Creative Research Publishers
https://www.crossref.org/06members/50go-live.html

Journal of Behavioral Informatics
Digital Humanities & Development Research
Vol 12, No 1, March , 2026 Series

Comparative Evaluation of AES, Camellia, and CLEFIA for Lightweight Environments: A Post-2023 Systematic Literature Review and Meta-Analysis

[1]Ojeniyi, J.A., [1]Fasola, O.O., [2]Onyeabor, G.A., [1]Abdulsalam, A., [1]Emmanuel, I.O., [1]Baba, S.U. & [1]Jiya, J.B.
[1]Department of Cyber Security Science, Federal University of Technology, Minna, Nigeria
[2]Department of Data Science, Federal University of Technology, Minna, Nigeria
E-mails: ojeniyija@futminna.edu.ng, Sanjo.fasola@futminna.edu.ng, grace.onyeabor@gmail.com, Abdulsalamamte25283@st.futminna.edu.ng, ibeheomte25256@st.futminna.edu.ng, suleimanubmte25247@st.futminna.edu.ng, jiyajbmte25253@st.futminna.edu.ng
Corresponding Author: ojeniyija@futminna.edu.ng

ABSTRACT

The rapid proliferation of resource-constrained Internet of Things (IoT) devices, embedded sensors, and edge computing platforms has intensified the demand for cryptographic primitives that strike a balance between security and stringent hardware and energy constraints. This paper presents a post-2023 systematic literature review and meta-analysis of three standardized block ciphers: the Advanced Encryption Standard (AES), Camellia, and CLEFIA, with a focus on their adaptation to lightweight environments. Drawing on Scopus-indexed research from 2021–2024, we evaluate architectural innovations, hardware/software optimizations, side-channel countermeasures, and quantum-resilience considerations. Our analysis demonstrates that while AES dominates in hardware-accelerated and certification-driven environments, CLEFIA is most efficient in ultra-constrained hardware, and Camellia provides a balanced solution for mid-range systems. Recent developments, including RISC-V cryptographic extensions and machine learning-assisted cryptanalysis, have reshaped performance and security expectations. Based on these findings, we propose a decision framework for cipher selection tailored to specific resource, energy, and certification constraints.

Keywords: Proof Construction, Procedural Fluency, Undergraduate Mathematics Majors, APOS Theory, Scaffolded Instruction.

Journal Reference Format:
Ojeniyi, J.A., Fasola, O.O., Onyeabor, G.A., Abdulsalam, A., Emmanuel, I.O., Baba, S.U. & Jiya, J.B. (2026): Comparative Evaluation of AES, Camellia, and CLEFIA for Lightweight Environments: A Post-2023 Systematic Literature Review and M-66eta-Analysis. Journal of Behavioural Informatics, Digital Humanities and Development Research. Vol. 12 No. 1. Pp 59-66.
https://www.isteams.net/behavioralinformaticsjournal. dx.doi.org/10.22624/AIMS/BHI/V12N1P5

I. INTRODUCTION

The landscape of lightweight cryptography has evolved significantly in the post-2023 era, driven by the proliferation of resource-constrained IoT devices, industrial control systems, and edge computing platforms. These devices often operate under severe limitations in memory, energy, and area, while simultaneously facing emerging threats such as side-channel attacks and

potential quantum adversaries. Evaluating cryptographic primitives under such constraints is critical for ensuring both security and operational efficiency.

The formal standardization of ASCON as the NIST Lightweight Cryptography standard (2023) established benchmarks for authenticated encryption, while simultaneously highlighting the continued relevance of classical block ciphers in legacy and compatibility-driven systems (Chakraborty et al., 2024). Concurrently, the maturation of RISC-V cryptographic extensions (RISC-V International, 2023) and the emergence of machine learning-assisted cryptanalysis (Alani & Zakaria, 2023) have introduced new evaluation criteria, reshaping the comparative landscape for lightweight block ciphers. It is anticipated that by 2028, RISC-V will achieve further standardization milestones, enhancing integration into a wider range of IoT devices. Additionally, developments in machine learning-assisted cryptanalysis are expected to advance attack sophistication, requiring ongoing updates to cryptographic defense strategies.

Within this context, this review focuses on three ciphers with distinct characteristics:

i. **AES:** Widely deployed, continuously optimized for hardware acceleration.
ii. **Camellia:** Balances performance and implementation flexibility, with no patent restrictions.
iii. **CLEFIA:** Specialized for ultra-constrained environments, demonstrating resilience to emerging attack vectors.

2. METHODS

2.1 Literature Search Strategy

A systematic search was conducted across five databases: **ScienceDirect, ACM Digital Library, IEEE Xplore, SpringerLink, and Web of Science**. The search targeted publications between 2021 and 2024 using keywords such as: “AES”, “Camellia”, “CLEFIA”, “lightweight cryptography”, “IoT security”, and “energy-efficient encryption”.

2.2 Inclusion and Exclusion Criteria

i. **Inclusion:** Peer-reviewed journal articles and conference papers addressing AES, Camellia, or CLEFIA in resource-constrained hardware/software environments; studies reporting performance metrics, security evaluations, or energy consumption.
ii. **Exclusion:** Non-peer-reviewed sources, duplicates, or studies without empirical or simulation-based results.

2.3 Data Extraction and Analysis

For each study, key parameters were extracted: hardware/software implementation details, energy consumption, memory footprint, fault resistance, side-channel vulnerability, and quantum-security considerations. Comparative analysis was conducted using meta-analytic methods and cross-referenced performance metrics.

3. ARCHITECTURAL INNOVATIONS AND OPTIMIZATIONS (2021–2024)

3.1 AES: Beyond Traditional Accelerations

Recent research has advanced AES implementations for memory-constrained platforms. Zhang et al. (2023) demonstrated a **bit-sliced AES** requiring only 1.9 KB of RAM on ARM Cortex-M4, reducing memory usage by 40% while maintaining constant-time execution. In hardware, Kumar et al. (2022) proposed a unified encrypt/decrypt architecture with composite-field S-boxes, achieving **2,350 GE** in 65nm technology—22% lower than previous designs.

RISC-V cryptographic extensions finalized in 2023 (Zkne/Zknd) enable dedicated AES instructions, yielding **8.7× performance improvement** over software-only implementations (Wang et al., 2024).

3.2 Camellia: Renaissance Through Balance

Camellia's Feistel structure enables lightweight and balanced implementations. Tanaka et al. (2023) developed a **"thin" Camellia** using 1,850 GE in 28nm technology. Its complex key schedule confers enhanced resistance against neural network-based key recovery in reduced-round scenarios (Alani & Zakaria, 2023), while full-round implementations remain secure.

3.3 CLEFIA: Specialized Evolution

CLEFIA has been optimized for ultra-constrained environments. Shimizu et al. (2022) implemented a **minimalist CLEFIA** variant using 1,420 GE (40nm technology) by removing decryption circuitry and optimizing the MDS matrix. Nguyen et al. (2023) demonstrated that CLEFIA's dual S-box structure confers **3.2× higher fault-injection resistance** compared to AES.

4. PERFORMANCE ANALYSIS: METRICS AND PLATFORMS

4.1 Energy-per-Bit

Energy-per-bit (E_b) is a fundamental metric in digital communications that measures the average amount of energy (in Joules) consumed to transmit a single bit of information, serving as a key indicator of network and hardware energy efficiency. It is calculated by dividing the total transmission power by the bit rate, allowing engineers to evaluate efficiency regardless of data rate. Lowering the energy per bit, often measured in femtojoules (fJ) or picojoules (pJ) per bit, is critical for enhancing battery life in mobile devices and reducing power consumption in data centers, with modern technologies specifically aimed at minimizing this value. Unlike SNR, which depends on bandwidth, E_b offers a consistent, normalized measure of how effectively energy is converted into transmitted data.

Table 1: Energy efficiency is critical in battery-limited devices. (Chen et al., 2024)

AES-128 (serial)	48.2	12.4	8
Camellia-128	39.7	10.2	6
CLEFIA-128	31.5	8.7	4
ASCON-128	29.8	7.9	3

CLEFIA demonstrates **34.7% lower energy consumption than AES**, remaining competitive with newer lightweight authenticated encryption designs.

4.2 Memory-Constrained Software

Memory-constrained software refers to application code designed to operate efficiently within severely limited on-chip memory (RAM or ROM), typically found in embedded systems, IoT devices, and digital signal processing (DSP) applications. Because these systems cannot rely on large amounts of DRAM, developers must use specialized optimization techniques—such as static scheduling, buffer reuse, and code compaction—to minimize the combined footprint of both code and data. Unlike traditional desktop software, this type of software prioritizes minimizing memory activation rates and buffer costs to ensure the entire system fits into constrained hardware, often employing techniques like [Pairwise Grouping of Adjacent Nodes (PGAN)] or [Recursive Partitioning by Minimum Cuts (RPMC)] during compilation

Using composite metrics (code size, stack usage, execution time), Garcia and Martinez (2023) show:

i. CLEFIA dominates in systems with <32 KB ROM
ii. AES excels in systems with >64 KB ROM
iii. Camellia exhibits consistent performance across memory profiles.

4.3 FPGA Throughput-Area Product

The FPGA Throughput-Area Product (or efficiency) is a performance metric used to evaluate the optimization of a digital design, calculated as the ratio of data throughput (e.g., in Mbps or Gbps) to the hardware resources utilized (e.g., number of logic slices, lookup tables, or DSP blocks). It represents a key trade-off analysis where designers aim to maximize data processing speed while minimizing area occupancy (resource usage). A higher Throughput/Area value indicates a more efficient design, essential for optimizing complex FPGA applications like cryptography, signal processing, and machine learning, ensuring that the design achieves high speed without wasting FPGA resources. Dynamic reconfiguration improves performance in FPGA implementations. Park et al. (2022) reported:

i. Camellia: 41% improvement
ii. AES: 28% improvement

5. SECURITY ANALYSIS

5.1 Machine Learning-Assisted Cryptanalysis

Machine Learning-Assisted Cryptanalysis leverages AI—specifically deep learning and neural networks—to identify non-linear relationships and structural vulnerabilities in cryptographic algorithms, often automating the discovery of distinguishers (identifying patterns) more efficiently than traditional statistical methods. By treating cryptanalysis as a classification problem, models can be trained to distinguish between random data and ciphertext, aiding in key recovery or reducing the complexity of breaking ciphers, such as lightweight ciphers (e.g., Speck, SIMON) or analyzing isogeny-based post-quantum protocols.

Though it does not replace conventional techniques, it complements them by enabling "black-box" approaches to find cryptographic weaknesses, such as identifying better differential trails for ciphers like.

Zheng et al. (2023) found:

i. AES exhibits the strongest correlation with power consumption, aiding profiling attacks
ii. CLEFIA's chaotic power signatures require ~40% more traces for key recovery
iii. Camellia's FL layers reduce attack accuracy by 22%

First-order masking countermeasures add **15–25% overhead** but maintain practical security.

5.2 Fault Attack Resilience

Fault Attack Resilience refers to the ability of a cryptographic system or embedded device to withstand malicious, intentional faults (such as power glitches or laser pulses) that attempt to alter its operation and extract secret keys. This resilience is achieved by incorporating countermeasures—such as redundancy, error detection, or randomized algorithms—that detect or nullify the impact of these faults, ensuring that erroneous data is not released and the key remains secure. A system with high fault resilience ensures that, despite physical tampering, the system either produces correct results or halts operations, preventing attackers from exploiting the relationship between input and faulty output.

Table 2: Fault Attack Resilience

Single-bit fault	86% key recovery	72%	64%
Random byte fault	94%	81%	70%
Instruction skips	Highly vulnerable	Moderate	Least vulnerable

5.3 Quantum Security Implications

Quantum security implications refer to the transformative threat and defensive paradigm shift caused by quantum computing, which can render conventional encryption methods—such as RSA and ECC—vulnerable by breaking them using algorithms like Shor's algorithm. As quantum technology matures, it enables "harvest now, decrypt later" attacks, allowing adversaries to seize encrypted data today to decrypt in the future, thus forcing an urgent, proactive shift towards post-quantum cryptography (PQC) and quantum key distribution (QKD). This shift is essential for safeguarding long-term, high-value data, including financial records and national intelligence, making it necessary to update secure communication frameworks and ensure long-term data integrity against the looming "Q-Day" when current encryption collapses

Post-quantum effective security against Grover's algorithm:

i. AES-128: ~64 bits
ii. Camellia-128: ~65 bits
iii. CLEFIA-128: ~63 bits

Using 256-bit keys ensures >128-bit post-quantum security.

6. IMPLEMENTATION ECOSYSTEM

i. **TLS 1.3** and industrial protocols favor AES
ii. CLEFIA is widely adopted in Asian IoT modules
iii. Camellia is increasingly validated in EU industrial control systems.
iv. FIPS 140-3 validation: AES (423), Camellia (37), CLEFIA (12)

7. EMERGING PLATFORMS AND FUTURE DIRECTIONS

7.1 RISC-V Extensions

i. AES: 6.8–9.2× speedup
ii. Camellia: 2.1–2.8×
iii. CLEFIA: 3.4×

7.2 Approximate Computing

i. AES tolerates a limited MixColumns approximation (4% error)
ii. CLEFIA is resilient to S-box approximations
iii. Camellia is sensitive to approximation in FL functions.

8. DECISION FRAMEWORK

Table 3: Decision Framework on Area Efficiency Versus Protocol Support

Ultra-constrained ASIC/FPGA (<2,000 GE)	CLEFIA	Camellia	Area efficiency vs. protocol support
Energy-harvesting IoT	CLEFIA	AES bit-sliced	Energy efficiency
RISC-V-based systems	AES	CLEFIA	Hardware acceleration benefits AES
Industrial/Medical Certification	AES	Camellia	Certification availability
Legacy System Integration	Camellia	AES	Feistel structure integration

9. CONCLUSION

This systematic review demonstrates that post-2023:

1. AES remains dominant in accelerated and certified environments
2. CLEFIA is optimal for ultra-constrained devices
3. Camellia provides balanced performance and IP/certification flexibility.

Future lightweight cipher evaluations should integrate **system architecture, threat models, and operational constraints** into the design process. All three ciphers are cryptographically robust; relative merits depend on implementation context rather than inherent properties alone.

REFERENCES

Ahmed, A., & Singh, R., "Power-Optimized AES for Energy-Constrained Embedded Systems," ACM Journal on Emerging Technologies in Computing Systems, vol. 21, no. 3, 2025.

Alani, M. M., & Zakaria, N. H. (2023). Machine Learning-Assisted Cryptanalysis of Block Ciphers: A Comparative Study. Computers & Security, 124, 102965.

Alani, M. M., & Zakaria, N. H., "Machine Learning-Assisted Cryptanalysis of Block Ciphers: Comparative Study," Computers & Security, vol. 124, 102965, 2023.

Alani, M., et al., "Resistance of CLEFIA Cipher Against Deep Learning-Based Side-Channel Attacks," Journal of Cryptographic Engineering, 2025.

Al-Bassam, F., et al., "Comprehensive Comparative Study of Lightweight Ciphers in Embedded and IoT Systems," IEEE Transactions on Very Large Scale Integration Systems, 2025.

Al-Bassam, F., et al., "Lightweight Encryption Architectures for Next-Generation IoT Sensors," IEEE Embedded Systems Letters, vol. 15, no. 1, pp. 12–19, 2023.

Aljuffri, A., et al., "The Security Evaluation of an Efficient Lightweight AES Accelerator," Cryptography, vol. 8, no. 2, 2024.

Al-Nofaie, S. M., Al-Momani, M. S., & Al-Bataineh, M. T., "Design Trends and Comparative Analysis of Lightweight Block Ciphers for IoTs," Applied Sciences, vol. 15, no. 14, pp. 7740, 2025.

Amrita, Ekwueme C. P., et al., "Lightweight Cryptography for Internet of Things: A Review," EAI Endorsed Transactions on IoT, vol. 9, no. 4, 2024.

Chakraborty, A., Singh, S., & Roy, B., "Impact of NIST Lightweight Cryptography Standardization on Existing Cryptographic Deployments," IACR Transactions on Symmetric Cryptology, vol. 2024(1), pp. 156–182, 2024.

Chandra, S., et al., "Approximate Computing Techniques for Energy-Harvesting IoT Cryptography," IEEE Transactions on Sustainable Computing, 2025.

Chandra, S., Gupta, A., & Reddy, K., "Approximate Computing for Cryptographic Primitives in Energy-Harvesting IoT Systems," IEEE Transactions on Sustainable Computing, vol. 9, no. 1, pp. 123–135, 2024.

Chen, L., & Xu, P., "Energy-Aware Lightweight Cryptography for Ultra-Low-Power IoT Nodes," Sensors, MDPI, vol. 24, no. 12, pp. 4008, 2024.

Chen, L., Wang, X., & Zhou, M. (2024). Energy-Per-Bit Analysis of Lightweight Cryptography for Battery-Free IoT Devices. ACM Trans. Embedded Comput. Syst., 23(2), 27.

Chen, L., Wang, X., & Zhou, M., "Energy-Per-Bit Analysis of Lightweight Cryptography for Battery-Free IoT Devices," ACM Transactions on Embedded Computing Systems, vol. 23, no. 2, Article 27, 2024.

Garcia, F., & Martinez, P., "Composite Metrics for Cryptographic Algorithm Evaluation in Constrained Microcontrollers," Microprocessors and Microsystems, vol. 96, 104758, 2023.

Gupta, A., et al., "Memory-Constrained Implementation of AES and CLEFIA for Embedded Devices," ACM Transactions on Embedded Computing Systems, 2025.

Jian Tew, J., et al., "Compact Hardware Implementation of the CLEFIA Block Cipher," Journal of Advanced Research in Computing and Applications, 2025.

Khairnar, S., et al., "A Light Weight Cryptographic Solution for 6LoWPAN Protocol Stack," arXiv, 2025.

Kim, H., & Lee, S., "Security Comparison of AES, Camellia, and CLEFIA under Power Side-Channel Attacks," IEEE Transactions on Dependable and Secure Computing, 2025.

Kumar, R., Singh, A., & Patel, S., "Low-Area Unified AES Architecture for Constrained Embedded Systems," IEEE Transactions on VLSI Systems, vol. 30, no. 8, pp. 1123–1132, 2022.

Kumar, S., Singh, A., & Patel, R. (2022). A Unified Low-Area Architecture for AES Encryption and Decryption in IoT Applications. IEEE Trans. VLSI Systems, 30(8), 1123–1132.

Li, J., & Chen, Y., "Post-Quantum Analysis of Lightweight Block Ciphers for IoT Applications," Quantum Information Processing, vol. 24, 2025.

Li, J., Zhang, Q., & Sun, Y., "Post-Quantum Security Margins of Classical Block Ciphers: Reevaluation and Implications," Quantum Information Processing, vol. 23, no. 1, pp. 45, 2024.
Nguyen, T. P., Lee, S., & Kim, H., "Comprehensive Fault Attack Evaluation of Lightweight Block Ciphers on 28nm Technology," IEEE Transactions on Information Forensics and Security, vol. 18, pp. 2456–2470, 2023.
Park, J., & Kim, S., "Side-Channel Vulnerabilities in Commercial IoT Devices: A Large-Scale Study," IEEE Internet of Things Journal, vol. 10, no. 4, pp. 3421–3434, 2023.
Park, S., Lee, J., & Kim, D., "Reconfigurable Camellia Implementation for Low-Power IoT Devices," IEICE Transactions on Electronics, vol. E107.C, no. 6, pp. 112–120, 2024.
Rakshit, H., Singh, V., & Kapoor, R., "Lightweight Session-Key Rekeying Framework for IoT-Edge Communication," arXiv, 2025.
RISC-V International, "RISC-V Cryptography Extensions Volume I: Scalar & Entropy Source," Technical Report, 2023.
Sharma, P., et al., "Bit-Sliced AES for Ultra-Low-Power RISC-V Platforms," IEEE Embedded Systems Letters, 2025.
Shimizu, K., Nakamura, Y., & Watanabe, T. (2022). Minimalist CLEFIA: A Sub-1500 GE Implementation for Sensor Network Applications. J. Information Processing, 30, 568–577.
Shimizu, K., Nakamura, Y., & Watanabe, T., "Minimalist CLEFIA: A Sub-1500 GE Implementation for Sensor Network Applications," Journal of Information Processing, vol. 30, pp. 568–577, 2022.
Soni, A., et al., "AESHA3: Efficient Sub-Key Generation for AES Using SHA-3," arXiv, 2025.
Suryateja, P. S., et al., "A Survey on Lightweight Cryptographic Algorithms in IoT," Cybernetics and Information Technologies, vol. 24, no. 2, pp. 105–122, 2024.
Tan, K., et al., "Fault Injection Analysis of Lightweight Block Ciphers for Embedded Devices," Cryptography, MDPI, vol. 9, no. 1, pp. 18, 2025.
Tan, K., et al., "FPGA-Based Low-Area Implementations of Camellia and CLEFIA for IoT," Journal of Hardware and Systems Security, 2025.
Tanaka, Y., et al., "Camellia Cipher Integration in Legacy Industrial Control Systems: Performance and Security Evaluation," IEICE Transactions on Information and Systems, 2025.
Tanaka, Y., Sato, H., & Kobayashi, T. (2023). Ultra-Thin Implementation of Camellia Cipher for Constrained Edge Devices. IEICE Trans. E106.A(1), 156–165.
Tanaka, Y., Sato, H., & Kobayashi, T., "Ultra-Thin Implementation of Camellia Cipher for Edge Devices," IEICE Transactions on Fundamentals of Electronics, Communications and Computer Sciences, E106.A(1), pp. 156–165, 2023.
Vahi, A., "Key Length-Oriented Classification of Lightweight Cryptographic Algorithms for IoT Security," arXiv, 2025.
Wang, H., Chen, T., & Liu, F., "Performance Evaluation of RISC-V Cryptographic Extensions for Embedded Security," Journal of Systems Architecture, vol. 136, 102841, 2024.
Wang, Y., et al., "Energy-Efficient Implementation of CLEFIA Cipher on Constrained FPGAs," Journal of Hardware and Systems Security, vol. 7, pp. 45–56, 2024.
Zhang, H., Liu, Y., & Wang, Q. (2023). Bit-Sliced AES for Memory-Constrained IoT Devices: Implementation and Evaluation. IEEE Trans. Computers, 72(5), 1347–1360.
Zhang, Y., Liu, J., & Wang, X., "Bit-Sliced AES for Ultra-Low-Power IoT Devices: Hardware/Software Co-Design," IEEE Access, vol. 11, pp. 11234–11246, 2023.
Zheng, W., Zhao, L., & Ma, J., "Deep Learning-Based Power Analysis Attacks on Cryptographic Implementations: Practical Evaluation," Journal of Cryptographic Engineering, vol. 13, no. 4, pp. 425–441, 2023.

Creative Research Publishers
https://www.crossref.org/06members/50go-live.html

Journal of Behavioral Informatics
Digital Humanities & Development Research
Vol 11, No 2, June 2025 Series

Systematic Literature Review: Risk Assessment of AES for Secure Data Communication: Capabilities, Limitations, and Research Directions

[1]Ojeniyi, J.A., [1]Fasola, O.O., [2]Onyeabor, G.A., [1]Yahaya, S.M., [1]Maigida, B.C., [1]Gana, E.M., & [1]Agbenyo, U.M.

[1]Department of Cyber Security Science, Federal University of Technology, Minna, Nigeria
[2]Department of Data Science, Federal University of Technology, Minna, Nigeria
E-mails; ojeniyija@futminna.edu.ng, Sanjo.fasola@futminna.edu.ng, grace.onyeabor@gmail.com, shehubnyahya@gmail.com, cathbaha1@gmail.com, elizabethgold877@gmail.com, miracleunekwu123@gmail.com

ABSTRACT

The most widely used symmetric encryption technique for protecting digital communications in a variety of applications, including cloud infrastructure and Internet of Things (IoT) devices, is still the Advanced Encryption Standard (AES). Even though AES has been widely used for 20 years and has a strong mathematical design (Daemen & Rijmen, 1998; NIST, 2023), side-channel exploitation, developments in quantum computing, and poor key management pose new risks to AES implementations (Altigani et al., 2021; Dheeba et al., 2025). The five crucial elements of AES security concerns are evaluated in this systematic literature review: implementation vulnerabilities, side-channel attack susceptibility, quantum computing dangers, key management issues, and AI-based attack detection. We examined 95 peer-reviewed papers from 2021 to 2025 in accordance with accepted systematic literature review guidelines for computer science research (Kitchenham et al., 2009; Kitchenham & Charters, 2007). According to the assessment, implementation issues lead to serious real-world vulnerabilities even though AES maintains strong mathematical security against conventional cryptanalysis (Bogdanov et al., 2011). With more than 50,000 traces, side-channel attacks especially those enabled by deep learning can effectively get keys from disguised implementations (Kuroda et al., 2021). Because Grover's approach essentially reduces AES-128 to 64-bit security (Grassl et al., 2016), quantum computing presents unequal risks. The most important operational vulnerability is key management, since attacks that go around AES's mathematical strength are made possible by lifecycle errors (Shakor et al., 2024). Although AI-based detection has potential for spotting cryptographic abuse, it has trouble generalizing across many implementations (Ghimire et al., 2024). In addition to identifying priority research directions for post-quantum transition, hardware-software co-design, and automated key management, this analysis synthesizes findings to offer evidence-based recommendations for safeguarding AES deployments.

Keywords: Advanced Encryption Standard (AES), Side-Channel Attacks, Quantum Cryptanalysis, Key Management, Implementation Security, Artificial Intelligence, Systematic Literature Review

Journal Reference Format:

Creative Research Publishers
https://www.crossref.org/06members/50go-live.html
Journal of Behavioral Informatics Digital Humanities & Development Research
Vol 11, No 2, June 2025 Series

Ojeniyi, J.A., Fasola, O.O., Onyeabor, G.A., Yahaya, S.M., Maigida, B.C., Gana, E.M., & Agbenyo, U.M. (2026): Systematic Literature Review: Risk Assessment of AES for Secure Data Communication: Capabilities, Limitations, and Research Directions. Journal of Behavioural Informatics, Digital Humanities and Development Research. Vol. 12 No. 1. Pp 67-80.
https://www.isteams.net/behavioralinformaticsjournal. dx.doi.org/10.22624/AIMS/BHI/V12N1P6

I. INTRODUCTION

A systematic technique for gathering, identifying, and critically analyzing existing research studies is called a Systematic Literature Review (SLR) (Pati & Lorusso, 2018). An SLR provides the reader with up-to-date literature on a topic (Kitchenham & Charters, 2007), highlighting important aspects of existing understanding in order to recommend areas for more research (Kitchenham et al., 2009). This evaluation was initially motivated by the importance of AES in protecting contemporary data transmission systems and the changing threat landscape that puts its practical security at risk. Although the mathematical underpinnings of AES are still solid (Daemen & Rijmen, 1998; NIST, 2023), recent studies have shown that sophisticated attacks can take advantage of implementation flaws, side-channel leaks, and quantum vulnerabilities (Altigani et al., 2021; Dheeba et al., 2025). In order to give practitioners thorough recommendations and identify research gaps that need more study, this review attempts to methodically evaluate these concerns.

2. METHODS

The methodology comprises two main phases: "Planning" described in Section 1, and "Conducting" described in Section 2.

2.1 Planning

Since it outlines the processes involved in the review and serves as a log of the tasks to be completed, defining the protocol is the first stage of an SLR. The protocol guarantees that the review can be repeated.

2.1.1 Define PICOc and Synonyms

The SLR's goals are broken down into searchable terms using the PICOc (Population, Intervention, Comparison, Outcome, and Context) criteria, which can aid in developing research questions (Petersen et al., 2015). The PICOc elements and synonyms used in this review are shown in Table 1.

Table 1. Planning Step 1: Defining PICOc keywords and synonyms.

PICOc Element	Description	Example (This Review)	Example (Synonyms)
Population	Specific role, application area, or industry domain	AES implementations	Embedded systems, cloud infrastructure, IoT devices, microcontrollers, hardware security modules

PICOc Element	Description	Example (This Review)	Example (Synonyms)
Intervention	Methodology, tool, or technology addressing a specific issue	Security analysis	Cryptanalysis, side-channel analysis, fault injection, quantum attacks, key management
Comparison	Methodology being compared (where appropriate)	Implementation approaches	Hardware vs. software, masked vs. unmasked, constant-time vs. table-based
Outcome	Factors of importance to practitioners and results	Security effectiveness	Key recovery success, attack complexity, trace requirements, resistance metrics
Context	Context in which the comparison takes place	Communication systems	Cloud computing, IoT networks, financial systems, healthcare, government communications

2.1.2 Define Research Questions

Based on the PICOc elements, we formulated five research questions:

RQ1: How do implementation weaknesses affect the overall security of AES in real-world data communication systems?

RQ2: To what extent can side-channel attacks compromise AES encryption in modern hardware and cloud computing environments?

RQ3: How vulnerable is AES encryption to future quantum computing threats, and what hybrid security models can reduce this risk?

RQ4: What are the key challenges in AES key management for large-scale distributed communication systems such as cloud and IoT networks?

RQ5: How can artificial intelligence be used to detect misuse, vulnerabilities, or attack attempts against AES-based secure communication systems?

2.1.3 Define Digital Library Sources

Because of their extensive coverage of computer science and cryptography research, we chose five digital libraries:

1. **IEEE Xplore:** The main resource for research in hardware security and computer engineering
2. **ScienceDirect:** Extensive coverage of journals in computer science
3. **SpringerLink:** A significant publisher of conference proceedings on cryptography

4. **IACR Cryptology ePrint Archive:** The main source for pre-publication cryptography research
5. **Google Scholar:** Extensive coverage in all pertinent fields

2.1.4 Define Search Strings

Primary Search String:

text
("Advanced Encryption Standard" OR "AES") AND
(("implementation vulnerability" OR "implementation weakness") OR
("side-channel" OR "power analysis" OR "timing attack" OR "electromagnetic") OR
("fault injection" OR "glitch attack") OR
("quantum" OR "Grover" OR "post-quantum") OR
("key management" OR "key distribution") OR
("machine learning" OR "deep learning" OR "AI") AND
("security" OR "attack" OR "vulnerability" OR "risk"))

2.1.5 Define Inclusion and Exclusion Criteria

Table 2: Inclusion and exclusion criteria.

Criteria Type	Description	This Review
Period	Time frame for article selection	**Inclusion:** 2021-2025
Language	Articles included based on language	**Inclusion:** English
Type of Literature	Categories of literature	**Exclusion:** Grey literature
Type of Source	Origin of articles	**Inclusion:** Peer-reviewed journals, conferences
Impact Source	Quality indicators	**Inclusion:** Q1, Q2, Q3 sources
Relevance to RQs	Articles relevant to at least one RQ	**Inclusion:** Relevant to ≥1 RQ

2.1.6 Define Quality Assessment (QA) Checklist

Table 3. Quality assessment checklist.

Quality Aspect	Assessment Question	Score (0-3)
Reporting	Are the research objectives clearly stated?	3
Reporting	Is the methodology clearly described?	3
Reporting	Are the results presented clearly?	3
Rigor	Is the experimental design appropriate?	3
Rigor	Are measurement techniques validated?	3
Rigor	Is statistical analysis performed?	3
Credibility	Are limitations and threats discussed?	3
Credibility	Are conclusions supported by evidence?	3
Relevance	Is the study relevant to at least one RQ?	3
Relevance	Are practical implications discussed?	3
Total		**30**

Cutoff Score: Articles scoring less than 15 (50% of maximum) were excluded.

2.1.7 Define Data Extraction Form

Table 4. Data extraction form fields.

Field	Description
Basic Information	
Paper ID	Unique identifier
Authors	Full author list
Year	Publication year
Venue	Journal/conference name
Classification	
Research type	Theoretical or empirical
Attack category	Primary attack methodology
Target environment	Implementation platform
Methodology	
Attack vector	Exploited vulnerability
Countermeasures	Defenses evaluated
Experimental setup	Hardware/software configuration
Results	
Key metrics	Quantitative measures
Attack complexity	Computational/trace requirements

Field	Description
Practical feasibility	Real-world applicability
Synthesis	
Key findings	Main contributions
Limitations	Stated limitations
Gaps identified	Unaddressed research questions
Quality Assessment	
QA score	Total quality score
Relevant RQs	Research questions addressed

2.2 Conducting

2.2.1 Gather Studies

Table 5. Database search results.

Database	Initial Records
IEEE Xplore	543
ScienceDirect	412
SpringerLink	389
IACR ePrint	276
Google Scholar	212
Total	**1,832**
After Duplicate Removal	1,247

2.2.2 Study Selection and Refinement

Table 6. Study selection summary.

Stage	Count
Initial records identified	1,832
After duplicate removal	1,247
After title/abstract screening	312
After full-text review	95
Final included studies	95

Table 7. **Distribution of included studies by category.**

Category	2021	2022	2023	2024	2025	Total
Side-Channel Attacks	8	6	7	5	4	30
Fault Injection	3	2	4	3	2	14
Machine Learning/AI	4	5	6	5	3	23
Quantum Threats	3	4	3	4	3	17
Key Management	2	3	2	2	2	11
Total	20	20	22	19	14	95

3. RESULTS AND SYNTHESIS

3.1 RQ1: Implementation Weaknesses

Quantitative Findings:

Twenty-three studies that addressed implementation vulnerabilities were analyzed, and the results showed:

i. Of the IoT devices surveyed, 23% had hard-coded keys (Shakor et al., 2024)
ii. Approximately 19% of embedded systems have entropy issues (Yoo et al., 2017)
iii. Approximately 15% of software implementations use the incorrect mode (Weiss et al., 2012)

Qualitative Synthesis:

The biggest practical problem in AES deployments is implementation flaws. Inadequate implementations can totally jeopardize security even when the basic algorithm is still secure. In embedded and Internet of Things deployments, hard-coded keys are common (Shakor et al., 2024). Another serious flaw in key generation is insufficient entropy; embedded devices frequently generate keys with effective entropy as low as 32 bits (Yoo et al., 2017). According to Sheikhpour, Ko, and Mahani (2021), compared to naive implementations, fault-resilient architectures increase area by 45% and power consumption by 38%, which puts financial pressure on designers to reduce security features.

Gaps Identified:

i. Lack of long-term side-channel data
ii. Underreported real-world key management mistakes
iii. There is little focus on combined attack vectors

3.2 RQ2: Side-Channel Attack Effectiveness

Quantitative Findings:

Analysis of 30 side-channel attack studies revealed:

i. Correlation Power Analysis (CPA) uses 2,000 traces to retrieve keys from unprotected implementations (Lo et al., 2016)
ii. Deep learning-based attacks retrieve keys from masked implementations using 50,000 traces (Kuroda et al., 2021)
iii. Multi-bit DDLA requires 40% fewer traces (Fukuda et al., 2025)
iv. Electromagnetic (EM) attacks have a 98% success rate with 15,000 traces at a distance of 10 cm (Negabi et al., 2023)

Qualitative Synthesis:

With the inclusion of deep learning, side-channel attacks have significantly changed. Convolutional Neural Networks (CNNs) can recover keys from masked AES implementations with 50,000 traces, whereas classical CPA requires over 500,000 traces, as demonstrated by Kuroda, Fukuda, Yoshida, and Fujino (2021). Because EM-based side channels only require close proximity rather than a physical device connection, they offer clear advantages to attackers (Wang, 2024).

Countermeasure Effectiveness:

Although it stops classical CPA, first-order masking is still susceptible to deep learning-based attacks. Although there is a significant performance overhead, higher-order masking (order ≥2) greatly increases attack complexity. Many cache-timing problems are eliminated by hardware-accelerated AES (Zhang et al., 2024).

3.3 RQ3: Quantum Computing Threats

Quantitative Findings:

Seventeen quantum threat studies were analyzed, and the results showed:

i. Grover's algorithm decreases AES-128 to 2^64 security (Grassl et al., 2016)
ii. Approximately 2,953 logical qubits and 1.26 × 10^8 T-gates are needed for a quantum attack (Grassl et al., 2016)
iii. 2^128 security is maintained by AES-256 against Grover
iv. AES and post-quantum Key Encapsulation Mechanisms (KEM) are combined in hybrid algorithms (Stebila & Mosca, 2017)

Qualitative Synthesis:

Grover's approach reduces effective key strength by half while offering a quadratic speedup for unstructured search (Grassl et al., 2016). However, without significant advancements, estimations of quantum resources indicate that AES-128 will be safe against quantum attacks for ten to twenty years (Baksi & Jang, 2024).

Hybrid Security Models:

For transitional security, hybrid cryptography blends post-quantum algorithms with traditional AES (Stebila & Mosca, 2017). If neither primitive is compromised, this approach guarantees security.

3.4 RQ4: Key Management Challenges

Quantitative Findings:

Eleven key management studies were analyzed, and the results showed:

i. The firmware of 23% of IoT devices stores keys in plaintext (Shakor et al., 2024)
ii. Automated key rotation is absent for 65% of cloud users surveyed
iii. 41% of IoT devices do not have a rotation mechanism, and 73% of them employ static keys (Vishwakarma & Singh, 2022)

Qualitative Synthesis:

The most important operational vulnerability is always key management. Embedded systems frequently produce keys with effective entropy as low as 32 bits, making entropy inadequacies a fundamental risk in key management (Yoo et al., 2017). Despite the risks associated with pre-shared keys, secure key distribution is still a fundamental concern (Vishwakarma & Singh, 2022).

3.5 RQ5: AI-Based Attack Detection

Quantitative Findings:

Twenty-three AI/ML experiments were analyzed, and the results showed:

i. With a false positive rate of 0.5%, CNN-based detection achieves 94% accuracy (Ghimire et al., 2024)

ii. Unsupervised learning detects 87% of compromise attempts (Sowmyadevi & Shanmugapriya, 2023)
iii. ML code analysis identifies 91% of vulnerable implementations (Grari et al., 2022)
iv. The accuracy of cross-platform transfer learning is only 62% (Dhanalakshmi, 2025)

Qualitative Synthesis:
Promising tools for identifying AES abuse and attacks are AI and machine learning. CNN-based systems with 94% detection accuracy for power analysis attacks were created by Ghimire, Baligoudugula, and Amsaad (2024). However, due to hardware variations, models trained on one device frequently fail on others, making cross-platform generalization tricky (Dhanalakshmi, 2025).

4. DISCUSSION AND SYNTHESIS

4.1 Summary of Evidence

Table 8. **Summary of findings by research question.**

RQ	Key Findings	Practical Implications
RQ1	Implementation flaws dominate; hard-coded keys (23%), entropy deficiencies (19%)	Prioritize secure implementation; use hardware-based key storage
RQ2	Deep learning-based attacks break masked AES with 50,000 traces	Adopt hardware-accelerated AES; implement higher-order masking
RQ3	AES-128 reduces to 2^64 security under Grover	Migrate to AES-256; implement hybrid post-quantum key exchange
RQ4	65% lack automated rotation; 41% lack any rotation	Implement hardware-based key storage; automate rotation
RQ5	AI detection achieves 94% accuracy; generalization limited (62%)	Deploy ML detection; use diverse training datasets

4.2 Five Key Themes

Theme 1: Implementation Flaws Dominate Real-World Security Failures

More often than not, AES is compromised by hard-coded keys, entropy flaws, and incorrect mode utilization (Shakor et al., 2024; Yoo et al., 2017; Weiss et al., 2012).

Theme 2: Side-Channel Attacks Continue to Evolve

Side-channel analysis has been revolutionized by deep learning, allowing attacks that get around first-order masking with realistic trace requirements (Kuroda et al., 2021; Fukuda et al., 2025).

Theme 3: Proactive but Measured Reactions Are Needed for Quantum Threats

For the foreseeable future, AES-256 offers sufficient defense against Grover's algorithm, while hybrid systems provide temporary security (Grassl et al., 2016; Stebila & Mosca, 2017).

Theme 4: The Crucial Operational Vulnerability Is Still Key Management

Attacks that get around AES's cryptographic strength are made possible by lifecycle management flaws (Shakor et al., 2024; Vishwakarma & Singh, 2022).

Theme 5: AI Provides Dual-Use Features

There is an arms race as ML approaches improve detection systems and side-channel attacks (Ghimire et al., 2024; Dhanalakshmi, 2025).

4.3 Research Gaps

i. **Long-Term Side-Channel Data:** The majority of research employs brief acquisition windows
ii. **Multi-Device Generalization:** Research is needed to determine whether models can be transferred between platforms
iii. **Combined Attack Vectors:** Research on hybrid attacks is scarce
iv. **Real-World Key Management Failures:** Extensive information is required
v. **Post-Quantum Integration:** Research is needed on migration tactics and performance effects

5. CONCLUSIONS

The five crucial elements of AES security concerns were evaluated in this systematic literature review. The analysis shows that although AES retains strong mathematical security, implementation quality, side-channel resilience, quantum readiness, and key management techniques are crucial for real-world security.

Key Conclusions:

i. **Implementation vulnerabilities** represent the biggest real threat. Although hardware-based key protection might reduce these dangers, it comes with expenses that organizations frequently avoid (Sheikhpour et al., 2021).
ii. **Side-channel attacks** have significantly changed with the incorporation of deep learning. With 50,000 traces or less, modern attacks retrieve keys from masked implementations (Kuroda et al., 2021; Negabi et al., 2023).
iii. **Quantum computing** presents asymmetric risks. Grover's approach reduces AES-128 to 64-bit security, which encourages switching to AES-256 (Grassl et al., 2016).
iv. **Key management** is the most significant operational vulnerability. IoT and cloud environments are especially susceptible to management errors (Shakor et al., 2024; Vishwakarma & Singh, 2022).
v. **AI-based detection** has tremendous potential; ML systems can identify side-channel threats with over 90% accuracy (Ghimire et al., 2024).

Recommendations:

Immediate Action:

i. Switch to AES-256 for all new deployments
ii. Implement hardware-based key storage
iii. Perform side-channel vulnerability assessments
iv. Set up automatic key rotation with a maximum interval of one year

Medium-Term Planning (2-5 years):

i. Develop crypto-agility to replace algorithms
ii. Create a hybrid post-quantum integration plan
iii. Use higher-order masking with AES software

Long-Term Strategy (5+ years):

i. Prepare for the post-quantum transition
ii. Develop side-channel resilience through hardware-software co-design
iii. Conduct ongoing cryptographic monitoring

Future Research Directions:

i. Post-quantum AES transition optimization
ii. Hardware-software co-design for side-channel resistance
iii. AI for cryptographic security with transfer learning
iv. Scalable key management for IoT
v. Combined attack vector countermeasures

Declaration of Competing Interest

The authors declare that they have no known competing financial interests or personal relationships that could have appeared to influence the work reported in this paper.

Data Availability

Data extracted from the 95 included studies is available from the corresponding author upon reasonable request.

Acknowledgments

The authors would like to thank the Department of Cyber Security, Federal University of Technology, Minna, Niger State, Nigeria, for providing access to research databases and resources used in this study.

REFERENCES

Baksi, A., & Jang, K. (2024). Quantum analysis of AES, implementation and analysis of ciphers in quantum computing. In Applications and Techniques in Information Security: 14th International Conference.

Bogdanov, A., Khovratovich, D., & Rechberger, C. (2011). Biclique cryptanalysis of the full AES. In Advances in Cryptology - ASIACRYPT 2011 (pp. 344-371).

Daemen, J., & Rijmen, V. (1998). The block cipher Rijndael. Lecture Notes in Computer Science, 1820, 277-284.

Dhanalakshmi, N. (2025). Unmasking encryption effects and modified deep learning approaches for attack classification in WSN. Expert Systems with Applications, 266, 126163.

Dheeba, J., Oberoi, V., Raja Singh, R., & Gautam Karthik, V. (2025). Securing electrical drive systems against man-in-the-middle attacks using S-box optimized AES encryption. IEEE Access, 13, 114713-114732.

Fukuda, Y., Yoshida, K., & Fujino, T. (2025). Multi-bit DDLA: Non-profiled deep learning side-channel attacks using multi-bit label against hardware-implemented AES. IEICE Transactions on Fundamentals of Electronics, Communications and Computer Sciences, E108A(3), 215-226.

Ghimire, A., Baligoudugula, V. V., & Amsaad, F. (2024). Power analysis side-channel attacks on same and cross-device settings: A survey of machine learning techniques. In Internet of Things (Vol. 684, pp. 24-38).

Grari, H., Zine-Dine, K., Azouaoui, A., & Lamzabi, S. (2022). Deep learning-based cryptanalysis of a simplified AES cipher. International Journal of Information Security and Privacy, 16, 1-16.

Grassl, M., Langenberg, B., Roetteler, M., & Steinwandt, R. (2016). Applying Grover's algorithm to AES: Quantum resource estimates. In Post-Quantum Cryptography - PQCrypto 2016 (pp. 29-43).

Kitchenham, B., & Charters, S. (2007). Guidelines for performing systematic literature reviews in software engineering. EBSE Technical Report, EBSE-2007-01.

Kitchenham, B., Brereton, O. P., Budgen, D., Turner, M., Bailey, J., & Linkman, S. (2009). Systematic literature reviews in software engineering - A systematic literature review. Information and Software Technology, 51(1), 7-15.

Kuroda, K., Fukuda, Y., Yoshida, K., & Fujino, T. (2021). Practical aspects on non-profiled deep-learning side-channel attacks against AES software implementation with two types of masking countermeasures including RSM. In Proceedings of the 5th Workshop on Attacks and Solutions in Hardware Security (pp. 29-40).

Lo, O., Buchanan, W., & Carson, D. (2016). Power analysis attacks on the AES-128 S-box using differential power analysis (DPA) and correlation power analysis (CPA). Journal of Cyber Security Technology, 1, 1-20.

Negabi, I., Ait El Asri, S., El Adib, S., & Raissouni, N. (2023). Deep learning-based power analysis attack for extracting AES keys on ATmega328P microcontroller. Arabian Journal for Science and Engineering, 49(3), 4197-4208.

NIST. (2023). Advanced Encryption Standard (AES). FIPS-197.

Pati, D., & Lorusso, L. N. (2018). How to write a systematic review of the literature. HERD: Health Environments Research & Design Journal, 11(1), 15-30.

Petersen, K., Vakkalanka, S., & Kuzniarz, L. (2015). Guidelines for conducting systematic mapping studies in software engineering: An update. Information and Software Technology, 64, 1-18.

Shakor, M. Y., Khaleel, M. I., Safran, M., Alfarhood, S., & Zhu, M. (2024). Dynamic AES encryption and blockchain key management: A novel solution for cloud data security. IEEE Access, 12, 26334-26343.

Sheikhpour, S., Ko, S.-B., & Mahani, A. (2021). A low cost fault-attack resilient AES for IoT applications. Microelectronics Reliability, 123, 114202.

Sowmyadevi, D., & Shanmugapriya, I. (2023). Unsupervised machine learning based key management in wireless sensor networks. Measurement: Sensors, 28, 100847.

Stebila, D., & Mosca, M. (2017). Post-quantum key exchange for the internet and the open quantum safe project. In Selected Areas in Cryptography - SAC 2016 (pp. 14-37).

Vishwakarma, A., & Singh, B. (2022). Implementation study of AES standard for IoT systems. In IEEE Global Conference on Computing, Power and Communication Technologies.

Wang, H. (2024). Amplitude-modulated EM side-channel attack on provably secure masked AES. Journal of Cryptographic Engineering, 14(3), 537-549.

Weiss, M., Heinz, B., & Stumpf, F. (2012). A cache timing attack on AES in virtualization environments. In Financial Cryptography and Data Security - FC 2012(pp. 314-328).

Yoo, T., Kang, J.-S., & Yeom, Y. (2017). Recoverable random numbers in an internet of things operating system. Entropy, 19(3), 113.

Zhang, Z., Petkova-Nikova, S., & Nikov, V. (2024). Glitch-stopping circuits: Hardware secure masking without registers. In Proceedings of the 2024 ACM SIGSAC Conference on Computer and Communications Security