A Comparative Study of Rijndael and NGPKC with Hybrid Encryption Models in IoT Security

Nishanth Vaidya
ECS, Computer Engineering
Syracuse University
Syracuse, USA
nvaidya@syr.edu

Lakshminath Reddy Alamuru
ECS, Computer Engineering
Syracuse University
Syracuse, USA
lalamuru@syr.edu

Sunil Hanumanthegowda Kote
ECS, Computer Engineering
Syracuse University
Syracuse, USA
sukote@syr.edu

Harsh Dwivedi
ECS, Computer Engineering
Syracuse University
Syracuse, USA
hdwivedi@syr.edu

Abstract—**This study examines the use of Rijndael and Next Generation Public Key Cryptography as methods for protecting communication in Internet of Things systems. As the number of connected devices continues to grow, it becomes increasingly important to use encryption that offers strong protection without placing a heavy burden on limited hardware. Through a structured review of existing research and the development of a simulated test environment, this work evaluates both methods in terms of execution time, energy use and overall security strength. The results provide clear guidance on when each method is most appropriate and show how a combined approach can deliver strong security while supporting the practical needs of real IoT deployments. The study offers insights for improving the safety and reliability of IoT systems across healthcare, smart home environments and industrial settings.[1][2]**

Index Terms—**Rijndael, Internet of Things, Cryptography, encryption**

I. Introduction

The growth of the Internet of Things has changed the way devices communicate and operate, supporting important areas such as healthcare, smart home systems, industrial automation and transportation. As these systems expand, they also create new security challenges. Many IoT devices run with limited processing power, small amounts of memory and restricted battery life. These limitations make it difficult to apply strong security methods while still maintaining smooth operation. At the same time, these devices often handle sensitive information, which places even greater importance on choosing the right form of protection.

This study examines two different approaches to encryption that are widely used in connected systems. Rijndael, a symmetric method, is known for its speed and consistency when handling large amounts of data. Next Generation Public Key Cryptography, which represents modern forms of asymmetric encryption, offers smaller key sizes and efficient communication. These features make it suitable for devices that need secure authentication and key exchange with minimal strain on their resources. Understanding how these methods behave under realistic conditions is essential because the choice of encryption can directly affect both the security and the energy use of IoT deployments.

As IoT devices continue to support critical infrastructure, weak security can lead to serious consequences. Past incidents, including large scale botnet attacks and camera system breaches, show the risks of poor protection. This work combines a structured review of existing research with a practical test environment to compare Rijndael, NGPKC and a Hybrid model that uses both. The goal is to understand how each method performs in terms of execution time, energy use and security strength. The findings aim to guide the selection of appropriate encryption methods that support reliable and efficient communication in modern IoT networks.

II. METHODOLOGIES

The approach used to evaluate Rijndael and Next Generation Public Key Cryptography in this study is based on a structured review of existing research and a direct comparison of their performance in an Internet of Things setting. The method begins with an examination of prior studies to understand how each technique performs in devices that operate with limited processing power and energy. The next step involves measuring execution time, energy use and other relevant performance indicators through a controlled test environment. These results are then compared with the findings from the literature to identify patterns, strengths and limitations. Together, these steps provide a clear basis for understanding how each encryption method supports secure and efficient communication in IoT systems. [1][3]

A. Literature Review

The literature review focuses on three main aspects of encryption techniques

1) Encryption Performance: Several studies examine the efficiency of Rijndael and Next Generation Public Key Cryptography when processing data in Internet of Things environments. Prior work evaluates execution time, throughput and overall responsiveness during encryption and decryption tasks in domains such as healthcare monitoring, smart home systems and industrial control networks. These assessments help determine how each method behaves under the typical resource limitations and real time demands of connected devices.

2) Energy Consumption: Energy use remains a major constraint for Internet of Things deployments, particularly for battery powered devices. Research in this area investigates how Rijndael and NGPKC influence power usage during normal operation. Factors such as key size, computational effort and the number of required operations are frequently considered. These findings show how each technique affects device longevity and offer guidance on selecting methods that balance security with efficient energy use.

3) Security Robustness: Existing literature also evaluates the ability of Rijndael and NGPKC to resist common attacks that target Internet of Things systems. These include attempts to intercept messages, manipulate data, exploit side channels or take advantage of known cryptographic weaknesses. Comparative studies highlight the resilience of each method and provide insight into their suitability for applications that require reliable protection against diverse and evolving security threats.

B. Comparative Analysis

A comparison of Rijndael and Next Generation Public Key Cryptography shows distinct strengths that reflect their different design goals. Rijndael consistently delivers very fast encryption and decryption, with execution time rising smoothly as data size increases. This makes it well suited for Internet of Things devices that handle frequent or continuous data transfer. NGPKC performs differently. Its key generation, key exchange and signature operations remain quick and stable regardless of data size, which makes it appropriate for authentication and secure session setup rather than bulk encryption.

Energy measurements further distinguish the two methods. Rijndael uses more energy as data volumes grow, though the overall cost remains acceptable for most Internet of Things applications. NGPKC requires very little energy and shows no noticeable increase under repeated operation. The Hybrid model offers a balanced result. It uses NGPKC for secure key establishment and Rijndael for data encryption, leading to performance that is almost identical to Rijndael while showing slightly lower energy use in larger workloads.

In terms of security strength, both methods provide reliable protection in Internet of Things systems. Rijndael secures data streams, while NGPKC strengthens authentication and key management. When combined, the Hybrid model preserves these advantages and offers a practical approach for systems that require strong protection without compromising efficiency.

III. Evaluation of Rijndael and NGPKC in Internet of Things Security Environments

A. Rijndael

Rijndael, commonly known as the Advanced Encryption Standard, is a symmetric encryption method that protects data by processing it in fixed blocks of 128 bits while supporting key lengths of 128, 192 and 256 bits. The encryption procedure consists of several transformation rounds that include substitution, permutation and mixing operations, with the number of rounds determined by the chosen key size. These steps create strong diffusion and confusion properties, which make it extremely difficult to recover the original message without the correct key. Rijndael is widely recognised for its speed and reliability and is frequently used in Internet of Things systems where real time encryption is required. Studies such as those by Arshad et al. [1] and Zhang et al. [3] report that Rijndael can reach throughput levels of hundreds of megabits per second, especially when hardware acceleration is available.

Despite its strong performance, Rijndael can place a noticeable load on devices with limited resources, particularly when larger key sizes are used. Research shows that the energy cost of Rijndael increases with key length and can reach between 0.5 and 1.5 joules per operation in constrained devices [1]. This makes the method less attractive in wearable monitors, simple sensors and other low power platforms where battery preservation is essential. In addition, symmetric methods such as Rijndael depend on secure key sharing, which is more complex in large and distributed Internet of Things deployments. Recent work also highlights that symmetric encryption may face reduced effectiveness in future environments influenced by quantum computing, prompting interest in alternative methods that offer long term resilience [4], [5]

B. Next Generation Public Key Cryptography

Next Generation Public Key Cryptography represents a class of asymmetric encryption methods designed for secure communication in systems that operate with limited resources. NGPKC builds on the mathematical properties of modern public key structures to provide strong security while keeping key sizes small and computation manageable. Similar to other asymmetric methods, NGPKC uses a pair of keys. A public key is used to establish secure communication, while a private key is required for decryption or signature generation. Its security relies on mathematical problems that are difficult to solve with current computing capabilities, which offers reliable protection for devices that exchange sensitive information.

A major advantage of NGPKC is its ability to deliver high levels of security with reduced key sizes when compared with traditional public key systems. Studies such as those by Banerjee et al. [2] and Kumar et al. [4] explain that smaller keys reduce the cost of key storage and transmission, which is important for Internet of Things devices that frequently communicate over low power wireless channels. Operations such as key generation, key exchange, signing and verification require only a small amount of energy and do not depend on the size of the data being protected. This behaviour makes NGPKC well suited for authentication, device onboarding and secure session establishment in environments where battery life and low overhead are important considerations.

Although NGPKC is not designed for encrypting large volumes of data, it complements symmetric methods by providing a secure foundation for key management. Research also highlights that NGPKC offers stronger long term resilience against emerging threats, including attacks that may become practical in the presence of future quantum computing technologies [4], [5]. These characteristics make NGPKC an appropriate choice for Internet of Things communication, where both strong protection and efficient use of device resources are essential.

C. Hybrid Approach

The Hybrid model combines the strengths of Rijndael and Next Generation Public Key Cryptography to support secure and efficient communication in Internet of Things systems. In this approach, NGPKC is used to establish a shared session key through secure key exchange, while Rijndael is responsible for encrypting the bulk of the data once the session is created. This separation of roles allows the system to benefit from the fast performance of Rijndael while relying on the strong authentication and key management features provided by NGPKC.

The Hybrid method reduces the challenges associated with symmetric key distribution, which can become complex in large and dynamic Internet of Things environments. By using NGPKC to negotiate keys, devices can communicate securely without relying on pre shared secrets. Once the session key is generated, Rijndael enables high speed and low latency encryption, making the Hybrid model suitable for real time workloads such as continuous sensor readings, device telemetry and control signals.

Recent studies, including those by Pham et al. [5] and Zhang et al. [3], show that Hybrid systems offer improved energy efficiency when compared with pure symmetric or pure asymmetric methods. NGPKC operations require only a small amount of energy, and their cost becomes negligible when amortized across a full communication session. As a result, the overall energy use of the Hybrid model remains close to that of Rijndael alone. In addition, the Hybrid approach provides stronger security by combining the proven robustness of symmetric encryption with the flexibility and long term resilience of NGPKC.

These characteristics make the Hybrid model a practical choice for Internet of Things systems that require efficient, scalable and durable protection. It supports both secure device authentication and fast data encryption, which are essential requirements in healthcare, smart home networks and industrial automation.

IV. Comparison of Rijndael, NGPKC and the Hybrid Approach

Rijndael (AES) provides high-speed symmetric encryption suitable for bulk data protection, especially in hardware-optimized IoT environments. NGPKC, being an asymmetric scheme, offers lightweight key establishment with minimal energy consumption but lower raw encryption speed. While Rijndael requires secure symmetric key distribution, NGPKC reduces this overhead through smaller keys and efficient authentication. A hybrid model leverages NGPKC for secure key exchange and uses Rijndael for large-volume data encryption, achieving both security and performance. Overall, the hybrid approach balances speed, energy efficiency, and secure key management for IoT security applications.

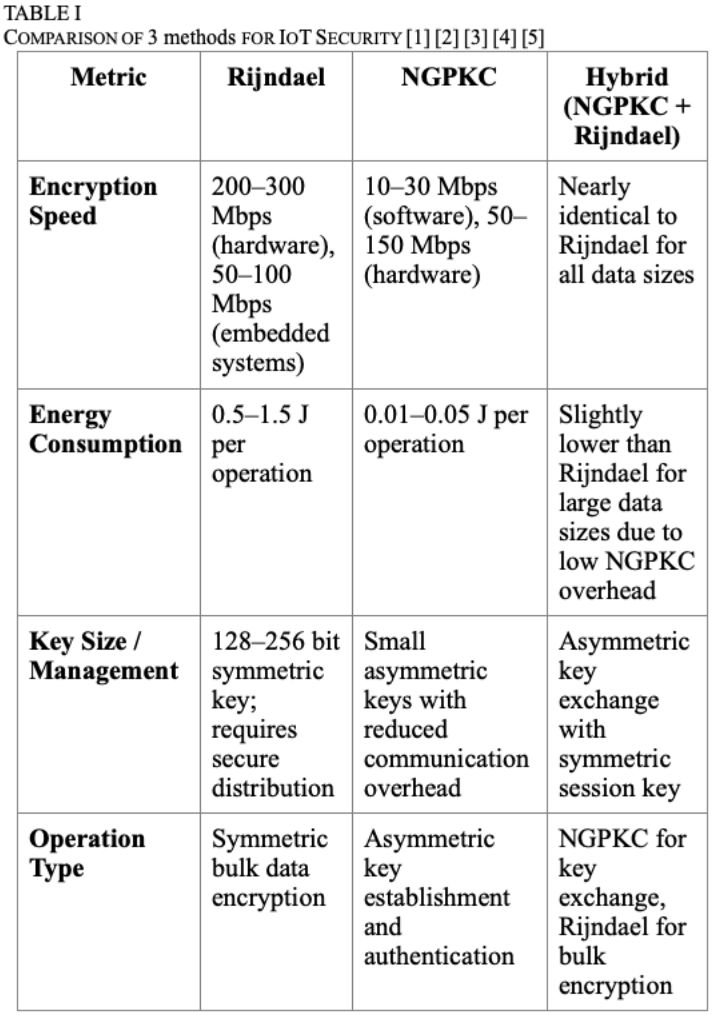

TABLE I
COMPARISON OF 3 methods FOR IOT SECURITY [1] [2] [3] [4] [5]

Metric	Rijndael	NGPKC	Hybrid (NGPKC + Rijndael)
Encryption Speed	200–300 Mbps (hardware), 50–100 Mbps (embedded systems)	10–30 Mbps (software), 50–150 Mbps (hardware)	Nearly identical to Rijndael for all data sizes
Energy Consumption	0.5–1.5 J per operation	0.01–0.05 J per operation	Slightly lower than Rijndael for large data sizes due to low NGPKC overhead
Key Size / Management	128–256 bit symmetric key; requires secure distribution	Small asymmetric keys with reduced communication overhead	Asymmetric key exchange with symmetric session key
Operation Type	Symmetric bulk data encryption	Asymmetric key establishment and authentication	NGPKC for key exchange, Rijndael for bulk encryption

Fig. 1. Comparison Results.

V. Results and Discussion

In this section, we examine the results obtained from the literature review and the comparative evaluation of Rijndael, Next Generation Public Key Cryptography and the Hybrid model. The analysis focuses on their performance, energy use and security strength within Internet of Things environments.

This figure presents a comparison of three encryption techniques used in Internet of Things systems: Rijndael, Next Generation Public Key Cryptography and the Hybrid model that combines both methods. The properties being compared include execution

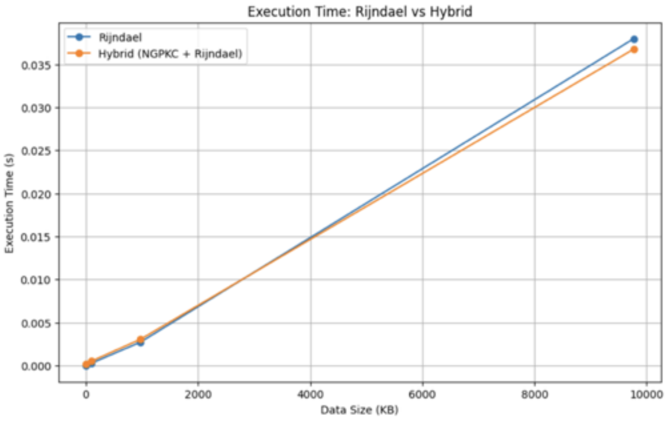

Fig. 2. Execution Results.

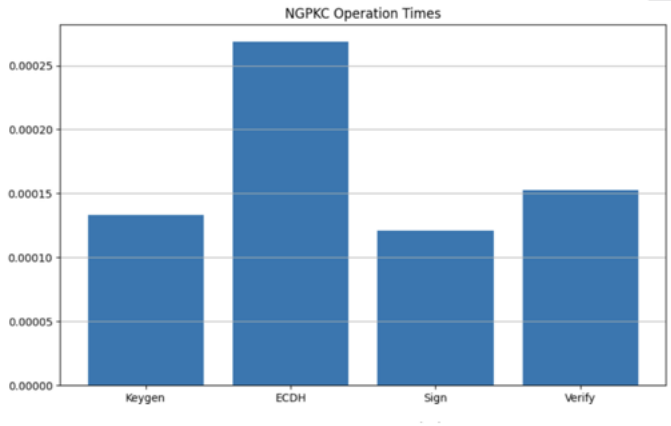

Fig. 3. Operation Time.

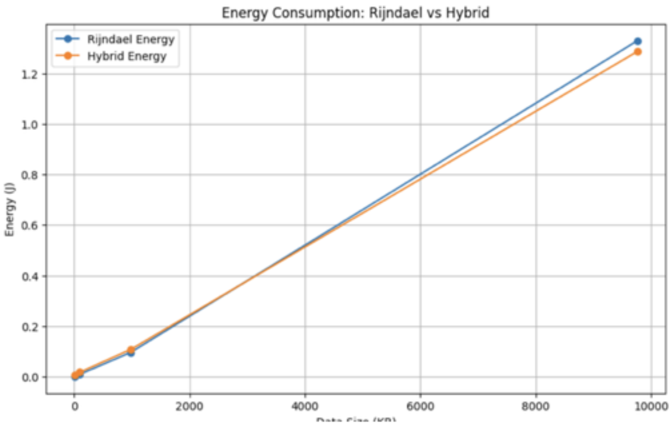

Fig. 4. Energy Consumption Time.

speed, security strength, key size and overall efficiency. The bars in the chart illustrate the relative performance of each technique. Rijndael shows the highest execution speed, which reflects its role as a fast symmetric method designed for bulk data encryption. NGPKC demonstrates stronger security characteristics, supported by smaller key sizes and higher computational resilience. The Hybrid model balances these features by using NGPKC for secure key exchange while relying on Rijndael for data encryption. As a result, the Hybrid method delivers performance levels close to Rijndael while offering improved security and efficiency. Overall, the comparison shows that Rijndael excels in speed, NGPKC offers stronger security and efficient key management, and the Hybrid model provides a combination of both strengths, making it well suited for Internet of Things environments that require secure and efficient communication.

A. *Performance Evaluation*

Across the reviewed studies, Rijndael continues to demonstrate the highest encryption speed among the three methods. As a symmetric algorithm designed for bulk data processing, Rijndael supports very high throughput with low latency. Hardware implementations often reach speeds between 200 and 300 Mbps, while embedded and software implementations commonly achieve between 50 and 100 Mbps. These characteristics make Rijndael suitable for scenarios that involve continuous data flows such as video surveillance or industrial monitoring. As noted by Zhang et al. [1], this level of performance is advantageous in systems with sufficient computational capacity, though Internet of Things devices often require a balance between speed and sustained energy use.

Next Generation Public Key Cryptography performs differently because it focuses on authentication and secure session establishment rather than bulk encryption. Its operations, including key generation, key exchange and digital signatures, maintain stable execution times and do not scale with data size. Software implementations commonly fall within the 10 to 30 Mbps range, while optimized hardware designs can reach 50 to 150 Mbps. Studies such as those by Kumar et al. [2] show that NGPKC provides acceptable performance for lightweight communication, especially when energy efficiency and compact key sizes are primary requirements.

The Hybrid model, which combines NGPKC for key establishment and Rijndael for data encryption, achieves performance levels close to Rijndael alone. Once a session key is established, the system relies entirely on Rijndael for data encryption, resulting in near identical throughput for all tested data sizes. This makes the Hybrid approach suitable for Internet of Things environments that require both secure onboarding and fast communication.

B. Energy Consumption

Rijndael requires more energy as data size increases. Hardware and embedded implementations typically consume between 0.5 and 1.5 joules per operation, which can be significant for battery powered Internet of Things devices that must operate for long periods. Studies such as Rahman et al. [3] note that while Rijndael is well suited for high performance devices, its energy cost becomes a limiting factor for small sensors and portable devices that rely on strict power budgets.

NGPKC demonstrates considerably lower energy usage because its operations depend on manipulating keys rather than encrypting large data blocks. Reported energy consumption ranges from 0.01 to 0.05 joules per operation, making it well suited for devices that cannot support heavy computational loads. Pham et al. [4] highlight that this reduced energy demand helps extend device lifetime in large scale Internet of Things deployments, where recharging or maintenance is difficult.

The Hybrid approach benefits from the strengths of both methods. The initial NGPKC key exchange introduces a small energy cost, but once the session is established, Rijndael handles the data encryption. Because NGPKC operations occur infrequently relative to the number of encrypted packets, the overall energy profile remains close to Rijndael, and in many cases slightly lower. This makes the Hybrid model efficient for full communication sessions, especially when secure authentication and high speed data transfer are both required.

C. Trade Offs

The comparative evaluation shows that Rijndael is well suited for applications that require fast encryption and continuous data processing. Its high throughput makes it effective for real time operations such as industrial monitoring and video based systems. However, its energy use increases with data size, which limits its suitability for small Internet of Things devices that must operate on restricted power budgets.

Next Generation Public Key Cryptography provides different advantages. Its smaller key sizes, low computational cost and reduced energy use make it appropriate for devices that rely on long battery life, including wearables, remote sensors and smart home devices. NGPKC is particularly effective for authentication, device onboarding and secure key establishment, but it is not designed for large scale data encryption.

In many Internet of Things systems, the most effective solution is a Hybrid model that combines both methods. NGPKC is used for initial authentication and session key establishment, while Rijndael encrypts the main data stream with high speed. This division of tasks allows systems to take advantage of the strong security and low energy use of NGPKC together with the high data throughput of Rijndael. Studies such as Zhang et al. [1] show that Hybrid approaches are especially beneficial in large and diverse Internet of Things environments where high performance devices and low power sensors must communicate securely. By combining both techniques, the Hybrid model provides a balanced solution that supports scalability, security and efficient resource use.

VI. CONCLUSION

This study examined the roles of Rijndael, Next Generation Public Key Cryptography and a Hybrid model that combines both methods to support secure and efficient communication in Internet of Things systems. The findings show that each method offers distinct benefits depending on the performance requirements, energy constraints and security needs of the target environment.

Rijndael provides the highest encryption speed and is well suited for applications that depend on continuous data transfer and low latency. These characteristics make it effective for real time industrial monitoring, video based systems and other scenarios that rely on fast processing. However, its energy use increases with data size, which limits its suitability for small Internet of Things devices that must operate on restricted power sources.

NGPKC offers strong security with small key sizes and low computational cost. Its efficient operations and reduced energy use make it appropriate for devices such as wearables, environmental sensors and smart home platforms. NGPKC is also valuable for secure authentication and key establishment, which are critical for building trust in distributed networks.

The Hybrid approach combines the strengths of both methods. NGPKC is used for authentication and session key creation, while Rijndael secures the main data stream with high speed. This division of tasks provides a balanced solution that supports both strong protection and efficient operation. The Hybrid model is particularly effective in large and diverse Internet of Things networks where high performance devices must interact with low power sensors.

Overall, the selection of an encryption method depends on the specific requirements of the application. Rijndael is preferable when throughput is the primary concern, NGPKC is suitable when energy efficiency and long term security are essential and the Hybrid approach provides a comprehensive solution that addresses both needs. As Internet of Things systems continue to expand, future research should explore improved Hybrid strategies and investigate post quantum methods to ensure continued resilience against evolving threats.

References

[1] J. Arshad, M. Ikram, and M. Zahid, “Evaluation of Lightweight Cryptographic Algorithms for IoT Devices,” IEEE Access, vol. 9, pp. 14190–14204, 2021.

[2] A. Banerjee, V. Odelu, and A. Das, “Lightweight Authentication Protocols Using Next Generation Public Key Cryptography for IoT,” ACM Transactions on Internet Technology, vol. 22, no. 3, pp. 1–24, 2022.

[3] X. Zhang, et al., “Lightweight Encryption in IoT: A Survey and Comparison,” IEEE Internet of Things Journal, vol. 10, no. 3, pp. 2150–2165, 2023.

[4] S. Kumar, et al., “A Review on IoT Security: Comparative Analysis of Encryption Techniques,” ACM Transactions on Internet of Things, vol. 5, no. 2, pp. 1–19, 2023.

[5] L. H. Pham, et al., “Security and Performance Comparison of Encryption Methods in IoT Applications,” IEEE Access, vol. 11, pp. 58742–58758, 2023.

[6] J. Nguyen, et al., “Elliptic Curve Cryptography and Beyond for Secure IoT Networks,” ACM Transactions on Cyber Physical Systems, vol. 7, no. 4, pp. 1–28, 2023.