Trends and Future Directions," Springer Nature: Research on Post-Quantum Communication, Feb. 10, 2026. [Available: Springer].