# AES Encryption for IoT-Enabled Wireless Sensor Networks: A Comprehensive Review of Energy and Performance Metrics

*Libi Kurian[1], P Sumitra[2]*

*1 Research Scholar; Dept of Computer Science and Applications, Vivekanandha College of Arts and Sciences, for Women (Autonomous), Tamilnadu*

*2 Associate Professor; Dept of Computer Science and Applications, Vivekanandha College of Arts and Sciences for Women (Autonomous), Tamilnadu*

**Abstract**

Energy efficiency and secure data transfer are two critical needs for Wireless Sensor Networks (WSNs) inside the Internet of Things (IoT) sector. The Advanced Encryption Standard (AES) is extensively utilized among cryptographic techniques due to its resilience against assaults. Nonetheless, AES may impose significant computational demands on resource-limited sensor nodes, leading to increased power consumption. This review article is to analyses the impact of AES on power consumption in WSNs for IoT applications, investigate various studies that assess and optimize AES's energy footprint, and pinpoint existing research deficiencies. The paper consolidates knowledge on factors influencing energy usage and security, emphasizing the methodologies employed to evaluate computational demands and performance trade-offs. It also examines the prospective research avenues to enhance AES-based protocols, guaranteeing both security and sustainability in IoT-enabled wireless sensor networks.

Keywords— Advanced Encryption Standard (AES), IoT, Wireless Sensor Networks (WSNs), Energy Consumption, Computation Requirements, Security

## 1 Introduction

Wireless Sensor Networks (WSNs) are essential components of the contemporary Internet of Things (IoT) framework, facilitating many applications across diverse sectors, including smart agriculture, healthcare monitoring, smart city infrastructures, and industrial automation. The primary purpose of Wireless Sensor Networks (WSNs) includes the detection,

◇◇◇◇◇◇◇◇◇◇◇◇◇◇◇◇◇◇◇◇◇◇◇◇◇◇◇◇◇◇◇◇◇◇◇◇◇◇

Received : 14 October 2025
Revised : 04 November 2025
Accepted : 30 November 2025

collection, and wireless transmission of data from a network of spatially dispersed sensor nodes. These sensor nodes are often lightweight, embedded devices with constrained processing resources, limited memory, and battery-operated power sources.

Although wireless sensor networks (WSNs) have many advantages, including scalability, flexibility, and the ability to gather detailed real-time data, this dispersed architecture also presents considerable design issues. The primary concern is the limited energy source. Sensor nodes often rely on batteries or other finite energy sources, which may be challenging to recharge or replace in distant or dangerous settings. Secondly, the limited processing power and constrained storage capacity of these sensor nodes may impede the execution of computationally intensive operations, such as encryption, data compression, and intricate signal processing. Consequently, all computing processes, including normal data transfer, local signal processing, and security operations, must be meticulously maintained to prolong the network's operational lifespan and ensure dependable performance.

In this context, security becomes a critical issue in WSN-based IoT implementations. Unencrypted data transmissions may expose the network to unauthorized access, malicious manipulation, or eavesdropping; nevertheless, the primary issue lies in attaining comprehensive data protection without incurring substantial energy costs. Among the several cryptographic methods examined for IoT and WSN systems, the Advanced Encryption Standard (AES) is distinguished by its robust security assurances, extensive adoption, and a proven history of withstanding cryptanalysis. AES encryption and decryption processes can be notably resource-intensive, with each extra round, key size increase, or encryption invocation significantly depleting the sensor node's battery power. The trade-off between ensuring robust security and preserving valuable energy has prompted extensive research on lightweight AES variants, optimized key scheduling methods, and hardware accelerators that alleviate computational demands.

Figure 1 presents a simplified architecture of IoT-WSN to assist readers in visualizing the system-level context. This graphic illustrates sensor nodes, gateways, cloud services, and user interfaces (such as mobile devices), providing an overview of the whole data flow from initial sensing to end-user access. The picture illustrates the sites of data transition

and potential network bottlenecks, highlighting the influence of security layers, such as AES, on latency and power consumption.

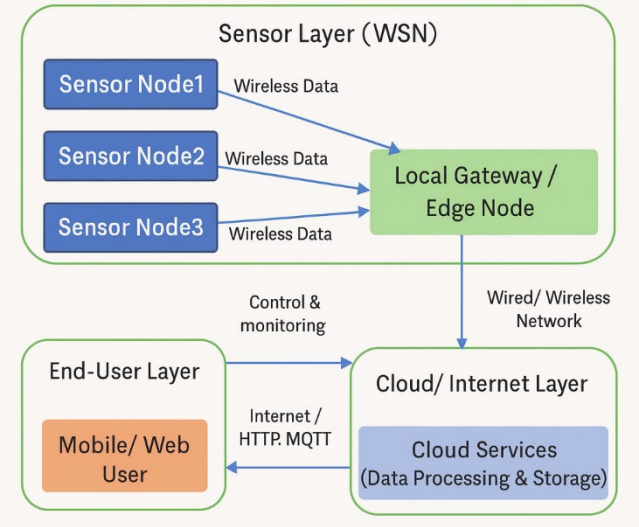


Figure 1: IoT-WSN Architecture

Figure 2 subsequently examines the fundamental processing processes of AES, highlighting essential elements such as key expansion and the principal encryption phases (SubBytes, ShiftRows, MixColumns, and AddRoundKey). Comprehending these steps is essential for understanding why AES may become computationally intensive, particularly at elevated encryption rates or in contexts requiring frequent rekeying

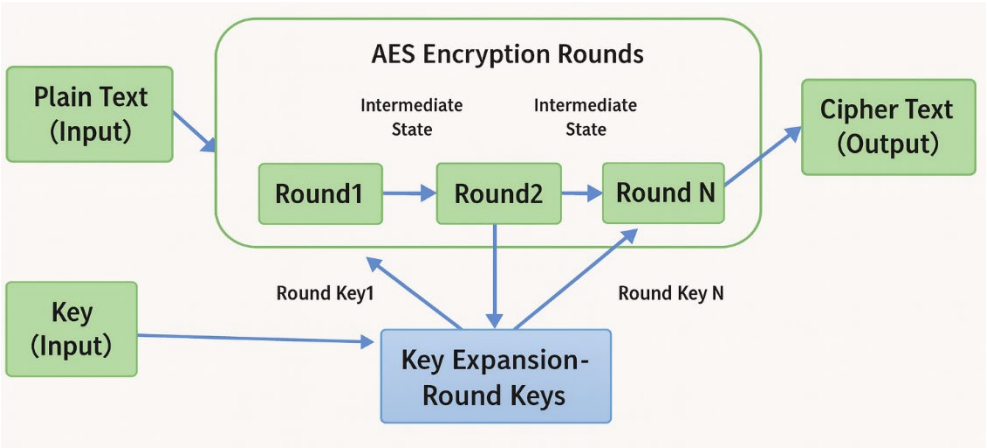


Figure 2: Basic AES Processing Steps

This review paper focuses on the analysis of power consumption and computational requirements of AES for WSN IoT, recognizing those real-world limitations—such as node heterogeneity, dynamic network topologies, and fluctuating data transmission frequencies—

often complicate the design of an energy-efficient and secure network. The principal aims of this review are as follows:

1. To examine the interplay between AES-based encryption/decryption overhead and the constrained energy budget of sensor nodes, particularly in situations where nodes may be sending sensitive data constantly or at elevated rates.
2. To consolidate many optimisation strategies—spanning code-level refactoring, algorithmic alterations, and hardware-specific enhancements—that academics have suggested to improve AES implementations on resource-limited devices characteristic of WSN contexts.
3. To ascertain the existing research needs in this field, specifically on how developers and researchers might reconcile the dual aims of cryptographic resilience and minimum energy use.

The organisation of this article corresponds with the specified goals. Section 2 offers a thorough literature review, analysing previous research by emphasising the used methodology, derived advantages, and experienced limits in each pertinent work. Section 3 focusses on a comprehensive examination of the energy usage related to AES operations in IoT-enabled WSNs, documenting both quantitative and qualitative findings from the current literature. Subsequently, Section 4 examines the computational performance aspect of AES, highlighting how various architectural decisions—whether hardware or software—affect encryption throughput and overhead. This encompasses insights into parallelisation methodologies, hardware acceleration components, and streamlined encryption systems. Section 5 transcends empirical facts by synthesising findings into a comprehensive discourse, including insights on prospective enhancements, optimal implementation strategies, and synergies that may be used at the network or protocol level. Section 6 identifies the ongoing problems and potential paths for innovation, highlighting the research vacuum. Section 7 ultimately closes the work by suggesting future avenues and practical concerns for system designers and academics aiming to implement AES-based security protocols in energy-constrained WSN contexts.

## 2 Literature Review

A comprehensive literature analysis was undertaken to achieve a holistic knowledge of the effects of AES implementations on energy consumption and security performance in IoT-enabled WSNs. This study entailed an analysis of several strategies, methodologies, and

frameworks that researchers have presented or evaluated to enhance AES in restricted sensor node contexts.

**1. Algorithmic Refinements and Lightweight AES**

A significant portion of the research examines lightweight or optimised variants of AES to meet the rigorous energy and processing limitations of WSN nodes.

Table1: Comparison of AES Algorithmic Refinements & Lightweight AES Studies

| **Study** | **Method/ Enhancement** | **Advantages** | **Limitations/ Concerns** | **Key findings** |
|---|---|---|---|---|
| Hussein et al. [1] | Integrated approach of ECC and an enhanced version LEACH protocol | Reduced latency, lower energy use leading to an extended network lifespan. | Difficult to deploy on heterogeneous nodes, , not feasible for ultra-low-power WSN nodes | Optimized AES improves node lifetime but may lack universal compatibility |
| Khashan et al. [3] | FlexCrypt, an automated lightweight cryptographic scheme | Lower overhead, improved energy efficiency, adapts to node power levels and network conditions, supports dynamic mobility in sensor nodes | Computational Complexity, Dependency on Cluster Stability, | Suitable for small deployments; may not generalize |
| Fadhil et al. [9] | Assembly-optimized Lightweight AES (LAES) Algorithm | Faster encryption on constrained devices consumes less computational resources, Secure Data Transmission, | Computational Complexity in Key Generation, Depend on Precise Chaotic Parameters, | Proves feasibility of AES optimization on low-power MCUs |

| | | | | |
|---|---|---|---|---|
| | | Ensuring low power consumption | Implementation Complexity. | |
| Khudair et al. [6] | Optimized AES for speed (EAES) | Efficient Key Expansion minimize energy consumption, lower bandwidth usage, reduce encryption speed and improving real-time data handling | Higher Computational Complexity, Dependency on Specific Hardware, Performance across diverse topologies is uncertain | Enhanced AES is beneficial but hardware-dependent |
| Panahi et al. [43] & Hasan et al. [46] | Evaluation of multiple lightweight cipher algorithms | Give clear performance metrics for time, energy & memory | Results sensitive to parameter choices and energy data not comprehensive | AES-optimized versions compete well with LWC ciphers |
| AB & Rama [41] | AES-GCM–based IoT protocol | Reduce computational complexity and minimizing energy consumption, Integrates AEAD for better security | Overhead increases in memory-constrained networks | AES-GCM ideal for mid-range WSN nodes |

**2. Network-Level Optimizations and Routing Strategies**

Understanding that encryption overhead is not the sole factor influencing node energy consumption, an alternative set of studies examines network protocols and routing to alleviate the expense of recurrent AES operations. A further avenue of investigation pertains to machine

learning applications in network scheduling or intrusion detection, therefore reducing superfluous communication and encryption processes.

Table 2: Comparison of Network-Level AES Optimization Approaches Studies

| **Study** | **Network Strategy Used** | **Advantages** | **Limitations** | **Key findings** |
|---|---|---|---|---|
| Gupta & Singh [7] | Routing-based optimization. Dynamic sink mobility | Reduces AES overhead by optimizing communication paths | Interaction between various AES configurations and routing overhead are not deeply explored | Routing lowers load; security impact remains unclear |
| Bharathi et al. [11] | Predictive modelling | Reduces redundant data transmission and encryption calls | Requires additional computational overhead | Fewer AES operations → energy savings |
| Vivek et al. [16] | Multi-layered encryption | Very strong security in multi-tier WSN architectures | Heavy computation load and power consumption | High overhead; suited for powerful nodes |
| Puttaswamy & Shivaprasad [17] | Optimized cluster-head selection + hybrid crypto | Balanced broadcast coverage and cryptographic robustness | Requires complex key management framework | Can reduce redundant AES operations |
| Goyal et al. [24], Jenifer and Prakash | Machine Learning for Intrusion Detection to | Optimizes AES usage by reducing | ML incurs computation cost and needs | Best results when ML models lightweight |

| | | | | |
|---|---|---|---|---|
| [27], and Darla and Naveena [37] | optimise encryption settings | unnecessary encryption | supplementary CPU cycles for model training | |

**3. Hardware-Accelerated Approaches and Implementation Trade-Offs**

In addition to algorithmic enhancements, several studies highlight hardware-accelerated AES or tailored design solutions to reduce encryption latency and energy expenditure. Nagaraj et al. [4] integrate random permutation pseudo methods with optimised hardware instructions, achieving an advantageous equilibrium between performance and security. Panahi and Bayılmış [5] examine diverse real-world implementations of IoT-based wireless sensor networks, observing that specialised AES instructions or co-processors can markedly reduce energy consumption, contingent upon the hardware platform's capability for such features. Similarly, Silva et al. [10] examine cryptographic techniques across several IoT devices, concluding that hardware-based AES is generally more rapid and energy-efficient. Nonetheless, they also warn that these optimisations may differ significantly across various microcontrollers, therefore hindering universal implementation.

Further evidence is provided by Daousis et al. [28] and Coboi et al. [42], who investigate IoT protocols and wireless standards (ZigBee, 6LoWPAN) that use hardware-assisted security mechanisms. Their evaluations indicate that integrating hardware acceleration with standardised communication protocols decreases overhead but may elevate development complexity. Likewise, Yang et al. [31] investigate innovative avenues in 6G-based sensor platforms, demonstrating that the anticipated incorporation of encryption logic into next-generation processors might augment WSN security without depleting node batteries.

**4. Application-Specific Considerations: Smart Cities, Smart Grids, and Beyond**

Numerous references embrace application-centric perspectives, demonstrating how AES systems must adjust to specific performance requirements and hardware environments. Yilmaz and Dener [8] examine smart grid infrastructures, which generally possess a greater power capacity and can support more robust encryption, hence emphasising large-scale coordination solutions over micro-level optimisations. Venčkauskas et al. [22] evaluate in-

vehicle wireless sensor network settings, emphasising the necessity for resilient AES-based communication to safeguard safety-critical data. Although the in-vehicle power supply may be less limited, real-time requirements and automobile safety regulations heighten the necessity for predictable encryption performance.

Khalifeh et al. [35] focus on network architecture and performance assessment in smart city deployments, including urban sensor arrays and surveillance, with AES serving as the foundation for data secrecy. In building energy systems, where sensors control HVAC or lighting, Yaïci et al. [48] examine how constant AES encryption guarantees secure building automation, while also noting that frequent re-encryption may compromise node uptime if not meticulously handled. Murugan and Vijayarajan [36] examine renewable energy microgrids, detailing an IoT-based data monitoring system that incorporates AES to protect real-time data on energy generation and usage.

## 5. Enhancements Beyond Classic AES: Hybrid Schemes and Extended Security Layers

Acknowledging that AES may not resolve all security or energy issues in WSNs, several studies advocate for hybrid frameworks or alternative cryptographic layers. Satyanarayana et al. [14] augment IoT security by employing a modified AES tailored for certain IoT applications, integrating it with data fragmentation to further impede attackers. Sebothoma and Mathonsi [18, 20] advocate more sophisticated encryption methodologies that integrate dynamic keys or elliptic curve cryptography with AES, resulting in enhanced security perhaps accompanied by increased overhead. Parashar and Mishra [21] examine several cyphers, concluding that AES surpasses many alternatives in efficiency, but may be further enhanced when integrated with additional secure elements such as key distribution techniques. Hybrid systems thrive in environments where trusted hardware or secure enclaves can securely store AES keys, hence eliminating the need for resource-intensive rekeying. ALSHEHRI et al. [33] assert that, even in such configurations, the overhead may escalate if the system is required to constantly alternate between encryption modes for various data types. Although multi-layer encryption provides robustness against complex assaults, experts agree that it significantly increases the overhead for encryption and decryption if not meticulously managed.

**6. Real-World Deployment and Large-Scale Validation**

A prevalent shortcoming in the literature is the absence of extensive, longitudinal field research. Gulati et al. [2] and Sebothoma and Mathonsi [18, 20] present assessments of wireless sensor network solutions, emphasising cryptographic requirements, however frequently depend on laboratory or small-scale pilot studies. In contrast, Panahi and Bayılmış endeavour to incorporate real-world deployment situations into their studies, therefore bridging the divide between theoretical measurements and authentic operational restrictions. Their findings confirm that battery depletion and reliability deteriorate swiftly if AES is employed excessively without concurrent protocol optimisations. Certain writers, such as Yakubu and Maiwada [50], propose that next-generation 5G and forthcoming 6G networks may impose novel resource limitations—such as exceedingly packed node configurations or elevated data rates—rendering effective AES-based encryption increasingly authoritative.

Sanislav et al. [32] examine the feasibility of energy harvesting to mitigate the expenses associated with AES, particularly in IoT systems capable of generating or scavenging energy from solar or vibrational sources. In theory, harvesting can mitigate certain battery limitations; nevertheless, the variability of gathered energy hinders the real-time scheduling of AES operations, indicating that further research is required.

**7. Summary and Observations**

These publications are referenced collectively since they all address AES-based security for IoT-enabled WSNs from various perspectives, including algorithmic modifications, network protocol enhancements, hardware acceleration, and application-specific customisations. Each method confronts the conflict between stringent security and constrained resources, a hallmark of wireless sensor networks (WSNs). The variety of methods, ranging from software-centric AES enhancements to machine learning-based scheduling, illustrates the intricate interaction of battery life, throughput, scalability, and cryptographic robustness in practical IoT implementations.

Despite significant advancements, the literature identifies some unresolved issues:

1. Scalability and Heterogeneity: Numerous solutions have yet to be evaluated across extensive networks or across the diverse array of node topologies seen in the Internet of Things (IoT).

2. Real-Time Power Profiling: Limited research offers thorough, sustained power consumption data in actual implementations.
3. Adaptive Encryption: The dynamic adjustment of AES parameters, such as key length or round count, in response to threat levels and energy availability is predominantly in the exploration phase.
4. Interoperability: Aligning proprietary AES variations with existing or developing standards (ZigBee, 6LoWPAN, 5G/6G protocols) necessitates uniform frameworks suitable for widespread industry adoption.

The literature underscores the necessity of co-designing cryptographic solutions in alignment with the network architecture, operational patterns, and hardware capabilities.

3 Analyses of Energy Consumption of AES Algorithms on IoT-Enabled WSN

Energy consumption has emerged as a critical issue in the implementation of Wireless Sensor Networks (WSNs) in the Internet of Things (IoT) framework. The Advanced Encryption Standard (AES), although secure and extensively utilised, requires computing resources that may overwhelm the constrained power supply of sensor nodes, especially during frequent data encryption. A main element affecting AES-induced energy usage is the key size and the number of iterations. Larger key sizes, such as 256-bit AES, provide enhanced security assurances but necessitate increased computing steps, thereby intensifying battery depletion. Conversely, smaller keys, such as 128-bit AES, might achieve a more advantageous equilibrium between security and durability, making it useful for sensor nodes that are not easily rechargeable or replaceable.

A further factor influencing energy consumption is the type of AES Implementation—hardware-accelerated solutions can enhance the speed of cryptographic operations and diminish CPU load, but they may elevate both hardware complexity and expense. The design of sensor nodes affects their power consumption; for example, 8-bit microcontrollers execute AES differently than 32-bit equivalents, often leading to increase per-operation overhead. Moreover, network structure and communication frequency significantly influence total consumption, since each encryption request necessitates supplementary energy for processing and data transfer.

Researchers evaluate the implementations of AES-128, AES-192, and AES-256 to demonstrate the relationship between key length and energy consumption in limited wireless sensor network nodes. It usually suggests that AES-128 provides a superior balance, enabling robust encryption with reduced energy use. AES-192 and AES-256 enhance cryptographic strength but often demand greater energy and incur higher delay, rendering them less feasible for ultra-low-power systems unless the security context necessitates increased protection.

Table 3 provides a brief overview of the trade-offs, illustrating a general comparison of AES key sizes for per-packet energy usage and delay under uniform network conditions.

Table 3: Comparison of AES key sizes with respect to energy usage and delay

| **Key Size** | **Relative Encryption Time** | **Relative Energy Consumption** | **Security Level** |
|---|---|---|---|
| AES-128 | Low | Low | Moderate to High Security |
| AES-192 | Medium | Medium | Higher Security |
| AES-256 | High | High | Very High Security |

Additional issues occur when these encryption choices connect with memory restrictions and real-time processing needs. For instance, a sensor node might need to encrypt and send data under stringent latency limitations to enable time-sensitive applications such as industrial control loops or health monitoring systems. Under these conditions, the overhead associated with bigger keys might create delays that weaken the responsiveness and dependability of the application. Moreover, the memory footprint of certain AES implementations or key storage systems might surpass the capabilities of severely limited nodes, resulting to increased development complexity or possibly rendering certain encryption settings infeasible.

Moreover, energy collecting technologies—such as solar or vibrational energy—offer a viable solution for mitigating some of the power demands imposed by AES. If a WSN deployment can occasionally recharge its energy reserves, then the choice of key size or encryption frequency may become more flexible without risking premature node depletion. Future

research and real-world deployments need to mix dynamic power management tactics with adaptive or lightweight AES implementations to produce truly sustainable, secure, and responsive WSNs in the IoT sector.

## 4 Analysis of Computation Speed of AES Algorithms on IoT-Enabled WSN

The speed of AES encryption, in conjunction with energy consumption, is a crucial factor influencing IoT device performance and user happiness. Extended encryption latencies in sensor nodes can lead to increased packet delays, adversely affecting real-time applications, reducing throughput, and jeopardising the timeliness of mission-critical data. The disparity in performance is fundamentally attributed to processor architecture: an 8-bit processor may execute the identical AES routine significantly slower than a 32-bit CPU equipped with hardware-assisted instructions. Moreover, compiler-level optimisations, such loop unrolling and memory retrieval using precomputed tables, can enhance the speed of encryption processes on software-only platforms.

Certain implementations investigate parallelisation or pipelined encryption, enabling segments of the AES process to operate simultaneously, thereby diminishing overall latency. The extent of speedup, however, is contingent upon the underlying hardware's capacity to facilitate parallel processes. Empirical testbed results generally indicate that AES-128 can handle a greater number of blocks per second compared to its larger-key alternatives, highlighting its suitability for resource-constrained networks. Hardware-accelerated instructions or tailored AES co-processors can achieve speed enhancements of 30–50% or greater; however, these advantages must be considered with the increased expense and design intricacy of specialised hardware.

In discussions of speed, it is crucial to recognise that rapid encryption does not necessarily result in substantial energy savings; if the hardware acceleration circuitry consumes considerable current, any time gained may be counterbalanced by heightened power consumption. Therefore, a comprehensive approach to both speed and energy is essential for optimising AES in WSN contexts.

### 4.1 Analysis Results

Case studies often demonstrate that AES-128 provides the optimal balance between speed, resource efficiency, and sufficient security. In scenarios where ultra-high encryption speed is critical, hardware-assisted or parallelised techniques frequently surpass conventional software-only solutions. Nonetheless, these speed enhancements may be negated if the node hardware is diverse or lacks consistent support for AES instructions. Meticulous system design is essential to guarantee that the implementation of modern cryptography does not excessively reduce node longevity or escalate device expenses.

### 4.2 Heterogeneity and Adaptive Techniques

Although much progress has been made in enhancing AES performance on IoT nodes, the diversity of hardware platforms presents challenges that may compromise speed optimisations. Networks frequently include a combination of 8-bit old boards, 32-bit ARM microcontrollers, and maybe proprietary System-on-Chip (SoC) solutions, all inside the same Wireless Sensor Network (WSN). In heterogeneous systems, a particular set of optimisations or hardware accelerators may produce significant improvements on certain nodes while resulting in minimal or detrimental impacts on others. Adaptive algorithms that assess node performance in real time and dynamically pick or modify encryption methods may mitigate this difference. A node with ample power and hardware capabilities may execute a hardware-accelerated AES routine, but a neighbouring node with constrained energy could choose a more lightweight software-based solution. Implementing this method of real-time adaptability necessitates extensive monitoring and a decision-making system capable of swiftly transitioning modes without incurring synchronisation overhead or security vulnerabilities.

## 5 Discussion and Future Direction

AES is the most extensively utilised block cypher, owing to its security assurances and proven efficacy against cryptanalysis. Conversely, the computing demands of key-scheduling, rounds, and data translation processes might deplete the finite energy resources of sensor nodes, especially in extensive or enduring networks. This has initiated a continuous endeavour to enhance AES implementations and, in certain instances, to reimagine network topologies that allocate the cryptographic workload more judiciously.

One area of investigation pertains to adaptive AES algorithms, in which key sizes or encryption settings dynamically modify according to real-time network circumstances. A network with low threat levels and modest data traffic may temporarily reduce encryption to AES-128 to save power, restoring to a higher key length only if attack indicators or sensitive data flows necessitate the change. Implementing such adaptability necessitates strong decision-making frameworks—frequently supported by machine learning—to guarantee that alterations in encryption settings do not introduce exploitable weaknesses. In conjunction with these adaptive solutions, lightweight cryptographic primitives specifically developed for power-constrained environments have experienced significant advancement. Although several primitives replicate AES's security attributes, they optimise internal processes to diminish computational burden, perhaps by modifying S-box lookups or simplifying the MixColumns phase.

In addition to software-centric enhancements, an increasing emphasis on hardware/software co-design seeks to incorporate partial AES acceleration at the semiconductor level. Embedding specialised instructions or dedicated cryptography cores within the microcontroller allows sensor nodes to markedly decrease encryption delay and related energy consumption. This methodology is particularly attractive in next-generation System-on-Chip (SoC) architectures, which may already include numerous processing units. The difficulty is in reconciling cost and performance objectives—hardware accelerators can increase the bill of materials and may necessitate specialised manufacturing procedures. Moreover, standardised accelerators do not consistently meet the specific constraints of all IoT applications. Thus, co-design solutions must be customised to certain device categories or use-case specifications to guarantee they effectively enhance energy efficiency.

A growing research initiative utilises machine learning to predict and regulate network demands. By forecasting future traffic patterns, a WSN may allocate encryption work during intervals of less node activity, thereby minimising peak energy consumption. Furthermore, learning-based frameworks can identify imminent assaults or abnormalities, autonomously activating enhanced AES setups alone in response to elevated threats. Although these approaches exhibit potential, they include their own overhead, since training and inference processes deplete resources. Current efforts focus on creating lightweight, on-node machine

learning algorithms that can extract insights from the network without overburdening the node's processing capacity.

A comprehensive strategy integrating cryptography, network protocol design, and resource allocation is progressively emerging. Future developments may involve enhanced collaboration among hardware manufacturers, cryptography experts, and network engineers to create integrated solutions. A coordinated design may include a bespoke SoC with partial AES acceleration, an optimised routing protocol that minimises unnecessary transmissions, and an adaptive software layer that adjusts encryption parameters according to energy metrics and threat data. This collaboration across several levels of the IoT stack is essential for directly addressing the intricate interactions of energy, security, and performance.

**6 Research Gap**

Despite significant advancements in energy-efficient AES implementations in WSNs, several inadequately investigated or poorly resolved challenges persist, hindering smooth real-world use. A significant deficiency is the lack of long-term, real-time deployment data. Despite the plethora of research yielding optimistic outcomes, they frequently depend on simulations or short-term testbeds with a restricted number of nodes. This gap raises enquiries on the performance of optimised AES implementations over extended periods, particularly in challenging or isolated environments where node failures, battery exhaustion, or environmental fluctuations may affect network behaviour.

A second issue is the influence of changing network circumstances on AES performance and energy consumption. Numerous assessments presume relatively fixed node deployments; nevertheless, actual wireless sensor networks sometimes exhibit mobile nodes, sporadic connection, or swiftly evolving topologies due to node malfunctions or energy constraints. These scenarios may result in unanticipated encryption costs, since nodes may be required to execute supplementary rekeying or authentication procedures if topological alterations transpire. Thus, the interaction of routing algorithms, node mobility, and continuous AES encryption is not fully understood, suggesting a potentially substantial area for study exploration.

Hardware heterogeneity is a significant barrier to standardised AES solutions. Sensor nodes from various manufacturers may include distinct microcontroller designs, memory

specifications, and power characteristics, complicating the implementation of a universal "best practice." An algorithm or hardware accelerator optimised for a 32-bit ARM Cortex-M may exhibit suboptimal performance on an 8-bit AVR or be completely incompatible with a bespoke SoC. Thus far, only a few multi-vendor comparative studies have been published, often focussing on restricted metrics or small node clusters. Progressing this research needs comprehensive testbeds or benchmarking suites that can systematically evaluate both performance and energy usage across many hardware platforms.

Ultimately, complete models that amalgamate security criteria with energy expenditures are few. Researchers frequently monitor parameters such as encryption speed, throughput, and average current draw; however, they seldom correlate these measures with security outcomes, like key recovery durations, cryptanalysis success rates, or resistance to side-channel attacks. An integrated technique might measure the impact of each incremental enhancement in security (e.g., transitioning from AES-128 to AES-256) on battery longevity and data availability in high-traffic networks. Comprehensive frameworks will allow IoT stakeholders to make informed judgements on encryption settings for each application scenario. Addressing these research deficiencies will be essential for enhancing and implementing sophisticated AES-based solutions that protect IoT-enabled WSNs while maintaining sustainability and performance.

## 7 Conclusion

This paper analyses the energy consumption and computational performance of AES algorithms in IoT-enabled WSNs, emphasizing both the robustness and resource requirements of AES. While lighter AES versions and hardware acceleration can substantially mitigate encryption costs, actual implementation frequently depends on the interaction of network topologies, node hardware, and real-world limitations. The results highlight the need for a cohesive, application-oriented strategy that reconciles security demands with operational durability. Future research will likely focus on adaptive cryptographic frameworks, extensive real-world validations, and cross-layer optimizations that integrate encryption techniques with network and application-level protocols. Thus, IoT-enabled WSNs may attain the stringent security required by contemporary applications without compromising the power efficiency essential for prolonged system longevity.

**References**

[1] Hussein, S. M., López Ramos, J. A., & Ashir, A. M. (2022). *A secure and efficient method to protect communications and energy consumption in IoT wireless sensor networks*. Electronics, 11(17), 2721.

[2] Gulati, K., Boddu, R. S. K., Kapila, D., Bangare, S. L., Chandnani, N., & Saravanan, G. (2022). *A review paper on wireless sensor network techniques in Internet of Things (IoT).* Materials Today: Proceedings, 51, 161-165.

[3] Khashan, O. A., Ahmad, R., & Khafajah, N. M. (2021). *An automated lightweight encryption scheme for secure and energy-efficient communication in wireless sensor networks.* Ad Hoc Networks, 115, 102448.

[4] Nagaraj, S., Kathole, A. B., Arya, L., Tyagi, N., Goyal, S. B., Rajawat, A. S., & Suciu, G. (2022). *Improved secure encryption with energy optimization using random permutation pseudo algorithm based on IOT in WSN*. Energies, 16(1), 8.

[5] Panahi, U., & Bayılmış, C. (2023). *Enabling secure data transmission for wireless sensor networks based IoT applications.* Ain Shams Engineering Journal, 14(2), 101866.

[6] Khudair, J., Abd Ghan, K., & Baharon, M. R. B. (2023). *Comparative Study in Enhancing AES Algorithm: Data Encryption.* Wasit Journal for Pure sciences, 2(2), 316-339.

[7] Gupta, S. K., & Singh, S. (2022). *Survey on energy efficient dynamic sink optimum routing for wireless sensor network and communication technologies*. International Journal of Communication Systems, 35(11), e5194.

[8] Yilmaz, S., & Dener, M. (2024). *Security with Wireless Sensor Networks in Smart Grids: A Review. Symmetry*, 16(10), 1295.

[9] [Fadhil, M. S., Farhan, A. K., & Fadhil, M. N. (2021). *A lightweight AES algorithm implementation for secure IOT environment*. Iraqi Journal of Science, 2759-2770.

[10] Silva, C., Cunha, V. A., Barraca, J. P., & Aguiar, R. L. (2024). *Analysis of the cryptographic algorithms in IoT communications*. Information Systems Frontiers, 26(4), 1243-1260.

[11] Bharathi, R., Kannadhasan, S., Padminidevi, B., Maharajan, M. S., Nagarajan, R., & Tonmoy, M. M. (2022). *Predictive Model Techniques with Energy Efficiency for IoT-Based Data Transmission in Wireless Sensor Networks*. Journal of Sensors, 2022(1), 3434646.

[12] Thaenkaew, P., Quoitin, B., & Meddahi, A. (2023). *Leveraging Larger AES Keys in LoRaWAN: A Practical Evaluation of Energy and Time Costs. Sensors*, 23(22), 9172.

[13] Surenther, I., Sridhar, K. P., & Roberts, M. K. (2024). *Enhancing data transmission efficiency in wireless sensor networks through machine learning-enabled energy optimization: A grouping model approach.* Ain Shams Engineering Journal, 15(4), 102644.

[14] Satyanarayana, P., Sriramdas*, N., Madhavi, B., Arun, M., Kumar, N. P. S., & Krishnan, V. G. (2023, November). Enhancement of Security in IoT Using Modified AES Algorithm for IoT Applications.* In 2023 International Conference on Sustainable Communication Networks and Application (ICSCNA) (pp. 380-386). IEEE.

[15] Tropea, M., Spina, M. G., De Rango, F., & Gentile, A. F. (2022). *Security in wireless sensor networks: A cryptography performance analysis at mac layer. Future Internet*, 14(5), 145.

[16] Vivek, K., Kale, M. R., Thotakura, V. S. K., & Sushma, K. (2021, November). *An Efficient Triple-Layered and Double Secured Cryptography Technique in Wireless Sensor Networks*. In 2021 IEEE International Conference on Distributed Computing, VLSI, Electrical Circuits and Robotics (DISCOVER) (pp. 117-122). IEEE.

[17] Puttaswamy, C., & Shivaprasad, N. P. K. (2024). *Enhancing wireless sensor network security with optimized cluster head selection and hybrid public-key encryption*. International Journal of Electrical and Computer Engineering (IJECE), 14(3), 2976-2987.

[18] Sebothoma, P., & Mathonsi, T. E. (2023, November). *An Enhanced Security Algorithm for Wireless Sensor Networks.* In 2023 International Conference on Electrical, Computer and Energy Technologies (ICECET) (pp. 1-6). IEEE.

[19] Urooj, S., Lata, S., Ahmad, S., Mehfuz, S., & Kalathil, S. (2023). *Cryptographic data security for reliable wireless sensor network.* Alexandria Engineering Journal, 72, 37-50.

[20] Sebothoma, P., & Mathonsi, T. E. (2024). Implementation of an Enhanced Security Algorithm for Wireless Sensor Networks.

[21] Parashar, V., & Mishra, B. *Performance Comparison of Various Cryptographic Algorithms Along with Energy Consumption in Wireless Sensor Network.*

[22] Venčkauskas, A., Taparauskas, M., Grigaliūnas, Š., & Brūzgienė, R. (2024). *Enhancing Communication Security an In-Vehicle Wireless Sensor Network. Electronics,* 13(6), 1003.

[23] Darshan, B. D., & Prashanth, C. R. *Performance Analysis of Cluster-Based Dynamic Multipath Trust Secure Routing (DMTSR)-Protocol in Wireless Sensor Networks (WSNs).*

[24] Goyal, A., Mishra, S., & Chaurasiya, V. K. (2023, May). *Intrusion Detection in Wireless Sensor Networks Using Deep Learning.* In 2023 4th International Conference for Emerging Technology (INCET) (pp. 1-13). IEEE.

[25] Ahmad, R., Wazirali, R., Abu-Ain, T., & Almohamad, T. A. (2022). *Adaptive trust-based framework for securing and reducing cost in low-cost 6LoWPAN wireless sensor networks.* Applied Sciences, 12(17), 8605.

[26] Shasi, P. V. S. D. S., & Vasudevan, A. V. *Quality of Service aware secure data transmission model for Internet of Things assisted wireless sensor networks.*

[27] Jenifer, R. R., & Prakash, V. S. J. (2023). *Detecting denial of sleep attacks by analysis of wireless sensor networks and the internet of things.* The Scientific Temper, 14(04), 1412-1418.

[28] Daousis, S., Peladarinos, N., Cheimaras, V., Papageorgas, P., Piromalis, D. D., & Munteanu, R. A. (2024). *Overview of Protocols and Standards for Wireless Sensor Networks in Critical Infrastructures.* Future Internet, 16(1), 33.

[29] Silambarasan, S., & Devi, M. S. (2022). *Hybrid simulated annealing with Lion Swarm Optimization Algorithm with modified elliptic curve cryptography for secured data transmission over wireless sensor networks* (WSN). International Journal of Computer Networks and Applications (IJCNA), 9(3), 316-327.

[30] El-Hajj, M., Mousawi, H., & Fadlallah, A. (2023). *Analysis of lightweight cryptographic algorithms on IOT hardware platform. Future Internet,* 15(2), 54.

[31] Yang, H., Zhou, H., Liu, Z., & Deng, X. (2023). *Energy optimization of wireless sensor embedded cloud computing data monitoring system in 6G environment. Sensors*, 23(2), 1013.

[32] Sanislav, T., Mois, G. D., Zeadally, S., & Folea, S. C. (2021). *Energy harvesting techniques for internet of things (IoT).* IEEE access, 9, 39530-39549.

[33] Alshehri, J., Alhamed, A., & Frikha, M. (2023). *The Countermeasures of Wireless Sensor Network Threats In IOT System.* Journal of Theoretical And Applied Information Technology, 101(19).

[34] Bhatia, S., Kumar, A., Kumar, A., & Alshuhail, A. S. (2022). *Performance analysis of energy efficient improved LEACH protocol in IoT networks*. IET Communications.

[35] Khalifeh, A., Darabkh, K. A., Khasawneh, A. M., Alqaisieh, I., Salameh, M., AlAbdala, A., ... & Rajendiran, K. (2021). *Wireless sensor networks for smart cities: Network design, implementation and performance evaluation*. Electronics, 10(2), 218.

[36] Murugan, G., & Vijayarajan, S. (2023*). IoT based secured data monitoring system for renewable energy fed micro grid system*. Sustainable Energy Technologies and Assessments, 57, 103244.

[37] Darla, S., & Naveena, C. (2024). *Improved Adaptive Spiral Seagull Optimizer for Intrusion Detection and Mitigation in Wireless Sensor Network.* SN Computer Science, 5(4), 394.

[38] Valluri, B. P., & Sharma, N. (2024). *Exceptional key based node validation for secure data transmission using asymmetric cryptography in wireless sensor networks*. *Measurement*: Sensors, 33, 101150.

[39] Bhardwaj, M., Kumari, U., Kumar, S., & Choudhary, S. (2023). *An Efficient User Authentication and Key Agreement Scheme Wireless Sensor Network and IOT Using Various Security Approaches*. SN Computer Science, 4(5), 574.

[40] Patil, K., & Banerjee, S. (2023). *Brief Overview on Wireless Sensor Network Technologies in the Internet of Things (IoT).* International Journal of Engineering and Management Research, 13(6), 1-8.

[41] AB, F. K., & Rama, D. K. (2023). *An enhanced AES-GCM based security protocol for securing the IoT communication.* Scientific and Technical Journal of Information Technologies, Mechanics and Optics, 2023, vol. 23(4), 711-719.

[42] Coboi, A. E., Nguyen, V., Nguyen, M., DUY, N., & TRAN, T. (2021). *An Analysis of ZigBee Technologies for Data Routing in Wireless Sensor Networks.* ICSES Transactions on Computer Networks and Communications (ITCNC).

[43] Panahi, P., Bayılmış, C., Çavuşoğlu, U., & Kaçar, S. (2021*). Performance evaluation of lightweight encryption algorithms for IoT-based applications*. Arabian Journal for Science and Engineering, 46(4), 4015-4037.

[44] Singh, Y., & Walingo, T. (2024). *Smart Water Quality Monitoring with IoT Wireless Sensor Networks. Sensors*, 24(9), 2871.

[45] Khalifa, M., Algarni, F., Khan, M. A., Ullah, A., & Aloufi, K. (2021). *A lightweight cryptography (LWC) framework to secure memory heap in Internet of Things.* Alexandria Engineering Journal, 60(1), 1489-1497.

[46] Hasan, M. K., Shafiq, M., Islam, S., Pandey, B., Baker El-Ebiary, Y. A., Nafi, N. S., ... & Vargas, D. E. (2021). *Lightweight cryptographic algorithms for guessing attack protection in complex internet of things applications*. Complexity, 2021(1), 5540296.

[47] Gaikwad, S. Y. (2024). *Secure Data Transmission in the Wireless Sensor Network with Blockchain Cryptography Network*. Journal of Sensors, IoT & Health Sciences, 2(2), 41-55.

[48] Yaïci, W., Krishnamurthy, K., Entchev, E., & Longo, M. (2021). *Recent advances in Internet of Things (IoT) infrastructures for building energy systems: A review.* Sensors, 21(6), 2152.

[49] AlJabri, Z., Abawajy, J., & Huda, S. (2023). [Retracted] *A Comprehensive Review of Lightweight Authenticated Encryption for IoT Devices. Wireless Communications and Mobile Computing,* 2023(1), 9071969.

[50] Yakubu, M. M., & Maiwada, U. D. (2023). *Resource limitations for wireless sensor networks to establish a comprehensive security system in the 5g network.* UMYU Scientifica, 2(2), 44-52.