EAI Endorsed Transactions
on Internet of Things
Research Article EAI.EU

Lightweight Cryptography for Internet of Things: A Review

Amrita[1,*], Chika Paul Ekwueme[2], Ibrahim Hussaini Adam[3], Avinash Dwivedi[4]

[1]Center of Excellence in Cyber Security and Cryptology, Computer Science & Engineering, Sharda School of Engineering & Technology, Sharda University, Greater Noida, Uttar Pradesh, India, https://orcid.org/0000-0001-6922-3403
[2]Computer Science & Engineering, Sharda School of Engineering & Technology, Sharda University, Greater Noida, Uttar Pradesh, India, https://orcid.org/0009-0000-1061-9382
[3]Computer Science & Engineering, Sharda School of Engineering & Technology, Sharda University, Greater Noida, Uttar Pradesh, India. https://orcid.org/0000-0003-4674-2213
[4]School of Computing Science and Engineering, Galgotias University, Greater Noida, Uttar Pradesh, India.

Abstract

The paper examines the rising significance of security in Internet of Things (IoT) applications and emphasizes the need for lightweight cryptographic solutions to protect IoT devices. It acknowledges the growing prevalence of IoT in various fields, where sensors collect data, and computational systems process it for action by actuators. Due to IoT devices' resource limitations and networked nature, security is a concern. The article compares different lightweight cryptographic block cipher algorithms to determine the best approach for securing IoT devices. It also discusses the merits of hardware versus software solutions and explores potential security threats, including intrusion and manipulation. Additionally, the article outlines future work involving the implementation of the trusted Advanced Standard Encryption block cipher in IoT devices, including its use in quick-response (QR) code scanning and messaging platforms. It acknowledges existing drawbacks and suggests areas for improvement in IoT system performance and security.

Keywords: Lightweight Cryptography, Internet of Things (IoT), Cryptography, Block Cipher, Advanced Standard Encryption (AES)

Received on 14 December 2023, accepted on 20 March 2024, published on 27 March 2024

doi: 10.4108/eetiot.5565

*Corresponding authors Email: amritaprasad_y@yahoo.com

1. Introduction

With computing becoming more prevalent in people's life, they are increasingly defined by a plethora of smart gadgets or devices, Internet of Things (IoT) is one of them. Approximately 13.8 billion active devices were reported in 2021, and projections suggest that this number could become 75 billion by the end of 2025 [1][2]. Things that can communicate and interact with one another via wired or wireless transmission are referred to as IoT. These devices are time-related in that they convey information based on real-time data acquired from sensors that connect with users through a network, allowing them to take action based on their needs [3][4].

IoT is a network of networked devices as shown on figure 1 that communicate information and data in real time. The three vital main components of IoT architecture are perception layer, network layer and application layer. The physical layer, where devices such as RFID tags, sensors, and cameras assist in collecting data from the environment. The network layer, which acts as the heart of IoT as it consists of both hardware and software components and transmits information collected by the physical layer. The application layer, which serves as a link between the user and the IoT device [5][6]. The

devices are used in a variety of industries as [7][8] [9][10][11]:

Figure 1. IoT Devices

(i) Home automation: when multiple IoT devices are connected in smart homes so that users can handle various activities such as turning on and off lights and controlling the temperature inside the house all from their phone.

(ii) In healthcare: IoT devices have greatly aided the monitoring of patients, resulting in a higher percentage of lives saved because doctors can monitor the devices connected to the patient on their tablets and obtain real-time data of the patient, allowing them to be notified immediately if something is wrong.

(iii) Surveillance has improved as a result of IoT devices connected to each other via network, making it easier to guarantee safety, such as by using cameras and motion detectors to monitor the movement of someone or an object being conveyed from one point to another where data can be presented in a device such as a smart phone.

(iv) Natural catastrophes: They have been aided by IoT technology, which have assisted us in preventing accidents and increasing disasters by assisting in disaster prediction. It can now collect data from sensors placed in various environments, which may assist us in disaster prediction.

This situation involves critical scenario of collecting highly sensitive data through IoT devices, often without individuals' awareness. The challenge lies in ensuring private and secure communication to safeguard data integrity and prevent unauthorized access to individual information. However, standard devices in IoT architecture face limitations in computational resources and power capacity, referred to as resource-constrained devices. To ensure the protection of data, it is necessary to employ a method, and this is where cryptography becomes crucial [12].

While the significance of security based on cryptography is growing, incorporating various cryptographic standards and algorithms in an IoT devices remain challenging due to significant area and power overhead. Additionally, effective encryption in IoT necessitates appropriate and efficient encryption key management processes, as inadequate key management can jeopardize overall security. IoT devices are inherently lightweight, implying limited storage space. Moreover, as IoT devices rely on batteries, minimizing power consumption is a key consideration.

Conventional ciphers like Advanced Encryption Standard (AES), Data Encryption Standard (DES), and RC6 are unsuitable for direct application in IoT domains due to the heterogeneous, scalable, and dynamic nature of these devices [13]. To address this, the scientific literature explores lightweight cryptographic algorithms as potential solutions. These algorithms aim to mitigate the computational impact of security measures, striking a balance between cost and performance to enhance human security and privacy [14][15][16].

In the review went through different and recent work done by researchers in determining best security options for IoT devices as going through different lightweight algorithm comparing them in terms of block ciphers and mainly approach in Advanced Standard Encryption (AES) for the IoT solution in terms of its security [17] [18] [19].

The following are the sections of the paper: Cryptography background is reviewed in Section 2. Section 3 provides the literature survey. In Section 4, it represents Lightweight Cryptography based AES. Section 5 and Section 6 represent discussion and conclusion and future research respectively.

2. Cryptography Background

2.1. Cryptography

Cryptography is the method of encrypting data into cipher text for safe transmission, preventing unauthorized users from accessing or altering information. Cryptography is categorized into two types: symmetric cryptography and asymmetric cryptography [12].

1) Symmetric Cryptography: Symmetric cryptography is a cypher technology that encrypts and decrypts data sent across a network using the same key Figure 2. It's secure and fast but the problem is sharing the key as when it falls in a wrong hand the encrypted data is compromised [12].

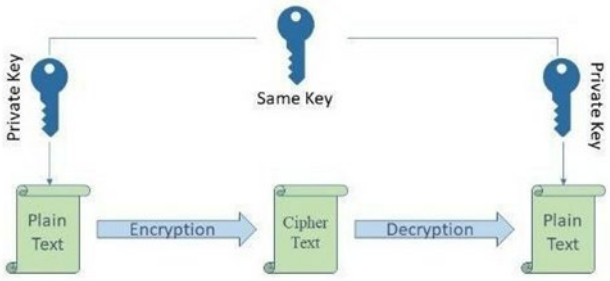

Figure 2. Symmetric Cryptography

Symmetric cryptography is composed of three ciphers stream cipher, block cipher, and hash function which contain algorithms such as AES, DES, and BLOWFISH etc.

2) Asymmetric Cryptography: Asymmetric cryptography is an encryption technology that communicates between the sender and receiver using two keys: a private key and a public key (Figure 3) (as encrypting and decrypting of data). In this approach, the sender employs the public key for encrypting the data, and the recipient utilizes the private key for decrypting it. It supports any security forces and provides a secure way for sharing keys, but it has the disadvantage of being more sophisticated and sluggish, as well as having a high key size. Asymmetric cryptography contains different algorithm such as RSA, Deffie-Hellmen and Elliptic Curve [12].

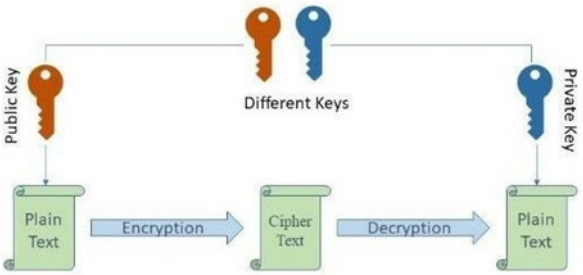

Figure 3. Asymmetric Cryptography

2.2. Lightweight Cryptography

IoT devices has it challenges which compute in applying cryptographic technique to secure them. IoT devices are compacted with small memory, small computing power, small physical area and need to have real time response where all of this compute in designing the cryptographic algorithm to protect the data in the devices [16] [18].

Although cryptographic methods are used to secure data, some methods not adequate to protect limited devices such as IoT thus were lightweight cryptographic comes in. Lightweight cryptography is a type of encryption whose techniques are intended to be used in pervasive device with low resources needed. As for protecting the data in IoT devices the algorithms to be accepted has to be qualified in terms of security and algorithm itself. For security requirements the cryptographic algorithm to be accepted it should ensure, confidentiality as the data to access by only the sender and receiver. Integrity where the data needs not to be altered when transmitted. Authentication is possible since the information and the client are both verifiable. The user cannot dispute the communication with the data sent due to non-repudiation [20].

As the usage of IoT device is increasing the need of secure and encrypted communication is important thus the algorithms need to meet the security requirements. As for algorithm itself it needs to consider in both hardware and software capabilities. In software, the algorithm's temporal complexity is taken into account. Also, memory is being considered as the amount of RAM and ROM for carrying out computation and the storage of the algorithm is compiled [19]. For specification in terms of hardware the algorithm is being categorized in different aspects. Power consumption was the algorithm needs low power consumption to be applicable in the IoT devices. Latency as it's the delay time is considered for algorithm used for securing IoT devices [21] [22].

Therefore, symmetric key cryptography algorithms are typically recommended for the design of IoT devices, given their lower storage space requirements, processing power, complexity, and bandwidth usage in comparison to asymmetric key cryptography algorithms.

1) Lightweight Cryptography Types: Light-weight cryptography is also categorized into symmetric and asymmetric key cryptography. As asymmetric key is more secure than symmetric encryption, it is more complex and take more time to compute which is not favoured for most IoT device, where symmetric encryption comes to picture as it is fast and secure and has low latency. Hence, it is generally recommended to utilize symmetric key cryptography algorithms in the design of IoT devices. This is because they demand lower complexity, storage space, processing power, and bandwidth compared to asymmetric encryption. Top of Form
As symmetric contains stream and block cipher where stream uses a key same as the data and block have fixed length of key bits [8].

Rather than stream cypher, block cypher is favoured because it is more adaptable, which is highly useful in IoT. Furthermore, because the procedure uses almost same encryption and decryption techniques, it consumes fewer resources, which benefits IoT devices [23]. A block cipher has been favored for creating resource constrained computing devices over the past decade. This preference is attributed to its simpler hardware and software implementation, along with superior error propagation and diffusion features. It demands significantly limited hardware resources when compared to a stream cipher. The factors of LWC requirements are — number of rounds, block size, key size, and structure.

2) Basic Design of Block Cipher:

Substitution-box (S-box): the input structure in it is usually 4 bits of block which result to 4 bits output from substitution function [24]. The S-box increases the computation and processing time thus if the encryption contains large number of active S-boxes the security is high.

Permutation-box (P-box): it processes by shuffling inputs bits into other bits as output. P-Box takes S-Box output as its inputs where it shuffles its bits by changing its order.

Rounds: In block ciphers, encryption and decryption processes consist of multiple rounds. Each round involves a set of operations, and a different sub-key is used for each round. These sub-keys are generated using a key generation algorithm [24][25].

Substitution-Permutation Network (SPN): Many modern block ciphers, including AES, use an SPN structure in each round. It involves substituting bytes (substitution) and then permuting the positions of these substituted bytes (permutation). This operation helps in achieving diffusion and confusion, two essential properties of secure ciphers.
The Feistel Network: divides the input block into equally halves with applied diffusion to only one half in each round, resulting in swapping at the start of each cycle.

2.3. Attacks in Lightweight Cryptography

Lightweight cryptography is vulnerable to attacks. Some of the attacks in lightweight cryptography are as follows [26][27]:

1) An exhaustive key assault: It attempts to identify a key that can be used to reconstruct a plain text using the procedure for a cypher text, often referred as a brute force assault. In theory, the attacker will try to deplete all possible keys. However, any encryption that can be computationally cracked by doing a thorough key search deemed unsafe by current standards. The theoretical attack limit is (2*128), meaning that with present technology, key length of 128 and above is possibly unbreakable.

2) Table lookup attacks: The attacker is aware of key size and has prepared a table of cypher text in advance all possible keys of that length for a similar message. All he needs to do when he intercepts a matching encrypted text is seek for the associated key. If somehow the intruder has sufficient memory to store blocks of cipher text, this attack is viable. By collecting related plaintexts and cypher text, the dictionary attack completely eliminates key recovery. When an intruder retrieves a cypher text, they look for a plaintext match. Only works in a large plaintext, cypher text dictionary, and requires the use of the identical key for each of these pairs.

3) Differential Attacks: The disparity between the plain text and the encrypted text is used to demonstrate the block cipher's vulnerability. Where the condition of the system may be exposed when the difference is applied.

4) Algebraic attack: It operates on the premise that many cryptographic systems can be characterized as a binary system featuring multidimensional non-linear equations, and the private key is revealed through the solution of these equations.
It was recently introduced and uses the notion that most cryptographic systems can be described as a binary system with multidimensional non-linear equations, with the private key exposed by solving the equations.

Although solving these issues is NP-hard, numerous theories are being examined as possible solutions, including Grobner bases and linearization.

3. Literature Survey

There is a significant demand for lightweight cryptography to tackle the constraints of data size, device power, and computing device costs, minimizing them effectively. Therefore, when developing a cryptography algorithm specifically for small computing devices, the primary goal should be to make it lightweight in various aspects, including memory usage, chip size, power consumption, and more [28].

In [29] they presented a method for avoiding the sharing of the secret key to the replacement box by producing a fake key to mask the secret key, resulting in a large power area and high algorithm performance on devices.

Related keys are used to increase the number of iterations in which an unacceptable situation is produced in order to lessen attack complexity [30]. The AES 192 cryptographic strength as determined by reduced round attacks and a new related key introduced in this article. The complexity of assaults on eight or maybe more rounds of AES may be reduced if a round is inserted before a round whereby the impossibility situation starts instead of after round in which the difficult condition ends.

They presented a wireless interceptive Side-Channel Attack (SCA) approach for (IoT) applications that uses Correlation Electromagnetic Analysis (CEMA) to disclose the AES-128 encryption system's 16-byte secret key in wireless communications [31]. As a result, our study can pinpoint which CPU module is leaking the linked EM signals.

They concentrated on DFA attacks on AES decryption because decryption is just as important as encryption. The suggested DFA attacks were successfully demonstrated to be effective against AES decryption, which is just as crucial as encryption. The computational time required to attack AES decryption is 511 ms longer than that required to attack AES encryption, according to the results [32]. They refined the suggested S-box distribution table is

used by the DFA assault reduced the necessary processing time using just two pairs of fault free and defective plaintexts.

They suggested a new AES mixed S-box/inverse S-box architecture in this study that would be both lighter and speedier than Canright's [33]. In terms of physical area of device and latency, our unique combination the S-box's design exceeds the best method known in the literature, according to our study and ASIC implementation findings.

They updated the Serpent Algorithm in terms of computing and algebra in order to make it compatible with a variety of applications [34]. The change is that it is now 31% less complicated and quicker than the previous method.

They designed and implemented a single highly beneficial approach for AES area efficiency as well as excellent performance by employing "mixing of column and inverse mixing of column operation," This is among the most important operational blocks in AES for achieving an excellence performance [35]. The results show that the suggested mix-column architecture is simpler than earlier work when it comes to gate length and clock rotations.

They created and showed a small architecture for AES mix-columns working as well as its inverse [36]. Previous work in this area is compared to the hardware implementation. They demonstrated that our architecture has fewer gates than existing designs that implement both the forward and inverse mix columns operations. The comparisons show that the suggested mix-column structures are less difficult than earlier work in this area.

They discovered the power used during the encryption cycle process of whatever block cipher with an r-round unwrapped structure is indeed a quadratic function by researching A CMOS gate's energy consumption model. They then used our approach to forecast the best value of (r) for unrolling an r-round design as it is believed that a cypher will be the most power efficient [37]. using well-known lightweight block cyphers. They demonstrated that the overall power spent during a functioning of encryption is generally proportional to the degree of unrolling.

They've submitted a design study for minimal AES Data encryption cores for IoT [38]. The theoretical lower bound for the clock rotation count per encryption has been investigated, and prior designs have indeed been examined. The advantages of native S-box designs have indeed been proved and quantified, as well as design advice for obtaining a desired achievement count.

The CLEFIA lightweight algorithm created by Sony Corporation in 2007, is a block cipher that imposed new approaches such as digital rights management, which improved security against attacks, and it also has a wider range of application in terms of hardware and software capabilities for implementing security [39].

As its goal is to assure hardware economy and security, the current lightweight algorithm is an ultralight cryptography that delivers security of block size of 64bit data guarded by a key with 80bit.

The HIGHT lightweight method introduced by Hong et al in 2006 was shown to be highly handy for severely restricted devices such as RFID tags, and it was also found to be quicker than other algorithms such as AES in 8-bit microcontrollers, however it was a generalized imbalanced fiestel network [40].

The author produced a variation of DES depending on the number of bits they processed, assigning 4bit and 6bit data rather than 32bit and 48bit data, meaning the shortest DES implementation but resulting in poor security [41]. The author added XOR gates to the DES to improve security, a process known as key whitening, where one is placed in plaintext before the cipher process and the other in the cipher-text result.

PRESENT algorithm was induced as block cipher algorithm for the lightweight cryptographic algorithm [42]. The authors explored the algorithm works as a secure algorithm working with 64 bits of block size and being processed with 80 bits key. The author explained the blowfish algorithm's execution using FGPA (field programmable get array), which produces a great result by being easy to implement at a high speed while also reducing the amount of time required to encrypt the data, resulting in higher throughput, all done in a highly integrated circuit description language (VHDL) [45].

Introducing a novel algorithm, GFRX, which amalgamates a generalized Feistel structure with Addition or AND, Rotation, XOR (ARX). The GFRX algorithm employs an ARX configuration with diverse non-linear components to address all branches of a generalized Feistel structure, enhancing diffusion effects in fewer rounds. Security analysis results for the GFRX algorithm indicate that effective differential attacks are contained within 19 rounds, and effective linear attacks do not exceed 13 rounds. Hence, the GFRX algorithm demonstrates a sufficient security level for both differential and linear analyses. Avalanche test results for GFRX underscore robust diffusion, achieving the avalanche effect in just six rounds. Moreover, the GFRX algorithm offers varying levels of serialization based on distinct hardware resource requirements, including the capability of achieving full serialization. This feature ensures operational flexibility in environments with resource constraints [46].

The study introduces LRBC, a novel encryption technique tailored for resource constrained IoT devices, providing enhanced data security at the sensing level. LRBC combines the structural benefits of SPN and Feistel structure for improved security. Experimental validation was conducted using the NEXYS 4 DDR FPGA (Artix-7) trainer kit and implementation on a TSMC 65 nm ASIC chip. The proposed technique demonstrates low power consumption (11.40 µW) and occupies a compact 258.9 GE area. Security analysis affirms robustness against various attacks, ensuring high security. LRBC also exhibits an average avalanche effect of 55.75% and 58% for key and plaintext respectively [47].

The LCB encryption strategy, tailored for IoT devices, enhances security by combining the advantages of the

Feistel structure and the substitution permutation network architecture. Tested on the (Virtex-7) XC7VX330T FPGA board, LCB occupies a minimal area of 224 GE and demonstrates high speed with a low combinational path delay of 0.877 ns. Extensive testing validates its ability to offer heightened security against cryptographic attacks. The Avalanche Effect of LCB is observed at 63.125% and 63.875% for the key and plaintext respectively [48].

This paper presents the development of a resilient and efficient lightweight cipher tailored for securing the IoT environment, specifically designed to accommodate the resource limitations inherent in IoT devices. Additionally, we introduce a lightweight cryptographic algorithm based on symmetric and block ciphers. This algorithm enhances the intricacy of the block cipher while minimizing computational demands. It effectively implements a key register updating method, decreases the number of encryption rounds, and introduces an additional layer between the encryption and decryption processes. [49].

Another algorithm proposed by where it tries to cover all the specs in terms of software and hardware were the researcher proposed the SIMON algorithm for as a lightweight algorithm for implementation of hardware specification and SPECK to which was introduced for optimal implementation of the software specification [50].

In [51], the presentation of four area-optimized S-boxes is featured, consisting of two 4-bit S-boxes (S1 and S2) and two 8-bit S-boxes (SB1 and SB2). These S-boxes are well-suited for the building of lightweight block ciphers. The outcomes indicate that the suggested structures exhibit reasonable utilization of hardware resources, timing characteristics, and security properties when compared to alternative approaches.

A lightweight block cipher called TWINE, consisting of 36 rounds, with a block size of 64 bits and a key size of 80/128 bits is introduced [52]. Meanwhile, a reassessment of the security of TWINE-80 is conducted by researchers in [27]. Their study focused on impossible differential cryptanalysis in a related-key model, and they enhanced the conventional impossible differential attack by introducing an additional round.

The Table 1 tries to give abroad visualization on the algorithm gone through basing on their characteristic such as size of their keys and blocks and rounds required by a specific key. Also, Table 2 expresses the different implementation based to different technology as expressing with the reference of their amount of throughput.

Table 1. Comparison between different light-weight algorithms

Ref.	Algorithm	Key Size (Bits)	Block Size(bits)	Rounds
[44]	AES	128,192,256	128	10,12,14
[45]	BLOWFISH	32-448	64	16
[39]	CLEFIA	128,192,256	128	18,22,26
[41]	DES	56	64	16
[43]	DESXL	184	64	48
[40]	HIGHT	128	64	32
[42]	PRESENT	80,128	64	32
[50]	SIMON	128	128	64
[50]	SPECK	128	128	32

Table 2. Performance in terms of Throughput

Ref	Algorithm	Key Size	Technology (μM)	Throughput (KBPS)
[44]	AES	128	0.13	56.64
[39]	CLEFIA	128	O.13	39
[40]	HIGHT	128	0.25	188.2
[42]	PRESENT	128	0.18	12.12
[50]	SIMON	128	0.13	22.9
[50]	SPECK	128	O.13	12.1

In the Table 3, the researcher tried to compare the implementation with AES in which we can see the HIGHT implementation resulted into higher throughput compared to the AES but rather than that we can't compare the two technologies as we can't compare different implementations with different technology, as some may be easier in other harder in the FGPAs [40].

Table 3. HIGHT and AES comparison

Technology	Algorithm	Throughput	Area
0.25μM	HIGHT	150 MBPS	3048
0.35μM	AES	9.9 MBPS	3400

In the Table 4, we described different algorithms by illustrating their different structures that they are composed of and to what remarks have the algorithm being given by different researchers who have explored the algorithms.

Table 4. Structure and Remarks of the Algorithms

Ref.	Algorithm	Structure	Remarks
[44]	AES	SPN	It has a great key size thus supporting both software and hardware
[45]	BLOWFISH	FN	It flexible and has a great security
[39]	CLEFIA	FN	Its fast in both encryption and decryption with less round
[41]	DES	FN	Not very secure
[43]	DESXL	FN	It has a larger key
[40]	HIGHT	FN	Its very lightweight as good for RFID devices
[36]	PRESENT	SPN	Used for small data encryption as it requires less memory
[50]	SIMON	SPN	Good for hardware implementations
[50]	SPECK	SPN	Better performance in the software implementation

4. Lightweight Cryptography Based on AES

AES as being a standardized algorithm (in 2001) by NIST is the block cipher which can work in different key size either in 128, 192 or 256 bits. Implored as a better algorithm as no attacks are able to distort its security as most end at round 6 thus AES with its extra rounds (10,12,14) according to the key size ensure better security and unbreakable algorithm as it works based on substitution and permutation network [53].

As different researchers went through different implementations, they came to different aspect to as improvement of AES such as efficiency in the power consumption as implied in paper also others implied to achieve better design of the energy as bringing the power consumption to the minimum while ensuring high throughput and ensure low cost of production as illustrated by [53][54].

In our work of finding a capable lightweight algorithm suitable for the small computing system of the IoT devices implementation was done on an application reviewing how encryption works which will help to create secure communication among the devices and also an app to encrypt the QR codes. The pursue of this creation uses the AES algorithm for encryption as found to be more secure than other algorithm to date, as QR encryption will bring benefits in a large area in IoT as many IoT activities uses QR to connect with the system [55][56].

5. Discussion

The majority of IoT research has been focused around cyber security. It is difficult to find a single apparent solution that works for all kinds of IoT applications. Several sorts of systems are connected in an IoT infrastructure. Some equipment can afford to be bulky and secure, but the vast majority of IoT devices are limited in their resources. They want a network security that is quick to react. Likewise, it must be easier to use and adapt. Lastly but not least, there's the question of dependable security. Currently, one guy owns four connected devices. The future can't be risked by relying on an unreliable algorithm.

This poll began with the goal of identifying the most appropriate approach for IoT security. Our study began by looking at Lightweight Cryptographic solutions, bearing the constraints that IoT gadgets face. Research was done based on symmetric and asymmetric key cryptography solutions. A solution needed for IoT needs to be both speedier and less difficult and discovered that a Symmetric Cryptographic solution was fit for the criteria.

Stream ciphers and block ciphers are the two most important Symmetric Cryptographic ciphers. were further explored and analyzed. Because block ciphers are more adaptable compared to stream ciphers, academics have developed a number of lightweight algorithms using block cipher technique that may be used in IoT.

The followed stage was to figure out which cryptography based on block algorithm was the most secure and well-researched. AES was decided as most trustworthy block cipher that has been studied that can protect and secure the IoT from cyber threats after reviewing and comparing different research papers. The problem with AES is it wasn't designed to meet the Lightweight criterion of a block cypher in the first place. This paper featured a review of hardware & system security mechanisms, and the conclusion was reached that a physical solution for IoT is now required.

The task on hand set for ourselves was to collect research on Lightweight algorithm using AES. Some AES architectural documents that were discovered meant to be lightweight. Conclusion was reached that the S-box and Mix-Column are key components of AES that contribute to its complexity. Research was done based on these topics. Work of many AES attacks were incorporated in the paper. This survey included a wide range of feasible security mechanisms, and based on our findings, lightweight AES might be an appropriate security solution for restricted IoT devices.

6. Conclusion and Future Research

Solutions of lightweight security for the IoT were covered in our study. The studies based on asymmetric cryptographic techniques and symmetric cryptography for the IoT (Stream Ciphers algorithm and Block Ciphers algorithm). In terms of design, mix-column and Substitution-box, and risks, was examined at recent research on Advanced Standard Encryption (AES) for IoT. As per our findings, lightweight algorithm by AES is an excellent security option for most of constrained IoT devices as have limited resources.

The AES block cypher is a well and investigated of all the block cyphers. Researchers are concentrating on making AES lighter and more IoT-friendly. Improvement on the AES design is our future with the goal of creating a lightweight IoT ecosystem.

References

[1] Global IoT and non-IoT connections 2010–2025 (accessed on 17 august 2023), 2023. URL https://www.statista.com/statistics/1101442/.

[2] Georgiev, D. Internet of Things Statistics, Facts & Predictions [2023′s Update]. Available online: https://review42.com/resources/internet-of-things-stats/

[3] Ding, J., Nemati, M., Ranaweera, C., and Choi, J. IoT Connectivity Technologies and Applications: A Survey. IEEE Access. 2020; 8: 67646-67673.

[4] Alfred Y. Network Security. Malaysia: Asia Pacific University; 2019. pp. 5-11.

[5] Tariq, U., Ahmed, I., Bashir, A.K., Shaukat, K. A. Critical Cybersecurity Analysis and Future Research Directions for the Internet of Things: A Comprehensive Review. Sensors. 2023; 23: 4117.

[6] Caraveo-Cacep, M.A., Vázquez-Medina, R., Zavala, A.H. A survey on low-cost development boards for applying cryptography in IoT systems. Internet of Things. 2023; 22: 100743.

[7] Majumdar, A., Laskar, N.M., Biswas, A., Sood, S.K., Baishnab, K.L. Energy efficient e-healthcare framework using HWPSO-based clustering approach. J Intell Fuzzy Syst. 2018; 36(5):1–13.

[8] Velmurugan, T., Prakasam, P., Mohameed, V.N., Saravanan, K. Smart garbage monitoring and navigation system using IoT. Int. J. Innov. Technol. Expl. Eng. 2019; 8 (11): 3992–3996.

[9] Mista, S., Roy, C., Mukherjee, A. Introduction to Industrial Internet of Things and Industry 4.0. 1st ed. Florida: CRC Press; 2021.

[10] Stolojescu-Crisan, C., Crisan, C., & Butunoi, B. P. An iot based smart home automation system. Sensors. 2021; 21(11): 3784.

[11] Abu-Tair, M., Djahel, S., Perry, P., et al. Towards secure and privacy-preserving IoT enabled smart home: architecture and experimental study. Sensors. 2020; 20(21): 6131.

[12] William, S. Cryptography and Network Security: Principles and Practice. 8th ed. London: Pearson; 2017.

[13] Gunathilake, N. A., Buchanan, W. J., and Asif, R. Next Generation Lightweight Cryptography for Smart IoT Devices: Implementation, Challenges and Applications. In: IEEE 5th World Forum on Internet of Things (WF-IoT). 2019.

[14] Bhagat, V., Kumar, S., Gupta, S.K., Chaube, M.K. Lightweight cryptographic algorithms based on different model architectures: A systematic review and futuristic applications. Concurrency and Computation Practice and Experience. 2023; 35(10): e7425.

[15] Silva, C., Cunha, V.A., Barraca, J.P. et al. Analysis of the Cryptographic Algorithms in IoT Communications. Inf Syst Front. 2023.

[16] Thakor, V.A., Razzaque, M.A., and Khandaker, M.R.A. Lightweight cryptography algorithms for resource-constrained IoT devices: A review, comparison and research opportunities. IEEE Access. 2021; 9: 28177-28193.

[17] Hassija, V., Chamola, V., Saxena, V., Jain, D., Goyal, P., and Sikdar, B. A survey on iot security: Application areas, security threats, and solution architectures. IEEE Access. 2019; 7: 82721-82743.

[18] Dutta, I. K., Ghosh, B., and Bayoumi, M.A. Lightweight Cryptography for Internet of Insecure Things : A Survey. In: IEEE 9th Annual Computing and Communication Workshop and Conference (CCWC). 2019. 475-481.

[19] Sadkhan, S. B. and Salman, A. O. A survey on lightweight-cryptography status and future challenges. In: International Conference on Advance of Sustainable Engineering and its Application (ICASEA), Wasit - Kut, Iraq. 2018. 105-108.

[20] Ammar, M., Russello, G., and Crispo, B. Internet of Things: A survey on the security of IoT frameworks. Journal of Information Security and Applications. 2018; 38: 8–27.

[21] Dhanda, S. S., Singh, B. and Jindal, P. Lightweight Cryptography: A Solution to Secure IoT. Wireless Personal Communications. 2020; 112(3): 1947–1980.

[22] Mousavi, S. K., Ghaffari, A., Besharat, S., et al. Security of internet of things based on cryptographic algorithms: a survey. Wireless Networks. 2021. 27(2): 1515-1555.

[23] Dutta, N.S., and Chakraborty, S. A survey on implementation of lightweight block ciphers for resource constraints devices. Journal of Discrete Mathematical Sciences and Cryptography. 2020; 1–22.

[24] Rana, M., Mamun, Q., and Islam, R. Lightweight cryptography in IoT networks: A survey. Future Generation Computer Systems. 2022; 129: 77-89.

[25] Bhardwaj, I., Kumar, A., and Bansal, M. A review on lightweight cryptography algorithms for data security and authentication in IoTs. In: International Conference on Signal Processing, Computing and Control (ISPCC), Solan, India; 2017. p. 504-509.

[26] Okello, W.J., Liu, Q., Siddiqui, F.A. and Zhang, C. A survey of the current state of lightweight cryptography for the Internet of things. In: International Conference on Computer, Information and Telecommunication Systems (CITS), Dalian, China; 2017. p. 292-296.

[27] Wei, Y., Xu, P., and Rong, Y. Related-key impossible differential cryptanalysis on lightweight cipher TWINE. J Ambient Intell Human Comput. 2019; 10(2): 509–517.

[28] Singh, S., Sharma, P.K., Moon, S.Y., Park, J.H. Advanced lightweight encryption algorithms for IoT devices: survey, challenges and solutions. J Ambient Intell Human Comput. 2017; 1–18.

[29] Yu, W., and Kose, S. A Lightweight Masked AES Implementation for Securing IoT Against CPA Attacks. IEEE Transactions on Circuits and Systems I: Regular Papers. 2017; 64(11) : 2934-2944.

[30] Jithendra, K. B. and Shahana, T.K. New Results in Related Key Impossible Differential Cryptanalysis on Reduced Round AES-192. International Conference On Advances in Communication and Computing Technology (ICACCT), Sangamner, India; 2018. p. 1-5.

[31] Pammu, A. A., Chong, K. -S., Ho, W.-G., and Gwee, B. -H. Interceptive side channel attack on AES-128 wireless communications for IoT applications. In: IEEE Asia Pacific Conference on Circuits and Systems (APCCAS), Jeju, Korea (South); 2016. p. 650-653.

[32] Zhu, L., Wang, Y., and Li, R. Efficient differential fault analysis attacks to AES decryption for low ost sensors in IoTs. In: IEEE International Symposium on Circuits and Systems (ISCAS), Montreal, QC, Canada; 2016. p. 554-557.

[33] Reyhani-masoleh, A., Taha, M., and Ashmawy, D. New Area Record for the AES Combined S-box / Inverse S-box. In: IEEE 25th Symposium on Computer Arithmetic (ARITH), Amherst, MA, USA; 2018. p. 145-152.

[34] Shah, T., Haq, T. U., Farooq, G. Serpent Algorithm: An improvement by 4 × 4 S - box from finite Chain ring. In: International Conference on Applied and Engineering Mathematics (ICAEM), Taxila, Pakistan; 2018. p. 1-6.

[35] Parikh, P., and Narkhede, S. High performance implementation of mixing of column and inv-mixing of column for AES on FPGA. In: International Conference on Computation of Power, Energy Information and Commuincation (ICCPEIC), Melmaruvathur, India; 2016. p. 174-179.

[36] Li, H., and Friggstad, Z. An efficient architecture for the AES mix columns operation. In: IEEE International Symposium on Circuits and Systems (ISCAS), Kobe; 2005. vol 5. p. 4637-4640.

[37] Banik, S., Bogdanov, A., and Regazzoni, F. Exploring Energy Efficiency of Lightweight Block Ciphers. In: Dunkelman, O., Keliher, L. (eds) Selected Areas in Cryptography – SAC, Lecture Notes in Computer Science, Springer; 2015. vol 9566.

[38] Zhao, W., Ha, Y., and Alioto, M. AES architectures for minimum energy operation and silicon demonstration in 65nm with lowest energy encryption. In: IEEE International Symposium on Circuits and Systems (ISCAS), Lisbon, Portugal; 2015. p. 2349-2352.

[39] Shirai, T., Shibutani, K., Akishita, T., Moriai, S., and Iwata, T. The 128-Bit Blockcipher CLEFIA (Extended Abstract). In: Biryukov, A. (eds) Fast Software Encryption. FSE Lecture Notes in Computer Science, Springer, Berlin, Heidelberg; 2007. vol 4593.

[40] Kim, B., Cho, J., Choi, B., Park, J., Seo, H. Compact Implementations of HIGHT Block Cipher on IoT Platforms. Security and Communication Networks. 2019; 5323578: 1-10.

[41] Leander, G., Paar, C., Poschmann, A., Schramm, K. New Lightweight DES Variants. In: Biryukov, A. (eds) Fast Software Encryption. FSE 2007. Lecture Notes in Computer Science, Springer, Berlin, Heidelberg; 2007. vol 4593. p. 196-210.

[42] Bogdanov. A., Knudsen, L.R., Leander, G., Paar, C., Poschmann. A., Robshaw, M.J.B., Seurin, Y., and Vikkelsoe, C. PRESENT: An Ultra-Lightweight Block Cipher. In: Paillier, P., Verbauwhede, I. (eds) Cryptographic Hardware and Embedded Systems - CHES. Lecture Notes in Computer Science, vol 4727. Springer, Berlin, Heidelberg; 2007.

[43] Majhi, S., and Mitra, P. Lightweight Cryptographic Techniques in 5G Software-Defined Internet of Things Networking. Lightweight Cryptographic Techniques and Cybersecurity Approaches. 2022. IntechOpen.

[44] Moradi., A. Pushing the Limits: A Very Compact and a Threshold Implementation of AES. In: Advances in Cryptology – EUROCRYPT, Lecture Notes in Computer Science, Springer; 2011. 6632. p. 69-88.

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

[46] Zhang, X.; Tang, S.; Li, T.; Li, X.; Wang, C. GFRX: A New Lightweight Block Cipher for Resource-Constrained IoT Nodes. Electronics. 2023; 12: 405.

[47] Biswas, A., Majumdar, A., Nath, S. *et al.* LRBC: a lightweight block cipher design for resource constrained IoT devices. J Ambient Intell Human Comput. 2023; 14: 5773–5787.

[48] Roy, S., Roy, S., Biswas, A., Baishnab, K. L. LCB: Light Cipher Block An Ultrafast Lightweight Block Cipher For Resource Constrained IOT Security Applications. KSII Transactions on Internet and Information Systems. 2021; 15(11): 4122-4144.

[49] Rana, M., Mamun, Q., and Islam, R. A block cipher for resource-constrained IoT devices. World Academy of Science, Engineering and Technology. 2023; 17(3): 266-271.

[50] Beaulieu, R., Treatman-Clark, S., Shors, D., Weeks, B., Smith, J., and Wingers, L. The SIMON and SPECK lightweight block ciphers. In: 52nd ACM/EDAC/IEEE Design Automation Conference (DAC), San Francisco, CA, USA; 2015. p. 1-6.

[51] Rashidi, B. Lightweight Cryptographic S-Boxes Based on Efficient Hardware Structures for Block Ciphers, ISeCure, 2023; 15(1): 137-151.

[52] Suzaki, T., Minematsu, K., Morioka, S., Kobayashi, E. Twine: a lightweight, versatile block cipher. In: ECRYPT workshop on lightweight cryptography; 2011, p. 146–169.

[53] Agwa, S., Yahya, E., and Ismail, Y. Power efficient AES core for IoT constrained devices implemented in 130nm CMOS. In: IEEE International Symposium on Circuits and Systems (ISCAS), Baltimore, MD, USA; 2017. p. 1-4.

[54] Bui, D. -H., Puschini, D., Bacles-Min, S., Beigné, E., and Tran, X. -T. AES Datapath Optimization Strategies for Low-Power Low-Energy Multisecurity-Level Internet-of-Things Applications. IEEE Transactions on Very Large Scale Integration (VLSI) Systems. 2017; 25(12): 3281-3290.

[55] Ibrahim, N, and Agbinya, J. Design of a Lightweight Cryptographic Scheme for Resource-Constrained Internet of Things Devices. Applied Science. 2023; 13(7): 4398.

[56] Thabit, F., Can, O., Aljahdali, A.O., Al-Gaphari, G.H., Alkhzaimi, H.A. Cryptography Algorithms for Enhancing IoT Security. Internet of Things. 2023; 22: 100759.