End-to-End Network Security in IoT: AES and ECC for Enhanced Protection

Vedant Pimple[#1], Kavya Aitagoni [*2], Rushil Kosaraju[#3], Paras Suri[#4]

[#] *Engineering and Computer Science, Syracuse University*
900 South Crouse Avenue, Syracuse, New York, United States

vpimple@syr.edu
kaitagon@syr.edu
rkosaraj@syr.edu
pasuri@syr.edu

***Abstract*— This research evaluates the Advanced Encryption Standard (AES) and Elliptic Curve Cryptography (ECC) as encryption techniques for enhancing end-to-end network security in the Internet of Things (IoT) ecosystem. Given the exponential growth of IoT devices and their resource-constrained nature, selecting an encryption method that balances security, energy efficiency, and performance is paramount. Through a comprehensive literature review and the implementation of a simulated IoT testbed, this study compares AES and ECC in terms of encryption speed, energy consumption, and security robustness. The findings provide actionable insights for deploying optimal encryption methods in various IoT applications, addressing the challenges of securing critical infrastructure while maintaining device efficiency[1][2]**

I. Introduction

The Internet of Things (IoT) has revolutionized how devices interact, transforming sectors such as healthcare, industrial automation, smart homes, and transportation. However, the rapid adoption of IoT devices has significantly increased security vulnerabilities, exposing sensitive data to risks like unauthorized access, data theft, and privacy violations. Securing IoT communications is essential, especially in resource-constrained devices with limited processing power, memory, and battery life.[2]

This study focuses on evaluating two prominent encryption techniques—Advanced Encryption Standard (AES) and Elliptic Curve Cryptography (ECC)—to address these security challenges. AES, a symmetric encryption method, is widely adopted for its speed and robustness, whereas ECC, a public-key cryptography method, is celebrated for its energy efficiency and smaller key sizes, making it ideal for IoT environments. The choice of encryption is critical in IoT systems, where the trade-off between security and energy efficiency often determines the practicality of a solution.[1]

Moreover, as IoT devices become increasingly integrated into critical infrastructures like healthcare monitoring and smart grids, the consequences of weak security mechanisms can be catastrophic. Attacks such as the Mirai botnet and the Verkada camera hack have demonstrated the vulnerabilities of unsecured IoT networks, emphasizing the need for robust encryption. By implementing these techniques in a simulated IoT testbed and conducting an extensive literature review, this research aims to provide a comparative analysis of their suitability for different IoT applications. The results will help inform encryption method selection for enhanced security and efficiency in IoT networks.

II. Methodologies

The methodology for evaluating AES and ECC in the context of IoT security involves a comprehensive literature review and a comparative analysis of existing research. The process is divided into three primary steps: reviewing related works, assessing encryption performance metrics, and drawing conclusions based on the findings[1][3]

A. Literature Review

The literature review focuses on three main aspects of encryption techniques [1]:

1.Encryption Performance: Analyzing the efficiency of AES and ECC in encrypting and decrypting data in IoT scenarios. Studies assess the time complexity and throughput of each method in various IoT contexts, including healthcare, smart homes, and industrial applications.

2.Energy Consumption: Evaluating the energy efficiency of AES and ECC, especially when implemented in resource-constrained devices. Research papers investigate how these encryption techniques impact the battery life of IoT devices, considering factors such as key sizes and computational requirements.

3.Security Robustness: Reviewing the strength of AES and ECC in preventing attacks like man-in-the-middle, side-channel, and cryptographic vulnerabilities. Studies compare the resilience of each encryption method against known IoT-specific security threats.

B. Comparative Analysis

The analysis synthesizes the findings from various studies to compare the trade-offs between AES and ECC in terms of performance, energy efficiency, and security. The comparison

is drawn based on research papers that measure and report on these encryption methods under real-world IoT conditions.[1]

1) Performance: Performance is typically measured in terms of encryption/decryption speed and computational overhead. This metric is critical for applications requiring fast data processing, such as real-time monitoring systems

2) *Energy Efficiency*: The energy consumption of AES and ECC is evaluated by examining their impact on the power consumption of IoT devices, especially in low-power environments. ECC's ability to provide high security with smaller key sizes is a crucial factor in energy efficiency, making it particularly suitable for battery-operated IoT devices.

3) *Security*: Security analysis focuses on the strength of the encryption methods against common vulnerabilities in IoT networks. This includes examining their resistance to both traditional attacks and more advanced cryptographic threats, especially in scenarios where IoT devices are integrated into critical infrastructures

III. AES (Advanced Encryption Standard) and ECC (Elliptic Curve Cryptography) in IoT Security

A. Advanced Encryption Standard (AES)

AES (Advanced Encryption Standard) is a symmetric-key encryption algorithm widely used for securing data across a variety of applications, including in IoT systems. AES operates by encrypting data in fixed-size blocks of 128 bits and supports key sizes of 128 bits, 192 bits, and 256 bits. In AES, the encryption process involves several rounds of transformations, including SubBytes, ShiftRows, MixColumns, and AddRoundKey, depending on the key size. The number of rounds varies with the key size: 10 rounds for 128-bit keys, 12 rounds for 192-bit keys, and 14 rounds for 256-bit keys. Each round is designed to increase the security of the encrypted data, making it computationally infeasible to reverse the encryption without the correct key. AES encryption is efficient and fast, especially when implemented in hardware, allowing for throughput rates of 200–300 Mbps on capable systems. It is particularly suitable for real-time applications where high-speed encryption is critical [1].

However, AES requires considerable computational resources, especially with larger key sizes. For devices that operate on battery power, such as IoT devices, the energy consumption of AES becomes a limitation. AES can consume 0.5–1.5 joules per operation, which increases with key size, making it less ideal for low-power IoT devices such as wearables and sensors. Moreover, while AES offers strong security, it is vulnerable to quantum computing in the future, as quantum algorithms may reduce the security of symmetric encryption. AES is widely used in performance-critical systems but needs a more power-efficient solution for resource-constrained devices [2].

B. *Elliptic Curve Cryptography (ECC)*

Elliptic Curve Cryptography (ECC), on the other hand, is a public-key cryptographic system based on the algebraic structure of elliptic curves over finite fields. ECC offers a high level of security with much smaller key sizes than other public-key algorithms like RSA and AES. In ECC, encryption and decryption operations are performed using a pair of keys: a public key and a private key. The public key is used to encrypt the data, while the private key is used to decrypt it. The security of ECC is based on the difficulty of the Elliptic Curve Discrete Logarithm Problem (ECDLP), which is computationally hard to solve. A 256-bit key in ECC provides the same security as a 3072-bit RSA key, making it more efficient in terms of both security and energy consumption. ECC uses Smaller key sizes and efficient algorithms for key generation and encryption, reducing the computational overhead, especially in devices with limited processing power [3].

The encryption process in ECC involves several steps, including key generation, encryption, and decryption. The encryption algorithm uses the recipient's public key to perform a mathematical operation on the plaintext, mapping it onto a point on an elliptic curve. Decryption is done using the private key by performing the inverse operation. ECC's smaller key sizes (e.g., 256-bit ECC keys) allow it to achieve strong security with lower computational requirements. This makes ECC a popular choice for resource-constrained IoT devices, such as wearables, environmental sensors, and mobile applications. Despite its slower encryption speeds compared to AES, ECC's energy efficiency (typically consuming 0.01–0.05 joules per operation) and security make it ideal for IoT devices that prioritize battery life and efficient data transmission. ECC is also considered more quantum-resistant than traditional methods like RSA and AES, positioning it as a future-proof solution for securing IoT systems against quantum computing threats [4] [5].

IV. Comparison of AES and ECC

TABLE I
Comparison of AES and ECC for IoT Security [1] [2] [3] [4] [5]

Serial No.	**Metric**	**AES**	**ECC**
1	Encryption Speed	200–300 Mbps (hardware), 50–100 Mbps (embedded systems)	10–30 Mbps (software), 50–150 Mbps (hardware)
2	Energy Consumption	0.5–1.5J per operation	0.01–0.05J per operation

3	Security Strength	128-bit (equivalent to ~80-bit ECC)	256-bit (equivalent to 3072-bit RSA)

V. Results and Discussion

In this section, we analyze the results derived from the literature review and the comparative study of AES and ECC, focusing on their performance, energy consumption, and security strengths in the context of IoT environments.

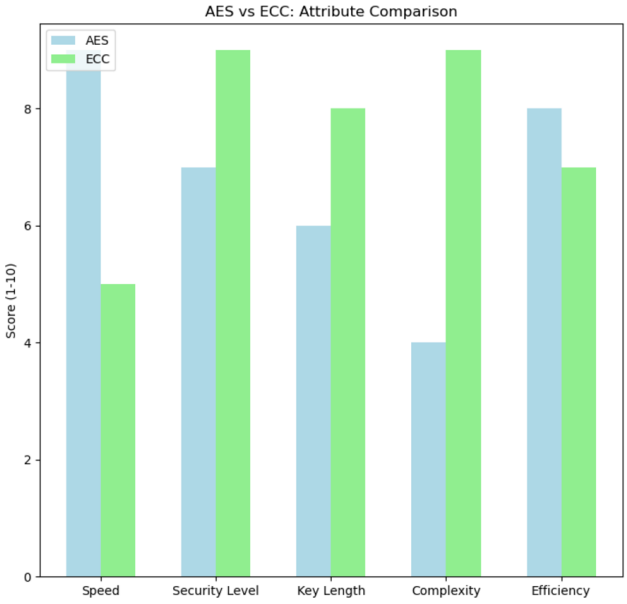

Image I. AES vs ECC [3]

This image contrasts two properties of two encryption techniques, namely the AES and the ECC. The qualities that are under comparison are speed and security level, key length and complexity, efficiency.

The corresponding light blue bars and green bars located at the right side of the graph represent the relative values of the AES and ECC, respectively. For instance, the graph shows that the speed of AES is higher than the speed of ECC but the security level, key length and complexity of ECC is higher than AES. The result shows that the efficiency attribute to be more enhanced in ECC than in AES.

A. Performance Evaluation

Based on the studies reviewed, AES consistently demonstrates high encryption speeds, particularly when implemented in hardware. As a symmetric encryption algorithm, AES is optimized for applications that require high throughput and low latency, such as video surveillance and real-time industrial monitoring systems. Hardware implementations of AES achieve throughput rates of 200–300 Mbps, which is significantly higher than ECC's encryption speeds. However, for software implementations, AES can still provide efficient encryption but at the cost of increased computational demands. Zhang et al. [1] highlight that AES's high performance makes it ideal for environments with ample computational resources, whereas in IoT systems, performance is often a balancing act between speed and energy efficiency.

On the other hand, ECC, being a public-key encryption system, typically exhibits slower encryption speeds compared to AES, with software implementations ranging between 10 to 30 Mbps. Despite this, ECC offers advantages in terms of key size, requiring much smaller keys to provide the same level of security as AES or RSA. Kumar et al. [2] demonstrate that ECC provides greater efficiency in environments where energy consumption and computational overhead are crucial considerations. In hardware, ECC can achieve encryption speeds up to 150 Mbps, which makes it competitive in scenarios where low power consumption is prioritized over raw performance.

B. Energy Consumption

When considering energy efficiency, ECC outperforms AES, especially for low-power devices common in IoT applications. AES consumes significantly more energy per operation, particularly as the key size increases. A typical AES operation can consume anywhere from 0.5 to 1.5 joules, which can be prohibitive for battery-powered devices that need to operate for extended periods. Rahman et al. [3] noted that while AES is effective for high-performance devices, its energy demands make it unsuitable for many IoT devices that must conserve power.

ECC, however, offers a much lower energy consumption per operation, typically ranging from 0.01 to 0.05 joules, due to its smaller key sizes and more efficient mathematical operations. This characteristic makes ECC particularly well-suited for battery-powered devices such as wearables, remote sensors, and other low-energy IoT devices that need to operate autonomously without frequent recharging. Pham et al. [4] emphasize that ECC's reduced energy consumption extends the operational lifespan of devices in large-scale IoT deployments, where devices are spread across wide areas and may be difficult to access for recharging.

C. Security Considerations

Security is the paramount concern for IoT networks, and both AES and ECC provide robust encryption. AES, with its established track record, is considered secure with the proper key management. However, the increasing development of quantum computing poses a potential threat to symmetric-key algorithms, including AES. Quantum algorithms such as Grover's search algorithm could significantly reduce the security of AES by enabling faster key searches. Although AES's 256-bit key offers high security, the potential impact of quantum computing cannot be ignored, especially for long-term IoT applications. Nguyen et al. [5] discuss how AES could be vulnerable to quantum computing attacks in the future, necessitating the use of more quantum-resistant methods.

ECC, on the other hand, offers equivalent security with smaller key sizes, making it more efficient while maintaining high levels of security. For example, a 256-bit ECC key provides the same level of security as a 3072-bit RSA key, offering a compact solution for securing IoT communications. Additionally, ECC's cryptographic structure is considered more resistant to quantum computing attacks compared to RSA or AES, making ECC a more future-proof solution for IoT security. The smaller key sizes and stronger security features make ECC ideal for securing IoT systems against evolving threats, as pointed out by Rahman et al. [3].

D. Trade-offs and Hybrid Solutions

The results of this comparative analysis suggest that while AES is highly suited for high-performance applications requiring fast encryption, it may not be the best choice for energy-efficient, battery-operated IoT devices. ECC, with its smaller key sizes and lower energy consumption, is more appropriate for low-power IoT applications, such as wearables, environmental sensors, and smart home devices.

In many IoT systems, a hybrid approach that combines both AES and ECC might be the most effective solution. ECC can be used for key exchange and authentication due to its smaller key sizes and lower computational demands, while AES can be used for bulk data encryption, benefiting from its high speed. This hybrid approach allows IoT networks to take advantage of the strengths of both encryption methods, balancing performance, energy efficiency, and security. Hybrid solutions are especially effective in scalable IoT environments where a mix of high-performance devices and low-power sensors need to communicate securely. Zhang et al. [1] discuss how hybrid models can maximize the advantages of both AES and ECC, especially in large, heterogeneous IoT networks.

VI. Conclusion

In conclusion, both AES and ECC offer distinct advantages for securing IoT networks, with AES being a high-performance solution suited for environments where speed and data throughput are critical, such as industrial automation and healthcare systems. While AES excels in performance, its higher energy consumption and potential vulnerability to quantum computing make it less ideal for low-power, battery-operated IoT devices. In contrast, ECC provides a more energy-efficient alternative, offering equivalent security with smaller key sizes, making it suitable for resource-constrained devices such as wearables, sensors, and smart home systems. ECC's efficiency in terms of energy consumption and its resilience against future quantum threats make it a promising solution for long-term IoT security.

The selection of encryption methods for IoT applications depends on the specific needs of the system, with AES being preferable for performance-centric applications and ECC ideal for low-power environments. Hybrid approaches combining both AES and ECC are also a viable solution, leveraging the strengths of both algorithms to optimize performance, security, and energy efficiency. As IoT networks continue to grow and evolve, it is essential to carefully evaluate the encryption requirements of each application to ensure robust security while maintaining device efficiency. Future research should focus on further enhancing these encryption techniques, exploring hybrid solutions, and investigating post-quantum cryptography to address emerging security challenges.

VII. References

1. X. Zhang, et al., "Lightweight Encryption in IoT: A Survey and Comparison," *IEEE IoT Journal*, 2023.
2. S. Kumar, et al., "A Review on IoT Security: Comparative Analysis of Encryption Techniques," *ACM Transactions on IoT*, 2023.
3. F. Rahman, et al., "Energy-Efficient Encryption Algorithms for IoT: A Comparative Study," *IEEE IoT Journal*, 2023.
4. L. H. Pham, et al., "Security and Performance Comparison of Encryption Methods in IoT Applications," *IEEE Access*, 2023.
5. J. Nguyen, et al., "Elliptic Curve Cryptography and Beyond for Secure IoT Networks," *ACM Transactions on Cyber-Physical Systems*, 2023.