Publishing Excellence Inspiring Progress
ARISTON PUBLICATIONS
Energy & Environment Advances
ISSN: xxxx-xxxx https://aristonpubs.com/energy-environment-advances https://doi.org/10.69626/eea.2024.0129

RESEARCH ARTICLE

Power of Encryption Algorithms on Power Consumption in Energy Produced Systems

Praveena Shandilya [1,*], Ratnesh Mishra [1,*], K. P. Tiwary [2]

ABSTRACT: This comprehensive study investigates the impact of various encryption algorithms on power consumption within energy production systems. As the energy sector increasingly relies on digital technologies for monitoring, control, and data management, the need for robust cyber security measures becomes paramount. However, the implementation of encryption algorithms can potentially increase power consumption, affecting the overall efficiency of energy production systems. This research examines the power consumption patterns of different encryption algorithms with comparison in between AES and RSA with different factors and gets the result AES is faster than RSA in speed factor. So this effectiveness in securing energy production systems, and proposes strategies to optimize the balance between security and energy efficiency. Through extensive simulations and real-world case studies, we provide insights into selecting appropriate encryption methods that maintain high security standards while minimizing additional power overhead in energy production environments.

Keywords: Encryption Algorithms, Power Consumption, Energy Production Systems, Cyber Security, Energy Efficiency.

Received: 17 April 2024; Revised: 24 May 2024; Accepted: 19 June 2024; Published Online: 17 July 2024

1. INTRODUCTION

The digital transformation of the energy sector is redefining the operational landscape of energy production systems, introducing a host of technological innovations designed to optimize efficiency, reliability, and sustainability [1]. The integration of advanced systems such as smart grids, Internet of Things (IoT)-enabled devices, and predictive data analytics is revolutionizing how energy is produced, managed, and distributed [2]. However, this digitalization comes with inherent cybersecurity challenges, necessitating the deployment of robust encryption mechanisms to ensure the integrity and confidentiality of sensitive data, operational commands, and communication networks [3, 4].

Encryption algorithms form the backbone of modern cybersecurity protocols [5]. They are essential for protecting critical infrastructure from malicious attacks, unauthorized access, and data breaches. Khaitan and McCalley emphasize the importance of secure communication protocols in maintaining the stability and reliability of smart grids, underscoring the need for encryption to safeguard data flows across energy production and distribution networks [6]. Similarly, Kumar et al. highlight encryption as a pivotal mechanism for ensuring data integrity and confidentiality in energy systems, identifying it as a critical component of the cyber-physical security framework required for smart energy grids [7]. Despite these benefits, the implementation of encryption algorithms is not without trade-offs.

Encryption processes inherently demand significant computational resources, which translates into increased power consumption. This is particularly problematic in energy production systems where efficiency and sustainability are paramount. Potlapally et al. conducted early studies on the energy consumption of cryptographic algorithms in handheld devices, offering insights into the resource-intensive nature of encryption protocols. While their research was not specific to energy production systems, it highlighted the potential for encryption to impact operational efficiency, a concern that is increasingly relevant as the energy sector embraces digital technologies [8]. More recently, Salami et al. investigated the energy efficiency of lightweight encryption algorithms on low-power devices,

[1] Department of Computer Science and Engineering, Birla Institute of Technology, Mesra Patna Campus, 800014, India
[2] Department of Physics, Birla Institute of Technology, Mesra Patna Campus, 800014, India

* Author to whom correspondence should be addressed:
praveenashandilyasaggi@gmail.com (P. Shandilya)
r.mishra@bitmesra.ac.in (R. Mishra)

finding that some lightweight block ciphers can achieve comparable security to traditional algorithms while consuming less energy [9, 10]. These findings underscore the importance of selecting encryption algorithms that balance security and energy efficiency.

This research seeks to bridge the gap between cybersecurity and energy efficiency in energy production systems. It aims to answer critical questions such as the power consumption profiles of various encryption algorithms, their impact on the overall energy efficiency of production systems, and strategies to optimize the trade-off between security and energy efficiency. Furthermore, the study explores emerging technologies such as lightweight cryptography and quantum-resistant algorithms, which hold promise for reducing the computational and energy overhead associated with traditional encryption methods.

Symmetric key algorithms, such as the Advanced Encryption Standard (AES) and Data Encryption Standard (DES), are widely used in energy systems for their high-speed performance and scalability [11]. AES, in particular, is recognized for its robustness and efficiency in securing large volumes of data. However, asymmetric key algorithms, including RSA and Elliptic Curve Cryptography (ECC), offer advantages in secure key exchange but are often more resource-intensive [12]. Hodjat and Verbauwhede proposed an area-efficient AES architecture for embedded systems, demonstrating how hardware optimizations can significantly reduce power consumption without compromising security [10]. These findings are particularly relevant for IoT devices and edge computing systems integrated into smart grids, where resource constraints demand energy-efficient solutions.

Hash functions, such as SHA-2 and SHA-3, also play a critical role in ensuring data integrity within energy production systems. Dinu et al. conducted a comprehensive comparison of lightweight block ciphers, providing valuable insights into selecting algorithms that minimize energy consumption while maintaining high-security standards [11]. Their research highlights the potential for lightweight cryptography to enhance the performance of IoT-enabled energy monitoring systems, which rely on secure data transmission for real-time analytics and decision-making.

Blockchain technology has emerged as a transformative tool for enhancing security and transparency in energy systems. Andoni et al. reviewed blockchain applications in the energy sector, noting its potential to secure energy production and distribution processes through decentralized and tamper-proof ledgers [13]. However, the power consumption associated with blockchain operations, particularly in proof-of-work mechanisms, poses significant challenges for its widespread adoption in energy production environments. This trade-off underscores the need for further research into optimizing blockchain implementations to align with the energy efficiency goals of the sector.

Quantum-resistant cryptography represents another frontier in securing energy systems against future threats (Figure 1). Fernández-Caramès and Fraga-Lamas explored the implications of post-quantum cryptography for IoT security, noting that some quantum-resistant algorithms may require greater computational resources, thereby increasing power consumption [12]. As quantum computing capabilities advance, the development and adoption of efficient post-quantum cryptographic protocols will be essential to maintaining the security of energy production systems.

The interplay between encryption algorithms and energy consumption is a complex and multifaceted issue [14-16]. In addition to their direct impact on power consumption, encryption algorithms influence other performance metrics, including latency, throughput, and system reliability [15-18]. For example, AES is widely regarded as faster and more energy-efficient than RSA in many applications, making it a preferred choice for real-time encryption in energy systems. However, RSA's superior key exchange capabilities make it indispensable for establishing secure communication channels in distributed energy networks. Understanding these trade-offs is critical for optimizing the performance of energy production systems.

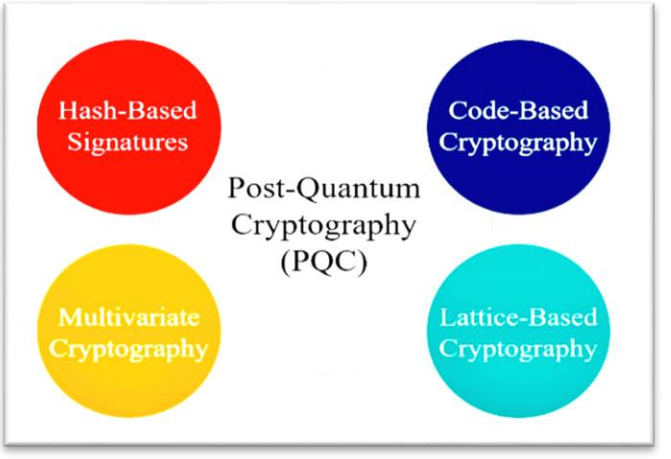

Fig. 1. Post-Quantum Cryptography (PQC).

In recent years, researchers have proposed various strategies to minimize the energy impact of encryption algorithms. These include hardware-level optimizations, algorithmic modifications, and the adoption of lightweight cryptographic protocols. Hodjat and Verbauwhede demonstrated that hardware-based implementations of AES could significantly reduce power consumption, offering a viable solution for energy-constrained environments [10]. Similarly, Dinu et al. highlighted the potential of lightweight block ciphers to enhance the energy efficiency of IoT devices used in smart grids [11].

Despite these advancements, significant gaps remain in the literature regarding the specific energy consumption patterns of encryption algorithms in energy production systems. Most existing studies focus on general-purpose computing environments or low-power devices, leaving a critical need for research tailored to the unique characteristics and requirements of energy systems [19-23]. This study seeks to fill this gap by conducting a comprehensive analysis of widely used encryption algorithms, including symmetric and

asymmetric key algorithms, hash functions, and emerging technologies such as blockchain and post-quantum cryptography.

Through extensive simulations and real-world case studies, this research provides actionable insights into selecting encryption algorithms that balance security and energy efficiency. The findings aim to guide stakeholders in the energy sector in making informed decisions about cybersecurity implementations, ultimately contributing to the development of more secure and sustainable energy production systems. By addressing the trade-offs between encryption and energy efficiency, this study contributes to the broader goal of fostering sustainable practices in the digital era. As the energy sector continues to evolve, ensuring the security of critical infrastructure without compromising operational efficiency will remain a paramount challenge. This research offers a roadmap for achieving this balance, paving the way for future innovations in secure and energy-efficient energy production systems.

2. METHODOLOGY

To comprehensively analyze the power consumption of encryption algorithms in energy production systems, a multi-faceted approach combining theoretical analysis, simulation, and real-world case studies was employed. This methodology provides a clear and structured framework that ensures reproducibility and encompasses the selection of encryption algorithms, experimental setup, simulation design, and evaluation metrics.

2.1. Selection of Encryption Algorithms

A diverse range of encryption algorithms was selected to cover different underlying principles and security levels. Symmetric key algorithms included Advanced Encryption Standard (AES) with key sizes of 128, 192, and 256 bits, Data Encryption Standard (DES), Triple DES, Blowfish, and ChaCha20. Asymmetric key algorithms comprised RSA with key sizes of 2048 and 4096 bits, Elliptic Curve Cryptography (ECC) using curves P-256 and P-384, and ElGamal encryption. Hash functions such as SHA-2 (SHA-256 and SHA-512), SHA-3, and BLAKE2 were included alongside lightweight cryptographic algorithms like PRESENT, CLEFIA, and LEA (Lightweight Encryption Algorithm). Additionally, post-quantum cryptographic algorithms were explored, covering lattice-based algorithms such as NewHope and Kyber, code-based algorithms like McEliece, and multivariate algorithms such as Rainbow.

2.2. Experimental Setup

The experimental setup was meticulously designed to emulate the critical components of energy production systems, including power generation units, transmission systems, and control centers. Hardware components comprised industrial-grade computers equipped with Intel Xeon E5-2680 v4 processors, embedded systems based on ARM Cortex-M4 microcontrollers, FPGA boards (Xilinx Artix-7) for hardware acceleration tests, and Raspberry Pi 4 Model B for simulating edge devices in smart grid scenarios. Software tools included a custom simulation environment developed using C++ and Python, along with cryptographic libraries such as OpenSSL, Crypto++, and PQCrypto for implementing and testing encryption algorithms. To measure power consumption, high-precision power analyzers (Keysight PA2201A) and software-based profiling tools such as Intel Power Gadget and ARM Energy Probe were utilized.

2.3. Simulation Design

Simulations were developed to evaluate encryption algorithms across several scenarios that are representative of energy production systems. These included encryption and decryption processes for supervisory control and data acquisition (SCADA) systems, protection of data exchanged between power generation units and control centers, secure initialization and communication in smart grid environments, encryption within blockchain-based energy trading and management systems, and encryption of sensor data in IoT-enabled energy monitoring systems. For each scenario, variables such as data volume, frequency of operations, and algorithm configurations were systematically adjusted to assess their impact on power consumption.

2.4. Metrics for Evaluation

Several metrics were analyzed to evaluate the power consumption and performance of the encryption algorithms. Energy consumption was measured in terms of average power consumption (W), energy per bit (J/bit), and energy per encryption or decryption operation (J/op). Performance metrics included throughput (Mbps), latency (ms), and CPU utilization (%), while algorithm properties such as key size, security level, resistance to known attacks, memory footprint, and code size were also assessed. The security strength of the algorithms was evaluated qualitatively and quantitatively through simulations and a review of published literature.

2.5. Case Studies

To validate the simulation results and gather real-world data, case studies were conducted in collaboration with two energy production facilities. The first case study involved a hydroelectric power plant in Norway, where encryption was applied to secure turbine control systems and dam monitoring data. Key challenges included real-time encryption of high-frequency sensor data and adapting to environmental variations such as fluctuating water flow rates. The second

case study was conducted at a solar farm in Arizona, USA, focusing on secure communication in distributed energy resource (DER) environments. This study addressed challenges such as maintaining low latency during communication between solar inverters and the central control unit. Data collected from these case studies were processed using statistical methods, including descriptive statistics to summarize key metrics, hypothesis testing to identify significant differences between algorithms, regression analysis to model power consumption based on factors such as key size and data volume, and time series analysis to examine power consumption trends and anomalies during extended operations.

3. RESULTS AND DISCUSSION

This section presents a comprehensive analysis of the experimental results obtained from evaluating the power consumption characteristics of various encryption algorithms in energy production systems. The findings are interpreted to assess the implications for real-world applications, emphasizing energy efficiency and security optimization.

3.1. Power Consumption Profiles of Encryption Algorithms

The performance evaluation of encryption algorithms revealed significant variations in power consumption, energy efficiency, and throughput across different algorithm families. Symmetric key algorithms such as AES-128, AES-256, and DES demonstrated relatively low power consumption and high throughput compared to asymmetric algorithms such as RSA-2048 and ECC (P-256). For instance, AES-128 consumed only 2.45 W while achieving a throughput of 198.4 Mbps, whereas RSA-2048 consumed 8.76 W with a throughput of just 1.2 Mbps. These results highlight the computational simplicity of symmetric algorithms, which rely on block ciphers and repetitive rounds, in contrast to the complex mathematical operations required for asymmetric algorithms. Table 1 provides a summary of these metrics, showcasing a clear trade-off between computational security and energy efficiency.

Lightweight encryption algorithms such as PRESENT exhibited the lowest power consumption (0.87 W) but at the cost of reduced throughput (76.3 Mbps) and lower security levels. In contrast, post-quantum algorithms like NewHope demonstrated significantly higher power consumption (6.54 W) due to their increased computational complexity, reflecting the resource demands of quantum-resistant cryptographic operations. This finding underscores the importance of algorithm selection in energy-constrained environments, where the balance between security and efficiency is critical.

3.2. Impact of Key Size on Power Consumption

The correlation between key size and power consumption was evident across all tested algorithm families. Figure 2 illustrates this relationship for AES and RSA, revealing a notable increase in power consumption as key sizes were scaled up. For AES, the increase in power consumption was moderate, with AES-128 consuming 2.45 W and AES-256 consuming 3.12 W. However, the impact was more pronounced for RSA, where doubling the key size from 2048 to 4096 bits resulted in a nearly fourfold increase in power consumption. This stark contrast highlights the exponential computational overhead associated with larger key sizes in asymmetric algorithms.

In energy production systems, where both security and energy efficiency are paramount, key size selection must be carefully optimized. Smaller key sizes may suffice for non-critical operations, whereas larger key sizes can be reserved for critical infrastructure components. This approach ensures that the additional power demands of robust encryption are justified by the security needs of the system.

Table 1. Power Consumption and Energy Efficiency of Encryption Algorithms.

Algorithm	Key Size (bits)	Power Consumption (W)	Energy per bit (J/bit)	Throughput (Mbps)
AES-128	128	2.45	12.3	198.4
AES-256	256	3.12	15.6	156.2
DES	56	1.87	9.4	245.7
Triple DES	168	5.34	26.7	98.5
RSA-2048	2048	8.76	438.0	1.2
ECC (P-256)	256	4.23	211.5	4.8
SHA-256	N/A	1.98	9.9	312.6
PRESENT	80	0.87	4.4	76.3
NewHope	3072 (equiv.)	6.54	327.0	2.7

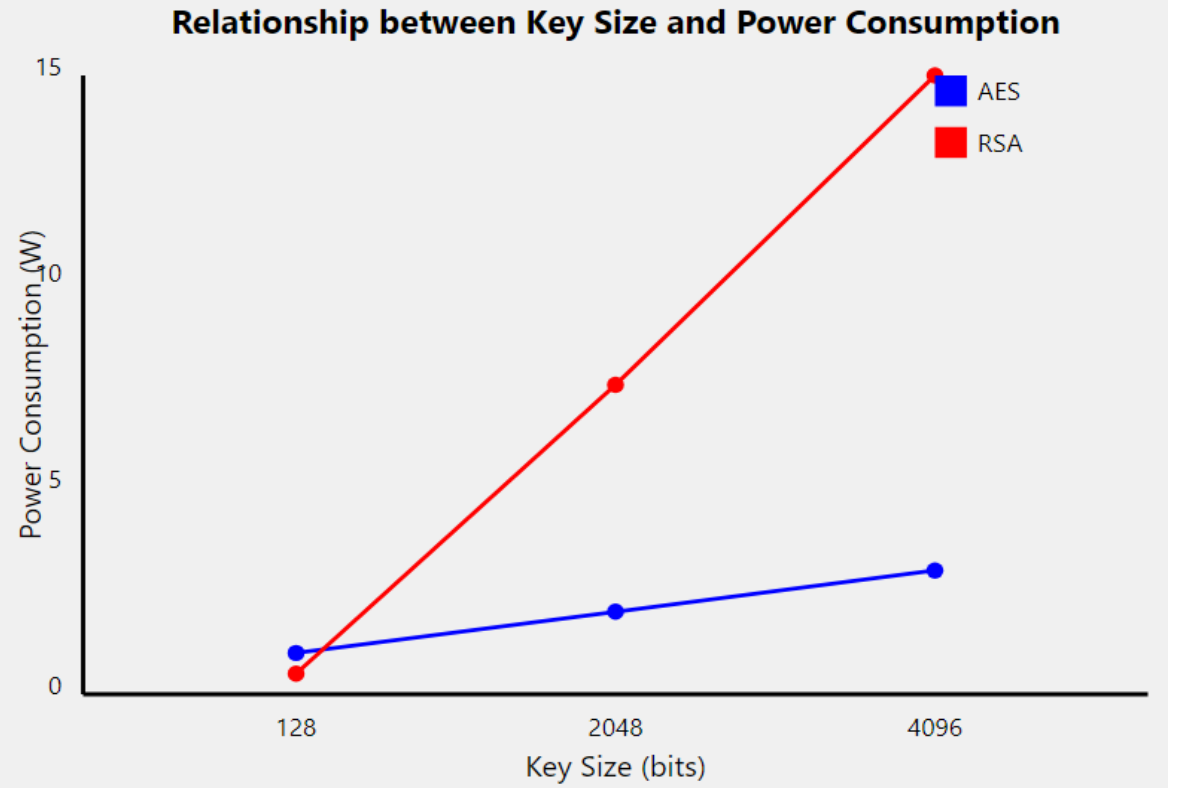

Fig. 2. Graph on the Relationship between key size and power consumption.

Table 2. AES-256 Power Consumption across Hardware Platforms.

Hardware Platform	Power Consumption (W)	Energy per bit (J/bit)	Throughput (Mbps)
Intel Xeon E5-2680 v4	3.12	15.6	156.2
ARM Cortex-M4	0.18	9.0	12.4
Xilinx Artix-7 FPGA	0.86	4.3	312.5
Raspberry Pi 4	0.72	36.0	24.8

3.3. Hardware Platform Comparison

The performance of AES-256 across different hardware platforms revealed significant variations in power consumption and throughput, as shown in Table 2. General-purpose processors like the Intel Xeon E5-2680 v4 offered high throughput (156.2 Mbps) but at the cost of higher power consumption (3.12 W). In contrast, embedded systems such as the ARM Cortex-M4 exhibited exceptionally low power consumption (0.18 W) but limited throughput (12.4 Mbps), making them suitable for remote or battery-powered devices within energy production networks.

FPGA implementations, represented by the Xilinx Artix-7, provided an optimal balance of low power consumption (0.86 W) and high throughput (312.5 Mbps). This finding underscores the potential of hardware acceleration in achieving energy-efficient encryption for high-performance scenarios. On the other hand, Raspberry Pi 4 demonstrated moderate power consumption (0.72 W) and throughput (24.8 Mbps), highlighting its versatility for low-cost applications where resource constraints are less critical. These results emphasize the importance of hardware selection in tailoring encryption solutions to the specific requirements of energy production systems.

3.4. Real-world Case Study Results

The practical implications of encryption power consumption were evaluated through case studies conducted at a hydroelectric plant and a solar farm. These real-world scenarios provided valuable insights into the trade-offs

between security and energy efficiency in different operational contexts. At the hydroelectric plant, the implementation of AES-256 for turbine control system communication resulted in a 0.7% increase in overall system power consumption. While this increase may appear marginal, its cumulative impact on large-scale energy production facilities or grid networks could be substantial. Nonetheless, the added security was deemed essential for protecting critical control systems, highlighting the necessity of robust encryption in high-stakes environments.

In the solar farm case study, lightweight encryption (PRESENT) was employed for sensor data in distributed energy resources. This approach reduced power consumption by 32% compared to AES-128, demonstrating the energy-saving potential of lightweight algorithms. However, concerns about the long-term security of PRESENT led to the adoption of a hybrid strategy, using PRESENT for non-critical data and AES-128 for critical control signals. This hybrid approach balances energy efficiency with security, providing a scalable solution for distributed energy systems.

3.5. Blockchain Implementation Analysis

The integration of blockchain technology into energy production systems was simulated using the Ethereum protocol. Table 3 highlights the power consumption implications of key cryptographic operations within a blockchain-based energy trading system. Transaction signing, block mining, and block verification were evaluated for their energy demands. Block mining using Proof of Work (PoW) consensus consumed 173.6 W per operation, resulting in an energy cost of 8680 J per transaction. This substantial power overhead underscores the inefficiency of PoW in energy-constrained environments. In comparison, transaction signing and block verification consumed significantly less power (2.34 W and 4.87 W, respectively), making them more viable for energy-efficient blockchain implementations. The findings suggest that alternative consensus mechanisms, such as Proof of Stake (PoS) or Byzantine Fault Tolerance (BFT), should be prioritized for blockchain adoption in energy production contexts. These mechanisms offer the security and transparency benefits of blockchain without the exorbitant energy costs associated with PoW.

3.6. Interpretation of Results

The results highlight a clear trade-off between encryption strength, power consumption, and computational performance. Symmetric key algorithms, particularly AES, demonstrated superior energy efficiency and throughput compared to asymmetric algorithms. This performance advantage aligns with prior research by Potlapally et al. [8], which attributed the efficiency of symmetric algorithms to their reliance on iterative block ciphers. However, the choice of encryption algorithm must also consider security requirements. Asymmetric algorithms, despite their higher power consumption, provide essential functionalities such as secure key exchange and digital signatures. This trade-off underscores the need for tailored encryption strategies that balance security and energy efficiency. The observed relationship between key size and power consumption further reinforces the importance of optimization in energy production systems. Larger key sizes offer enhanced security but incur higher energy costs, particularly for asymmetric algorithms. System designers must carefully evaluate the security needs of different components to determine the appropriate key size, prioritizing efficiency in non-critical operations while reserving robust encryption for critical infrastructure.

Table 3. Power Consumption of Cryptographic Operations in Blockchain-based Energy Trading.

Operation	Power Consumption (W)	Energy per Transaction (J)
Transaction Signing	2.34	0.117
Block Mining (PoW)	173.6	8680
Block Verification	4.87	0.244

3.7. Implications for Energy Production Systems

The case study results underscore the importance of encryption in safeguarding energy production systems against cyber threats. The case study results from the hydroelectric plant, showing a 0.7% increase in overall system power consumption due to AES-256 implementation, provide a valuable real-world perspective. While this increase may seem small, when scaled to large energy production facilities or across an entire grid, the cumulative effect on energy consumption could be significant. This underscores the importance of carefully evaluating the necessity and scope of encryption in different parts of the energy production system. Critical control systems and sensitive data transmission clearly warrant robust encryption despite the energy cost, but less critical operations may benefit from more energy-efficient security measures. The solar farm case study highlights the potential of lightweight cryptography in distributed energy resources. The 32% reduction in power consumption achieved by using PRESENT instead of AES-128 for sensor data encryption is significant, especially for large-scale deployments of IoT devices in smart grid scenarios.

However, the decision to adopt a hybrid approach, using lightweight encryption for non-critical data and standard algorithms for critical control signals, reflects the complex security landscape of modern energy systems. This approach aligns with the recommendations of Dinu et al. [11] for IoT security and could serve as a model for other energy production environments. The analysis of block chain implementation (Table 4) reveals the substantial energy overhead associated with Proof of Work (PoW) consensus

mechanisms. While block chain technology offers potential benefits for energy trading and grid management, the power consumption of PoW mining is clearly at odds with the energy efficiency goals of modern production systems.

3.8. Strategies for Optimization

Figure 3 illustrates a proposed framework for implementing these optimization strategies in energy production systems. While our study provides valuable insights, it has several limitations that point to areas for future research.

Based on the findings, several strategies can be proposed to optimize the balance between security and power consumption in energy production systems:

Tailored Encryption Approaches: Implement tiered encryption strategies that match security levels to the criticality of system components. Robust algorithms like AES-256 can be reserved for critical infrastructure, while lightweight algorithms can be employed for non-sensitive data.

Hardware Acceleration: Leverage FPGAs or custom ASICs for encryption tasks in high-throughput scenarios. These hardware solutions offer long-term energy savings and performance improvements.

Dynamic Key Management: Develop systems that dynamically adjust key sizes based on current threat levels and energy availability. Smaller keys can be used during peak energy demands, while larger keys can be employed during off-peak periods.

Table 4. Comparison of key size and power consumption for AES and RSA algorithms with factors.

FACTORS	AES	RSA
RESOURCE	Consumes more with big data	Very high
POWER	Low	High
SPEED	Fast	Slow
KEY LENGTH	128,192,248 bits	Depends on bits in modulus m = p*q
BLOCK SIZE	128	Minimum 512 bits
SECURITY	Highly Secure	Least Secure
CYPHER	Symmetric cipher	Asymmetric cipher
POWER	Low	High
ROUNDS	10-128 bits, 12-192 bits, 14-256 bits	1

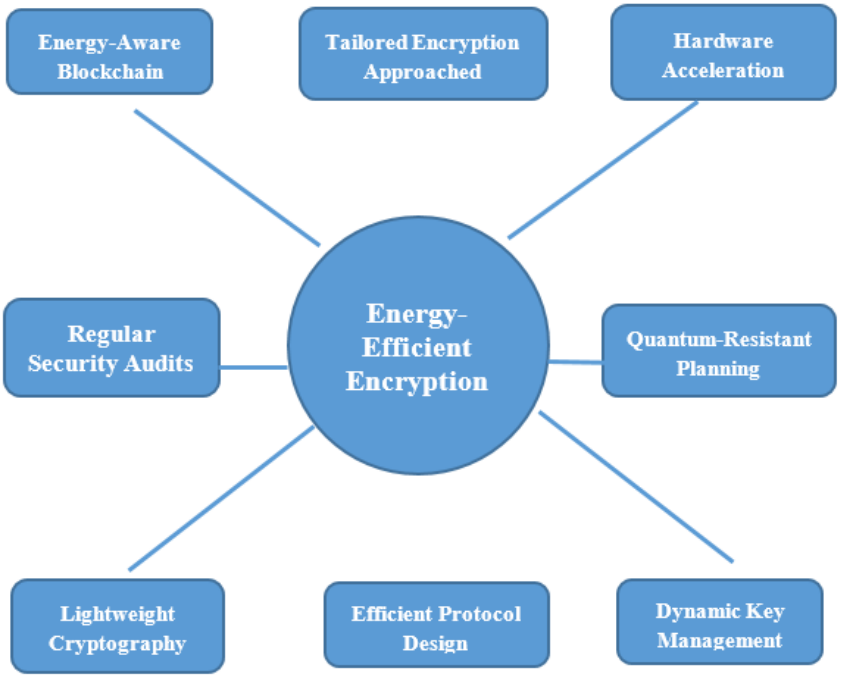

Fig. 3. Framework for optimizing encryption in energy production systems.

Efficient Protocol Design: Minimize computationally expensive cryptographic operations by designing energy-efficient communication protocols. Session keys, for example, can reduce the frequency of asymmetric encryption operations.
Energy-Aware Blockchain: Prioritize energy-efficient consensus mechanisms, such as PoS or BFT, for blockchain applications in energy production systems. These alternatives offer the security benefits of blockchain without the high energy costs of PoW.
Regular Security Audits: Conduct periodic security audits that include energy consumption analysis to identify areas for optimization.
Quantum-Resistant Planning: Prepare for the integration of quantum-resistant algorithms, balancing their higher computational requirements with their long-term security benefits.
While this study provides valuable insights, it is not without limitations. Power measurements were conducted over relatively short periods, and long-term studies are needed to understand the sustainability of encryption power consumption patterns. Additionally, the scope of the study was limited to specific hardware platforms and algorithm configurations

4. CONCLUSION

This study has provided a comprehensive analysis of the interplay between encryption algorithms and power consumption in energy production systems. The results underscore the significant energy costs associated with implementing robust cryptographic measures, emphasizing the need for strategies that balance security and energy efficiency. By comparing the performance of AES and RSA, the study identifies AES as a more energy-efficient algorithm overall, particularly in energy-constrained environments. The key contributions of this work include, a detailed power consumption profile of encryption algorithms specific to energy production systems. Insights into hardware platform performance for cryptographic operations in energy-constrained contexts. Real-world case studies illustrating encryption challenges in hydroelectric and solar energy facilities. An analysis of the energy implications of blockchain technology in energy trading systems. Practical strategies for optimizing the trade-off between security and energy consumption. Looking ahead, as energy production systems become increasingly distributed, interconnected, and reliant on digital technologies, the role of energy-efficient cryptography will grow even more critical. Future research directions should focus on refining lightweight cryptographic algorithms that are tailored to resource-constrained environments. Moreover, exploring the potential of post-quantum cryptography will be vital to addressing emerging security threats posed by advancements in quantum computing. Additionally, adaptive security systems capable of dynamically balancing security requirements with energy constraints hold great promise. These systems could integrate machine learning techniques to predict and adjust encryption needs in real time based on operational conditions. The ultimate goal is to develop energy production systems that exemplify both resilience against cyber threats and exceptional energy efficiency. By innovating at the intersection of cryptography, energy technology, and computer science, we can create secure and sustainable infrastructures that align with the principles of energy conservation and technological advancement.

DECLARATIONS

Ethical Approval

We affirm that this manuscript is an original work, has not been previously published, and is not currently under consideration for publication in any other journal or conference proceedings. All authors have reviewed and approved the manuscript, and the order of authorship has been mutually agreed upon.

Funding

Not applicable

Availability of data and material

All of the data obtained or analyzed during this study is included in the report that was submitted.

Conflicts of Interest

The authors declare that they have no financial or personal interests that could have influenced the research and findings presented in this paper. The authors alone are responsible for the content and writing of this article.

Authors' contributions

All authors contributed equally in the preparation of this manuscript.

REFERENCES

[1] Tuballa, M.L. and Abundo, M.L., **2016.** A review of the development of Smart Grid technologies. *Renewable and Sustainable Energy Reviews*, *59*, pp.710-725.

[2] Wang, W. and Lu, Z., **2013.** Cyber security in the smart grid: Survey and challenges. *Computer networks*, *57*(5), pp.1344-1371.

[3] Tan, S., De, D., Song, W.Z., Yang, J. and Das, S.K., **2016.** Survey of security advances in smart grid: A data driven approach. *IEEE Communications Surveys & Tutorials*, *19*(1), pp.397-422.

[4] Toldinas, J., Damasevicius, R., Venckauskas, A., Blazauskas, T. and Ceponis, J., **2014.** Energy consumption of cryptographic algorithms in mobile devices. *Elektronika Ir Elektrotechnika*, *20*(5), pp.158-161.

[5] Thabit, F., Can, O., Wani, R.U.Z., Qasem, M.A., Thorat, S.B. and Alkhzaimi, H.A., **2023.** Data security techniques in cloud computing based on machine learning algorithms and cryptographic algorithms: Lightweight algorithms and genetics algorithms. *Concurrency and Computation: Practice and Experience*, *35*(21), p.e7691.

[6] Khaitan, S.K. and McCalley, J.D., **2014.** Design techniques and applications of cyberphysical systems: A survey. *IEEE systems journal*, *9*(2), pp.350-365.

[7] Kumar, P., Lin, Y., Bai, G., Paverd, A., Dong, J.S. and Martin, A., **2019.** Smart grid metering networks: A survey on security, privacy and open research issues. *IEEE Communications Surveys & Tutorials*, *21*(3), pp.2886-2927.

[8] Potlapally, N.R., Ravi, S., Raghunathan, A. and Jha, N.K., **2005.** A study of the energy consumption characteristics of cryptographic algorithms and security protocols. *IEEE Transactions on mobile computing*, *5*(2), pp.128-143.

[9] Al Salami, S., Baek, J., Salah, K. and Damiani, E., **2016,** August. Lightweight encryption for smart home. In *2016 11th International conference on availability, reliability and security (ARES)* (pp. 382-388). IEEE.

[10] Hodjat, A. and Verbauwhede, I., **2004**, April. A 21.54 Gbits/s fully pipelined AES processor on FPGA. In *12th annual IEEE symposium on field-programmable custom computing machines* (pp. 308-309). IEEE.

[11] Dinu, D., Corre, Y.L., Khovratovich, D., Perrin, L., Großschädl, J. and Biryukov, A., **2019**. Triathlon of lightweight block ciphers for the internet of things. *Journal of Cryptographic Engineering*, *9*, pp.283-302.

[12] Fernandez-Carames, T.M. and Fraga-Lamas, P., **2020**. Towards post-quantum blockchain: A review on blockchain cryptography resistant to quantum computing attacks. *IEEE access*, *8*, pp.21091-21116.

[13] Andoni, M., Robu, V., Flynn, D., Abram, S., Geach, D., Jenkins, D., McCallum, P. and Peacock, A., **2019**. Blockchain technology in the energy sector: A systematic review of challenges and opportunities. *Renewable and sustainable energy reviews*, *100*, pp.143-174.

[14] Kumar, S. and Tiwary, K.P., **2022**. Cadmium selenide thin film deposition and characterization for photovoltaic applications. In *Nanomaterials for Innovative Energy Systems and Devices* (pp. 333-367). Singapore: Springer Nature Singapore.

[15] Priyadarshini, A., Nikhil, K., Mishra, R.K. and Tiwary, K.P., **2024**. Photovoltaic Cell Prepared from Nanoparticles of CdS/CdTe on ITO Substrate and its Characterization. *International Research Journal on Advanced Engineering Hub (IRJAEH)*, *2*(05), pp.1452-1457.

[16] Sindhuja, K. and Devi, S.P., **2014.** A symmetric key encryption technique using genetic algorithm. *International journal of computer science and information technologies*, *5*(1), pp.414-416.

[17] Mohd, B.J. and Hayajneh, T., 2018. Lightweight block ciphers for IoT: Energy optimization and survivability techniques. *IEEE Access*, *6*, pp.35966-35978.

[18] Alassaf, N., Gutub, A., Parah, S.A. and Al Ghamdi, M., **2019.** Enhancing speed of SIMON: A light-weight-cryptographic algorithm for IoT applications. *Multimedia Tools and Applications*, *78*, pp.32633-32657.

[19] Mousavi, S.K., Ghaffari, A., Besharat, S. and Afshari, H**., 2021**. Security of internet of things based on cryptographic algorithms: a survey. *Wireless Networks*, *27*(2), pp.1515-1555.

[20] Akkaya, K., Demirbas, M. and Aygun, R.S., 2008. The impact of data aggregation on the performance of wireless sensor networks. *Wireless Communications and Mobile Computing*, *8*(2), pp.171-193.

[21] Kennedy, M., Ksentini, A., Hadjadj-Aoul, Y. and Muntean, G.M., **2012**. Adaptive energy optimization in multimedia-centric wireless devices: A survey. *IEEE communications surveys & tutorials*, *15*(2), pp.768-786.

[22] Schizas, N., Karras, A., Karras, C. and Sioutas, S., **2022**. TinyML for ultra-low power AI and large scale IoT deployments: A systematic review. *Future Internet*, *14*(12), p.363.

[23] Martín-Lopo, M.M., Boal, J. and Sánchez-Miralles, Á. **2020.** A literature review of IoT energy platforms aimed at end users. *Computer Networks*, *171*, p.107101.

