Journal of Theoretical and Applied Information Technology
15th April 2023. Vol.101. No 7
© 2023 Little Lion Scientific
ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

LWC: EFFICIENT LIGHTWEIGHT BLOCK CIPHERS FOR PROVIDING SECURITY TO CONSTRAINED DEVICES A SOLUTION FOR IOT DEVICES

ASHU ABDUL[1], GARLAPATI NARAYANA[2], R. SUDHA KISHORE[3], B. SRIKANTH[4], K. KRANTHI KUMAR[5], D.N.V.S.L.S. INDIRA[6]

[1]Assistant Professor, Department of Computer Science and Engineering, SRM University-AP, Andhra Pradesh, India.
[2]Associate Professor, Department of Computer Science and Engineering, CVR College of Engineering, Ranga Reddy, TS.
[3]Associate Professor, Department of Information Technology, Vasireddy Venkatadri Institute of Technology, Namburu, Guntur.
[4]Professor, Department of Computer Science and Engineering, Kallam Haranadhareddy Institute of Technology, Chowdavaram, Guntur District AP.
[5]Assistant Professor, Department of Information Technology, Vasireddy Venkatadri Institute of Technology, Namburu, Guntur
[6]Professor, Department of Information Technology, Seshadri Rao Gudlavalleru Engineering College, Gudlavalleru, AP, India-521356,

Email: ashu.a507@gmail.com, narayanag.1973@gmail.com, sdhkishore@gmail.com, Srikanth.busa@gmail.com, kk97976@gmail.com, indiragamini@gmail.com

ABSTRACT

Internet of things (IoT) is the infrastructure of global network for the information to the nation for societal use and enabling smart services by interconnecting virtual and physical devices or things based on previous, current and future technologies. IoT application is important to people yet in case the IoT system can't safeguard the customer data from software engineer, attacks, and shortcomings. Lightweight encryption is a space of a customary cryptographic estimation that is proper for resource obliged contraptions in IoT. Related work for lightweight techniques used for secure data transmission is portrayed in this paper. Security in IoT is still difficult task, to address security issues Lightweight Cryptography Techniques were introduced and to answer security aspects here the paper is going to present some techniques PRESENT, and its equivalent Methods. The term Lightweight came into picture when Lightweight wireless technology is used to run Lightweight IoT devices. Because the sensors used in IoT Devices are low power and less weight so the need of low power, less weight became reason to create Lightweight wireless technologies. This paper discusses major security challenges of IoT devices besides the performance evaluation of various Lightweight cryptographic algorithms.

Keywords: *Lightweight, Cryptography, Security, Iot Devices, Block Ciphers, Lightweight Protocols*.

1. INTRODUCTION

Internet of Things is the environment where networked things connected together to enable things communication over Internet [1]. IoT provides technical solutions to societal problems to make society as Smart [2]. IoT devices became part of our life as they are being used in our daily life [3]. At present situation Internet of Things attracting everyone because of its vast applications. IoT is the one of the leading innovative technological enhancements in the present world to kame everything as smart, meanwhile it has some security wholes

[4]. Through its rapid developments and broad relevance in certifiable apps that have changed our lives. The conventions that provide lightweight, safe and solid correspondence without trading off the computational and vitality impediments of the used compulsory IoT gadgets for good correspondence in IoT are the need for time. Writing exposes such conventions, such as CoAP, MQTT, XMPP, RESTFUL Facilities, 6LoWPAN, RPL, etc., which can be transmitted at various layers to communicate [5]. Information confidentiality and reliability can be provided by cryptographic algorithm [6]. Newly adapted technology can use Low-power enabled devices they need low-power cryptographic algorithms such as lightweight cryptographic algorithms [7]. The use of Lightweight Cryptographic algorithms may make system efficient [8]. One of the main problems in Lightweight technologies is security [9]. Integrity of data is accomplished by using hash function in lightweight cryptography [10]. The next generation of IoT devices will be assisted on Lightweight cryptographic techniques [11]. Lightweight cryptography is the better solution for lightweight devices like sensors [12]. The goal of LWC (Lightweight cryptography) to encourage the instalment and use of RFID, Sensors, Wireless cards, wireless devises with low power and energy consumption [13]. Light-weight cryptography centres around a wide scope of resource commitment devices, for example, IoT end centres and RFID names,[14] which can be executed with various correspondence progresses both on gear and on programming [15]. Due to the size, speed, or power consumption, it is not possible for an asset-restricted climate to perform standard cryptographic calculations [16]. Slight cryptography compromises the cost, speed, safety, running and use of energy on asset limited gadgets [17]. Lightweight cryptography is inspired by using fewer memory,[18] fewer material and less power to provide a safety system which can work on gadgets with limits on assets [19]. The lightweight encryption is less complicated and faster than conventional cryptography [20]. There is less weakness in lightweight encryption [21].

Addressing all these aspects the system is going to provide how Lightweight Cryptography is useful for an efficient running of IoT devices and also without worrying about security issues. Meanwhile it focuses performance evaluation of various cryptographic algorithms. Remaining paper is as follows, Literature Study, Limitations of Existing system, Related Work, Implementation Results and Evaluation and Conclusion and future scope.

2. LITERATURE STUDY

The Internet of Things (IoT) gives clear and reliable union of heterogeneous and assorted end systems [22]. It has been extensively used in various applications including astute metropolitan regions like public water structure, power lattice, water the leaders, and vehicle traffic signal system [23]. In these sharp city applications, a colossal number of IoT contraptions are sent that can recognize, pass on, figure, and conceivably enact [24]. The persistent and exact working of these devices are fundamental to clever city applications as critical decisions will be made ward on the data got [25. One of the troublesome tasks is to ensure the validity of the devices so we can rely upon the powerful cycle with a high sureness [26]. One of the characteristics of IoT contraptions sent in such applications is that they have limited battery power [27]. A test is to design a secured shared confirmation show which is sensible to resource obliged devices [28]. In this paper, we propose a lightweight common approval show reliant upon a novel public key encryption plot for splendid city applications [29]. The proposed show takes an amicability between the adequacy and correspondence cost without relinquishing the security [30]. It surveys the show of our show in programming and hardware conditions [31]. On a comparative security level, our show execution is by and large better contrasted with existing RSA and ECC based shows [32]. It moreover gives security examination of the proposed encryption plot and the normal affirmation show [33]. AES is quite possibly the most mainstream block figures utilized in cryptography [34]. The more renowned and extensively accepted symmetric encryption computation inclined to be capable these days is the Significant level Encryption Standard (AES) [35]. It is sorted out in any occasion six time speedier than triple DES.A trade for DES was needed as its key size was unnecessarily little [36]. With growing enlisting power, it was

thought about unprotected against careful key pursuit attack. Triple DES was proposed to vanquish this disadvantage yet it was found sluggish [37]. The features of AES are according to the accompanying −Symmetric key symmetric square cipher128-bit data, 128/192/256-cycle keys More grounded and faster than Triple-DES Give full specific and setup nuances Programming implementable in C and Java

Time is the one of the main constraints when both AES and PRESENT algorithms are compared for their performance evaluation as mentioned and presented AES has produced many rounds to make plain text as cypher text but if it applies the same with PRESENT algorithm it has given cypher text by taking plaintext with shorter time than AES algorithm. The performance evaluation of AES and PRESENT has shown in Results and Discussion Section.

3. NEED OF LWC:

1. Point-Point Communication.
2. Encouraging Lower Resource Devices.
3. Reducing Size of Circuits.
4. Optimizing Power Consumption.
5. Increasing Processing Speed.

The end hubs have a symmetrical key calculation to achieve safety beginning. The cryptographic activity with a restricted energy consumption is significant for the low asset gadgets, such as battery-fuelled gadgets. Low energy utilisation for end gadgets can be reduced by the use of lightweight symmetric key calculations. It is less than the ordinary cryptographic impression of the lightweight cryptographic natives. The lightweight cryptographic indigenous peoples would open up a different network association with smaller asset gadgets.

4. LIMITATIONS OF EXISTING WORK

While the SHA-256 (hazing) and the RSA/Elliptic Bend (marking) of the AES (encryption) have worked admirably with our regular encryption technology, frames with sensible handling power and capabilities, these don't spread to a world where frames and sensor organisations have been installed. Therefore, lightweight encryption strategies are proposed to overcome many ordinary encryption problems. This includes requirements with actual size, handling, memory and energy channel requirements. This paper traces many strategies which are characterised as ordinary cryptography within a space web, and examines a number of patterns in the lightweight calculation plan. Another factor is GE (Gate Equivalent) requirements it is clear that lightweight encryption algorithms were developed for low power security and circuits with lower power resistance. 2000-3000 GE is the determined limit, but with the creation of Lightweight encryption algorithms it is decreased into 1000 GE.

5. METHODOLOGY

Lightweight Cryptography

The process of practicing and applying techniques for secure communication is often called as Cryptography or cryptology [38]. Cryptography is the concept of building and doing analysis of protocols that prevent adversaries as it stops public reading confidential messages such as private messages or communications [39]. Current Cryptography is the intersection of different disciplines such as mathematics, Computer Science, Communication Science and so on. Especially in Computer Science at Network Security there is a need of lot of secure algorithms as to provide a secure communication [40]. Meanwhile Information Security includes data authentication, confidentiality, Integrity and Non-repudiation to be considered as modern cryptography, the origin of cryptography comes with the concepts of Encryption and decryption. Encryption is the conversion of readable form to non-readable form and the reverse is decryption.

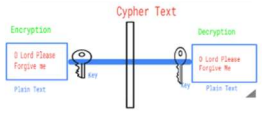


Fig-1 Encryption And Decryption

As it is mentioned Encryption is the process of creating human unreadable formatted text. As plaintext, the message found in an encoded message is referred to as ciphertext in its scrambled, garbled framework. As simple as

exchanging messages, fundamental forms of encryption could be as basic. As cryptography progressed, more innovations were made by cryptographers, and decoding proved to be more problematic. To make complicated encryption systems, Haggles will be unified. Mechanical encryption has now been replaced by PC calculations. Two categorized keys Symmetric and Asymmetric are seldom used in all types of algorithms. In the below table list of algorithms are mentioned. Lightweight Protocols were introduced to implement Internet of things as it is mentioned IoT devices are Lightweight, low in power and energy but to provide security to these devices it needs lightweight Cryptography that's the reason behind combining Lightweight Cryptography and Lightweight protocols to achieve data fusion in Internet of Things (IoT).Three algorithms PRESENT, CLEFIA and CAMELLIA are being used for achieving lightweight cryptography as it is mentioned in MQTT protocol for providing security AES - Advanced Encryption Standard algorithm is used, the actual purpose of MQTT protocol is to implement Lightweight wireless technologies. As it is described in our proposal, it is going to present PRESENT instead of AES it can be better if the system uses PRESENT Cryptographic algorithm. Let k_0, k_1, k_2…k_n be the sub-keys for all rounds, and then the plain text can be divided into two equal parts Left and Right, are indicated as (L_0, R_0) for each round i=0, 1... encryption $L_{i+1}=R_i$ and $R_{i+1}=Li \oplus F$ (R_i, Ki). Decryption $R_i=L_{i+1}$ and $L_i= R_i \oplus F(L_i+1+K_i)$.

PRESENT:

It is a cryptographic block cipher developed for the implementation of Lightweight technology, as described here and as PRESENT is very much notable for its small size, compared to AES is 2.5 times smaller. Actually, Advanced Encryption Standard (AES) is best for security in all aspects but it is complex and has lot of rounds that's the reason behind of not considering this algorithm and considering PRESENT algorithm. PRESENT follows substitute method for encryption and decryption. PRESENT algorithm follows SP network or substitution-permutation network is a combined sequential logical numerical operation used in block cipher, the main aim of the algorithm is to produce cipher text by taking input as plain text and key and to follow several rounds by applying several combinations of substitutions and permutations. Above script is the common interface for encryption algorithm, to make algorithm specific it has declared a constant variable **Const as CipherAlgo** and to find size of text here it uses size of () function, the block size is 64 bits.

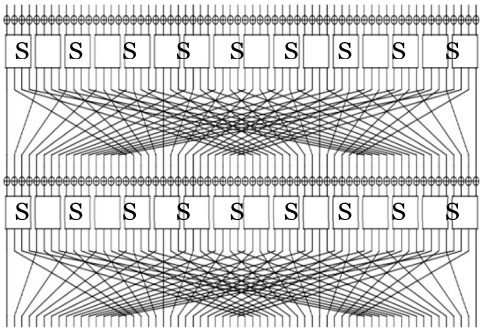


Fig-2 Present S/P-N/W

present can take keys of one or the other 80 or 128 pieces. Be that as it may we centre around the adaptation with 80-piece keys. The client provided key is put away in a key register K and addressed as k79k78 . . . k0. At round I the 64-bit round key Ki = κ63κ62 . . . κ0 comprises of the 64 furthest left pieces of the current substance of register K. In this manner at round I we have that: Ki = κ63κ62 . . . κ0 = k79k78 . . . k16. In the wake of extricating the round key Ki the key register K = k79k78 . . . k0 is refreshed as follows.

C)**Proposed Model:**

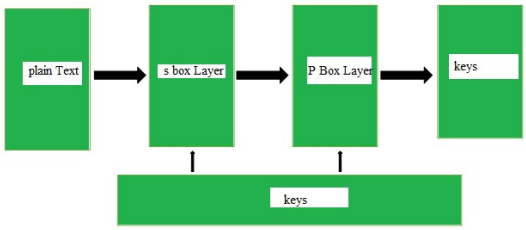


Fig-3 Proposed Architecture

Encryption is a cycle by which ordinary information is changed into a confused structure, while decoding is a framework by which unintelligible/coded information is changed over into its unique structure. Encryption is performed by the individual who sends the information to the objective, however the individual getting the information is decoded. A similar encryption-

unscrambling calculation with a similar key is utilized for both. Present day encryption plans use the ideas of public-key and symmetric-key. Current encryption strategies guarantee security since present day PCs are wasteful at splitting the encryption. On another figuring environment called IoT associations, a huge load of obliged devices is related with the Internet. The contraptions work together with each other through the organize and give new understanding to us. To see the value in this new environment, security of constrained end centre points is critical. In case one of the centres were sabotaged, the association might be suffered really. Regardless, it is hard to complete sufficient cryptographic limits on obliged contraptions due to the hindrance of their resources. Function for converting an array of bytes to a 64-bit integer unit 64_t fromBytesToLong (byte* bytes) here 64-bit integer is the output by taking a block of array and will be converted into 64-bit integer.

Table-1 Lightweight Protocols And Its Description

Sno	Protocol	Description
1	Lightweight Directory Access Protocol	Application protocol for accessing and maintaining distributed directory information services over an Internet Protocol (IP) network.
2	Lightweight Extensible Authentication Protocol	Wireless LAN authentication method, they are dynamic and WEP Keys, Re-authentication is achieved frequently?
3	Lightweight Presentation Protocol	Lightweight Presentation Protocol (LPP) describes an approach for providing "streamlined" support of Open Systems Interconnection (OSI) application services on top of Transmission Control Protocol/Internet Protocol (TCP/IP)-based network for some constrained environments.
4	Internet Content Adaption Protocol	It is a LWP (Lightweight Protocol) used for Transparency purpose in Internet.
5	Skinny client control protocol	The Skinny Client Control Protocol is a proprietary network terminal control protocol SCCP is a lightweight IP-based protocol for session signalling
6	Open LDAP	Open DAP is a free, open-source implementation of the Lightweight Directory Access Protocol
7	MQTT	Lightweight protocol
8	COAP	Constrained Application based
9	XMPP	Middle based protocol

6. RESULTS

Let the system to describe the hardware implementation of PRESENT block cipher, as it has mentioned running time of two algorithms AES-Advanced Encryption Standard and PRESENT differ in hardware implementation, because the hardware it has been taken by two systems is differ in terms of block ciphers and the number of rounds will it be taken by the system to implement any Device.

Test vectors for PRESENT with an 80-bit key are shown in hexadecimal notation.

plaintext	*key*	*ciphertext*
00000000 00000000	00000000 00000000 0000	5579C138 7B228445
00000000 00000000	FFFFFFFF FFFFFFFF FFFF	E72C46C0 F5945049
FFFFFFFF FFFFFFFF	00000000 00000000 0000	A112FFC7 2F68417B
FFFFFFFF FFFFFFFF	FFFFFFFF FFFFFFFF FFFF	3333DCD3 213210D2

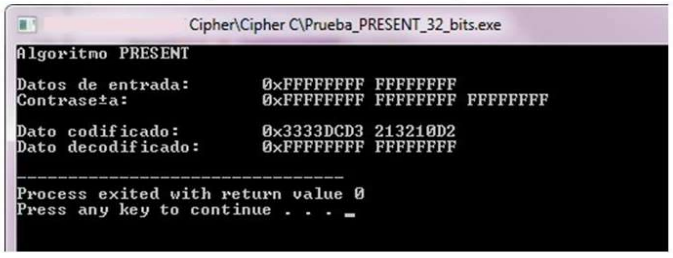


Fig-4 PRESENT Results

Journal of Theoretical and Applied Information Technology
15th April 2023. Vol.101. No 7
© 2023 Little Lion Scientific
ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

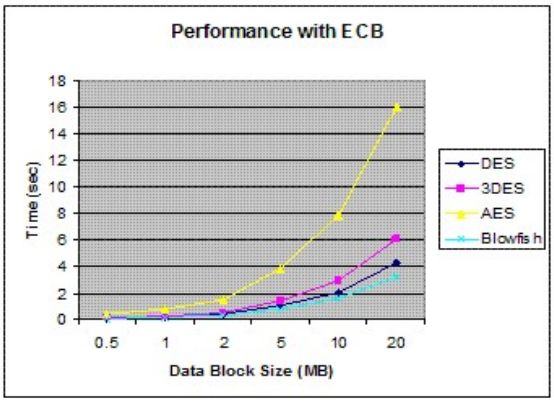
Table 2 Size Requirements

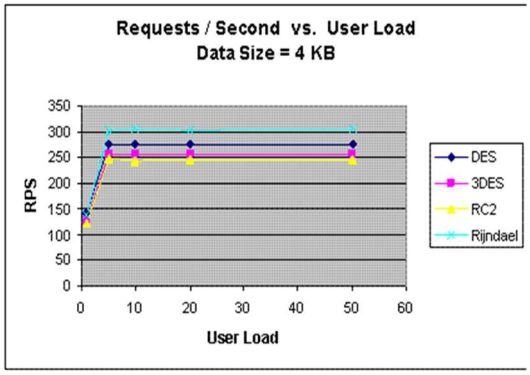
Sate/Layer	GE	%	module	GE	%	Ref
State of Data	384.39	24.48	KS: key state	480.49	30.61	
Layer of S	448.45	28.57	KS: S-box	28.03	1.79	
Layer of P	0	0	KS: Rotation	0	0	[41]
State Status of counter	28.36	1.81	KS: counter-XOR	13.35	0.85	
counter: combinatorial	12.35	0.79	key-XOR	170.84	10.88	
Other	3.67	0.23				
			sum	1569.93	100	

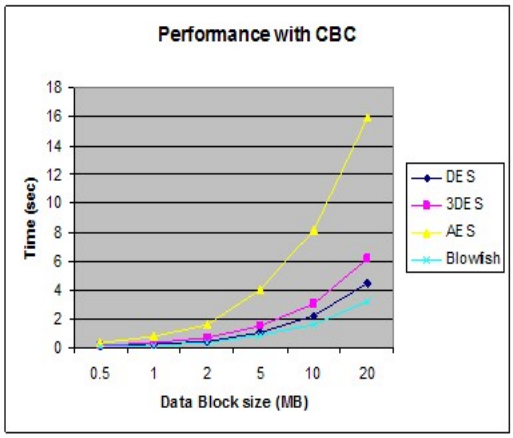
Table 3 Various Ciphers Requirements

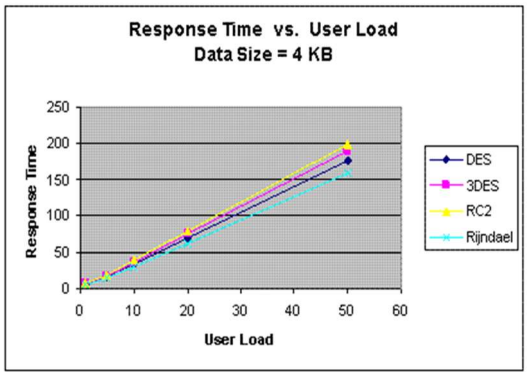
Block ciphers	Key size	Block size	Cycles per block	Throughput at 100KHz (Kbps)	Logic process	Area		Ref
						GE	rel.	
PRESENT-80	80	64	32	200	0.18μm	1570	1	
AES-128	128	128	1032	12.4	0.35μm	3400	2.17	
HIGHT	128	64	34	188.2	0.25μm	3048	1.65	[41]
mCrypton	96	64	13	492.3	0.13μm	2681	1.71	
Camellia	128	128	20	640	0.35μm	11350	7.23	
DES	56	64	144	44.4	0.18μm	2309	1.47	
DESXL	184	64	144	44.4	0.18μm	2168	1.38	
Stream ciphers								
Trivium	80	1	1	100	0.13μm	2599	1.66	
Grain	80	1	1	100	0.13μm	1294	0.82	

Various Cryptographic Performance Analysis:









7. CONCLUSION AND FUTURE SCOPE

Lightweight block ciphers play significant role for providing better security to IoT devices because IoT devices are in Low-power energy consumption devices, having Less weighted sensors. Lightweight and minimal expense cryptographic calculations are being produced for IoT devices. These are assessed based on chip instalment involved in equipment or memory prerequisites for their software execution. Devices carrying information needs security with minimum latency. Two factors significantly drawing major changes in the design of IoT devices, one is memory and the other one is Latency. Design of Block ciphers or stream ciphers is very crucial for IoT devices because lightweight block ciphers performance can be evaluated based on some of the important requirements such as latency, memory occupancy, efficiency, security, throughput, hardware and software's. Advanced Encryption Standard (AES) stood one of the best algorithms for providing security. As stated above it is needed Lightweight Cryptographic Algorithms for Lightweight powered devices, for that it is proposed to change the block ciphers, many block ciphers introduced they have its own efficiencies and deficiencies. PRESENT is one of the good algorithms as discussed in this paper it gives best results compared to other algorithms.GE requirements can be fulfilled by PRESENT Algorithm. The Future work of this paper is to provide alternative to PRESENT Algorithm.

REFERENCES:

[1] Goyal, T. K., Sahula, V., & Kumawat, D. (2019). Energy efficient lightweight cryptography algorithms for IoT devices. *IETE Journal of Research*, 1-14.

[2] Sehrawat, D., Gill, N. S., & Devi, M. (2019, March). Comparative analysis of lightweight block ciphers in IoT-enabled smart environment. In *2019 6th International Conference on Signal Processing and Integrated Networks (SPIN)* (pp. 915-920). IEEE.

[3] Dutta, I. K., Ghosh, B., & Bayoumi, M. (2019, January). Lightweight cryptography for internet of insecure things: A survey. In *2019 IEEE 9th Annual Computing and Communication Workshop and Conference (CCWC)* (pp. 0475-0481). IEEE.

[4] Medileh, S., Laouid, A., Euler, R., Bounceur, A., Hammoudeh, M., AlShaikh, M., ... & Khashan, O. A. (2020). A flexible encryption technique for the internet of things environment. *Ad Hoc Networks*, *106*, 102240.

[5] Girija, M., Manickam, P., & Ramaswami, M. (2020). PriPresent: an embedded prime LightWeight block cipher for smart devices. *Peer-to-Peer Networking and Applications*, 1-11.

[6] Su, Y., Gao, Y., Kavehei, O., & Ranasinghe, D. C. (2019, March). Hash functions and benchmarks for resource constrained passive devices: A preliminary study. In *2019 IEEE International Conference on Pervasive Computing and Communications Workshops (PerCom Workshops)* (pp. 1020-1025). IEEE.

[7] Dar, A. B., Lone, M. J., & Hussain, N. (2021). Revisiting Lightweight Block Ciphers: Review, Taxonomy and Future directions. *Computer Science Review, Forthcoming*.

[8] Mishra, Z., Mishra, S., & Acharya, B. (2021). High throughput novel architecture of sit cipher for iot application. In *Nanoelectronics, Circuits and Communication Systems* (pp. 267-276). Springer, Singapore.

[9] Singh, P., Acharya, B., & Chaurasiya, R. K. (2019). A comparative survey on lightweight block ciphers for resource constrained applications. *International Journal of High-Performance Systems Architecture*, *8*(4), 250-270.

[10] Sadkhan, S. B., & Hamza, Z. (2017, April). Cryptosystems used in IoT-current status and challenges. In *2017 International Conference on Current Research in Computer Science and Information Technology (ICCIT)* (pp. 58-62). IEEE.

[11] Saraiva, D. A., Leithardt, V. R. Q., de Paula, D., Sales Mendes, A., González, G. V., & Crocker, P. (2019). Prisec: Comparison of symmetric key algorithms for iot devices. *Sensors*, *19*(19), 4312.

[12] Khan, M. N., Rao, A., & Camtepe, S. (2020). Lightweight Cryptographic Protocols for IoT Constrained Devices: A Survey. *IEEE Internet of Things Journal*.

[13] Li, S., Song, H., & Iqbal, M. (2019). Privacy and security for resource-constrained IoT devices and networks: Research challenges and opportunities.

[14] Pohrmen, F. H., Das, R. K., Khongbuh, W., & Saha, G. (2018, July). Blockchain-based security aspects in Internet of Things network. In *International Conference on Advanced Informatics for Computing Research* (pp. 346-357). Springer, Singapore.

[15] Batra, I., Verma, S., Malik, A., Ghosh, U., Rodrigues, J. J., Nguyen, G. N., ... & Mariappan, V. (2020). Hybrid logical security framework for privacy preservation in the green internet of things. *Sustainability*, *12*(14), 5542.

[16] Zakaria, A. A., Azni, A. H., Ridzuan, F., Zakaria, N. H., & Daud, M. (2020). Extended RECTANGLE Algorithm Using 3D Bit Rotation to Propose a New Lightweight Block Cipher for IoT. *IEEE Access*, *8*, 198646-198658.

[17] Lee, S. K. (2018). A Study on Lightweight Block Cryptographic Algorithm Applicable to IoT Environment. *Journal of the Korea Academia-Industrial Cooperation Society*, *19*(3), 1-7.

[18] Samuel, C. P. J., Dharani, K. G., & Bhavani, S. (2020). Power algorithm to improve the IoT device for lightweight cryptography applications. *Materials Today: Proceedings*.

[19] Dalal, T., Verma, P., & Bhatt, R. (2019). Information Security in IoT Devices Using Lightweight Cryptography.

[20] Sadkhan, S. B., & Hamza, Z. (2017, April). Cryptosystems used in IoT-current status and challenges. In *2017 International Conference on Current Research in Computer Science and Information Technology (ICCIT)* (pp. 58-62). IEEE.

[21] Sadhukhan, D., Ray, S., Biswas, G. P., Khan, M. K., & Dasgupta, M. (2021). A lightweight remote user authentication scheme for IoT communication using elliptic curve cryptography. *The Journal of Supercomputing*, *77*(2), 1114-1151.

[22] Noura, H., Couturier, R., Pham, C., & Chehab, A. (2019, October). Lightweight stream cipher scheme for resource-constrained iot devices. In *2019 International Conference on Wireless and Mobile Computing, Networking and Communications (WiMob)* (pp. 1-8). IEEE.

[23] Saldamli, G., Ertaul, L., & Shankaralingappa, A. (2019, June). Analysis of lightweight message authentication codes for IoT environments. In *2019 Fourth International Conference on Fog and Mobile Edge Computing (FMEC)* (pp. 235-240). IEEE.

[24] Samaila, M. G., Sequeiros, J. B., Simões, T., Freire, M. M., & Inácio, P. R. (2020). IoT-HarPSecA: A framework and roadmap for secure design and development of devices and applications in the IoT space. *IEEE Access*, *8*, 16462-16494.

[25] Arseni, Ş. C., Miţoi, M., & Vulpe, A. (2016, June). Pass-IoT: A platform for studying security, privacy and trust in IoT. In *2016 International Conference on Communications (COMM)* (pp. 261-266). IEEE.

[26] Aakash, D., & Shanthi, P. (2016). Lightweight security algorithm for wireless node connected with IoT. *Indian J. Sci. Technol*, *9*, 1-8.

[27] Shamala, L. M., Zayaraz, G., Vivekanandan, K., & Vijayalakshmi, V. (2021, January). Lightweight Cryptography Algorithms for Internet of Things enabled Networks: An Overview. In *Journal of Physics: Conference Series* (Vol. 1717, No. 1, p. 012072). IOP Publishing.

[28] Lata, N., & Kumar, R. (2020, September). Analysis of Lightweight Cryptography Algorithms for IoT Communication. In *Congress on Intelligent Systems* (pp. 397-406). Springer, Singapore.

[29] Aruna, S., Usha, G., Madhavan, P., & Kumar, M. R. (2020). Lightweight Cryptography Algorithms for IoT Resource-Starving Devices. *Role of Edge Analytics in Sustainable Smart City Development: Challenges and Solutions*, 139-169.

[30] Jadhav, S. P. (2019). Towards light weight cryptography schemes for resource constraint devices in IoT. *Journal of Mobile Multimedia*, *15*(1), 91-110.

[31] Khomlyak, O. (2017). An investigation of lightweight cryptography and using the key derivation function for a hybrid scheme for security in IoT.

[32] Sarker, V. K., Gia, T. N., Tenhunen, H., & Westerlund, T. (2020, June). Lightweight security algorithms for resource-constrained IoT-based sensor nodes. In *ICC 2020-2020 IEEE International Conference on Communications (ICC)* (pp. 1-7). IEEE.

[33] Latif, M. A., Ahmad, M. B., & Khan, M. K. (2020, October). A Review on Key Management and Lightweight Cryptography for IoT. In *2020 Global Conference on*

Wireless and Optical Technologies (GCWOT) (pp. 1-7). IEEE.

[34] Luo, X., Yin, L., Li, C., Wang, C., Fang, F., Zhu, C., & Tian, Z. (2020). A lightweight privacy-preserving communication protocol for heterogeneous IoT environment. *IEEE Access*, *8*, 67192-67204.

[35] Guria, P., & Bhattacharyya, A. (2021). Lightweight Cryptography in Cloud-Based IoT: An Analytical Approach. In *Integration and Implementation of the Internet of Things Through Cloud Computing* (pp. 190-216). IGI Global.

[36] Patil, A., Bansod, G., & Pisharoty, N. (2015). Hybrid lightweight and robust encryption design for security in IoT. *International Journal of Security and Its Applications*, *9*(12), 85-98.

[37] El Hadj Youssef, W., Abdelli, A., Dridi, F., & Machhout, M. (2020). Hardware Implementation of Secure Lightweight Cryptographic Designs for IoT Applications. *Security and Communication Networks*, *2020*.

[38] Rana, M., Mamun, Q., & Islam, R. (2020, October). Current Lightweight Cryptography in IoT Security: A Survey. In *Extended Abstracts* (p. 27). Charles Sturt University.

[39] Al-Aboosi, A. M. M., Kamil, S., Abdullah, S. N. H. S., & Ariffin, K. A. Z. (2021, January). Lightweight Cryptography for Resource Constraint Devices: Challenges and Recommendation. In *2021 3rd International Cyber Resilience Conference (CRC)* (pp. 1-6). IEEE.

[40] Venkatraman, S., & Overmars, A. (2019). New method of prime factorisation-based attacks on RSA Authentication in IoT. *Cryptography*, *3*(3), 20.

[41] 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.

[42] https://www.cse.wustl.edu/~jain/cse567-06/ftp/encryption_perf/