Power System Technology
ISSN:1000-3673

Received: 16-04-2025 Revised: 05-05-2025 Accepted: 22-07-2025

Secure and Efficient IOT Communication using Lightweight Cryptography in MQTT Networks

V.Ramanjaneyulu[1], M.Ravichandra[2], M.Paul Sundar Singh [3],B.Nagarjun Singh[4], M.Suseela [5]

[*1](PG student, Dept of CSE, Mandava Institute of Engineering and Technology- Jaggaiahpet-521175,India.)

[*2] (Asst Professor, Dept of CSE, Santhiram Engineering College- Nandyal-518501,India.)

[*3,4,5] (Asst Professor, Dept of CSE, Mandava Institute of Engineering and Technology- Jaggaiahpet-521175,India.)

Abstract:-

The Internet of Things (IOT) is rapidly expanding and quietly revolutionizing various industries by enabling seamless communication between devices. From smartphones to smart home systems, IOT has become an essential part of our everyday lives, offering a wide array of applications. However, while IOT devices are highly efficient in their functionality, they often lack robust security measures. This is a significant concern, as these devices typically operate with limited computing power, memory, and energy resources. These constraints create a resource-constrained environment, making IOT systems particularly vulnerable to security threats. To address these challenges, this project implements a method that integrates lightweight cryptographic algorithms, such as AES, PRESENT, SPECK, and RECTANGLE with the MQTT protocol. This combination ensures strong data encryption and decryption while facilitating secure and efficient data transmission.

Key words: IoT, Lightweight Cryptography, DTC, GSC, MQTT, AES, PRESENT, RECTANGLE, SPECK, MQTT.

1. Introduction

The Internet of Things (IoT) has become a cornerstone of modern technology, seamlessly connecting devices equipped with sensors, software, and computing capabilities through the internet. From fitness trackers monitoring our health to smart home systems automating our daily routines, IoT devices are transforming the way we live and work. However, as the number of interconnected devices grows, so do the security risks. Many IoT devices operate with limited processing power, memory, and battery life, making them easy targets for cyberthreats. Traditional security measures, which require significant computational resources, are often too heavy for these constrained environments. This gap highlights the urgent need for lightweight, efficient security solutions designed specifically for IoT systems.

Power System Technology
ISSN:1000-3673
Received: 16-04-2025 Revised: 05-05-2025 Accepted: 22-07-2025

In resource-constrained IoT environments, solutions like Dynamic Tree Chaining (DTC) and Geometric Star Chaining (GSC) have been explored to improve efficiency and security. DTC organizes devices in a hierarchical

tree structure, reducing resource usage but still facing issues like delays and vulnerability to attacks. GSC, on the other hand, uses a star topology to simplify communication and reduce delays. However, it consumes more

energy and remains susceptible to Distributed Denial of Service (DDoS) attacks. Traditional cryptographic methods, while effective, are simply too resource-intensive for IoT devices.

The integration of lightweight cryptographic algorithms with MQTT offers a promising alternative. This approach not only addresses the limitations of existing solutions but also provides a scalable and secure framework for IoT communication. By balancing security and efficiency, it ensures that IoT devices can operate safely and effectively in an increasingly connected world..

II. LITERATURE SURVEY

1.X. Li et al.(2019) explored secure and efficient communication for the Internet of Things(IoT) in their study published in IEEE/ACM Transactions on Networking. They emphasized the need for lightweight cryptographic solutions to address the unique challenges of IoT environments, such as limited computational resources and energy constraints. Their work laid the foundation for optimizing communication protocols to ensure both security and efficiency in IoT systems [1].

2.El-Hajj, Mousawi, and Fadlallah (2023) analyzed the performance of lightweight cryptographic algorithms on IoT hardware platforms in their article in Future Internet. They provided valuable insights into computational efficiency and energy consumption but focused primarily on hardware implementations. Their study highlighted the need for further research into software-based solutions and integration with IoT communication protocols [2].

3.Yarali, Srinath, and Joyce (2018) conducted a comprehensive study on network security challenges in IoT. They identified vulnerabilities in IoT systems and discussed the importance of adopting lightweight cryptographic algorithms to mitigate these risks. Their work underscored the growing need for robust security measures in IoT applications [3].

4.Sri Ramya Siraparapu and S.M.A.K. Azad (2024) reviewed secure systems for IoT in their paper published in e-Prime. They provided a detailed analysis of existing security frameworks and emphasized the importance of lightweight cryptography in addressing the resource constraints of IoT devices. Their work highlighted the need for scalable and adaptable security solutions [4].

Power System Technology
ISSN:1000-3673
Received: 16-04-2025 Revised: 05-05-2025 Accepted: 22-07-2025

5.Ch. Jnana Ramakrishna et al. (2024) analyzed lightweight cryptographic algorithms for IoT gateways in their study published in Procedia Computer Science. They evaluated various algorithms based on their suitability for resource-constrained environments and emphasized the importance of balancing security and

efficiency in IoT systems [5].

III. EXISTING SYSTEM

In today's rapidly advancing technological landscape, the Internet of Things (IOT) has become an integral part of our daily lives, connecting everything from household appliances to industrial machinery. However, despite its many benefits, securing IOT systems remains a significant challenge, mainly due to the reliance on traditional security measures and communication protocols that are not tailored for environments with limited resources like IOT networks.

In an attempt to address these challenges, researchers have proposed innovative solutions such as Dynamic Tree Chaining (DTC) and Geometric Star Chaining (GSC). DTC is particularly interesting because it organizes devices in a hierarchical tree structure, which helps to minimize resource usage. Yet, this method isn't without its flaws; it often leads to communication delays and leaves the system vulnerable to potential security breaches.

On the other hand, GSC adopts a star topology for network communication, aiming to simplify the data exchange process and effectively reduce delays. While this approach improves upon certain limitations of DTC by speeding up communication processes, it comes at the cost of higher energy consumption. Moreover, like many other IOT solutions, GSC is not immune to Distributed Denial of Service (DDoS) attacks, which pose a significant threat to network stability and security.

Traditional cryptographic methods, although powerful, are inherently resource- heavy, making them unsuitable for IOT devices that operate under stringent power and processing constraints. As a result, the security community continues to explore and develop novel strategies that can balance efficiency and security in IOT environments, paving the way for a more secure and efficient future in the world of connected devices.some of the disadvantages are

•High resource consumption, making traditional cryptographic methods unsuitable for IOT devices with limited processing power and memory.

•Delays in communication due to hierarchical structures like DTC.

•Vulnerability to cyber threats, such as DDoS attacks, in star-based topologies like GSC.

Power System Technology
ISSN:1000-3673
Received: 16-04-2025 Revised: 05-05-2025 Accepted: 22-07-2025

•Increased energy consumption in GSC, reducing the lifespan of battery-operated IOT devices.

•Lack of scalability and adaptability for diverse IOT applications

IV. SYSTEM ARCHITECTURE

The proposed system architecture strategically integrates cutting-edge lightweight cryptographic algorithms with the MQTT protocol, forming a robust framework to effectively tackle the intricate security and performance challenges prevalent in IOT systems. This integration is pivotal in safeguarding data exchanges and optimizing performance in resource-constrained environments typical of IOT devices.

IOT devices, which are often limited in computational power and memory, employ cryptographic algorithms such as AES, PRESENT, SPECK, or RECTANGLE. These algorithms are specifically engineered to provide high security levels while maintaining low-resource utilization. By encrypting sensor data using these efficient algorithms, IOT devices ensure that the data remains secure during transmission, thereby mitigating risks associated with data breaches or unauthorized access.

Once encrypted, the data is transmitted to an MQTT broker, a component central to this architecture that facilitates the publish-subscribe model. The MQTT broker plays a critical role in managing the topics under which data is published, enabling a structured approach to data dissemination and ensuring that only authorized subscribers can access specific data streams.

Subscribers, designated to receive this data, use the same cryptographic algorithm to decrypt the incoming data, ensuring that only those with the correct credentials can access and interpret the data. The decrypted data is subsequently stored in a reliable MySQL database, which is well-suited for further processing or analytical applications. This database acts as a secure repository, allowing for the efficient retrieval and analysis of the IOT data.

Power System Technology
ISSN:1000-3673
Received: 16-04-2025 Revised: 05-05-2025 Accepted: 22-07-2025

By adopting this approach, the system architecture not only addresses immediate security concerns but also ensures efficient and scalable communication in IOT networks. The use of lightweight cryptography and the MQTT protocol together create a harmonious balance between security, performance, and scalability, making it an ideal solution for modern IOT applications.

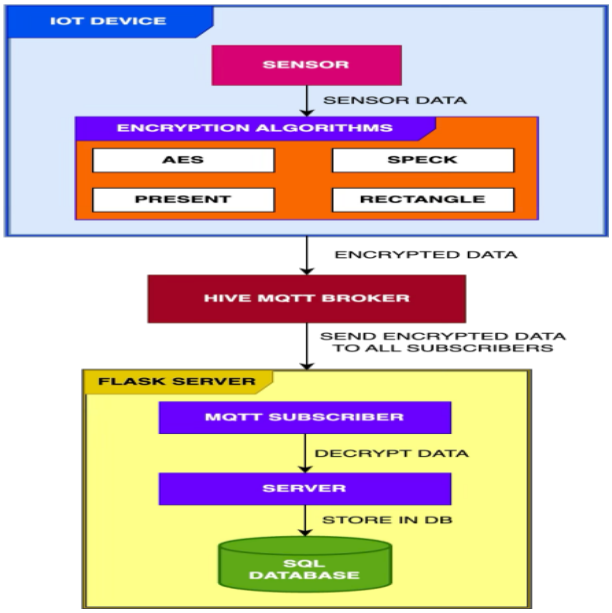


Fig 1. System Architecture

The proposed system architecture leverages lightweight cryptographic algorithms and the MQTT protocol to address the security and performance challenges of IoT systems. The methodology is described below:

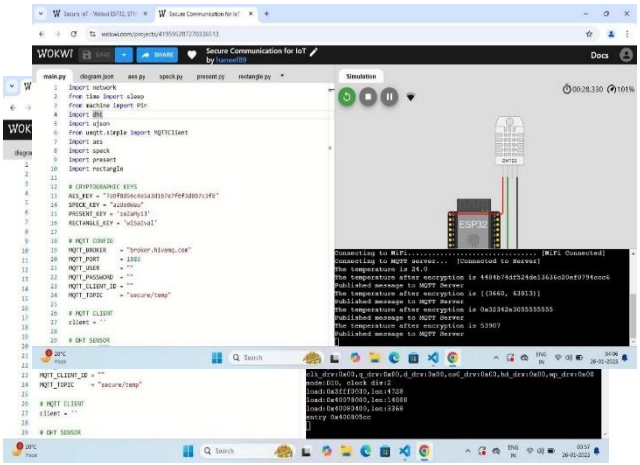
1. Data Encryption: IOT devices encrypt sensor data using lightweight cryptographic algorithms such as AES, PRESENT, SPECK, or RECTANGLE. These algorithms are chosen for their efficiency in resource-constrained environments.

2. Data Transmission: The encrypted data is published to an MQTT broker using the MQTT protocol. The publisher sends the data to the broker using a specific MQTT topic.

3. Data Reception: The subscriber receives the encrypted data from the MQTT broker and decrypts it using the same lightweight cryptographic algorithm.

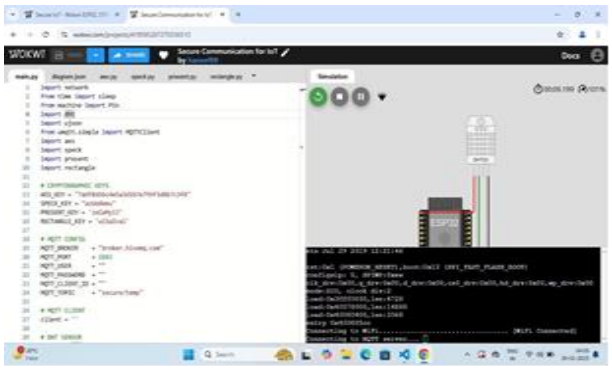
4. Data Storage: The decrypted data is used by the subscriber application and stored in a MySQL database for further processing or analysis.

Power System Technology
ISSN:1000-3673
Received: 16-04-2025 Revised: 05-05-2025 Accepted: 22-07-2025

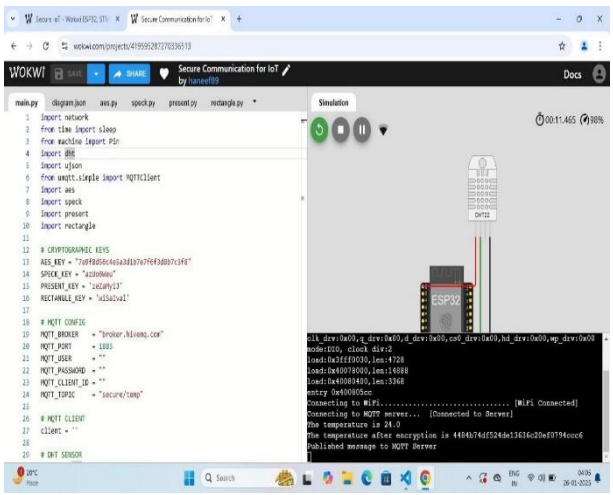


V. EXPERIMENTAL RESULT

Fig(a): Run IOT Device on Wokwi Simulator

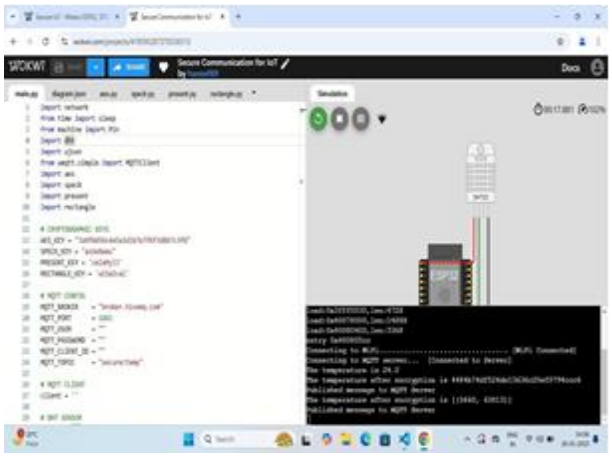


Fig(b): IOT device connected to Wi-Fi and MQTT server

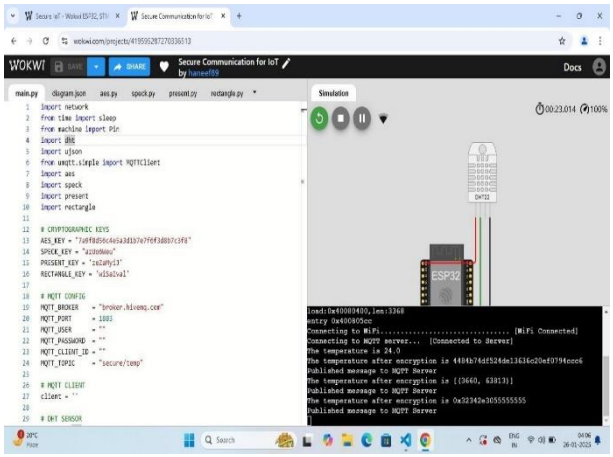


Fig(c): Encryption using Lightweight AES Algorithm.

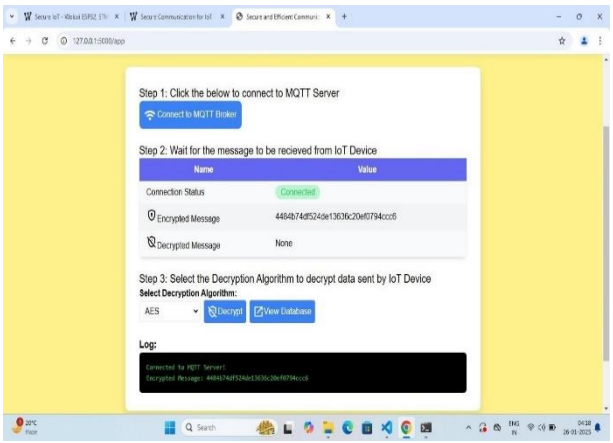
Power System Technology
ISSN:1000-3673
Received: 16-04-2025 Revised: 05-05-2025 Accepted: 22-07-2025



Fig(d): Encryption using SPECK Algorithm.

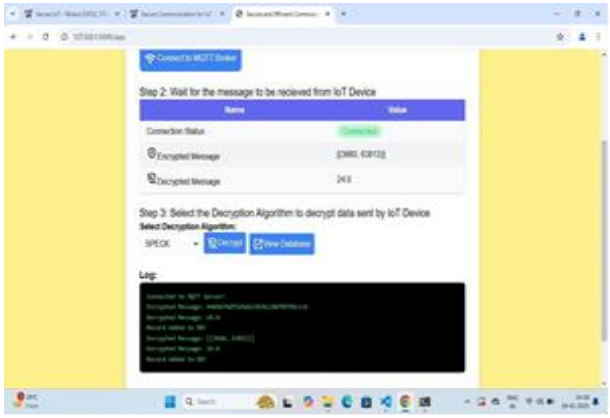


Fig(e): Encryption using PRESENT Algorithm

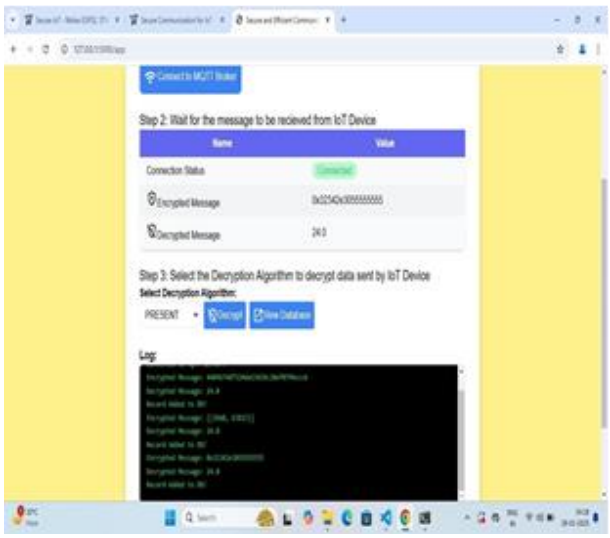


Fig(f): Encryption using RECTANGLE Algorithm.

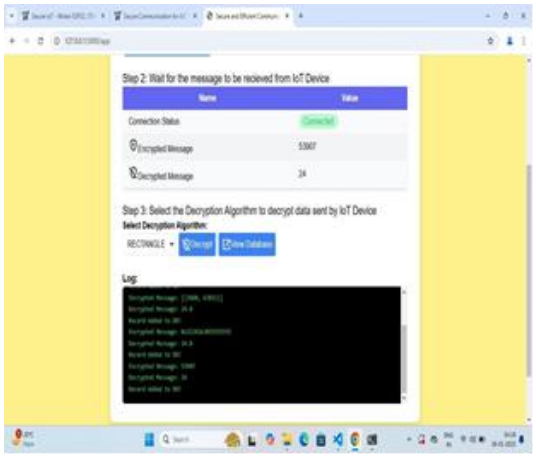
Power System Technology
ISSN:1000-3673
Received: 16-04-2025 Revised: 05-05-2025 Accepted: 22-07-2025



Fig(i): Decryption using SPECK Algorithm

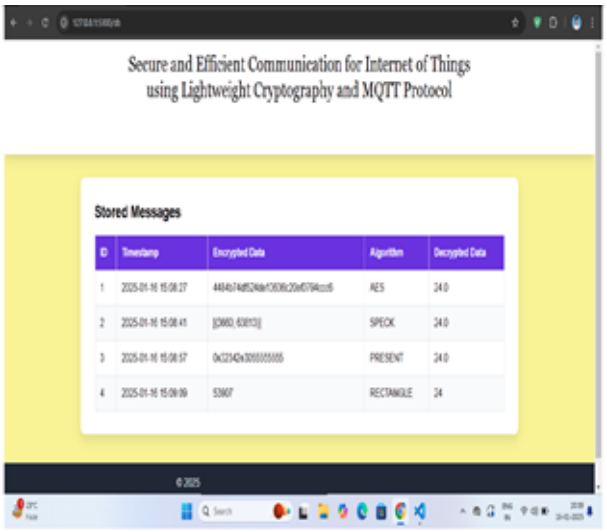


Fig(j): Decryption using PRESENT Algorithm



Fig(k): Decryption using RECTANGLE Algorithm

Power System Technology
ISSN:1000-3673
Received: 16-04-2025 Revised: 05-05-2025 Accepted: 22-07-2025



Fig(l) Messages stored in DB with timestamp.

Table 1: Performance Analysis of Lightweight Cryptographic Algorithms

Algorithm	Confidentiality and Integrity	Computational Requirements	Memory Requirements	Suitable for IoT Environments
Lightweight AES	High	Moderate	Moderate	Suitable
PRESENT	High	Low	Low	Highly Suitable
SPECK	High	Low	Low	Highly Suitable
RECTANGLE	High	Low	Low	Highly Suitable

AES: While AES provides strong security, its moderate computational and memory requirements make it suitable for IoT devices with slightly higher resources.

PRESENT, RECTANGLE, and SPECK: These algorithms excel in resource-constrained environments due to their low computational and memory requirements, making them highly suitable for IoT applications.

Power System Technology
ISSN:1000-3673
Received: 16-04-2025 Revised: 05-05-2025 Accepted: 22-07-2025

Table 2: Simulation Results and Protocol Efficiency of Proposed Approach

Metric	Proposed Approach	Advantage
Computational Overhead	Minimal	Efficient for resource-constrained IoT devices.
Memory Usage	Low	Supports lightweight IoT devices with limited memory.
Protocol Overhead	Minimal	Reduced overhead due to the lightweight nature of MQTT.
Communication Security	High	Ensures confidentiality and integrity of data.
Overall Efficiency	Secure and efficient system	Provides a balanced solution for secure and efficient communication in IoT.

VI. CONCLUSION

In this project, The Internet of Things (IOT) connects various devices, improving efficiency in healthcare, transportation, agriculture, and manufacturing. Smart homes and wearable devices automate daily tasks and monitor health, respectively. Despite its benefits, IOT faces security challenges due to limited device resources, making them vulnerable to attacks. Traditional security methods aren't suitable for IOT. The project suggests using lightweight cryptographic algorithms with the MQTT protocol to secure data without overloading resources. This approach enhances IOT security and performance, facilitating the adoption of IOT technologies while promoting a secure environment for future growth.

VII.REFERENCES:

[1] X. Li, M. Wang, H. Wang, Y. Yu and C. Qian, "Toward Secure and Efficient Communication for the Internet of Things," in IEEE/ACM Transactions on Networking, vol. 27, no. 2, pp. 621-634, April 2019.

[2] El-hajj, M., Mousawi, H., & Fadlallah, A. (2023). Analysis of Lightweight Cryptographic Algorithms on IOT Hardware Platform. Future Internet, 15(2), 54

[3] Yarali, Abdulrahman, Manu Srinath, and Randal G. Joyce. "A Study of Various Network Security Challenges in the Internet of Things (IOT)." (2018).

[4] Sri Ramya Siraparapu, S.M.A.K. Azad, Securing the IOT Landscape: A Comprehensive Review of Secure Systems in the Digital Era, e-Prime - Advances in Electrical Engineering, Electronics and Energy, Volume 10, 2024, 100798, ISSN 2772-6711.

Power System Technology
ISSN:1000-3673
Received: 16-04-2025 Revised: 05-05-2025 Accepted: 22-07-2025

[5] Ch. Jnana Ramakrishna, D. Bharath Kalyan Reddy, B.K Priya, P.P Amritha, K.V Lakshmy, Analysis of Lightweight Cryptographic Algorithms for IOT Gateways, Procedia Computer Science, Volume 233, 2024, Pages 235-242,
[6] Radhakrishnan, I., Jadon, S., & Honnavalli, P. B. (2024). Efficiency and Security Evaluation of Lightweight Cryptographic Algorithms for Resource- Constrained IOT Devices. Sensors, 24(12), 4008.
[7] O. Sadio, I. Ngom and C. Lishou, "Lightweight Security Scheme for MQTT/MQTT-SN Protocol.
[8] Thakor, V. A., Razzaque, M. A., & Khandaker, M. R. A. (2020, June 24). Lightweight Cryptography for IOT: A State-of-the-Art. arXiv.org.
[9] [10] Sleem, Lama & Couturier, Raphaël. (2021). Speck-R: An ultra light-weight cryptographic scheme for Internet of Things. Multimedia Tools and Applications
[10] A. Baneasa, R. Donca, S. Besoiu and D. Buleandra, "Lightweight Implementation of the AES Encryption Algorithm for IOT Applications Constrained by Memory and Processing Power," 2024 IEEE International Conference on Automation, Quality and Testing, Robotics (AQTR), Cluj- Napoca, Romania, 2024.
[11] [11] A. A. Zakaria, A. H. Azni, F. Ridzuan, N. H. Zakaria and M. Daud, "Extended RECTANGLE Algorithm Using 3D Bit Rotation to Propose a New Lightweight Block Cipher for IOT," in IEEE Access
[12] A. Mhaouch, W. Elhamzi, A. B. Abdelali and M. Atri, "Efficient Serial Architecture for PRESENT Block Cipher," 2022 IEEE 9th International Conference on Sciences of Electronics, Technologies of Information and Telecommunications (SETIT), Hammamet, Tunisia, 2022.
[13] Y. S. Vaz, J. C. B. Mattos and R. I. Soares, "Improving an Ultra Lightweight AES for IOT Applications," 2023 IEEE 9th World Forum on Internet of Things (WF-IOT), Aveiro, Portugal, 2023, pp. 01-06, doi: 10.1109/WF- IOT58464.2023.10539597.
[14] Gharat, N.N., Jolly, L. (2024). Hybrid Lightweight Cryptography Using AES and ECC for IOT Security. In: Roy, N.R., Tanwar, S., Batra, U. (eds) Cyber Security and Digital Forensics. REDCYSEC 2023. Lecture Notes in Networks and Systems, vol 896. Springer, Singapore. doi: 10.1007/978-981-99-9811- 1_19.
[15] B. Ray, S. Douglas, J. Smith, and others, “The SIMON and SPECK lightweight block ciphers,” in Proceedings of the 52nd Annual Design Automation Conference, 2015, p. 175.
[16] Alex Biryukov and Léo Paul Perrin. State of the art in lightweight symmetric cryptography 2017.
[17] George Hatzivasilis and others, A review of lightweight block ciphers. Journal of Cryptographic Engineering, 8(2):141–184, 2018.

Power System Technology
ISSN:1000-3673
Received: 16-04-2025 Revised: 05-05-2025 Accepted: 22-07-2025

[18] F. Medeleanu, C. Racuciu and M. Rogobete, "Considerations about the possibilities to improve AES S-box cryptographic properties by multiplication", Proceedings of the Romanian Academy - Series A: Mathematics Physics Technical Sciences Information Science, vol. 16, pp. 339-344, 2015.

[19] H. Mohammad and A. Abdullah, "Enhancement process of AES: a lightweight cryptography algorithm-AES for constrained devices", TELKOMNIKA, no. 20, pp. 551-56.