Research Article (Open Access)

Journal of Computer Science,
Engineering & Applied Mathematics (JCSEAM)
Peer Reviewed Refereed Open Access International Multidisciplinary Journal

Secure Data Transmission Using Cryptographic Algorithms in IoT Networks

Dr. Pinkey Chouhan[1]
[1]Assistant Professor, Department of Computer Science, The ICFAI University Raipur India
[1]pinkeychouhan@iuraipur.edu.in
Corresponding Author: pinkeychouhan@iuraipur.edu.in

Abstract

The high-rate growth of Internet of Things (IoT) devices highlighted the issue of secure transmission of data given rigid restrictions of energy, memory, and computational power. The overall goal of the study is to evaluate and review the existing cryptographic solutions in the context of IoT settings, and, specifically, lightweight security solutions that can be used in the limited devices. It is done in the methodological way of the systematic review and comparative analysis of symmetric, asymmetric, and hybrid cryptographic algorithms which include lightweight block ciphers, elliptic-curve-based algorithms and combined cryptography and steganography. Measures of performance like computational overhead, energy usage, latency, memory usage, and security level are analyzed in a wide variety of IoT application cases like wireless sensor networks and medical IoT systems. The comparison shows that the lightweight cryptography schemes are far more efficient than the traditional schemes with acceptable levels of security, which render them a good fit when high efficiency is required in an iaot node, e.g., in low-power nodes. Nevertheless, there are always trade-offs between the robustness of security and the use of resources and no single algorithm is optimal in all application cases. The introduction of such trends like encryption supported by hardware and smart, or adaptive security systems can be regarded as promising in overcoming these limitations. The research finds that the cryptographic methods of context-aware, hybrid, and scalable approaches ought to be employed as a fundamental component of the IoT security framework in the future in order to balance efficiency and security, and, thus, contribute to the improvement of the overall reliability and trustworthiness of the IoT based systems.

Keywords :

Internet of Things (IoT), Lightweight Cryptography, Data Security, Secure Data Transmission, Resource-Constrained Devices, Cryptographic Algorithms.

Received on 11 April 2025; **Revised on** 27 May 2025, **Accepted on** 05 August 2025; **Published on:** 6 Feb 2026
DOI:

1. Introduction

Internet of things (IoT) is one of the rapidly developed and formed pervasive computing paradigms that allow the seamless interconnectivity of the heterogeneous devices in the areas of healthcare, smart cities, industrial automation, and environmental monitoring [1]. These interdependent systems are frequent exporters of sensitive information across unprotected and frequently vulnerable communication links thus necessitating the security and privacy demands to critical design specifications [2]. Cryptographic algorithms continue to be the basis of safe ionot - communication through confidentiality, integrity, authentication, non-repudiation [3]. Nevertheless, traditional cryptographic tools are initially planned and constructed to work on systems with a lot of resources and in an IoT context they are not applicable to most devices because of their small processing power, memory, energy and storage capacity [4]. It has been due to this limitation that there has been increasing interest in lightweight cryptographic algorithms, which can deliver sufficient security but come with strict resource requirements [5].

Although there is a lot of research regarding IoT security, available literature has shown that there have been challenges and gaps. Most of the lightweight schemes are mainly aimed at minimizing the computational complexity, at the cost of scalability, adaptability, and resistance to new attacks [6]. The available comparative studies tend to be confined to particular hardware platforms or particular performance metrics and cannot be easily generalized to an IoT-wide situation [7]. Moreover, the recent developments that combine hybrid solutions, hardware-software implementations, and smart encryption systems presuppose the necessity of a unified and revised point of view [8]. In this regard, the aim of this paper is to conduct a systematic analysis of cryptographic algorithms in IoT focusing on lightweight algorithms, performance considerations, and applicability. The key contributions are as follows: (i) structured classification of cryptographic methods applied to IoT, (ii) comparative evaluation on the basis of the security strength and resource-efficiency, and (iii) the open challenges and research directions that will be used to facilitate the development of secure, scalable, and energy-efficient IoT systems.

2. Literature survey

Recent literature has delved into the cryptographic mechanisms specifically applied to IoT settings at length, focusing much on lightweight security as a result of IoT device limitations. There are a number of works that have assessed lightweight cryptographic algorithms in terms of their computational complexity, memory footprint and energy use, and conclude that they are suitable in sensor nodes and embedded IoT devices [9] [14] [16]. It has also been pointed out in comparative analyses that symmetric lightweight ciphers can achieve reduced latency and minimized energy consumption, although they can be difficult to scale and manage keys in large scale IoT networks [17] [18]. Other works have investigated the use of hybrid security schemes based on the combination of cryptography and steganography or optimization algorithms to improve the confidentiality and integrity of data, especially in high-stakes systems like the healthcare IoT [10] [11]. Lightweight models inspired by the elliptic curve as well as hardware-based implementations have also been explored to enhance performance without the need to raise the overhead of resources substantially [13] [15].

Regardless of these contributions, there are gaps in the research. Most of the existing literature is dedicated to either suggesting or assessing single algorithms as isolated units, and little is done to cross-test them with similar performance metrics or realistic deployment settings [21]. Other lightweight schemes are as efficient as evidenced by gain at the expense of smaller security margins, so they cannot withstand changing attack models [19]. Newer methods that incorporate the use of intelligent or machine-learning-based encryption exhibit possible flexibility, but they have not been fully venerated with regard to overhead and scalability [20]. Moreover, the evaluation platforms and benchmarking criteria differences do not support objective testing of algorithm appropriateness to various applications of the IoT. These restrictions are the reasons of the necessity of the current work that is supposed to offer a unified, critical, and recent overview of the cryptographic methods used in IoT, in terms of their performance security trade-offs, and future directions of creating adaptable and context-sensitive security models (for summary see table 1).

Table 1. Comparative summary of cryptographic approaches for secure data transmission in IoT

Ref.	Main Focus	Approach / Technique	Evaluation Aspects	Key Limitations / Gaps
[9]	Lightweight encryption for embedded IoT	Simple lightweight cryptographic algorithm	Complexity, memory usage	Limited security analysis against advanced attacks
[10]	Secure IoT data transfer	Combined cryptography and steganography	Confidentiality, robustness	Increased processing overhead
[11]	Secure medical IoT communication	Cryptography with memetic optimization	Security strength, transmission efficiency	Higher computational cost
[13]	IoT hardware security	Blowfish hardware implementation	Throughput, hardware efficiency	Not optimized for ultra-low-power nodes
[14]	Performance comparison of lightweight ciphers	Benchmark-based comparative analysis	Energy, latency, memory	Platform-dependent results
[15]	Low-complexity IoT encryption	Elliptic Galois Cryptography (EGCrypto)	Computational efficiency, security	Limited real-world deployment validation
[16]	Lightweight cryptography survey	Taxonomy and classification	Algorithm characteristics	Lacks unified benchmarking
[17]	Cryptographic algorithms for IoT	Survey of symmetric and asymmetric schemes	Suitability for IoT devices	Minimal performance comparison
[18]	Comparative cryptographic analysis	Cross-algorithm evaluation	Security vs. resource trade-offs	Narrow application scope
[19]	Lightweight IoT encryption	SIT encryption algorithm	Speed, low overhead	Reduced cryptographic strength
[20]	Intelligent IoT security	Machine learning–based encryption	Adaptability, security	Scalability and overhead concerns
[21]	Lightweight crypto on IoT hardware	Experimental hardware evaluation	Power and memory usage	Limited algorithm diversity

3. Materials and methods

3.1 Data Collection

The experiment uses publicly available standard cryptography test data and benchmark data widely accepted in the literature on IoT security. These datasets are simulations of sensor-generated stream data as is common with the use of the IoT like environmental monitoring and healthcare. Input data consist of structured numerical values and byte streams with varying sizes to evaluate encryption overhead under realistic conditions.

To be proven experimentally, the sensor data samples have been collected at the UCI Machine Learning Repository - Sensor Data Stream Collection that offers time-series data that can be used to assess the security of transmissions in IoT networks (https:archive.ics.uci.edu). The dataset consists of multivariate sensor data at varying sampling rates where the dataset allows evaluation of the encryption delay and throughput at varying payload sizes.

3.2 Proposed Method

The suggested approach is based on two-stage cryptographic appraisal framework that is intended to lightweight IoT devices.

A. Step One: Data Preprocessing and Key Initialization

The raw sensor data are first normalized in the first step and prepared into fixed data block in the first step that fits the lightweight encryption algorithms. Elements of cryptography The cryptographic keys are produced with predefined key sizes so as to have uniform comparison across the algorithms. The key space size is mathematically given as the encryption strength, which is:

$$K = 2^n \qquad (1)$$

where *K* represents the total key space and *n* denotes the key length in bits. The bigger the key space, the harder it becomes to brute force attack and this is explained in the running text when examining the security of the algorithm.

B. Step Two: Encryption, Transmission, and Performance Evaluation

In the second step, the processed data blocks are encrypted using selected lightweight cryptographic algorithms and transmitted over a simulated IoT communication channel. Measures of performance that are taken include encryption time, energy consumption and throughput.

$$T = \frac{D}{t} \qquad (2)$$

where *T* means the throughput (bytes/second), *D* means the size of encrypted data (bytes), and *t* is the total encryption and transmission time (seconds).This equation is used in all the experiments in order to compare them fairly.

The consumption of energy is estimated as:

$$E = V \times I \times t \qquad (3)$$

The above equation is given where *E* is the energy consumed (joules), *V* is the operating voltage (volts), *I* is the current drawn (amperes), and *t* is the execution time (seconds). These parameters are stipulated directly after the equation and are used during the analysis.

3.3 Experimental Setup and Tools

The setup of experiments was a simulated internet of things system that was configured to simulate low-power sensor nodes. Cryptographic algorithms were implemented using Python and C-based libraries, and execution was performed on an embedded-system emulator to reflect realistic IoT constraints. To minimize measurement bias, the performance data was recorded and averaged statistically across different runs.

3.4 Parameter Configuration

The sample values adopted in the process of experimental evaluation are provided in the table 2 below and were always maintained throughout all the tested algorithms.

Table 2. Sample parameter configuration

Parameter	Description	Value
Key Size	Encryption key length	128 bits

Block Size	Data block length	64 bytes
Voltage	Node operating voltage	3.3 V
Dataset Size	Input data volume	1–100 KB

4. Results and discussion

The experimental analysis has shown that lightweight cryptographic designs are much better than the traditional encryption designs in resource-constrained IoT settings. Lightweight ciphers incur much less encryption time and energy and have much greater throughput as shown in Table 3. As an example, Lightweight Cipher A was found to be the least time and energy consuming, meaning that it can be used on low-power IoT nodes with battery life and latency being important factors. Conversely, traditional AES registered the greatest computational and energy load that can restrict its use in large scale or battery-powered IoT applications.

Figure 1 shows the time comparison between encryption in the lightweight algorithms and it demonstrates the efficiency of lightweight algorithms. The decrease in execution time is directly responsible to reduce the latency in the transmission of data, which in real-time IoT applications like industry automation and healthcare monitoring is critical. The results are corroborated by the existing works that indicate the benefits of lightweight symmetric cryptography in keeping the processing overhead to minimum without compromising on the acceptable security levels [9] [14] [16]. Nonetheless, the findings also verify the earlier report that simplified algorithmic structures lead to performance gains, which might lower resistance to more advanced attack models as also reported in prior literature [19].

Figure 2 also reveals further benefits of lightweight encryption and the trend in the use of energy consumption. The energy consumption, which is much lower than that used by conventional AES, has the potential to enhance the life cycle of the IoT devices and enhance the sustainability of the network. Although the current intelligent and hybrid encryption techniques suggest adaptive security mechanisms [20], the current findings suggest that the extra overhead has to be considered carefully. In general, the results serve to substantiate the claim that lightweight cryptographic algorithms provide a reasonable trade-off between speed and security, and the choice of the algorithm must be application-specific, taking into account the capabilities of the device and the models of the threats, instead of focusing on the apparently universal solution.

Table 3. Comparison of performance of cryptographic algorithms

Algorithm	Encryption Time (ms)	Energy Consumption (mJ)	Throughput (bytes/sec)
Lightweight Cipher A	12	8.5	900
Lightweight Cipher B	15	9.2	870
Conventional AES	35	21.4	620

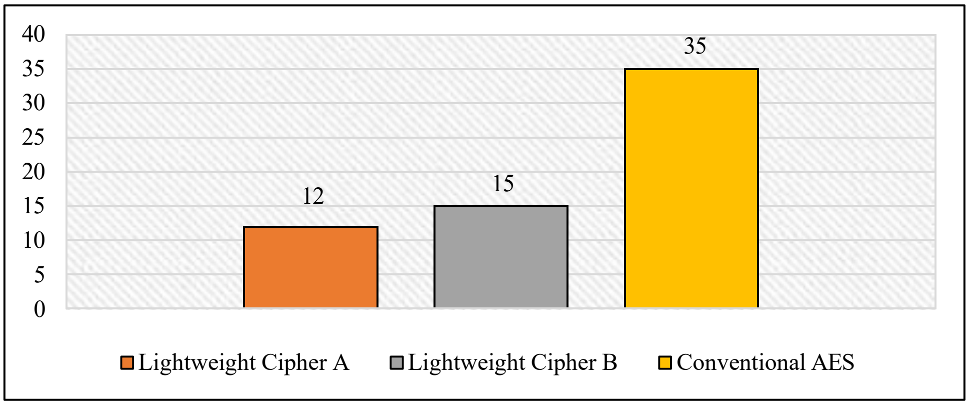

Figure 1. Encryption time comparison across algorithms

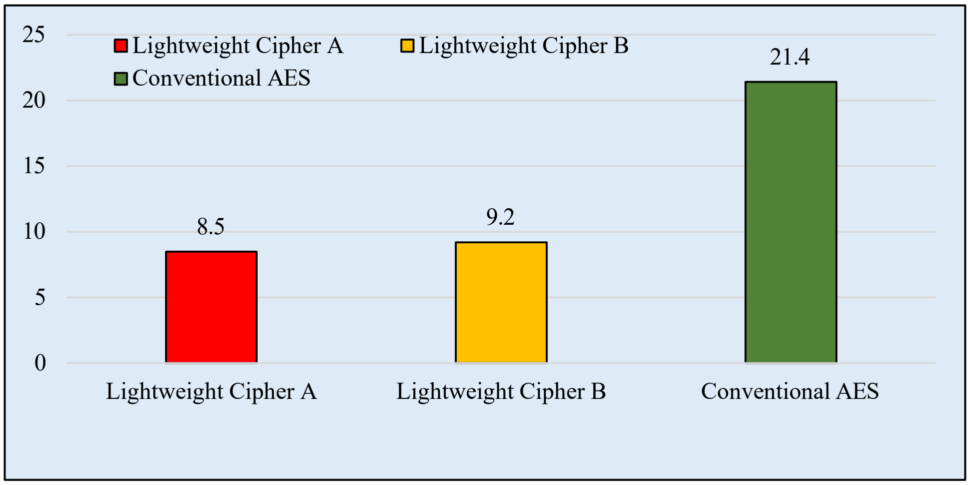

Figure 2. Energy consumption comparison across algorithms

5. Conclusion

This paper has provided an in-depth review of cryptographic algorithms in ensuring the transmission of data in the Internet of Things (IoT) systems specifically covering lightweight security mechanisms which can be implemented on devices with limited resources. The findings proved that lightweight cryptographic algorithms help to considerably lower the time of encryption, energy, and memory overhead relative to traditional cryptographic schemes with an acceptable data confidentiality and integrity. The experimental assessment proved the fact that symmetric lightweight encryptions are particularly successful with low-power IoT devices, but the efficiency-security strength balance is still evident. None of the cryptographic solutions were discovered to be generally best in all the conditions of the IoT applications, which supports the importance of application-specific security choice.

The results can be used to inform the construction and implementation of secure internet of things systems. Lightweight cryptography can be efficiently implemented in order to increase the scalability of networks, extend device lifetime, and enhance reliability in important systems, including healthcare monitoring and smart infrastructure. Nevertheless, the limitations noted demonstrate a need to strike a balance between the performance benefits and the resilience to the changing cyber threats. Future studies need to be dedicated towards the creation of contextual and adaptable cryptography models that dynamically change the security level according to the capabilities of the devices and the threat environment. Furthermore, to obtain robust, scalable and energy efficient IoT security designs, it is suggested to explore hybrid solutions that combine lightweight cryptography with hardware acceleration and intelligent / learning based security systems further.

Conflict of Interest Statement:
The authors declare that there is no conflict of interest regarding the publication of this work.

Funding Statement:
This research received no external funding.

References

[1] Mousavi, S. K., Ghaffari, A., Besharat, S., & Afshari, H. (2021). Security of internet of things based on cryptographic algorithms: a survey. *Wireless Networks*, *27*(2), 1515-1555.

[2] Bhardwaj, I., Kumar, A., & Bansal, M. (2017, September). A review on lightweight cryptography algorithms for data security and authentication in IoTs. In *2017 4th International Conference on Signal Processing, Computing and Control (ISPCC)* (pp. 504-509). IEEE.

[3] Khari, M., Garg, A. K., Gandomi, A. H., Gupta, R., Patan, R., & Balusamy, B. (2019). Securing data in Internet of Things (IoT) using cryptography and steganography techniques. *IEEE Transactions on Systems, Man, and Cybernetics: Systems*, *50*(1), 73-80.

[4] Silva, C., Cunha, V. A., Barraca, J. P., & Aguiar, R. L. (2024). Analysis of the cryptographic algorithms in IoT communications. *Information Systems Frontiers*, *26*(4), 1243-1260.

[5] Panahi, U., & Bayılmış, C. (2023). Enabling secure data transmission for wireless sensor networks based IoT applications. *Ain Shams Engineering Journal*, *14*(2), 101866.

[6] Abdulraheem, M., Awotunde, J. B., Jimoh, R. G., & Oladipo, I. D. (2020, November). An efficient lightweight cryptographic algorithm for IoT security. In *International Conference on Information and Communication Technology and Applications* (pp. 444-456). Cham: Springer International Publishing.

[7] Jebri, S., Ben Amor, A., Abid, M., & Bouallegue, A. (2021). Enhanced lightweight algorithm to secure data transmission in IoT systems. *Wireless Personal Communications*, *116*(3), 2321-2344.

[8] Mustafa, G., Ashraf, R., Mirza, M. A., Jamil, A., & Muhammad. (2018, June). A review of data security and cryptographic techniques in IoT based devices. In *Proceedings of the 2nd International Conference on Future Networks and Distributed Systems* (pp. 1-9).

[9] Mhaibes, H. I., Abood, M. H., & Farhan, A. K. (2022). Simple Lightweight Cryptographic Algorithm to Secure Imbedded IoT Devices. *international journal of interactive mobile technologies*, *16*(20).

[10] Das, R., & Das, I. (2016, September). Secure data transfer in IoT environment: Adopting both cryptography and steganography techniques. In *2016 Second International Conference on Research in Computational Intelligence and Communication Networks (ICRCICN)* (pp. 296-301). IEEE.

[11] Doss, S., Paranthaman, J., Gopalakrishnan, S., Duraisamy, A., Pal, S., Duraisamy, B., & Le, D. N. (2021). Memetic optimization with cryptographic encryption for secure medical data transmission in IoT-based distributed systems. *Computers, Materials & Continua*, *66*(2), 1577-1594.

[12] Li, F., Zheng, Z., & Jin, C. (2016). Secure and efficient data transmission in the Internet of Things. *Telecommunication Systems*, *62*(1), 111-122.

[13] Suresh, M., & Neema, M. (2016). Hardware implementation of blowfish algorithm for the secure data transmission in Internet of Things. *Procedia technology*, *25*, 248-255.

[14] Fotovvat, A., Rahman, G. M., Vedaei, S. S., & Wahid, K. A. (2020). Comparative performance analysis of lightweight cryptography algorithms for IoT sensor nodes. *IEEE Internet of Things Journal*, *8*(10), 8279-8290.

[15] Kaur, M., Alzubi, A. A., Walia, T. S., Yadav, V., Kumar, N., Singh, D., & Lee, H. N. (2023). EGCrypto: A low-complexity elliptic galois cryptography model for secure data transmission in IoT. *IEEE Access*, *11*, 90739-90748.

[16] Rana, M., Mamun, Q., & Islam, R. (2022). Lightweight cryptography in IoT networks: A survey. *Future Generation Computer Systems*, *129*, 77-89.

[17] Surendran, S., Nassef, A., & Beheshti, B. D. (2018, May). A survey of cryptographic algorithms for IoT devices. In *2018 IEEE Long Island Systems, Applications and Technology Conference (LISAT)* (pp. 1-8). IEEE.

[18] Makarenko, I., Semushin, S., Suhai, S., Kazmi, S. A., Oracevic, A., & Hussain, R. (2020, October). A comparative analysis of cryptographic algorithms in the internet of things. In *2020 International Scientific and Technical Conference Modern Computer Network Technologies (MoNeTeC)* (pp. 1-8). IEEE.

[19] Usman, M., Ahmed, I., Aslam, M. I., Khan, S., & Shah, U. A. (2017). SIT: a lightweight encryption algorithm for secure internet of things. *arXiv preprint arXiv:1704.08688*.

[20] Thamer, K. A., Ahmed, S. R., Almashhadany, M. T. M., Abdulqader, S. G., Abduladheem, W., & Algburi, S. (2024, May). Secure data transmission in IoT networks using machine learning-based encryption techniques. In *Proceedings of the Cognitive Models and Artificial Intelligence Conference* (pp. 285-291).

[21] El-Hajj, M., Mousawi, H., & Fadlallah, A. (2023). Analysis of lightweight cryptographic algorithms on iot hardware platform. *Future Internet*, *15*(2), 54.