A Review on Lightweight Cryptography for IoT

Komal[1], Naveen Kumar[2]
[1]Dept of Computer Science
[2]Assistant Professor, Dept of Computer Science
[1, 2] Himachal Pradesh University, Shimla

Abstract- *Nowadays, security is a top issue for every gadget due to the explosive growth of internet usage. Many limited devices are connected to the Internet in a brand-new computing environment called the Internet of Things (IoT), and they communicate with one another through networks to provide us new experiences. IoT is subject to attacks as a result of data sharing on the internet, and security of confined devices is crucial to preventing intrusions. IoT device security is achieved via lightweight cryptography. To protect information, data, resource-constrained IoT devices, RFID tags, and sensors lightweight cryptography is a necessary technology. This technology makes it possible for network devices to communicate securely and effectively. This paper gives an overview of lightweight cryptography technology and presents a detailed review and comparative study of various lightweight algorithms with their structure, size, performance, attacks and merits. The comparative study of various existing security block ciphers helps in deciding which technique is best for security purposes.*

Keywords- Internet of Things (IoT), Lightweight Cryptography, Block cipher, AES, PRESENT, CLEFIA, TWIN, HIGHT

I. INTRODUCTION

Internet of Things (IoT) Overview:

IoT emerges in research era because of its used in various fields like healthcare, smart infrastructure, etc. It is a network of connected objects each with a unique identification able to collect and exchange data over the internet with or without human interaction [1]. The core idea of IoT is to connect anyone with anything and anytime [2]. The IoT has created new values by connecting various devices to the network, but has also led to security threat becoming important issues as seen in the recent reports of illegal surveillance camera manipulation and automobile hacking etc. [3]. Even employing sensors to collect data from the real world might make an IoT system vulnerable to cyber-attacks, which is the primary security problem that differentiates IoT systems from typical IT systems [4]. Even if there isn't an issue right now, it's important to think about the impact of any potential dangers down the road. When encryption is used on sensor equipment, data security for confidentiality and integrity is implemented, which can be a powerful defense against threats. Secure encryption can be used even on low-resource devices thanks to the function of lightweight cryptography [5].

The study of lightweight cryptography contributes to meeting the needs of smart devices. It is an encryption technique for compact devices with little computational power like RFID tags, sensors, contactless smart cards, medical equipment, and other devices all use cryptography protocols [6]. To provide efficiency and security, a variety of lightweight algorithms are created to simplify the traditional algorithms.

Requirement of Lightweight Cryptography for IoT

Applicability to lower resource devices [7] The lightweight cryptographic primitives have a smaller physical footprint than the traditional cryptographic ones. The use of additional network connections with less resource-intensive devices is made possible by the lightweight cryptographic primitives.

Efficiency of end-to-end communication [8] End nodes must implement a symmetric key method in order to achieve end-to-end security. The cryptographic operation with a restricted quantity of energy consumption is crucial for low resource devices, such as battery-powered devices. The use of a lightweight symmetric key method enables end devices to use less energy.

II. LITERATURE REVIEW

In this section a survey on lightweight cryptography algorithms and security of IoT devices is done. Based on it comparison of ciphers is shown. It gives way to research directions in which further work can be done.

A. Lightweight Block Ciphers

Amir Moradi et al. [9] described a very compact hardware implementation of AES-128. The implementation of AES improves the level of resistance against first order side-channel attacks. The design goal was solely low area and thus

ability for setting the time-area and power-area tradeoffs were possible. To pursue the goal, a holistic approach that optimizes the total design has taken. In total, an implementation that requires only 2400GE and needs 226 clock cycles has achieved.

James and Kumar et al. [10] proposed a technique to implement AES as a lightweight block cipher in immediate requirement of time. They aim to develop AES into a lightweight block cipher by taking parameters latency and power as taking into considerations. Their proposed technique is applicable in sensor nodes and RFID tags.

A. Bogdanov et al. [11] describes drawbacks of AES cipher such as AES is not suitable for extremely constrained environments like sensor networks and RFID tags. To improve these drawbacks a new ultra-lightweight block cipher PRESENT is discussed. PRESENT was amongst the first lightweight block cipher that was recommended for restricted hardware environments. Both security and hardware efficiency have been equally important during the design of the cipher and at 1570GE, the hardware requirements for PRESENT are competitive with today's leading compact stream ciphers.

Deukjo Hong et al. [12] proposed a block cipher HIGHT (High Security and Lightweight) with 64 bit block length and 128 bit key length. It provides low resource hardware implementation, which is proper to ubiquitous computing device such as a sensor or RFID tag. This cipher was proposed considering the core features like less cost, less power and super-light implementation. HIGHT does not only consist of simple operations to be ultra-light but also has enough security as a good encryption algorithm. The hardware implementation of HIGHT requires 3048 gates on 0.25 μm technology. The comparative analysis of HIGHT and AES cipher also carried out in the paper.

Toru Akishita & Harunga Hiwatari [13] presents CLEFIA as a lightweight cipher that was standardized by NIST. CLEFIA is a well balanced block cipher in performance and security. It has good hardware performance in comparison to other block ciphers. The paper proposes very compact hardware implementations of CLEFIA-128. The implementations are based on novel serialized architectures in the data processing block. Comparison between AES and CLEFIA also carried out. Best known result of CLEFIA and low-area implementation results of AES taken for comparison

Tomoyasu Suzaki et al. [14] presents a 64-bit lightweight block cipher TWINE supporting 80 and 128-bit keys. TWINE realizes quite small hardware implementations similar to the previous lightweight block cipher proposals, yet enables efficient software implementations on various CPU's, from microcontrollers to high end CPU's. It fits in very small hardware and provides a notable performance on embedded software. A thorough security analysis, in particular for the impossible differential and saturation attacks has performed. The result implies the sufficient security of full-round TWINE.

Ray Beaulieu et al. [15] has proposed two families of block ciphers, SIMON and SPECK. They were designed specifically to offer security on constrained devices, where simplicity of design is crucial. However, the intended use cases are diverse and demand flexibility in implementation. Simplicity, security and flexibility are ever present yet conflicting goals in cryptographic design. The paper outlines how these goals were balanced in the design of Simon and Speck.

WenTao Zhang [16] proposed a new lightweight block cipher named RECTANGLE. It is a bit-slice ultra-lightweight cipher suitable for multiple platforms that have very low gate area in hardware. This paper shows great performance of RECTANGLE in both hardware and software environment which provides security for different devices and compares RECTANGLE with different lightweight block ciphers in both hardware and software implementations. RECTANGLE achieves a very good security performance tradeoff due to good selection of S-box.

B. Internet of Things

Abdurrahman Beg et al. [17] has talked about Internet-of-Things that are employed in a variety of applications, such as industrial and military systems, as well as the platform itself are susceptible to security risks. However, because of the nature of the devices utilized and their resource limitations, traditional security measures may be burdensome and may interfere with the application's goal. Lightweight cryptographic methods have been suggested as a solution to this issue. This paper categorized lightweight cryptography algorithms and a few are chosen to be simulated and compared using metrics relevant to an Internet-of-Things environment.

K N Pallavi et al. [18] Suggested that IoT consists of a collection of constrained sensor-based devices and connected for communication. During this process, the sensors produce a huge quantity of data and transmitted in the network. Due to the uninterrupted transmission of sensitive data over the network, IoT devices are targeted for a different type of attacks. To nullify the attacks and to safeguard the sensitive information security is required. Given this, lightweight cryptographic algorithms are introduced. The paper compares

various lightweight cryptographic algorithms for data security between and cloud.

Effy Raja Naru et al. [19] described Internet of Things as a new-fashioned technology that is the future of the next era of the internet which connects various physical objects that communicate with each other without the aid of human interactions. Security plays important role in network to prevent the unauthorized access, misuses of data, monitoring and data, modification etc. All layer in IoT architecture security considered as extremely important from viewpoint of designing criteria from bottom label to top label. IoT application is useful to people but if the IoT system can't protect the user data from hacker, attacks, and vulnerabilities. Lightweight encryption is a sector of a classical cryptographic algorithm that is pertinent for resource constrained devices in IoT. Related work for lightweight techniques used for secure data transmission is described in this paper.

Sanaah Al salami et.al [20] suggested a lightweight encryption algorithm for smart homes that provides confidentiality with a favorable level of efficiency and reduces overhead cost.

Deepti Dehrawat et al. [21] discuss the rapid technological growth in the Internet of Things (IoT). It has attracted the worldwide attention and has become pivotal technology in the smart computing environment of 21st century. IoT provides a virtual view of real-life things in resource-constrained environment where security and privacy are of prime concern. Lightweight cryptography provides security solutions in resource-constrained environment of IoT. Several software and hardware implementation of lightweight ciphers have been presented by different researchers in this area. This paper presents a comparative analysis of several lightweight cryptographic solutions along with their pros and cons, and their future scope. The comparative analysis may further help in proposing a 32-bit ultra-lightweight block cipher security model for IoT enabled applications in the smart environment.

Isha Bhardwaj et al. [22] discuss the various IoT applications and architectures. Further, the security concerns regarding information sharing and attacks have been highlighted. To overcome from these attacks safety measures regarding data security and authentication are discussed in detail resulting in use of cryptography as a solution. The comparative analysis of various lightweight encryption and authentication algorithms is carried out. The comparative analysis results show that the lightweight algorithms have good performance as compared to conventional cryptography algorithm in terms of memory requirement, their operations, and power consumption. Also, some research directions defined in which further work can be done on lightweight cryptography algorithms.

Biswas et al. [23] surveyed numerous proposed security mechanisms, such as AES, LED, KATAN, and TWINE, for sensor networks to be able to achieve data confidentiality. However, these security mechanisms have drawbacks, security vulnerabilities, and high computational complexities. They addressed these challenges and proposed lightweight block ciphers using chaotic maps and genetic operations. Their proposed scheme utilizes points on an elliptic curve to identify the communicating nodes.

Vishal A. Thakor [24] focuses on resource-constrained IoT devices (such as RFID tags, sensors, smart cards, etc.) as securing them in such circumstances is a challenging task. The communication from such devices can be secured by a mean of lightweight cryptography, a lighter version of cryptography. More than fifty lightweight cryptography (plain encryption) algorithms are available in the market with a focus on a specific application(s), and another 57 algorithms have been submitted by the researchers to the NIST competition recently. To provide a holistic view of the area, in this paper, comparison on the existing algorithms in terms of implementation cost, hardware and software performances and attack resistance properties. Also, we have discussed the demand and a direction for new research in the area of lightweight cryptography to optimize balance amongst cost, performance and security.

III. COMPARATIVE ANALYSIS

This study shows the comparison between different lightweight ciphers AES, PRESENT, HIGHT, CLEFIA, TWINE and so on, on the basis of their key size, structure, performance and attacks. After reviewing lightweight cryptography algorithms comparison of ciphers is shown in table 1. By analyzing these ciphers based on their performance the best cipher suitable for the security of IoT devices is concluded. It is done by reviewing literature which helps in providing necessary information on the theoretical work for conducting research on various lightweight cryptography algorithms.

Various performance metrics which are used for the comparative analysis of lightweight cryptography ciphers are described:

Performance Metrics

a) Memory Requirements

Generally, it's measured in KB [25]. RAM is used to store intermediate values that can be used in computations, whereas ROM is required to store the program/algorithm as well as static data, such as algorithm key, S-box, etc[26].

b) Power Requirements

The amount of power required by the circuit to process the algorithm can be measured in µw [24].

c) Gate Area

It is the physical area required to implement the algorithm on a board/circuit, measured in μm^2. This space can be specified using logical blocks or using GE for ASIC (1GE = 2 INPUT-NAND Gate) [26]. Normally, 200 to 2000GE (out of 1000 to 10000 GE of total available) are allocated for security reasons in an economical RFID tag [27].

d) Throughput

Throughput, in hardware, can be measured in terms of plain text processed per unit (bit per second) at 100 kHz frequency, whereas in software, it is the average amount of plaintext processed per CPU clock cycle at 4MHz frequency [28].

Table 1 presents comparative analysis of the different lightweight cryptography algorithms for smallest Gate Area. This table contains lightweight ciphers based on different performance parameters like memory, power, Gate Area and throughput. The cipher having lowest area gives better performance for the security of IoT devices.

Algorithm	Key size / Block size / Rounds			Structure	Performance			Attacks	Merits
					Power (µW)	Gate Area (GE)	Throughput(kbps)		
AES[9]	128	128	10	SPN	2.48	2400	56.64	Related key attack, Boomerang, Rectangle, Cryptanalysis	Supports larger key sizes, faster in hardware and software
PRESENT [11]	80 128	64	32	SPN	1.54 2.00	1570	12.4	Integral, bottle neck, truncated differential cryptanalysis , side channel attack	Ultra light weight cipher, energy efficient
HIGHT[12]	128	64	32	FN	5.48	3048	188.20	Impossible differential attack	Ultra light weight, provide high security, good for RFID tagging
CLEFIA [13]	128	128	18	FN	2.48	2488	39	Key recover attack on 10th round, saturation cryptanalysis	Energy efficient, fast encryption and decryption, lesser round.
TWINE[14] [22]	80 128	64	36	FN	1.30	1503 1866	178	Meet in the middle attacks, saturation attack	Efficient software performance, good for small hardware
CAMELLIA [22][24]	128	128	-	SPN	9.76	6511	290.1	Impossible differential attack, Cache timing attack	Security levels comparable to AES
RECTANGLE[16][29]	128	64	32	SPN	1.78	1787	188.20	Side attack, related-key cryptanalysis	Fast implementations using bit slice techniques
SIMON[15]	128	128	64	SPN	1.32	1317	22.9	Differential fault attacks	Supports several key sizes, performs well in hardware
SPECK[15]	128	128	32	SPN	1.40	1396	12.1	Key recovery, Boomerang attack	Performs better in software

IV. CONCLUSION

The lightweight cryptographic block cipher has played an important role in the development of the IoT. Lightweight cryptography contributes to the security and authentication of IoTs because of its efficiency. This paper presents recent developments, performance and implementations of lightweight block ciphers. A comparative analysis was presented, with the information presented in table 1. This helps in deciding the best algorithm for the security of IoT devices. From the literature review PRESENT cipher is suitable of IoT devices due to its low Gate Area as compare to other block ciphers.

V. FUTURE SCOPE

Performance evaluation of different lightweight algorithms based on different parameters like power consumption and processing time can be performed for the security of IoT devices. The result of this paper can be used as a performance reference for the implementation of lightweight algorithms in lightweight devices. In the future new lightweight cryptographic algorithms can be implemented in hardware that may produce much better results.

REFERENCES

[1] Thakor, Vishal & Razzaque, Mohammad Abdur & Khandaker, Muhammad. (2020). Lightweight Cryptography for IoT: A State-of-the-Art.

[2] M. A. Latif, M. B. Ahmad and M. K. Khan, "A Review on Key Management and Lightweight Cryptography for

IoT," 2020 Global Conference on Wireless and Optical Technologies (GCWOT), 2020, pp. 1-7, doi: 10.1109/GCWOT49901.2020.9391613.

[3] NEC(2017), Available at: (NEC, 2017) (Accessed: 27/10/22)

[4] Sajid, A., Abbas, H., & Saleem, K. (2016). Cloud-assisted IoT-based SCADA systems security: A review of the state of the art and future challenges. *IEEE Access*, *4*, 1375-1384.

[5] Dual Authentication-Based Encryption with a Delegation System to Protect Medical Data in Cloqud Computing - Scientific Figure on ResearchGate. Available from: https://www.researchgate.net/figure/Lightweight-cryptography-LWC-diagram_fig1_330819474 [accessed 11 Oct, 2022]

[6] McKay, K., Bassham, L., Turan, M. S., & Mouha, N. (2017). Report on lightweight cryptography (nistir8114). *National Institute of Standards and Technology (NIST)*.

[7] James, Mary, and Deepa S. Kumar. "An implementation of modified lightweight advanced encryption standard in FPGA." *Procedia Technology* 25 (2016): 582-589.

[8] 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, doi: 10.1109/ACCESS.2021.3052867.

[9] Moradi, A., Poschmann, A., Ling, S., Paar, C., & Wang, H. (2011, May). Pushing the limits: A very compact and a threshold implementation of AES. In *Annual International Conference on the Theory and Applications of Cryptographic Techniques* (pp. 69-88). Springer, Berlin, Heidelberg.

[10] James, M., & Kumar, D. S. (2016). An implementation of modified lightweight advanced encryption standard in FPGA. *Procedia Technology*, *25*, 582-589.

[11] Bogdanov, A., Knudsen, L. R., Leander, G., Paar, C., Poschmann, A., Robshaw, M. J., ... & Vikkelsoe, C. (2007, September). PRESENT: An ultra-lightweight block cipher. In *International workshop on cryptographic hardware and embedded systems* (pp. 450-466). Springer, Berlin, Heidelberg.

[12] Hong, D., Sung, J., Hong, S., Lim, J., Lee, S., Koo, B. S., ... & Chee, S. (2006, October). HIGHT: A new block cipher suitable for low-resource device. In *International workshop on cryptographic hardware and embedded systems* (pp. 46-59). Springer, Berlin, Heidelberg.

[13] Akishita, T., & Hiwatari, H. (2011, August). Very compact hardware implementations of the blockcipher CLEFIA. In *International Workshop on Selected Areas in Cryptography* (pp. 278-292). Springer, Berlin, Heidelberg

[14] Suzaki, T., Minematsu, K., Morioka, S., & Kobayashi, E. (2012, August). $\textnormal {\textsc {TWINE}} $: A Lightweight Block Cipher for Multiple Platforms. In *International Conference on Selected Areas in Cryptography* (pp. 339-354). Springer, Berlin, Heidelberg.

[15] Beaulieu, R., Shors, D., Smith, J., Treatman-Clark, S., Weeks, B., & Wingers, L. (2015, June). The SIMON and SPECK lightweight block ciphers. In Proceedings of the 52nd annual design automation conference (pp. 1-6).

[16] Zhang, W., Bao, Z., Lin, D., Rijmen, V., Yang, B., & Verbauwhede, I. (2015). RECTANGLE: a bit-slice lightweight block cipher suitable for multiple platforms. *Science China Information Sciences*, *58*(12), 1-15.

[17] A. Beg, T. Al-Kharobi and A. Al-Nasser, "Performance Evaluation and Review of Lightweight Cryptography in an Internet-of-Things Environment," 2019 2nd International Conference on Computer Applications & Information Security (ICCAIS), 2019, pp. 1-6, doi: 10.1109/CAIS.2019.8769509.

[18] K. N. Pallavi, V. R. Kumar and S. Srikrishna, "Comparative Study of Various Lightweight Cryptographic Algorithms for Data Security Between IoT and Cloud," 2020 5th International Conference on Communication and Electronics Systems (ICCES), 2020, pp. 589-593, doi: 10.1109/ICCES48766.2020.9137984.

[19] E. R. Naru, H. Saini and M. Sharma, "A recent review on lightweight cryptography in IoT," 2017 International Conference on I-SMAC (IoT in Social, Mobile, Analytics and Cloud) (I-SMAC), 2017, pp. 887-890, doi: 10.1109/I-SMAC.2017.8058307.

[20] S. Al Salami, J. Baek, K. Salah and E. Damiani, "Lightweight Encryption for Smart Home," 2016 11th International Conference on Availability, Reliability and Security (ARES), 2016, pp. 382-388, doi: 10.1109/ARES.2016.40.

[21] D. Sehrawat, N. S. Gill and M. Devi, "Comparative Analysis of Lightweight Block Ciphers in IoT-Enabled Smart Environment," 2019 6th International Conference on Signal Processing and Integrated Networks (SPIN), 2019, pp. 915-920, doi: 10.1109/SPIN.2019.8711697.

[22] I. Bhardwaj, A. Kumar and M. Bansal, "A review on lightweight cryptography algorithms for data security and authentication in IoTs," 2017 4th International Conference on Signal Processing, Computing and Control (ISPCC), 2017, pp. 504-509, doi: 10.1109/ISPCC.2017.8269731.

[23] Biswas, K., Muthukkumarasamy, V., & Singh, K. (2014). An encryption scheme using chaotic map and genetic operations for wireless sensor networks. *IEEE Sensors Journal*, *15*(5), 2801-2809.

[24] 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, doi: 10.1109/ACCESS.2021.3052867.

[25] Hatzivasilis, G., Fysarakis, K., Papaefstathiou, I., & Manifavas, C. (2018). A review of lightweight block ciphers. *Journal of cryptographic Engineering*, *8*(2), 141-184.

[26] McKay, K., Bassham, L., Turan, M. S., & Mouha, N. (2017). Report on lightweight cryptography (nistir8114). *National Institute of Standards and Technology (NIST)*.

[27] Juels, A., Weis, S.A. (2005). Authenticating Pervasive Devices with Human Protocols. In: Shoup, V. (eds) Advances in Cryptology – CRYPTO 2005. CRYPTO 2005. Lecture Notes in Computer Science, vol 3621. Springer, Berlin, Heidelberg. https://doi.org/10.1007/11535218_18

[28] Okello, W. J., Liu, Q., Siddiqui, F. A., & Zhang, C. (2017, July). A survey of the current state of lightweight cryptography for the Internet of things. In *2017 International Conference on Computer, Information and Telecommunication Systems (CITS)* (pp. 292-296). IEEE.

[29] Zhang, W., Bao, Z., Lin, D., Rijmen, V., Yang, B., & Verbauwhede, I. (2015). RECTANGLE: a bit-slice lightweight block cipher suitable for multiple platforms. *Science China Information Sciences*, *58*(12), 1-15.