ITM.J. Ad. Comp. Intell. System.2026, 1(1)

ITM Journal of Advanced
COMPUTING & INTELLIGENT SYSTEM

Lightweight Cryptography in IoT: A Review

Hirendra Singh Sengar*

ITM University Gwalior

Review/Article

ABSTRACT

The IoT system expansion has created essential security problems because of its requirement for devices to operate with restricted power and memory and processing resources. The resource demands of traditional cryptographic algorithms make them unsuitable for use in these specific environments. Lightweight cryptography has emerged as a viable solution to address these challenges by providing efficient and secure communication. The paper provides an extensive evaluation of lightweight cryptographic methods used in IoT systems which includes performance testing through different evaluation criteria and research challenges that need to be addressed in upcoming studies. The study shows that lightweight algorithms enhance efficiency but organizations still need to find ways to balance security protection and performance optimization.

Keywords: IOT, Lightweight Cryptography, Security, Encryption, Resource Constraints

INTRODUCTION

Network resource availability The Internet of Things (IoT) connects billions of devices through its network which includes sensors and smart appliances and industrial systems. The rapid expansion of this technology has created more security weaknesses which have resulted in increased cyber threats to organizations [1][2]. The traditional cryptographic algorithms RSA and AES deliver strong security protection but need extensive computational resources which makes them impractical for use on devices with limited resources in IoT environments [3][4]. The devices operate with restrictions on their battery life and available memory and processing power [5]. Lightweight cryptography was created to solve these problems by reducing the need for computing power while still providing fundamental security functions which include confidentiality and integrity and authentication [6]. These techniques are widelyapplied in smart homes, healthcare systems, and industrial IoT environments [7].

*Corresponding Author: Hirendra Singh Sengar, Assistant Professor, ITM University Gwalior
Tel: 9301163117
Email: hirendra.cse@itmuniversity.ac.in

REVIEW OF LITERATURE

The initial research on DDoS Researchers developed lightweight cryptographic systems which they specifically designed for Internet of Things (IoT) environments. The three block ciphers PRESENT, SIMON, and SPECK have been researched extensively to evaluate their ability to operate with minimal system resources and deliver efficient performance [8], [9].People use Elliptic Curve Cryptography (ECC) because it needs shorter key lengths while providing stronger security than traditional public-key cryptography methods [10]. Researchers developed lightweight hash functions like PHOTON and SPONGENT to protect data integrity through their ability to operate with minimal processing requirements [11].Current research investigates hybrid cryptographic systems which merge symmetric and asymmetric encryption techniques to optimize system performance and scalability [12].The combination of blockchain technology and artificial intelligence with lightweight cryptography protects Internet of Things (IoT) systems according to emerging security requirements [13], [14]. The existing advancements have not solved three main problems which include the absence of standardized solutions and the difficulties associated key management and the potential for security breaches [15].

PROPOSED METHODOLOGY

The research paper examines lightweight cryptographic methods used in Internet of Things systems by employing a systematic review method for its investigation.

A. Data Collection

Researchers gathered IoT security research papers from journals and conference proceedings and technical reports which contained studies about lightweight cryptography.

B. Selection Criteria

The studies were selected based on the following criteria:

• IoT security had to be the main focus of the study.
• Lightweight cryptography techniques required to be used in the study.
• The study has to use known evaluation indicators to gauge performance.
• The information used in the study needs to come from reliable publication sources.

C. Parameters for Analysis

The following evaluation criteria were applied to the chosen techniques:

• The evaluation assessed how well the system performed computing tasks. • Memory utilization was assessed.
• Energy use was assessed.
• Security strength was assessed.
• Scalability was assessed

D. Evaluation by Comparison

To ascertain the advantages and disadvantages of several lightweight algorithms in diverse Internet of Things applications, the study carried out a comparative evaluation.

Algorithm

The algorithm

Input

technical reports, journal articles, and conference proceedings.

Results
A ranked collection of lightweight cryptography methods appropriate for Internet of Things settings.

Input

technical reports, journal articles, and conference proceedings.

Results
A ranked collection of lightweight cryptography methods appropriate for Internet of Things settings.

Procedures

Gather research articles about lightweight cryptography and IoT security.
Eliminate research that are redundant or unnecessary.
Use the following selection criteria:

Pay attention to IoT security employs simple cryptography techniques comprises measures for performance evaluation published in reputable publications

Take analytical parameters out of a few chosen studies:
Efficiency of computation
Memory usage
Use of energy
Strength of security
Scalability

Create a comparison table with the retrieved data.
To provide fair comparisons, normalize evaluation scores.

Calculate each technique's overall performance score.
Sort algorithms based on their total score.

Determine each technique's advantages and disadvantages.
Produce a report on comparative analysis.

LCEA algorithm

Input: A compilation of academic papers on IoT security
Results: Lightweight cryptography approaches ranked

Start

Step 1: Set up
Make a blank list called Selected_Papers.
Make the Technique_Data table empty.

Step 2: Gathering Information
Gather documents from Journals
Proceedings of the conference
Technical reports

Step 3: Use the Selection Criteria for Every Paper in Collected_Papers

If the paper employs lightweight cryptography, focuses on IoT security, and includes evaluation metrics Additionally, the paper comes from a reliable source.

Next, add the paper to Selected_Papers. Finally, if

Finish For

Step 4: Extract Analysis Parameters: For every paper in Selected_Papers, do

RESULTS AND DISCUSSION

The study shows that symmetric lightweight algorithms SPECK and PRESENT execute faster and consume less energy which makes them suitable for real-time IoT applications

according to reference [8]. The security of ECC and other asymmetric methods provides stronger protection through multiple security mechanisms which require additional computational resources according to reference [10].The lightweight hash functions show they can verify data integrity with their efficient performance that requires only minimal system resources according to reference [11]. The hybrid system achieves better system performance and greater scalability through its use of multiple cryptographic methods according to reference [12].

Table 1. Comparison of Lightweight Cryptographic Algorithms

Algorithm	Type	Key Size	Advantages	Limitations	Suitable Use
PRESENT	Symmetric	64-bit	Low power, simple	Moderate security	RFID, sensors
SPECK	Symmetric	64/128-bit	Fast, efficient	Some concerns	Embedded systems
SIMON	Symmetric	64/128-bit	Hardware efficient	Limited adoption	IoT hardware
ECC	Asymmetric	160–256-bit	Strong security	Higher computation	Key exchange
PHOTON	Hash	~80-bit	Low memory	Lower throughput	Data integrity
SPONGENT	Hash	~88-bit	Lightweight	Limited use	Authentication
AES (Lite)	Symmetric	128-bit	Strong security	Higher energy	General IoT

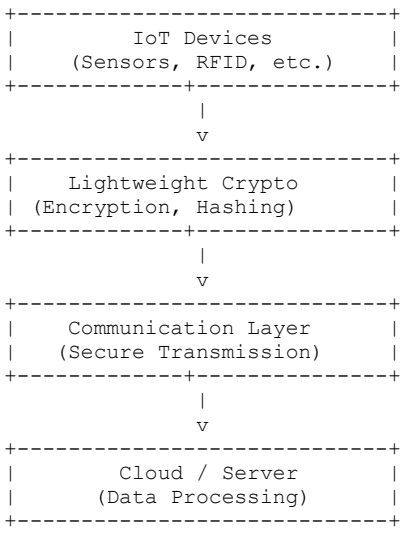

Figure.1. IoT Lightweight Security Architecture

The research identifies main difficulties which need to be solved:

- Trade-off between security and efficiency [5]
- Lack of standardized evaluation methods [15]
- Key management complexity [6]
- Vulnerability to side – channel attacks [20]

The study demonstrates that no single algorithm can meet all requirements for Internet of Things systems which creates a demand for both adaptive and hybrid cryptographic systems.

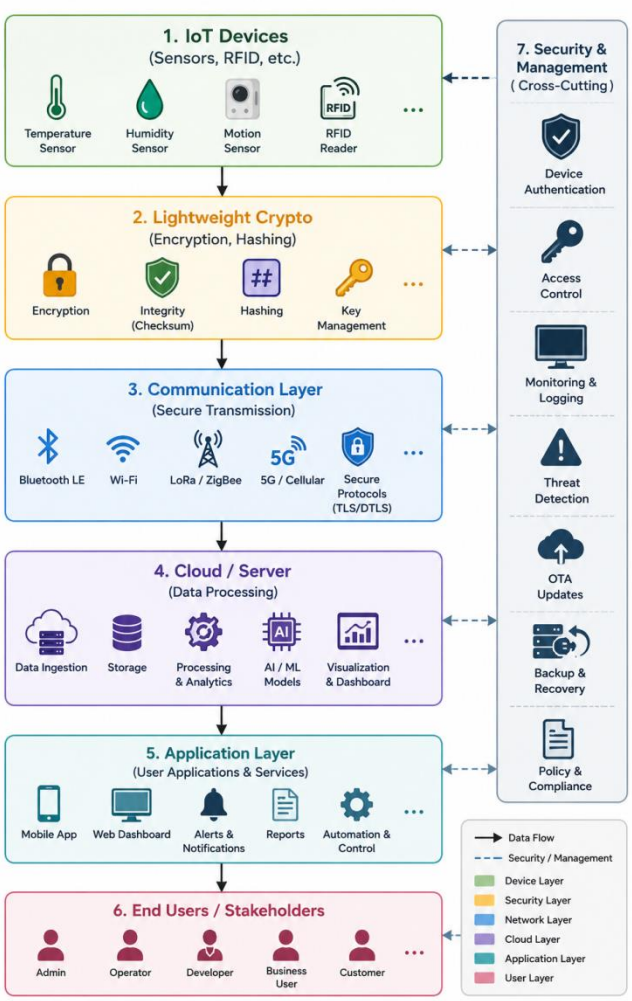

Figure.2 Secure IoT Architecture with Lightweight Cryptography, Intelligent Cloud Processing, and End-User Applications

IoT devices like sensors and RFID readers gather real-time data and send it through a lightweight cryptography layer for encryption, hashing, integrity checking, and key management. This image depicts a safe and scalable IoT architecture. After that, the secure data is sent via secure protocols over a variety of communication technologies, including as Wi-Fi, Bluetooth LE, LoRa/ZigBee, and 5GFollowing transmission, data ingestion, storage, analytics, AI/ML-based processing, and visualization are carried out via the cloud/server layer. The application layer uses the processed data for a variety of end users, including administrators, operators, developers, business users, and customers, through mobile apps, dashboards, alerts, reports, and automation services. Furthermore, a cross-cutting security and management layer guarantees system-wide authentication,

monitoring, threat detection, OTA updates, backup, and policy compliance.

CONCLUSION

Lightweight cryptography protects Internet of Things systems because it delivers security solutions which operate effectively on devices with limited processing power. The current state of development has achieved progress yet it still faces three main obstacles which include standardization issues and problems with system scalability and defense against sophisticated attacks. The future of research should concentrate on creating cryptographic systems which use adaptive intelligence-based design principles.

ACKNOWLEDGMENTS

The authors would like to express their sincere gratitude to ITM University, Gwalior, for providing the necessary academic environment and resources to carry out this research work. The authors also extend their appreciation to the faculty members and domain experts for their valuable guidance, constructive feedback, and continuous support throughout the study. Special thanks are given to colleagues and peers who contributed through discussions and insights that helped improve the quality of this paper. We would especially like to thank colleagues and peers who helped to improve the quality of this paper through discussions and insights.

REFERENCES

[1] D. Evans, "The Internet of Things: How the Next Evolution of the Internet Is Changing Everything," Cisco, 2011.

[2]L. Atzori, A. Iera, and G. Morabito, "The Internet of Things: A survey," Computer Networks, vol. 54, no. 15, pp. 2787–2805, 2010.

[3] W. Stallings, Cryptography and Network Security: Principles and Practice, 7th ed., Pearson, 2017.

[4]N. Koblitz and A. Menezes, "A survey of public-key cryptosystems," SIAM Review, vol. 46, no. 4, pp. 599–634, 2004.

[5]A. Poschmann, Lightweight Cryptography, Ph.D. dissertation, Ruhr University Bochum, 2009.

[6]M. H. Alsharif et al., "IoT security using lightweight cryptography," IEEE Access, vol. 8, pp. 119964–119984, 2020.

[7]S. Sicari et al., "Security, privacy and trust in IoT," Computer Networks, vol. 76, pp. 146–164, 2015.

[8]A. Bogdanov et al., "PRESENT: An ultra-lightweight block cipher," in CHES, 2007.

[9]R. Beaulieu et al., "SIMON and SPECK block ciphers," in DAC, 2015.

[10]V. Miller, "Elliptic curve cryptography," in CRYPTO '85, Springer, 1986.

[11]J. Guo et al., "PHOTON hash function," in CRYPTO 2011, Springer.

[12] M. Ambrosin et al., "Hybrid cryptographic IoT security," Ad Hoc Networks, 2017.

[13] S. Nakamoto, "Bitcoin," 2008.

[14]Y. Liu et al., "AI-based IoT security," IEEE IoT Journal, 2019.

[15] NIST, "Lightweight Cryptography Standardization," 2023.

[16] IEEE Xplore Digital Library, IoT papers.

[17] ScienceDirect Database, IoT research.

[18] MDPI Computers Journal, 2025.

[19] Springer Journal of Network Systems, 2024–25.

[20] P. Kocher et al., "Differential power analysis," CRYPTO '99, 1999.