e-ISSN: 2582-5208
International Research Journal of Modernization in Engineering Technology and Science
(Peer-Reviewed, Open Access, Fully Refereed International Journal)
Volume:07/Issue:02/February-2025 Impact Factor- 8.187 www.irjmets.com

SECURE AND EFFICIENT IOT COMMUNICATION USING LIGHTWEIGHT CRYPTOGRAPHY IN MQTT NETWORKS

Shaik Mahammed Haneef*[1], Dr. C. Venkata Subbaiah*[2]

*[1]PG Scholar, Department Of Computer Science And Engineering, Annamacharya Institute Of Technology And Sciences, Kadapa, A.P., India.

*[2]Associate Professor & HOD, Department Of Computer Science And Engineering, Annamacharya Institute Of Technology And Sciences, Kadapa, A.P., India.

DOI : https://www.doi.org/10.56726/IRJMETS67176

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 paper introduces 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.

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

I. 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 cyber threats. 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.

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 REVIEW

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].
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].
6. **Radhakrishnan, Jadon, and Honnavalli (2024)** evaluated the efficiency and security of lightweight cryptographic algorithms for IoT devices in their article in Sensors. They identified vulnerabilities such as susceptibility to differential and linear cryptanalysis and stressed the need for integrating these algorithms with IoT communication protocols to enhance overall security [6].
7. **O. Sadio, I. Ngom, and C. Lishou** proposed a lightweight security scheme for MQTT/MQTT-SN protocols. Their work focused on optimizing these protocols for resource-constrained IoT environments but lacked real-world testing and integration with cryptographic algorithms. This gap highlights the need for practical implementations in dynamic IoT settings [7].
8. **Thakor, Razzaque, and Khandaker (2020)** reviewed over 50 lightweight cryptographic algorithms for IoT in their study published on arXiv.org. They categorized these algorithms based on their structures, such as SPN, Feistel Network, and ARX, and highlighted their low memory usage and energy efficiency. However, their study did not explore the integration of these algorithms with IoT communication protocols [8].
9. **A. Baneasa et al. (2024)** proposed a lightweight implementation of the AES encryption algorithm for IoT applications in their paper presented at the IEEE International Conference on Automation, Quality and Testing, Robotics (AQTR). Their work demonstrated the feasibility of using AES in memory- and processing-power-constrained environments, contributing to the development of efficient IoT security solutions [9].
10. **Sleem and Couturier (2021)** introduced Speck-R, an ultra-lightweight cryptographic scheme for IoT, in their article in Multimedia Tools and Applications. They demonstrated its effectiveness in securing IoT communications while minimizing resource usage, making it a promising solution for resource-constrained devices [10].
11. **A. A. Zakaria et al.** proposed an extended RECTANGLE algorithm using 3D bit rotation for IoT in their study published in IEEE Access. Their work introduced a new lightweight block cipher designed to enhance security without compromising performance, addressing the unique challenges of IoT environments [11].
12. **A. Mhaouch et al. (2022)** presented an efficient serial architecture for the PRESENT block cipher in their paper at the IEEE International Conference on Sciences of Electronics, Technologies of Information and Telecommunications (SETIT). Their work focused on optimizing the PRESENT algorithm for IoT applications, highlighting its potential for secure and efficient data encryption [12].

III. METHODOLOGY

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.

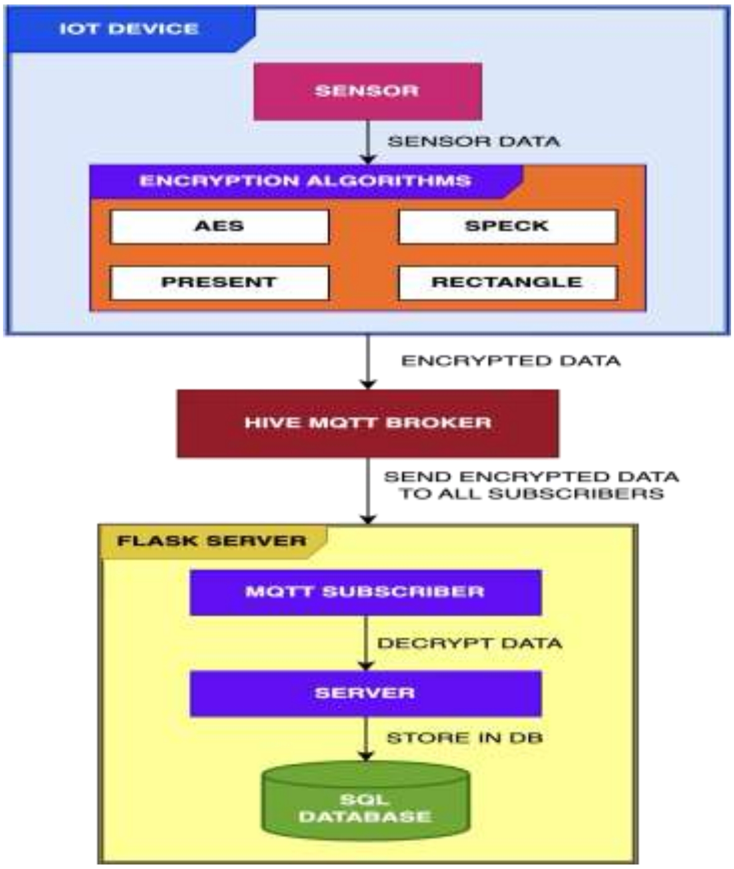


Figure 1: System Architecture

Lightweight Cryptographic Algorithms

The following lightweight cryptographic algorithms are discussed in this paper:

Lightweight Advanced Encryption Standard (AES)

AES is a symmetric-key algorithm widely used for encryption and decryption. It supports key lengths of 128-bit, 192-bit, and 256-bit. The lightweight variant of AES is particularly suitable for IoT applications due to its balance of security and performance.

PRESENT

PRESENT is a lightweight block cipher with a 31-round Substitution-Permutation Network structure. It supports key lengths of 80-bit or 128-bit and is efficient in hardware-constrained environments.

SPECK

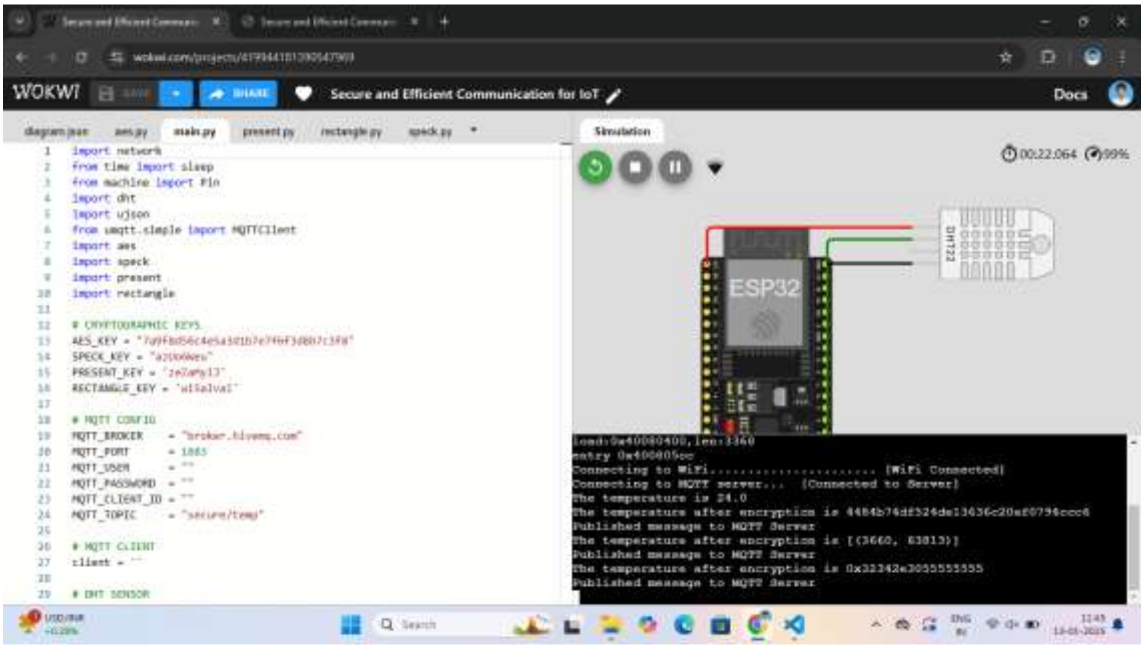
SPECK is a lightweight block cipher that uses a Feistel network structure. It supports various block sizes and key lengths and is efficient in both hardware and software environments.

RECTANGLE

RECTANGLE is a lightweight block cipher with a 25-round Substitution-Permutation Network structure. It supports key lengths of 80-bit or 128-bit and is designed for resource-constrained environments.

IV. RESULTS

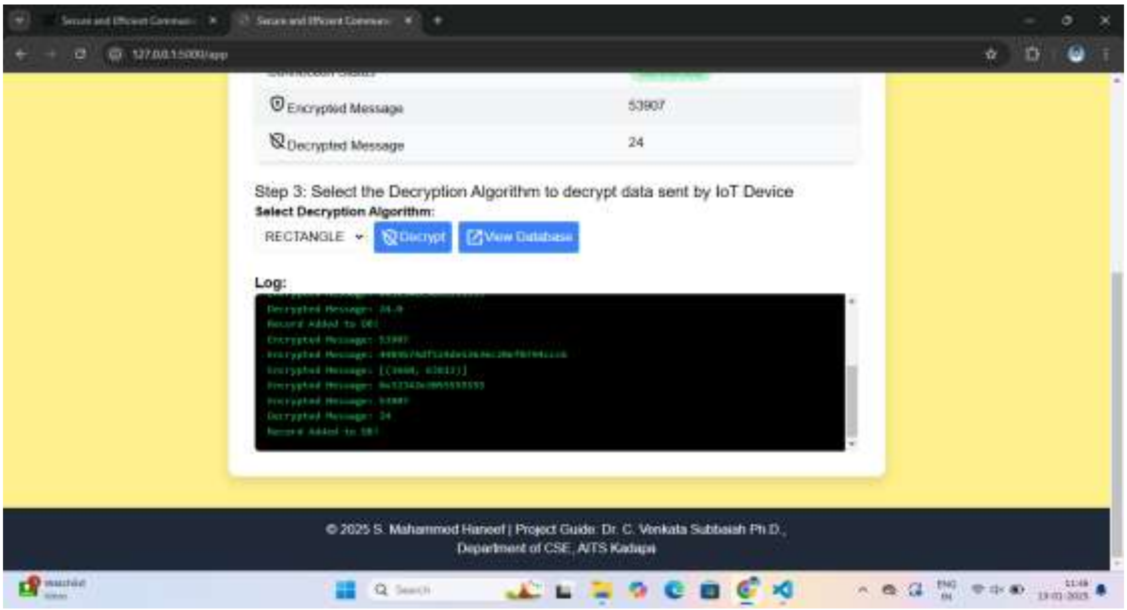
Simulation results demonstrate that the proposed approach provides secure and efficient communication for IoT systems while imposing minimal overhead on the devices. Below is a detailed analysis of the performance of the lightweight cryptographic algorithms and the overall efficiency of the proposed approach.



```
import network
from time import sleep
from machine import Pin
import dht
import ujson
from umqtt.simple import MQTTClient
import aes
import speck
import present
import rectangle

# CRYPTOGRAPHIC KEYS
AES_KEY = "7a9f8d56c4e5a3d1b7e7f6f3d8b7c3f8"
SPECK_KEY = "a2Uk6Wev"
PRESENT_KEY = 'ze7amy13'
RECTANGLE_KEY = 'wl5alval'

# MQTT CONFIG
MQTT_BROKER    = "broker.hivemq.com"
MQTT_PORT      = 1883
MQTT_USER      = ""
MQTT_PASSWORD  = ""
MQTT_CLIENT_ID = ""
MQTT_TOPIC     = "secure/temp"

# MQTT CLIENT
client = ""

# DHT SENSOR
```

```
load:0x40080400,len:3460
entry 0x400805cc
Connecting to WiFi......................... [WiFi Connected]
Connecting to MQTT server...  [Connected to Server]
The temperature is 24.0
The temperature after encryption is 4484b74df524de13636c20af0794ccc6
Published message to MQTT Server
The temperature after encryption is [(3660, 63813)]
Published message to MQTT Server
The temperature after encryption is 0x32342e3055555555
Published message to MQTT Server
```

Figure 2: The ESP 32 MQTT Publisher is sending encrypted data to the MQTT Broker.



Encrypted Message	53907
Decrypted Message	24

Step 3: Select the Decryption Algorithm to decrypt data sent by IoT Device

Select Decryption Algorithm: RECTANGLE

Log:

```
Decrypted Message: 24.0
Record Added to DB!
Encrypted Message: 53907
Encrypted Message: 4484b74df524de13636c20af0794ccc6
Encrypted Message: [(3660, 63813)]
Encrypted Message: 0x32342e3055555555
Encrypted Message: 53907
Decrypted Message: 24
Record Added to DB!
```

© 2025 S. Mahammed Haneef | Project Guide: Dr. C. Venkata Subbaiah Ph.D.,
Department of CSE, AITS Kadapa

Figure 3: After receiving data, the Flask Server (MQTT Subscriber) decrypts it and stores it in the database.

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.

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.

V. CONCLUSION

In conclusion, the proposed system combines lightweight cryptographic algorithms such as AES, PRESENT, SPECK, and RECTANGLE with the MQTT protocol to address the security and performance challenges of IoT systems. This approach ensures efficient encryption, secure data transmission, and reliable storage, making it well-suited for resource-constrained environments. The methodology provides a robust framework for enhancing IoT security without compromising system performance.

VI. 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.

[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, ISSN 1877-0509.

[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] 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.

[10] Sleem, Lama & Couturier, Raphaël. (2021). Speck-R: An ultra light-weight cryptographic scheme for Internet of Things. Multimedia Tools and Applications.

[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.