International Journal of
INTELLIGENT SYSTEMS AND APPLICATIONS IN ENGINEERING
ISSN:2147-6799 www.ijisae.org Original Research Paper

A Novel Lightweight Algorithm for IoT Data in Cold Chain Applications

Divya James[1], T. K. S. Lakshmi Priya[2], Yaseen Mohemed[3]

Submitted: 05/12/2023 **Revised**: 14/01/2024 **Accepted**: 28/01/2024

Abstract: Supply Chain Management (SCM) involves the coordination and management of various interconnected activities and processes across different organizations and functions within a supply chain. Effective supply chain management activities depend on extensive data handling, continuous tracking and monitoring, and reliable business transactions. There are several fundamental issues in supply chain management, particularly in temperature-controlled supply chains or "cold chain networks." Environment-related factors like temperature and humidity levels can have an impact on the supply chain's operational or business environment. The integrity and auditability of the supply chain may be impacted by security risks in the cold chain network. For cold-chain applications, our suggested architecture offers data in real-time gathering at the user-end, and secure communications. To address the concern of secure transactions within the supply chain management entities, our proposed architecture employs a novel dynamic key dependent cryptographic algorithm. The integrity of the sensor data gathered by the IoT devices are guaranteed by this method. By using cryptographic techniques, the architecture provides a secure and tamper-resistant communication channel for transmitting the sensor data to the cloud. Encryption of IoT data using these algorithms can contribute to the secure transmission of data of cold chain applications. The performance analysis has been done on average encryption time, decryption time, throughput, and memory consumption.

Keywords: *Lightweight Cryptography, Dynamic S-Box, IoT, Security, ColdChain*

1. Introduction

Supply chain management (SCM) encompasses the activities involved in the movement and management of materials, products, and information throughout the entire supply chain network. Key components and activities involved in supply chain management include Planning, Sourcing, Production, Transportation, Warehousing, Inventory management, Distribution, Information systems, Risk management and Collaboration and communication. SCM has become increasingly important in today's global environment. Effective supply chain management can result in improved efficiency, faster time-to-market, increased profitability, and greater resilience in the face of disruptions.

Supply chain management (SCM) encompasses various activities and processes that can have environmental impacts throughout the entire supply chain. Temperature and humidity have significant effects on supply chain management, particularly in industries where temperature-sensitive or humidity-sensitive products are involved. Monitoring temperature and humidity conditions throughout the supply chain is essential for maintaining product quality and ensuring compliance with regulations. Supply chain managers need to implement robust monitoring systems to track temperature and humidity levels at various stages, such as production, warehousing, and transportation. Real-time data monitoring and alert systems enable quick response to any deviations, allowing proactive measures to be taken, such as adjusting storage conditions or rerouting shipments to avoid unfavorable environmental conditions.

With the increasing reliance on digital systems and interconnected networks, data breaches have become a significant concern. Breaches in supply chain management systems can result in the theft of sensitive information.Conventional cryptography and lightweight cryptography are two approaches for securing information and communications, but they differ in terms of their design principles and target applications. Conventional cryptographic algorithms typically use larger key sizes and require significant computational resources, such as processing power and memory. They are often implemented on devices with sufficient resources, such as desktop computers, servers, or high-end mobile devices. Lightweight cryptography is specifically designed for Internet of Things (IoT) devices, and low-power microcontrollers. Its primary focus is on providing efficient and lightweight cryptographic solutions with a smaller code size, reduced memory requirement, and lower energy consumption. Fixed or static S-Box can enable attackers in exploring S-Box and identifying any

[1] *Assistant Professor, Department of Information Technology, Rajagiri School of Engineering & Technology, Kochi, Kerala, India*
ORCID ID: 0000-0003-3283-9049
[2] *Adjunct faculty, Sardar Vallabhbhai Patel international school of textiles and management Coimbatore, Tamil Nadu, India.*
ORCID ID: 0000-0002-0667-2292
[3] *Department of Information Technology, Rajagiri School of Engineering & Technology, Kochi, Kerala, India*
** Corresponding Author Email: divyaj@rajagiritech.edu.in*

weakness. Here, a non-linear S-Box is generated which can be used to develop a newly defined dynamic key dependent algorithm for securing communications between IoT devices and platforms for any cold chain application.

Section 2 deals with the relevant work of lightweight cryptographic algorithm and its limitations. Section 3 elucidates this proposed algorithm. Section 4 highlights implementation and performance analyses of proposed algorithm and Section 5, concludes the paper.

2. Related Work

Supply Chain Management [1][2] may be defined as the process by which how a product from one end reaches the other end. The temperature-controlled supply chain system, referred to as the Cold Chain[3]. Information security risks and environmental impact has been common in supply chain sector which can in turn affect the supply chain performance [4]. Both the risks can be eliminated using IoT's [5] in cold chain sector. Security is one of the major concerns in IoT. Lightweight encryption algorithms (LWC) are considered which provides efficient encryption systems for resource constrained devices [6].

Simon and Speck [7] are families of lightweight block ciphers developed by National Security Agency (NSA). Simon uses block sizes of 32, 48, 64, 96, and 128 bits, while Speck uses block sizes of 32, 48, 64, 96, and 128 bits as well. PRESENT [8] is a simple block cipher operating on 64-bit blocks and allows keys having 80 or 128 bits in length. It is designed for efficient implementations at hardware level and is widely used in applications where resource-constrained devices are involved. KATAN and KTANTAN [9] are lightweight block ciphers that balance the security and efficiency aspects and are suitable for lightweight applications and constrained environments. Chaskey[10] is a lightweight message authentication code (MAC) algorithm designed for efficient implementation on devices with less resources, like low-power microcontrollers. It provides authentication and integrity for data without requiring heavy computational resources.

A low-energy block cipher called GIFT[11] is compact and lightweight. It uses 64-bit blocks for operation and accepts keys with lengths of 128, 192, and 256 bits. GIFT seeks to strike a balance between energy efficiency and security.

A collection of simple block ciphers called SKINNY[12] is geared at effective implementations and resistance to a range of assaults, like differential and linear cryptanalysis. It accepts sizes of 64, 128, and 256 bits and operates on block sizes of 64 and 128 bits. In contexts with limited resources, the lightweight block cipher, RECTANGLE[13] provides high performance and security. It supports keys with sizes of 80, 128, or 160 bits and 64-bit blocks. RECTANGLE is made to offer a nice balance between security and productivity. The MIDORI[14] family of lightweight block ciphers includes the MIDORI64 and MIDORI128 versions. These ciphers seek to offer compact implementations with a high degree of security. A simple block cipher called PRINCE[15] allows key sizes of 64 or 128 bits and operates on blocks of 64 bits. It is made with a high level of security in mind, but is also intended to be effective in hardware and software implementations.

A flexible block cipher and a cryptographic hash function are combined in the lightweight authenticated encryption scheme PRIDE[16]. It is made to provide authenticity, integrity, and confidentiality in contexts with limited resources. Sony Corporation created CLEFIA[17], a simple block cipher. It accepts key sizes of 128, 192, or 256 bits and operates on 128-bit blocks. On many platforms, CLEFIA is built to offer security while keeping great efficiency. TWINE[18] is a simple block cipher that seeks to offer effective implementations on devices with limited resources. In addition to key sizes of 80, 128, or 160 bits, it offers block sizes of 64 and 128 bits. TWINE is renowned for its ease of use and small memory footprint. A block cipher that accepts 64-bit blocks and operates on keys up to 128 bits in size is called HIGHT[19]. In addition to offering security appropriate for lightweight applications, it is created to be extremely efficient in hardware and software implementations. FEW [20] is a lightweight encryption algorithm specifically designed for wireless sensor networks. It focuses on efficiency and low resource consumption, making it suitable for energy-constrained devices. FEW provides both encryption and authentication functionalities.

It's crucial to keep in mind that the usefulness of these simple algorithms depends on the demands and limitations of the application. Before choosing a lightweight algorithm, it's recommended to assess its security features, performance characteristics, and any available analyses or evaluations.

Static S-boxes are fixed, pre-defined substitution tables that do not change during the encryption or decryption process. However, static S-Boxes are fixed in nature and vulnerable to attacks that need to be considered in the design of secure cryptographic systems. Therefore, the selection and design of S-boxes are crucial aspects of constructing a secure cryptographic algorithm for communication between the IoT devices and the web application.

3. Proposed Algorithm

The novel algorithm with Dynamic Key Dependent S-Box and flowchart description is given below:

A. *Proposed Algorithm*

Cryptographic Algorithm with Dynamic Key Dependent S-Box

Start

1. Read data
2. Let key = master key
3. Master Key, K = K =$K_{79,}$ K_{78} .....K_0
4. Import key, rounds, newly generated Dynamic Sbox from main function
5. i = 1
6. While i<rounds+1
    a. Rightshift key by 16 and append it to round keys
    [Round keys are K_i=K_{63},K_{62},..K_0=K_{79},K_{78}.....K_{16}]
    b. Let k be the last round key
    c. Let x=0, i=0
    d. Extract the 8,16, 24, 32, 40, 48, 56, 64 bits and store it in x as a 4-bit number that has bit 0 = (8th XOR 16th), bit 1 = (24th XOR 32nd), bit 2 = (40th XOR 48th), bit 3 = (56th XOR 64th)
    e. Store Sbox[x] in Sbox_temp
    f. Append Sbox_temp to Sbox_n
    g. For each round the key register is updated as follows:
        i. $[K_{79}K_{78}\ldots\ldots K_1K_0] = [K_{18}K_{17} \ldots\ldots\ldots K_{20}K_{19}]$
        ii. $[K_{79}K_{78}K_{77}K_{76}] = S[K_{79}K_{78}K_{77}K_{76}]$
        iii. $[K_{19}K_{18}K_{17}K_{16}K_{15}] = [K_{19}K_{18}K_{17}K_{16}K_{15}] \oplus round\_counter$
7. End Loop
8. Output round keys to main function
9. For each line, ti in data
    a. Append padding to ti and name it plain text
    b. Encrypt plain text, encrypted
    c. Output encrypted
    d. Decrypt it and output
    e. Remove padding

Stop

The key components and steps in the algorithm are:

B. *Flowchart*

Figure1 depicts the overall workflow of this proposed algorithm.

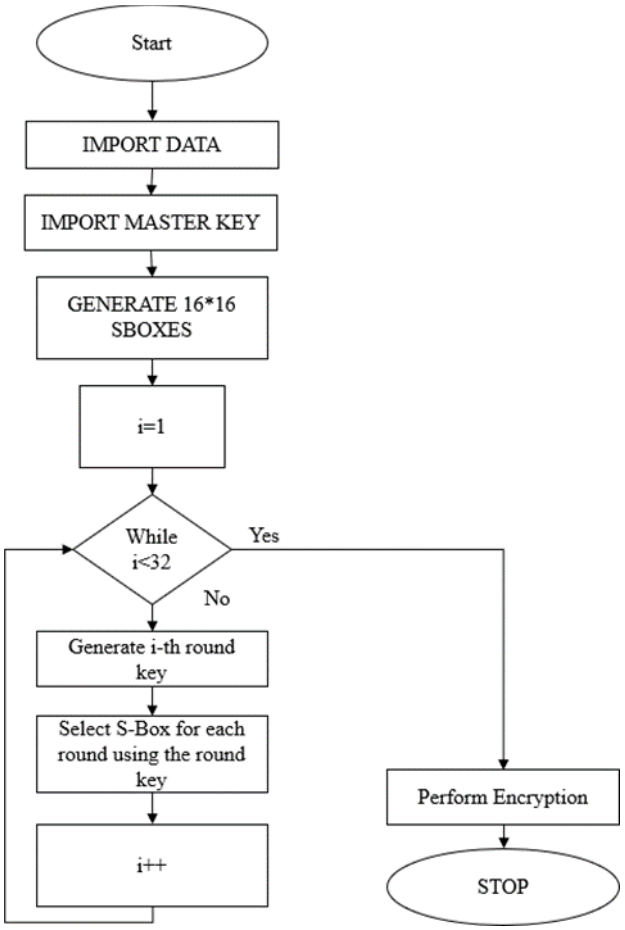

Fig. 1. FlowChart

Initially the data and master key has been imported. Using one dimensional logistic chaotic map a 16*16 S-Box is generated. Selecting S-Box for every round of the algorithm depends on a dynamic basis,using the round key generated. Finally, the encryption is performed.

4. Implementation & Performance Evaluation

The proposed system can be used to secure data for cold chain applications. Figure 2 and Figure 3 shows the encryption and decryption at raspberry pi and node.js server.

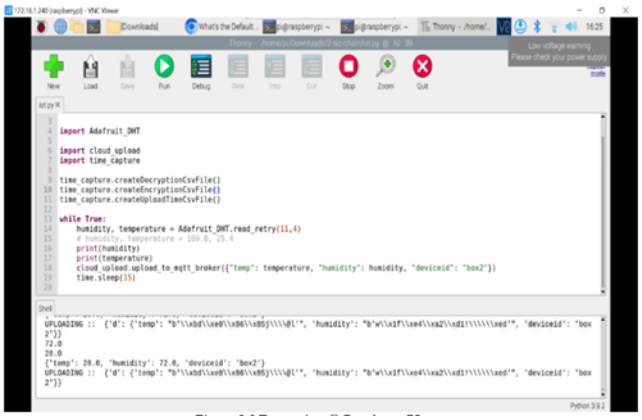

Fig 2. Encryption @ Raspberry PI

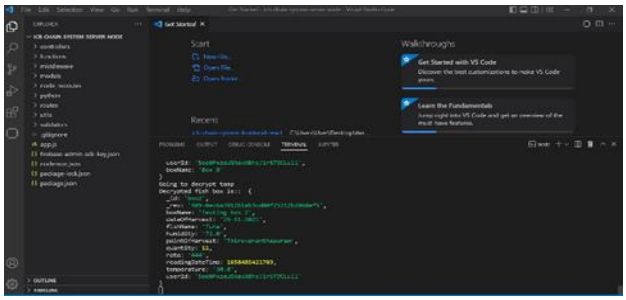

Fig 3. Decryption @ Node.js Server

The temperature and humidity values along with the device ID is fetched. The values are encrypted and uploaded to cloud via MQTT broker. These values are decrypted in Node.js server. Once decrypted, the values are shown in the dashboard of the web application. The temperature, humidity values along with the current location using GPS module helps to track and monitor the spoilage of food kept in primary, secondary, and tertiary packages.

The performance analysis has been done on encryption time, decryption time and throughput.

The length of time it takes an encryption algorithm for conversion of plain text into cipher text is termed the encryption time. The throughput of an encryption technique explains the encryption's speed and computed as follows:

Throughput= No of bytes/Encryption Time

The unit of throughput is bytes/second. The details of the original and proposed algorithms are shown in Figures 4, 5, 6, and 7.

Both algorithms are evaluated based on average encryption time, throughput and average decryption time. Table1 explains memory consumption of original and proposed algorithms. The graphical representation of the above are shown below:

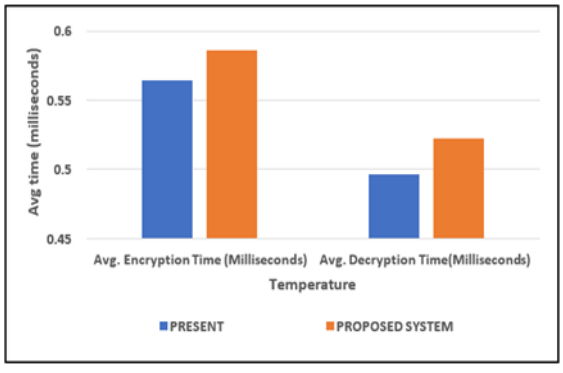

Fig 4. Average Encryption/Decryption Throughput for Temperature

The average encryption and decryption throughput for temperature and humidity parameters does not vary much for the original and proposed algorithms.

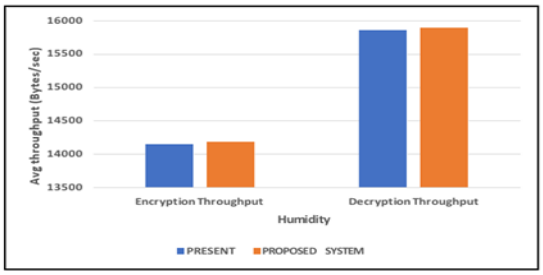

Fig 5. Average Encryption/Decryption Throughput for Humidity

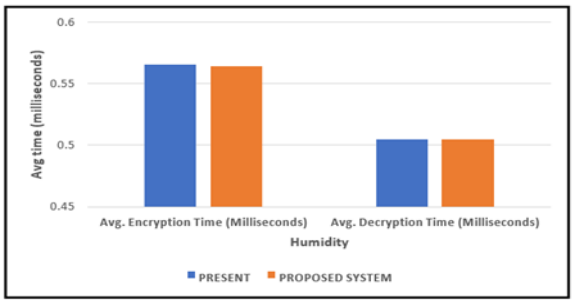

Fig 6. Average Encryption/Decryption Time for Humidity

The average encryption and decryption time for temperature and humidity parameters for the original and proposed algorithms has negligible differences. The same is applicable for RAM consumption as depicted in Table.1.

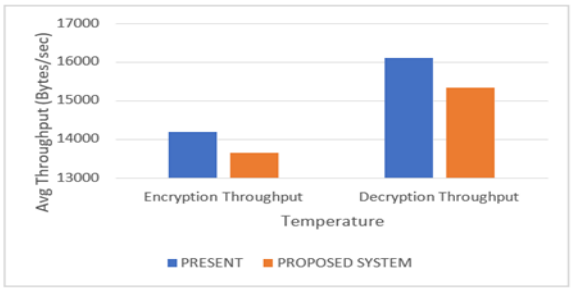

Fig 7. Average Encryption/Decryption Time for Temperature

Table 1. Memory Consumption

ALGORITHMS	Memory Consumption (Kilobytes)
PRESENT	9.64
PROPOSED SYSTEM	10.12

5. Conclusion

Security is a crucial concern in today's world, especially when it comes to digital data sharing. With the increasing reliance on technology and the interconnectedness of systems, protecting data from various attacks has become

paramount. Cold chain organizations strive to enhance security measures to safeguard sensitive information and maintain the integrity, confidentiality, and data availability. So, a lightweight dynamic key dependent algorithm is proposed for securing communications between IoT devices and platforms for any cold chain application. Experimental reading has been taken for multiple trails and worked on performance analysis of this proposed algorithm. The algorithm outperforms better than other lightweight algorithms.

References

[1] G. Richey, A. S. Roath, F. G. Adams, and A. Wieland, "A Responsiveness View of logistics and supply chain management," *J. Bus. Logist.*, 2021.

[2] H. Birkel and J. M. Müller, "Potentials of industry 4.0 for supply chain management within the triple bottom line of sustainability – A systematic literature review," *J. Clean. Prod.*, vol. 289, no. 125612, p. 125612, 2021

[3] S. Mercier, M. Mondor, U. McCarthy, S. Villeneuve, G. Alvarez, and I. Uysal, "Optimized cold chain to save food," in *Saving Food*, Elsevier, 2019, pp. 203–226.

[4] Yudi Fernando, Ming-Lang Tseng, Ika Sari Wahyuni-Td, Ana Beatriz Lopes de Sousa Jabbour, Charbel Jose Chiappetta Jabbour & Cyril Foropon (2023) Cyber supply chain risk management and performance in industry 4.0 era: information system security practices in Malaysia, Journal of Industrial and Production Engineering, 40:2, 102-116.

[5] Gillespie, J., da Costa, T. P., Cama-Moncunill, X., Cadden, T., Condell, J., Cowderoy, T., ... & Ramanathan, R. (2023). Real-Time Anomaly Detection in Cold Chain Transportation Using IoT Technology. Sustainability, 15(3), 2255.

[6] V. A. Thakor, M. A. Razzaque and M. R. A. Khandaker, "Lightweight Cryptography Algorithms for Resource-Constrained IoT Devices: A Review, Comparison and Research Opportunities," in *IEEE Access*, vol. 9, pp. 28177-28193, 2021.

[7] Dwivedi, A. D., & Srivastava, G. (2023). Security analysis of lightweight IoT encryption algorithms: SIMON and SIMECK. *Internet of Things*, 100677.

[8] Muhalhal, L. A., & Alshawi, I. S. (2023). A hybrid modified lightweight algorithm for achieving data integrity and confidentiality. *International Journal of Electrical and Computer Engineering (IJECE)*, *13*(1), 833-841.

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

[10] To'xtajon, Q. (2023). LIGHTWEIGHT CRYPTOGRAPHY IN IOT NETWORKS. Innovations in Technology and Science Education, 2(10), 999-1007.

[11] Lara-Nino, C. A., Diaz-Perez, A., & Morales-Sandoval, M. (2018, October). Fpga-based assessment of midori and gift lightweight block ciphers. In *Information and Communications Security: 20th International Conference, ICICS 2018, Lille, France, October 29-31, 2018, Proceedings* (pp. 745-755). Cham: Springer International Publishing.

[12] Xiao, L., Xu, H., Zhu, F., Wang, R., & Li, P. (2020). SKINNY-based RFID lightweight authentication protocol. *Sensors*, *20*(5), 1366.

[13] Zhang, W., Bao, Z., Lin, D., Rijmen, V., Yang, B., & Verbauwhede, I. (2014). RECTANGLE: a bit-slice lightweight block cipher suitable for multiple platforms. Cryptology ePrint Archive.

[14] Mishra, R., Okade, M., & Mahapatra, K. (2023). Novel substitution box architectural synthesis for lightweight block ciphers. IEEE Embedded Systems Letters.

[15] Kumar, A., Singh, P., Patro, K. A. K., & Acharya, B. (2023). High-throughput and area-efficient architectures for image encryption using PRINCE cipher. *Integration*, *90*, 224-235.

[16] Chauhan, J. A., Patel, A. R., Parikh, S., & Modi, N. (2022, November). An Analysis of Lightweight Cryptographic Algorithms for IoT-Applications. In International Conference on Advancements in Smart Computing and Information Security (pp. 201-216). Cham: Springer Nature Switzerland.

[17] Saba, S. J., Al-Nuaimi, B. T., & Suhail, R. A. (2023, March). A review of traditional, lightweight and ultra-lightweight cryptography techniques for IoT security environment. In AIP Conference Proceedings (Vol. 2475, No. 1). AIP Publishing.

[18] Chatterjee, K., Chaudhary, R. R. K., & Singh, A. (2022). A lightweight block cipher technique for IoT based E-healthcare system security. Multimedia Tools and Applications, 1-30.

[19] Nayancy, Dutta, S., & Chakraborty, S. (2022). A survey on implementation of lightweight block ciphers for resource constraints devices. Journal of Discrete Mathematical Sciences and Cryptography, 25(5), 1377-1398.

[20] Xiao, H., Wang, L., & Chang, J. (2022). The differential fault analysis on block cipher FeW. Cybersecurity, 5(1), 28.