World Academy of Science, Engineering and Technology
International Journal of Computer and Information Engineering
Vol:17, No:3, 2023

A Block Cipher for Resource-Constrained IoT Devices

Muhammad Rana, Quazi Mamun, Rafiqul Islam

Open Science Index, Computer and Information Engineering Vol:17, No:3, 2023 publications.waset.org/10013036/pdf

Abstract**—**In the Internet of Things (IoT), many devices are connected and accumulate a sheer amount of data. These Internet-driven raw data need to be transferred securely to the end-users via dependable networks. Consequently, the challenges of IoT security in various IoT domains are paramount. Cryptography is being applied to secure the networks for authentication, confidentiality, data integrity and access control. However, due to the resource constraint properties of IoT devices, the conventional cipher may not be suitable in all IoT networks. This paper designs a robust and effective lightweight cipher to secure the IoT environment and meet the resource-constrained nature of IoT devices. We also propose a symmetric and block-cipher based lightweight cryptographic algorithm. The proposed algorithm increases the complexity of the block cipher, maintaining the lowest computational requirements possible. The proposed algorithm efficiently constructs the key register updating technique, reduces the number of encryption rounds, and adds a layer between the encryption and decryption processes.

Keywords**—**Internet of Things, IoT, cryptography block cipher, s-box, key management, IoT security.

I. Introduction

THE IoT refers to the billions of electronic gadgets worldwide that are connected to the internet and collect and share data. In the last few years, IoT has grown exponentially, and it occupies our lives in several areas such as the city, agriculture, hospital, environment, homes, roads and so on. The IoT device is typically outfitted with a variety of sensors and actuators that collect a large amount of data and transfer it over the internet for monitoring, analysis, control, and various conclusions [1]. The majority of these data are real-time and assist us in making informed decisions about various service domains. However, this Internet-driven raw data need to be transferred securely and switched to human-understandable information to gather knowledge and use it in various domains such as smart grid, agriculture, city, environment, and transport.

Maintaining the security and privacy of IoT devices are challenging for various reasons: (i) The CPUs of IoT devices are nominal, making it harder to compute complex algorithms [2]-[9]. (ii) The power requirement of the algorithm should be minimum as IoT devices are battery-operated [4], [6], [7], [9]-[12]. (iii) The security implementation cost should be minor as an enormous number of devices need to deploy [13], [14].

Traditional cipher such as Encryption Standard (DES), Advanced Encryption Standard (AES), and RC6 cannot be used directly in these IoT domains since these devices are heterogeneous, scalable, and dynamic [12]. AES consume a high amount of memory, like 2.9 kilobytes flash and 1.2 kilobytes RAM [15]. Some WSN sensor devices have two kilobytes (kB) Random Access Memory (RAM) and 1 KB Electrically Erasable Programmable Read-Only Memory (EEPROM) [12]. Thus, the conventional cipher is not suitable for such resource-constrained sensors [16], [17]. Developing a lightweight cryptographic cipher (LWC) is one of the significant concerns for low power and lossy networks.

Hence, this paper focuses on developing a lightweight cipher for IoT resource-restricted devices and evaluating the cipher. The suggested cipher considers 12 rounds of encryption with a 4-bit static S-box, modify S-box and P-layer. A 4-bit static S-box uses less memory and CPU power. Modifying the S-box makes the cipher harder to break and reduces the round. Every round generates 64-bit keys and performs XOR operation with 64-bits blocks. The substitution layer uses 4-bit S-boxes for input and output bits, and the cipher uses a straightforward Permutation layer.

The rest of the paper is organised as follows. Section II illustrates the recently developed lightweight cipher and block cipher elements discussed in Section III. Section IV demonstrates a brief design of a new lightweight block cipher and assessment metrics of a block cipher. Finally, Section V outlines the conclusion.

II. Related Work

Lightweight hybrid cryptography [18] is a combination of LED and PRESENT block cipher and uses SPECK algorithm for key scheduling purposes. This system used RECTANGLE substitution box (S-Box), which made it more robust. With 12 to 14 rounds of encryption, the Lightweight Stream Cipher Scheme (LSC) is a mix of CR4, Pseudo-random number generator (PRNG), and Linear-feedback shift register (LFSR). SAT_Jo [19], [20] system is appropriate for IoT tag-based functions. This system processes a $4\ x\ 4$ S-box by 2^4 orders of the Galois field involved in 31 rounds encryption and decryption process. The Generalised Triangle Based Security Algorithm (G-TBSA) block cipher is suitable for wireless sensor networks (WSNs) with low power Wi-Fi [9]. G-TBSA has used an efficient key generation mechanism. Modified Block Cipher Technique (MBCT) is a pattern of XOR, Matrix Rotation, and Expansion function [21] which needs less encryption and decryption time and memory.

The most recent lightweight cryptography is primarily divided into the two categories such as symmetric and

Muhammad Rana, Quazi Mamun, and Md Rafiqul Islam are with School of Computing, Mathematics and Engineering, Charles Sturt University, NSW, Australia (e-mail: mrana@csu.edu.au, qmamun@csu.edu.au, mislam@csu.edu.au).

Open Science Index, Computer and Information Engineering Vol:17, No:3, 2023 publications.waset.org/10013036/pdf

asymmetric cipher. The symmetric lightweight algorithm is further divided into Lightweight Block Cipher (LWBC) and Lightweight Stream Cipher (LWSC). Elliptic curve cryptography (ECC) falls under asymmetric cryptography, which requires more resources than the symmetric cipher. Several new lightweight ciphers have been developed; nonetheless, there is still room for improvement in terms of security, latency reduction, energy demand, power consumption, and chip area decrease. Different types of ciphers face different obstacles; for example, LCC is resistant to a variety of attacks, but key management solutions have yet to be established [6]. G-TBSA, on the other hand, uses very little energy and is only appropriate for wireless communication [9]. None of the modern lightweight ciphers are secure enough for both block cipher and stream cipher [22].

Stream ciphers encode or decode a single bit of data at a time with a continually changing key. These ciphers are suitable for real-time communications such as audio and video. Alternatively, block ciphers encrypt or decrypt a block of data at a time. This cipher is ideal for long message size. Block cipher is practically more efficient, easier to execute, and can achieve higher diffusion and error propagation than stream ciphers. Block ciphers can be designed to deliver security authentication or integrity shield which stream ciphers cannot deliver. Block ciphers are the most suitable security algorithm to secure the IoT edge network compared to a stream cipher. The efficiency of the block ciphers depends on the S-box, P-box, key management, block size, key size, number of rounds, and structures of the cipher.

Minimise key length: Key length or key size plays a crucial part in cryptographic security in IoT devices. A larger key length helps the algorithm to generate more complexity which makes the network communication more secure. However, such a key length demands more computational power and memory, which IoT devices may not effort. On the contrary, a shorter key length increases the possibility to be compromised by the intruders. The trade-off between the security and key length must be maintained to design an efficient cipher for resource-constrained edge devices. A more frequent dynamic key can facilitate maintaining the key size optimum. A combination of shorter session keys with smaller key lengths will be able to protect the network even though the cipher uses a low number of rounds. An intruder cannot get enough time to discover the key as the key will expire before they calculate the key.

Generate simpler and fewer rounds of an algorithm: More straightforward and small number of cryptographic rounds are suitable for resource-constrained IoT devices as they require less power to implement the cipher. A complex structure with few rounds can provide security to such a node like sensors, actuators etc.

Use more frequent dynamic key: The periodic dynamic key provides complexity to the cipher, which can certainly secure the IoT node. A PRNG with various chaotic systems can generate the dynamic key. This process requires additional processing power, which should be considered while designing a block cipher. It is important to carefully address the balance between developing frequent key and security needs during the process.

Apply smaller block of data: A smaller block of data means less capacity to generate the algorithm appropriate for IoT edge devices. However, adjustment needs to be considered between device security and block size.

Develop a simple structure: The simple key structure indicates less complexity of the cipher, which leads to a security vulnerability. A combination of S-layer and P-layer and key mixing creates a round of Substitution Permutation structures that can secure communication. However, a robust S-box and P-box need to generate to develop a simple structure cipher.

III. A Lightweight Block Cipher

We present a LWBC to secure the resource-constrained IoT devices communications. Fig 1 depicts the structure of the proposed cipher. The proposed cipher would be more complex and more efficient with a smaller number of encryption rounds. The proposed cipher uses 64 bits of plaintext as input and 64 bits of the key from 80 bits pool key. Four steps are involved in the proposed cipher in one round: First, plaintext will XOR with the generated key; second, output from the first step goes through the suggested S-box, then padding with an additional layer finally goes through the P-box. A linear bitwise permutation uses a P-box, and a nonlinear substitution layer uses a static S-Box.

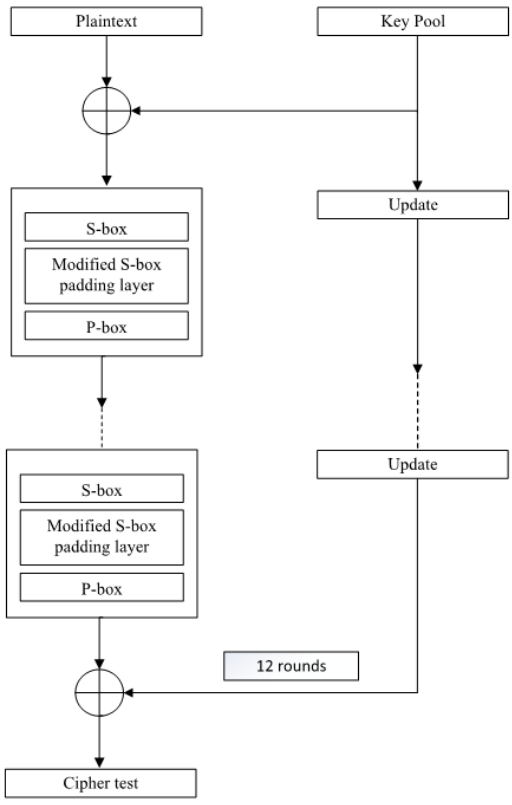

Fig. 1 The structure of the proposed cipher

Initially, a 64-bit plaintext and 64-bit key go through XOR operation and generate 64-bit output. The output goes through the nonlinear layer element called S-box. This is the only nonlinear element that provides the cipher confusion property

Open Science Index, Computer and Information Engineering Vol:17, No:3, 2023 publications.waset.org/10013036/pdf

and makes the cipher stronger against various attacks. The proposed cipher uses a single static 4-bit S-box to use less memory and computational power. This S-box is applied 16 times in parallel in each round. It is then padding the output to increase the complexity and decrease the number of rounds of this block cipher. A 64-bit output generates and permuted with the straightforward P-box. The cipher's robustness is enhanced by updating the round key after each round. The process is repeated 12 times in the same way then ciphertext produces.

A. S-box and P-box

Substitution box (S-box) and permutation box (P-box) are two critical factors in generating a robust block cipher that provides concussion and diffusion. S-box provides confusion, and diffusion comes from P-box. S-box secretes the relationship between ciphertext, key and plaintext, which makes the cipher harder to break. P-box helps to hide the connection between ciphertext and plaintext. Using a robust S-box is essential for a reliable and efficient block cipher [22]. A 4-bit S-box demands a relatively lower physical area and memory than an 8-bit S-box. 8-bit S-box requires a rather more significant gate area and memory than 4-bit S-box. In this research, we use an S-box, which is appropriate for resource-constrained IoT devices. The S-box is constructed on 4 x 4 bits suitable for a LWBC. The constructed S-box uses an irreducible polynomial equation from Galois Field $GF(2^4)$ followed by multiplicative inverse and affine transformation. Empirical results demonstrate that the suggested S-box is robust to statical and differential cryptanalysis [23].

TABLE I
S-BOX

x	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F
$S(x)$	**3**	**D**	**A**	**2**	**1**	**7**	**B**	**5**	**C**	**E**	**F**	**6**	**9**	**8**	**0**	**4**

The PRESENT P-box use in this cipher is given from Table II. The i^{th} bit position moved to the $P(i)$ bit position.

TABLE II
P-BOX

i	*P(i)*	*i*	*P(i)*	*i*	*P(i)*	*i*	*P(i)*
0	0	16	4	32	8	48	12
1	16	17	20	33	24	49	28
2	32	18	36	34	40	50	44
3	48	19	52	35	56	51	60
4	1	20	5	36	9	52	13
5	17	21	21	37	25	53	29
6	33	22	37	38	41	54	45
7	49	23	53	39	57	55	61
8	2	24	6	40	10	56	14
9	18	25	22	41	26	57	30
10	34	26	38	42	42	58	46
11	50	27	54	43	58	59	62
12	3	28	7	44	11	60	15
13	19	29	23	45	27	61	31
14	35	30	39	46	43	62	47
15	51	31	55	47	59	63	63

B. Key Management

There is a potential risk for using a fixed P-Box. Especially if any node is compromised. That is why the plain text should be XOR-ed with the key. As shown in Fig. 1, the plaintext is XOR-ed with the key before passing it to the S-box and P-Box at each stage. However, maintaining a large pool of keys requires extra storage and producing dynamic keys requires processing power. To mitigate these problems, we suggest using partial keys which would be loaded with the IoT devices during the installation time. This process is known as pre-distribution.

The two main characteristics of the proposed key management are: i) pre-distribution of keys, ii) using partial (half) keys instead of full keys.

A key pool can be inserted into each IoT device at the time of their deployment, known as pre-distribution. The pre-distribution of keys is generally considered safe as the IoT system is safe at the deployment stage. Pre-distribution is also useful to identify an intruder if an outside IoT device or node tries to use a key not listed in the key pool at the stage of pre-distribution. Additionally, each node (IoT device) stores a set of partial keys rather than the full set of keys, which has two advantages: lower storage requirement and attackers cannot obtain the encryption/decryption keys even a node is captured.

Two communicating nodes in a cluster establish their encryption/decryption key by applying some functions between the partial keys. To make it simple, we assume the function is a concatenation function.

A key pool is generated first. This pool contains partial keys (or half keys). These partial keys are assigned to each node randomly from the key pool. A node can generate many encryption/decryption keys by applying the pre-set function on its partial keys with that of other nodes, and each time a pair of nodes communicates, they use a different key. This feature enables IoT to achieve resilience to attacks and data freshness.

If A and B are two nodes having a list of partial keys {a, b, c, d, e} and {p, q, r, s, t} respectively, the nodes send messages each other, before starting the encryption, negotiating their list of partial keys and the preference or order of the partial keys. Suppose A sends an order list to B as {3, 2, 0, 1, 4}. Thus, B will sort the partial key list of A as {d, c, a, b, e}. Similarly, B sends an order list to A of {0, 2, 4, 1, 3}. As a result, A will reorder the B's list of partial keys as {p, r, t, q, s}. If both A and B agree on a concatenation function to build the full key using their partial keys, both A and B will now know the full key series would be {dp, cr, at, bq, and es}.

The detailed description of the key management scheme can be found in [24].

C. Padding Layer between S and P Layers

Fig. 2 illustrates the flowchart of the padding layer of this cipher. S-box output divided by 2x32 bits in the planned cipher. Later XOR is done at the left 32 bits with the right part of the operation with the lowest possible rounds. Finally, combining two 32 bits produce 64 bits improved S-box. This output adds to the P-layer for further process. The decoding method is similar to encoding; however, rotation is done by left rather than right.

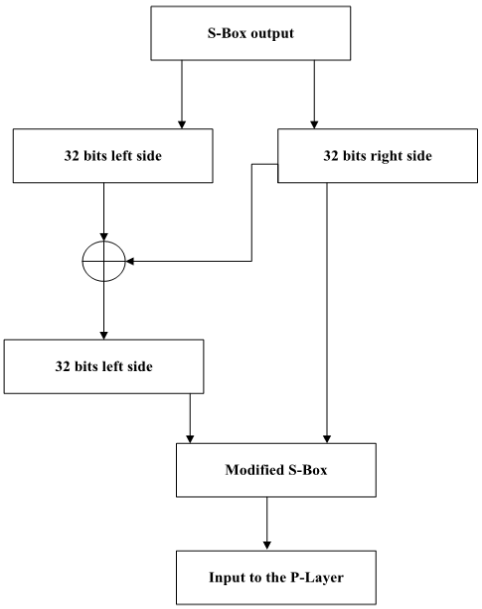

Fig. 2 Additional layer block diagram

According to the ISO/IES standard lightweight criteria, the PRESENT is a LWBC suitable for resource-constrained devices. PRESENT is an SPN (Substitution Permutation Network) based LWBC. This cipher works with 64 bits block of plaintext and 80 bits or 128 bits of the key. PRESENT considers 31 rounds of encryption and decryption with S-Box and P-layer. Each round generates 64-bits keys and performs XOR operation with bit block. Cipher uses a straightforward Permutation layer. The proposed cipher is more complex; however, it uses fewer rounds than the PRESENT cipher, making the proposed cipher faster and robust. The proposed block cipher uses a robust S-box, which is generated from irreducible polynomial and affine transformation. This strong S-box provides more confusion properties making the cipher more complex to the attackers.

IV. An Evaluation of the Proposed Block Cipher

The nonlinearity is a necessary measure of the modern cipher. The cipher should deliver a robust cryptographic character against differential and linear cryptanalysis. Linear Approximation Table (LAT) and Difference Distribution Table (DDT) can explain these two properties.

TABLE III
Linear Approximation Table

		Output S-box															
		0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F
Input S-box	0	8	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
	1	0	-2	0	2	4	-2	0	-2	-2	0	2	0	2	0	2	4
	2	0	-2	2	0	0	-2	2	0	-2	-4	-4	2	2	0	0	-2
	3	0	0	2	-2	0	-4	-2	-2	4	0	-2	-2	0	0	-2	2
	4	0	2	-4	-2	-2	0	-2	0	-2	0	-2	0	4	-2	0	2
	5	0	0	0	4	-2	2	-2	-2	0	-4	0	0	-2	-2	-2	2
	6	0	0	2	2	-2	-2	-4	4	0	0	2	2	2	2	0	0
	7	0	2	-2	4	2	0	0	2	2	0	-4	-2	0	2	2	0
	8	0	-4	-2	-2	2	2	-4	0	2	-2	0	0	0	0	2	-2
	9	0	2	-2	0	2	-4	0	2	0	-2	2	0	-2	-4	0	-2
	A	0	-2	0	2	-2	0	2	0	4	2	0	2	2	-4	2	0
	B	0	0	0	0	2	2	2	2	2	-2	2	-2	4	0	-4	0
	C	0	2	2	0	4	2	-2	0	0	2	-2	4	0	-2	-2	0
	D	0	0	-2	-2	0	0	2	2	2	-2	0	4	-2	2	0	4
	E	0	-4	0	0	0	0	0	4	-2	2	-2	-2	-2	-2	-2	2
	F	0	-2	-4	2	0	-2	0	-2	0	2	0	2	0	2	-4	-2

A. LAT Analysis of S-box

The linear cryptanalysis explains a linear approximation between the ciphertext, key and plaintext. The global approximation table can be produced from the nonlinear mapping of the LATs. S-box can be measured by the linear vulnerabilities.

A linear approximation of the S-box is shown in Table III. The table "input" shows the number of matches between the linear equation which is denoted in hexadecimal. The "output" denotes the sum of the output bits less than 8. Henceforth, the probability bias for the particular linear combination of input and output bits can be found from an element value dividing by 16. The probability of any addition of a non-zero subset of output bits is equal to the addition involving no input bits is precisely half. The linear combination of output bits is equal to 0, and 1 for a bijective S-box column of the table are all zeros except the leftmost value of the row and the top value of the column. In addition, the total sum of any row or column must be either +8 or -8.

B. DDT Analysis of S-box

It is easy to do differential cryptanalysis if one element is greater than the other. Thus, S-box should have a nominal differential value. The differential analysis finds a high probability of specific plaintext differences and differences to the last round of the cipher.

Table IV illustrates the DDT of our S-box. It has 16 rows, 16 columns and 265 cells. Each row and column represent each output difference from 0 to F for each input difference. Zero

Open Science Index, Computer and Information Engineering Vol:17, No:3, 2023 publications.waset.org/10013036/pdf

represents the absence of that output difference for the following input difference. Too high or too low zero reveals more information regarding concerning output difference. The DDT shows that it has three values 0, 2 and 4. Each row and column has only one 4. Therefore, S-box can show good resistance against differential cryptoanalysis.

V. Conclusion

In this paper, we propose a lightweight cryptographic protocol using a symmetric block cipher. The lightweight protocol is suitable for resource-constraint IoT devices. Our proposed lightweight protocol offers an ideal solution for such devices. As part of the protocol design, we developed an S-box using carefully selected irreducible polynomials. A couple of transformations, such as the multiplicative inverse of irreducible polynomial in Galois field $GF\ (2^4)$ and an affine transformation has been used to produce 4×4 S-boxes. Empirical analysis shows that the proposed S-boxes will ensure a high level of confusion (measured using LATs and differential distribution tables), maintaining the low resource requisitions for scarce resource profiled IoT devices. In addition, a key generation scheme was designed as a part of the lightweight cryptographic protocol. A prominent feature of the schemes is the pre-distribution of partial keys. To enhance security and mitigate threats, the use of partial keys, as opposed to full keys, is implemented. This approach ensures that even if a node is compromised and an intruder gains access to all the keys, the security of the system remains intact. The system is still protected until the full keys are created using the partial keys. Another feature indicates the freshness of the keys for each round of communication. A new full key is generated using the partial keys.

TABLE IV
Difference Distribution Table

		Output Difference S-box															
		0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F
Input Difference S-box	0	16	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
	1	0	2	2	0	2	0	2	0	2	2	0	0	0	0	4	0
	2	0	0	2	2	0	0	0	0	2	4	2	0	2	0	0	2
	3	0	4	0	0	2	0	0	2	2	0	2	0	2	2	0	0
	4	0	2	4	0	0	2	2	2	0	0	2	0	0	0	0	2
	5	0	0	0	0	4	0	2	2	0	2	0	2	2	0	0	2
	6	0	0	0	0	0	2	2	0	4	0	2	2	2	0	2	0
	7	0	0	0	2	0	0	4	2	2	0	0	0	0	2	2	2
	8	0	2	0	2	2	2	0	0	2	0	0	2	0	0	0	4
	9	0	2	0	0	0	2	0	0	0	2	0	0	2	4	2	2
	A	0	2	2	2	0	0	2	0	0	0	0	2	4	2	0	0
	B	0	0	2	2	2	4	0	2	0	0	0	0	2	0	2	0
	C	0	0	0	2	2	2	2	0	0	2	4	0	0	2	0	0
	D	0	0	2	0	2	0	0	0	0	0	2	4	0	2	2	2
	E	0	2	0	4	0	0	0	2	0	2	2	2	0	0	2	0
	F	0	0	2	0	0	2	0	4	2	2	0	2	0	2	0	0

References

[1] A. Hameed and A. Alomary, "Security Issues in IoT: A Survey," *2019 International Conference on Innovation and Intelligence for Informatics, Computing, and Technologies (3ICT),* 2019, doi: 10.1109/3ICT.2019.8910320. IEEE.

[2] X. Jiang, M. Lora, and S. Chattopadhyay, "An Experimental Analysis of Security Vulnerabilities in Industrial IoT Devices," *ACM Transactions on Internet Technology,* 2020, doi: doi.org/10.1145/3379542. ACM Digital Library.

[3] L. Cui, G. Xie, Y. Qu, L. Gao, and Y. Yang, "Security and Privacy in Smart Cities: Challenges and Opportunities," *IEEE Access,* vol. 6, pp. 46134-46145, 2018, doi: 10.1109/access.2018.2853985. IEEE Access.

[4] Y. Yang, L. Wu, G. Yin, L. Li, and H. Zhao, "A Survey on Security and Privacy Issues in Internet-of-Things," *IEEE Internet of Things Journal,* vol. 4, no. 5, pp. 1250 - 1258, 2017, doi: 10.1109/JIOT.2017.2694844. IEEE.

[5] V. Rao and K. V. Prema, "Comparative Study of Lightweight Hashing Functions for Resource Constrained Devices of IoT," *4th International Conference on Computational Systems and Information Technology for Sustainable Solution (CSITSS),* 2019, doi: 10.1109/CSITSS47250.2019.9031038. IEEE.

[6] S. Roy, U. Rawat, and J. Karjee, "A Lightweight Cellular Automata Based Encryption Technique for IoT Applications," *IEEE Access,* vol. 7, pp. 39782 - 39793, 2019, doi: 10.1109/ACCESS.2019.2906326. IEEE Access.

[7] R. Yugha and S. Chithra, "A survey on technologies and security protocols: Reference for future generation IoT," *Journal of Network and Computer Applications,* vol. 169, 2020, doi: 10.1016/j.jnca.2020.102763. Elsevier.

[8] F. A. Alabaa, M. Othmana, I. A. T. Hashema, and F. Alotaibi, "Internet of Things security: A survey," *Journal of Network and Computer Applications,* vol. 88, pp. 10-28, 2017, doi: 10.1016/j.jnca.2017.04.002. Elsevier.

[9] S. F. Ahmed, M. R. Islam, T. D. Nath, B. J. Ferdosi, and A. S. M. T. Hasan, "G-TBSA: A Generalized Lightweight Security Algorithm for IoT," *2019 4th International Conference on Electrical Information and Communication Technology (EICT),* 2020, doi: 10.1109/EICT48899.2019.9068848. IEEE.

[10] Q. Mamun, "A Qualitative Comparison of Different Logical Topologies for Wireless Sensor Networks," *Sensors,* 2012, doi: 10.3390/s121114887. Sensors.

[11] A. Lepekhin, A. Borremans, I. Ilin, and S. Jantunen, "A systematic mapping study on the internet of things challenges," *IEEE/ACM 1st International Workshop on Software Engineering Research & Practices for the Internet of Things (SERP4IoT),* 2019, doi: 10.1109/SERP4IoT.2019.00009. IEEE Digital Library.

[12] N. A. Gunathilake, W. J. Buchanan, and R. Asif, "Next Generation Lightweight Cryptography for Smart IoT Devices: Implementation, Challenges and Applications," *IEEE 5th World Forum on Internet of Things (WF-IoT),* 2019, doi: 10.1109/WF-IoT.2019.8767250. IEEE.

[13] K.-M. Chew, S. C.-W. Tan, G. C.-W. Loh, N. Bundan, and S.-P. Yiiong, "IoT Soil Moisture Monitoring and Irrigation System Development,"

Open Science Index, Computer and Information Engineering Vol:17, No:3, 2023 publications.waset.org/10013036/pdf

ICSCA 2020: Proceedings of the 2020 9th International Conference on Software and Computer Applications, pp. 347-252, 2020, doi: 10.1145/3384544.3384595. ACM Digital Library.

[14] S. Zeadallya, A. K. Das, and N. Sklavos, "Cryptographic technologies and protocol standards for Internet of Things," *Internet of Things,* 2019, doi: 10.1016/j.iot.2019.100075. Elsevier.

[15] C. Pei, Y. Xiao, W. Liang, and X. Han, "Trade-off of security and performance of lightweight block ciphers in Industrial Wireless Sensor Networks," *EURASIP Journal on Wireless Communications and Networking,* 2018, doi: 10.1186/s13638-018-1121-6. Springer Nature.

[16] A. R. Sfar, E. Natalizio, Y. Challal, and Z. Chtourou, "A roadmap for security challenges in the Internet of Things," *Digital Communications and Networks,* vol. 4, no. 2, pp. 118-137, 2018, doi: 10.1016/j.dcan.2017.04.003. Science Direct.

[17] R. Hamzaab, Z. Yancd, K. Muhammade, P. Bellavistaf, and F. Titouna, "A privacy-preserving cryptosystem for IoT E-healthcare," *Information Sciences,* vol. 527, pp. 493-510, 2020, doi: 10.1016/j.ins.2019.01.070. Elsevier.

[18] V. Prakash, A. V. Singh, and S. K. Khatri, "A New Model of Light Weight Hybrid Cryptography for Internet of Things," *2019 3rd International conference on Electronics, Communication and Aerospace Technology (ICECA),* 2019, doi: 10.1109/ICECA.2019.8821924. IEEE.

[19] M. J. R. Shantha and L. Arockiam, "SAT_Jo: An enhanced Lightweight Block Cipher for the Internet of Things.," *2018 Second International Conference on Intelligent Computing and Control Systems (ICICCS),* 2019, doi: 10.1109/ICCONS.2018.8663068. IEEE.

[20] H. Noura, R. Couturier, C. Pham, and A. Chehab, "Lightweight Stream Cipher Scheme for Resource-Constrained IoT Devices," *2019 International Conference on Wireless and Mobile Computing, Networking and Communications (WiMob),* 2019, doi: 10.1109/WiMOB.2019.8923144. IEEE.

[21] R. R. K. Chaudhary and K. Chatterjee, "An Efficient Lightweight Cryptographic Technique for IoT based E-healthcare System," *2020 7th International Conference on Signal Processing and Integrated Networks (SPIN),* 2020, doi: 10.1109/SPIN48934.2020.9071421. IEEE.

[22] X. Wang, A. Akgul, U. Cavusoglu, V.-T. Pham, D. V. Hoang, and X. Q. Nguyen, "A Chaotic System with Infinite Equilibria and Its S-Box Constructing Application," *Applied Sciences,* vol. 8, no. 11, 2018, doi: 10.3390/app8112132. MDPI.

[23] M. Rana, Q. Mamun, and R. Islam, "An S-box Design using Irreducible Polynomial with Affine Transformation for Lightweight Cipher," presented at the EAI QSHINE 2021 - 17th EAI International Conference on Heterogeneous Networking for Quality, Reliability, Security and Robustness, Melbourne, Australia, 2021.

[24] M. Rana and Q. Mamun, "A robust and lightweight key management protocol for WSNs in distributed IoT applications," *International Journal of Systems and Software Security and Protection (IJSSSP),* vol. 9, no. 4, 2018, doi: 10.4018/IJSSSP.2018100101. IGI Global.

Open Science Index, Computer and Information Engineering Vol:17, No:3, 2023 publications.waset.org/10013036/pdf