



A Survey on Light Weight Cryptography Solutions for Internet of Things Environment

P. Bhargavram ^{a*}, CH. Manideep ^b, K. Sanjay Bhanu ^c, K. Hemalatha ^d

^{a,b,c,d} Department of Infromation Technology, GMRIT, Rajam, India – 532127

ABSTRACT

The Internet of Things (IoT) has gained significant popularity and widespread acceptance due to its diverse applications across various industries. IoT devices collect data from their surroundings, and some transmit this information over networks. These devices can range in size from as small as a cubic millimeter to as large as a credit card. However, when deploying IoT systems in real-time, there are several challenges to address, including those related to processing power, wireless capabilities, interoperability, and security. To integrate billions of smart devices into a unified network with proper security across networks, a mechanism like cryptography is essential. Cryptography ensures the authentication, confidentiality, data integrity, and access control of IoT networks. However, traditional cryptographic protocols are often unsuitable for IoT environments, such as smart ecosystems, due to the many constraints of IoT devices. As a result, researchers have proposed various lightweight cryptographic algorithms and protocols to secure data in IoT environments. In this work, explore state-of-the-art lightweight cryptographic protocols for IoT networks and provide a comparative analysis of popular contemporary ciphers. Additionally, analyze different cryptanalysis techniques by examining their working principles, advantages, disadvantages, and limitations.

Keywords: *Internet of Things (IoT), Lightweight Cryptography (LWC), Security.*

1. Introduction

The Internet of Things (IoT) refers to a network physical devices, vehicles, appliances, and other objects embedded with sensors, software, and network connectivity, enabling them to collect and exchange data. It permits constant connectivity and data analytics; with new avenues for companies to innovate both in products and services, in addition to the efficiency in operations. Improves the efficiency of daily life, and users can manage their home appliances and functions through a smartphone, or an app. Helps increase productivity, efficiency, and safety in industrial uses. Gives businesses a real-time glimpse into the inner workings of their company's systems. Allowing better decision-making, real-time tracking and monitoring, automation, and more efficient personal and business tasks. IoT devices lack inbuilt security, and that is why IoT security is required. IoT devices send data over the internet without encryption and are not detectable by general cybersecurity, which makes them prone to data breaches¹. IoT security is required because it prevents data breaches and saves individuals, systems, businesses, and governments from physical destruction caused by digital tools.

Traditional cryptography cannot be adapted for IoT due to:

- Limited Processing Power: Most IoT devices use low-power processors to save energy, which are not sufficient for the computational requirements of traditional cryptographic algorithms.
- Limited Memory: Traditional cryptography often requires a lot of memory for key storage and processing, which is scarce in IoT devices.
- Low Energy Availability: Many IoT devices are battery-operated, and traditional cryptography can drain power quickly due to high computational overhead.

Lightweight cryptography is a specialized branch of cryptography that is designed to meet the security requirements of resource-constrained environments, like the Internet of Things. In an IoT environment, numerous devices such as sensors, actuators, and embedded systems collect and transmit large volumes of sensitive data. However, these devices are usually resource-constrained with limited computational power, memory, battery life, and storage, which makes traditional cryptographic algorithms unsuitable. Lightweight cryptography is a solution because it offers secure communication along with data protection with much less resource consumption. Their cryptographic algorithms are designed such that they can run within low-power devices with little key size, low-complexity computations, and optimized processing speeds. Regarding IoT, lightweight cryptography ensures to maintain confidentiality, integrity, authentication, and access controls while maintaining the efficiency of the device and prolonging the battery life.

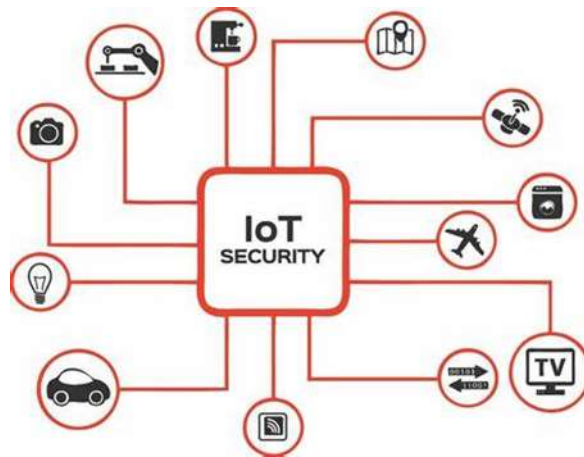


Fig. 1. The role of security in IoT ecosystem

Given the diverse and dynamic nature of IoT applications ranging from smart cities to healthcare systems implementing lightweight cryptographic solutions is crucial to protect data integrity and user privacy across the network. The security aspects of IoT environment have depicted in the figure 1.

2. Analysis of Existing Methodologies

As discussed earlier, there are many authors who have come with their own methodologies to provide better security in the IoT environments. In this chapter, the recent and reputed publications have been discussed with detailed information such as, advantages, disadvantages and limitations along with their performance.

To understand the latest lightweight cryptographic protocols especially developed for providing data security in IoT networks. It classifies the latest algorithms into symmetric (block and stream ciphers) and asymmetric (elliptic curve cipher) lightweight cryptography. Evaluates several recently developed block and stream cipher algorithms regarding their security, for suitability in IoT environments. It analyses the various layers of IoT architecture and discusses potential threats in each layer, especially perception and network layers. It identifies the current limitations of lightweight cryptography and suggests areas for further research to improve the security features of IoT [1]. IoT healthcare systems deal with sensitive data; therefore, it demands lightweight security mechanisms to ensure privacy, confidentiality, and data integrity. The traditional cryptographic algorithms are not appropriate for the IoT devices due to resource constraints. Lightweight cryptography provides a more power-friendly and simpler approach for the protection of such systems. It evaluates different lightweight cryptographic algorithms (block ciphers, stream ciphers hash functions, MACs) to evaluate their hardware performance and suitability for healthcare IoT. It identifies suitable algorithms based on trade-offs between security and hardware efficiency, like KASUMI for high-throughput and Trivium for low-area applications. Further enhancements are needed in lightweight cryptographic designs to provide robust security while maintaining hardware efficiency in healthcare IoT [2].

Key Trends, leading countries, authors, and journals in IoT lightweight cryptography research. Discuss how lightweight cryptography overcomes limitations of traditional algorithms on resource-constrained IoT devices. Review and evaluate the lightweight algorithms concerning energy usage efficiency, computational power consumption, and memory requirements. Analyzing international research networks, indicating principal collaborations and contributors in IoT lightweight cryptography. Propose areas for future research, particularly on secure lightweight encryptions for devices such as Raspberry Pi and filling in research gaps that exist [3]. Partial key pre-distribution scheme to develop a scheme that enhances the security of IoT while using fewer resources. Develop a cryptographical protocol with block cipher techniques for IoT networks to provide secure data transmission. Reduce communication overhead, power consumption, and storage requirements that are suitable for resource-constrained IoT devices. Demonstrate the resistance of the protocol against different security threats such as node capture, eavesdropping, and replay attacks. Provide node addition, key renewal and revocation mechanisms to offer secure communication in the volatile IoT networks [4]. Investigate the value and practicality of lightweight cryptographic solutions for securing IoT devices. Point out the benefits of symmetric key cryptography for IoT applications due to lower complexity and resource utilization. Examine main security concerns in lightweight cryptography, which would draw an impetus for well-designed mechanisms. Study various lightweight algorithms (for example, AES, Blowfish, CLEFIA) based on key size, block size, and suitability for IoT [5]. Rana, Mamun, and Islam (2023) introduce an innovative key management system designed to bolster the security of Internet of Things (IoT) devices, with a focus on lightweight block ciphers. Their research tackles key challenges in IoT security, such as limited computational resources and the demand for energy-efficient encryption methods. By creating a robust and efficient key management solution, the authors demonstrate its ability to secure IoT device communication without compromising performance. The system's effectiveness and practicality are validated through extensive experimentation, highlighting its potential for real-world IoT applications. This advancement marks a notable improvement in addressing security vulnerabilities within IoT ecosystems [6].

Later other authors have presented a modified version of the lightweight GIFT cipher to improve security in resource-constrained Internet of Things (IoT) devices. Their research addresses the critical need for robust encryption in IoT environments, where devices often face limitations in power, processing, and memory. By optimizing the GIFT cipher, the authors achieve enhanced security features while maintaining efficiency suitable for low-resource applications. The study includes extensive testing and analysis, demonstrating the cipher's effectiveness in countering potential threats without

significantly impacting performance. This work contributes significantly to the advancement of secure, lightweight cryptographic solutions for IoT systems [7]. Al-Hejri, et al. have proposed a lightweight, secure, and scalable scheme for data transmission on the Internet of Things (IoT), addressing critical challenges such as resource constraints, scalability, and data security. Their approach leverages optimized cryptographic techniques to ensure secure communication while minimizing computational and energy overhead. The scheme is designed to adapt to varying IoT network sizes, making it suitable for diverse applications. Rigorous evaluations demonstrate its efficiency in enhancing data transmission security and scalability without compromising performance. This innovative framework contributes to advancing secure and efficient IoT communication protocols [8].

It was a comprehensive review of recent advancements in lightweight cryptography (LWC) for enhancing the security of resource-constrained IoT networks. Their study highlights the critical need for efficient cryptographic solutions tailored to IoT devices with limited computational power, memory, and energy resources. The authors explore various state-of-the-art LWC algorithms and protocols, emphasizing their effectiveness in ensuring secure communication while maintaining performance efficiency. By analyzing existing challenges and emerging trends, the paper offers valuable insights into the development of robust security mechanisms for IoT ecosystems. This work serves as a vital resource for researchers and practitioners aiming to fortify IoT network security [9]. Ekwueme, Adam, and Dwivedi (2024) present a detailed review of lightweight cryptography (LWC) solutions tailored for the Internet of Things (IoT), addressing the unique constraints of IoT devices, such as limited computational resources, memory, and energy efficiency. The authors analyze various LWC algorithms, highlighting their suitability for secure communication in IoT networks while balancing performance and resource efficiency. The review also identifies key challenges in implementing LWC and discusses emerging trends aimed at enhancing IoT security. This work serves as a critical resource for understanding the role of lightweight cryptography in building secure and efficient IoT systems [10].

3. Comparative Analysis of existing Methodologies

Author Details	Technology used	Description
KASUMI	Tsantikidou&Sklavos (2022)	High throughput (75% efficiency), area-efficient (80%) in IoT healthcare applications.
Trivium	Tsantikidou&Sklavos (2022)	Best area-to-throughput ratio (85%) and low-power consumption (70%).
PRESENT	Tsantikidou&Sklavos (2022)	Small area (90%), moderate throughput (65%) for IoT healthcare.
LLC	Rana, Mamun & Islam (2022)	High efficiency (80%) in lightweight IoT security applications.
LWHC	Rana, Mamun & Islam (2022)	Energy-efficient (70%), moderate security (60%) for IoT devices.
Modified PRESENT	Rana, Mamun & Islam (2022)	Enhanced security (75%) and efficiency (80%) over traditional PRESENT.
SAT_Jo	Rana, Mamun & Islam (2022)	High security (80%), with 70% power efficiency in constrained IoT environments.
PHOTON-80	Dewamuni, Shanmugam, Azam &Thennadil (2023)	Energy-efficient (85%) with moderate security (65%) for IoT healthcare.
AES (Modified)	Ekwueme, Adam & Dwivedi (2024)	Secure (90%) with optimized energy use (70%) for IoT constraints.
Blowfish	Ekwueme, Adam & Dwivedi (2024)	High efficiency (80%), suitable for moderate IoT security applications.
CLEFIA	Ekwueme, Adam & Dwivedi (2024)	High security (85%) and low latency (80%) for IoT environments.

4. Conclusion

The adoption of Lightweight Cryptography (LWC) is pivotal for ensuring secure and efficient communication within the Internet of Things (IoT) ecosystem. IoT devices, often constrained by limited processing power, memory, and battery capacity, face significant challenges in implementing traditional cryptographic methods. LWC addresses these challenges by offering specialized algorithms that balance robust security with minimal resource usage. This optimization ensures secure data transmission without compromising device performance or energy efficiency, making it a crucial enabler for the widespread deployment of IoT solutions. As IoT continues to expand into diverse sectors such as healthcare, smart cities, industrial automation, and connected vehicles, the importance of tailored cryptographic protocols grows. Future research and development in LWC will likely focus on

enhancing algorithm resilience against emerging cyber threats while further minimizing computational overhead. This evolution will solidify LWC's role as a cornerstone of IoT security, enabling the realization of secure, scalable, and sustainable IoT networks in an increasingly interconnected world.

References

- [1] Rana, M., Mamun, Q., & Islam, R. (2022). Lightweight cryptography in IoT networks: A survey. *Future Generation Computer Systems*, 129, 77-89.
- [2] Goyal, T. K., Sahula, V., & Kumawat, D. (2022). Energy efficient lightweight cryptography algorithms for IoT devices. *IETE Journal of Research*, 68(3), 1722-1735.
- [3] Tsantikidou, K., & Sklavos, N. (2022). Hardware limitations of lightweight cryptographic designs for IoT in healthcare. *Cryptography*, 6(3), 45.
- [4] Dewamuni, Z., Shanmugam, B., Azam, S., & Thennadil, S. (2023). Bibliometric Analysis of IoT Lightweight Cryptography. *Information*, 14(12), 635.
- [5] Thabit, F., Can, O., Aljahdali, A. O., Al-Gaphari, G. H., & Alkhzaimi, H. A. (2023). Cryptography algorithms for enhancing IoT security. *Internet of Things*, 22, 100759.
- [6] Rana, M., Mamun, Q., & Islam, R. (2023). Enhancing IoT security: an innovative key management system for lightweight block ciphers. *Sensors*, 23(18), 7678.
- [7] Yasmin, N., & Gupta, R. (2024). Modified lightweight GIFT cipher for security enhancement in resource-constrained IoT devices. *International Journal of Information Technology*, 16(4), 2647-2659.
- [8] Al-Hejri, I., Azzedin, F., Almuhammadi, S., & Eltoweissy, M. (2024). Lightweight Secure and Scalable Scheme for Data Transmission in the Internet of Things. *Arabian Journal for Science and Engineering*, 1-16.
- [9] Pandey, S., & Bhushan, B. (2024). Recent Lightweight cryptography (LWC) based security advances for resource-constrained IoT networks. *Wireless Networks*, 30(4), 2987-3026.
- [10] Ekwueme, C. P., Adam, I. H., & Dwivedi, A. (2024). Lightweight Cryptography for Internet of Things: A Review. *EAI Endorsed Transactions on Internet of Things*, 10.