Lightweight Cryptography Algorithms for Security of IoT Devices: A Survey

Dr. Subhash Chander

Associate Professor, Department of Computer Science, Pt. CLS Govt College Karnal, Haryana

---

ABSTRACT:

In a new computing world called "Internet of Things (IoT)" or " Smart Objects " networks, a lot of devices are connected to the Internet. They interact with each other through the network and give a new experience to us. In order to enjoy this new context, security of constrained end point is important. However, the network might be suffered seriously, If one of the end points were compromised. Still, it is not easy to apply sufficient cryptographic functions on constrained resources due to the limitation of their resources [1]. In this paper, a short discussion on the different IoT applications and challenges has been done. Further, the security worries concerning information sharing and following have been included. A comparable assessment of various lightweight encryption and approval estimations is finished. Also, some assessment headings described which further work ought to be adopted on lightweight cryptography estimations [2].

Keywords- IoT Security, Cryptography, Internet of Things, Lightweight Ciphers, Privacy.

1. INTRODUCTION:

Cryptography is that the preparation and examination of hiding information. It is the investigation of further developing messages to approach them secure and impenetrable to attack. In cryptography, the primary message is changed over into other message at encryption side and changed over into a special message at the gatherer side. For obliged devices, normal cryptography estimations can be unnecessarily drowsy, excessively huge or too energy-consuming. The term light-weight cryptography focuses on new estimations to beat this issue. Light-weight cryptography is for the most part characterized as cryptography for asset obliged gadgets, for which RFID labels and WSN are commonly referenced as specific illustrations. Light-weight encryption is an intersection of two terms "Light and weight", and it is an area of an old-style cryptographic calculation. Light-weight encryption and decoding are executed on stages as well as equipment and programming. In this paper, present breaking down study on the common use of recent stuff H/ W and software S/ W performances of symmetric as well as asymmetric ciphers(3).

The Internet of Things (IoT) being a promising development addressing things to come should interact with billions of devices or gadgets. The extended number of correspondence should deliver heaps of data and the security of data can be a risk. The contraptions in the plan are essentially more humble in size and low fuel. Standard encryption estimations are generally computationally exorbitant on account of their unpredictability and require many rounds to scramble, essentially wasting the obliged energy of the contraptions. Less stunning estimation, in any case, may mull over needed decency [4].

This paper will contains sections as follows :

The Section 1 covers an Introduction to IoT and its Architecture, Applications, and Challenges. Section 2 covers the overview of Lightweight Cryptography, section 3 covers about the Lightweight Cryptography Algorithms. Section 4: Related work and literature survey on lightweight cryptography algorithms for IoT security. Section 5 provides the information related to analysis on lightweight cryptography algorithms for iot security analysis. Section 6 introduces the conclusions related to this work. Section 7 describes the Future Scope related to the review.

1.1 IoT ARCHITECTURE [2] :

Three Layer	Four Layer	Five Layer
Physical/Perception Layer Smart cards, RFID Tags, Sensors	**Data Perception Layer** RFID tags, 3G Phones, Sensor Embedded Devices	**Perception Layer** Physical Objects, RFID, Barcode, Infrared Sensors.
Network Layer Secure Transmission, 3G, UMTS, WiFi, Bluetooth, Infrared, Zigbee	**Heterogeneous Network AccessLayer** Wireless links, GSM, WCDMA, WiFi, Zigbee	**Network Layer** 3G, WiFi, Bluetooth, Zigbee Infrared Technology

	Data Management Layer Cloud Computing Centers, Web service servers, management servers	**Processing Layer** Database, Ubiquitous Computing, Service Management, Info Processing
Application Layer Smart Applications and Management	**Intelligent Service Layer** Intelligent Applications as in agriculture, environment, smart cities etc	**Application Layer** Intelligent systems, devices, Applications in various Domains
		Business Layer Business Models, Graphs, System Management

1.2 IoT APPLICATIONS:

1.2.1 Home Automation System:

Home Automation System are where one have some control over the electronic things in their home by means of their cell phones and PCs in this way making a framework that empowers a savvy home. It additionally gives the office of identifying crises; keep up with energy utilization inside the house, and so forth.

1.2.2 Intelligent Transportation System:

Intelligent Transportation System in which traffic observing should be possible, mishaps, gridlocks and infringement of traffic rules can be accounted for to specialists.

1.2.3 Prediction of natural disasters and reporting critical temperature changes:

The Prediction of natural disasters by consistent observing of climate utilizing sensors. Checking Environmental conditions like estimating level of poisonous gases in the air, and the content of harmful material in water.

1.2.4 Healthcare Facilities:

Healthcare facilities can be given like remote checking of patients, consistent observing of well-being boundaries and exercises, support for autonomous living, observing medications admission by the patient, and some more.

1.2.5 Surveillance and Tracking:

Surveillance and tracking individuals, articles and creatures, examining spaces and abandoned regions, upkeep of framework and hardware, disturbing frameworks and a lot more offices have become conceivable with IoTs [2].

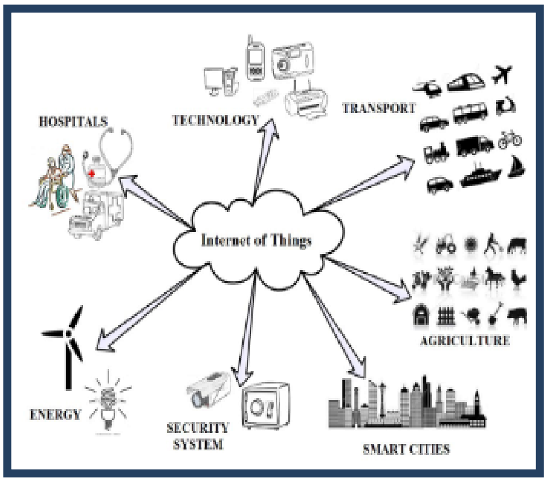

Fig: IoT Applications

1.3 IoT Challenges

The authors, M. Chiang and T. Zhang, in [5], discussed about how fog computing can figure out many of IoT challenges.

1.3.1 Latency Constraints: If the information began by IoTs expected to send at cloud for practicing and stockpiling then it consumes additional time, which isn't reasonable for continuous applications like brilliant traffic the executives. To manage latency limitations application is the test for IoT. As the haze performs calculation near end clients ,it is great for time delicate application.

1.3.2 Uninterrupted Services: To offer continuous types of assistance to IoT is the huge test. Notwithstanding of having unpredictable organization accessibility to the cloud, the mist processing can run alone to guarantee unending functionalities regardless.

1.3.3 IoT Security Challenges: With the fast enlarging of IoT everything is being savvy. These shrewd gadgets create an enormous measure of information (counting individual data). Security and protection of this security delicate information and individual data is a major test. Since IoT gadgets have extremely less power and memory, conventional security instruments, for example, a cryptographic capacity, which requires complex computations can't be executed at the asset - obliged IoT gadget. Be that as it may, the security and protection related issues have not been proficiently perceived in haze figuring. We are currently toward the starting period of exploration on the protection and security related issues of haze processing.

1.3.4 IoT Privacy: As articles are becoming recognizable through IoT, protection related dangers have expanded complex. Getting information is significant so it isn't abused by any third individual. Regardless of this, issues connected with information proprietorship ought to likewise be tended to. To cause the client to feel great in being essential for the IoT framework measures should be taken. The responsibility for data gathered from various smart objects should be particularly settled. The proprietor should be ensured that the information won't be utilized without their assent, explicitly when it will be shared over the web [9].

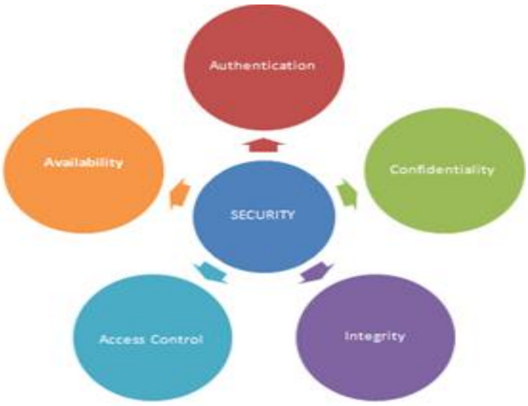

Fig: Trust Areas in Security

2. LIGHTWEIGHT CRYPTOGRAPHY

Light-weight cryptography is the part of another cryptography, which is cover cryptographic calculations planned for involving in unavoidable gadgets with low assets. LWC doesn't find extreme rules for grouping a cryptographic calculation as light-weight, however the normal face of light-weight calculations are exceptionally low necessities to primary assets for target gadgets. Underneath make sense of momentarily the two sorts of lightweight cryptography (symmetric and Asymmertic). The accompanying variables on the execution are expected for lightweight cryptography.

- Size (circuit size, ROM/RAM sizes)
- Power
- Power consumption
- Processing speed (throughput, delay)

Below Fig illustrates the block diagram of light-weight cryptography (LWC)[3].

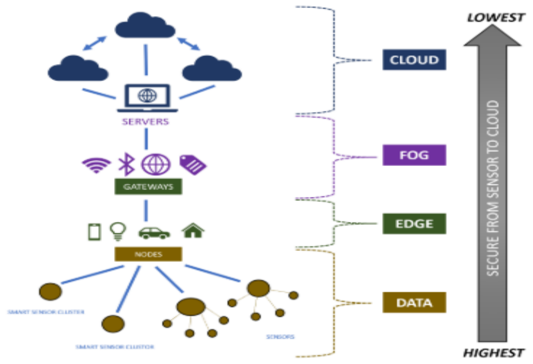

Fig: Block Diagram of Lightweight Cryptography

The ongoing cryptographic natives can be separated into two classes. Deviated key cryptography and Symmetric key cryptography.

A. Asymmetric or Unbalanced Key Cryptography:

Asymmetric or Unbalanced key cryptography is known as open key cryptography, on the grounds that in this procedure, a couple of public key and confidential key are required. As of late the focal point of lightweight cryptography moved towards topsy-turvy key cryptography, however the outcomes are not yet consistent and productive like symmetric key cryptography.

Lightweight Asymmetric cryptography are perplexing concerning activity and are not time productive. The size of the operands and persistent development of assault models are likewise making these calculations defenceless [6].

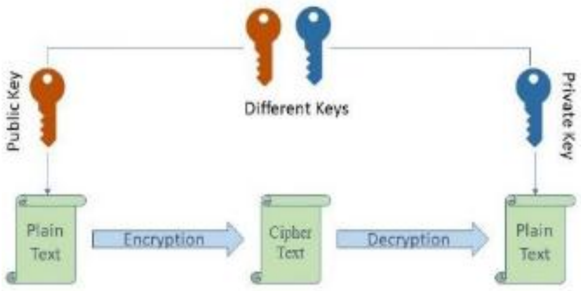

Fig: Asymmetric Cryptography

B. Symmetric Key Cryptography:

Symmetric key cryptography is known as shared key cryptography or secret key. In this cycle, a sender and a receiver both offer a typical key through secret correspondence for both encryption and unscrambling. Symmetric cryptography is more reasonable for IoT applications as a result of its quick tasks which are for the most part XOR and stages. The handling speed is quicker and they don't utilize numerous assets [7].

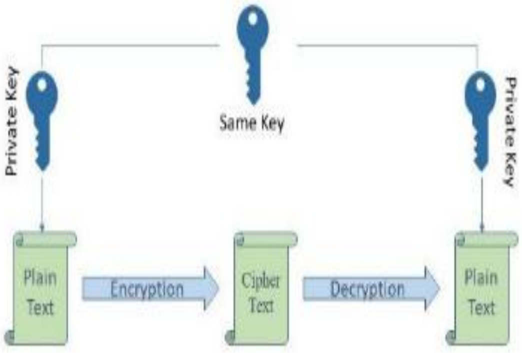

Fig: Symmetric Cryptography

2.1 CHALLENGES IN LIGHTWEIGHT CRYPTOGRAPHY:

Lightweight cryptography focuses on an exceptionally wide assortment of asset compelled gadgets, for example, IoT end hubs and RFID labels [6] that can be executed on both equipment and programming with various correspondence innovations. It is undeniably challenging for asset restricted climate to execute the standard cryptographic calculations because of the execution size, speed or throughput and energy utilization. The lightweight cryptography compromises execution cost, speed, security, execution and energy utilization on asset restricted gadgets. The inspiration of lightweight cryptography is to utilize less memory, less figuring asset and less power supply to give security arrangement that can work over asset restricted gadgets. The lightweight cryptography is normal easier and quicker contrasted with ordinary cryptography. The burden of lightweight cryptography is less gotten [8].

3. LIGHTWEIGHT CRYPTOGRAPHY ALGORITHMS:

Lightweight Cryptography (LWC) is a cryptography field that spotlights on quick turn of events and productive cryptographic strategies for asset obliged conditions that can supplant the customary computationally costly ones while accomplishing a satisfactory degree of safety [10]. Lightweight arrangements are intended to be lighter concerning their key size, memory necessities, and execution time. This works with lesser assets for utilized contrasted with heavyweight arrangements. There are no obliged necessities for any lightweight calculation to fit in; be that as it may, the key size, block size, code measures, clock cycles, and significantly more are given higher significance. The objective of making a lightweight calculation configuration is to think twice about factors like low asset prerequisites, execution, and cryptographic strength of the calculation.

3.1 Requirements of LWC

It is based on the plan difficulties, the lightweight calculations are indented to utilize more modest block sizes (32, 48, or 64 pieces) than a customary code, which has a bigger block size (64 or 128 pieces). LWC likewise utilizes more modest key sizes (under 96 pieces). The most un-key size, as per NIST, is 112 pieces. In ISO/IEC 29192, lightweight properties are nitty gritty laid out on their objective stages. Lightweight properties of equipment, right off the bat, are assessed by fundamental measures, for example, chip size and energy utilization. Furthermore, RAM size with more modest code is leaned toward for lightweight applications in programming executions.

3.2 Design considerations of LWC

The Design considerations of LWC are as following:

- A diminishing in the algorithm’s fundamental factors like block size, key length, and the calculation's inner state can cause security issues, for example, CBC disintegrates and beast force key assaults.
- Lightweight calculations ought to be based upon components that are generally utilized and completely broke down.
- Changes with worked on layers like diminishing the ROM prerequisites.
- Utilization of useful parts like information subordinate piece following, shift registers, minimal expense, and a lot more.
- Planning less complex key timetables that can determine sub-keys quickly forward or in reverse.
- Applying essential tasks with a more critical number of rounds.
- Utilizing tasks as per the assets accessible on the objective stage that permit execution compromises.

3.3. Why lightweight cryptography is required for IoT?

Lightweight cryptography is required for IoT because of the accompanying reasons:

3.3.1 Efficient end-to-end communication:

End nodes should be furnished with a symmetric key calculation for accomplishing start to finish security. For asset compelled IoT gadgets, having a cryptographic activity with less asset consumption is urgent. Carrying out a lightweight symmetric key calculation on end gadgets consumes less energy.

3.3.2 Resource-Constrained devices:

The lightweight cryptographic natives consume more modest space than customary natives. Consequently, lightweight cryptographic natives would open the probability of more organization associations even with asset compelled gadgets [26].

4. RELATED WORK AND LITERATURE SURVEY ON LIGHTWEIGHT CRYPTOGRAPHY ALGORITHMS FOR IOT SECURITY

This section will giving the connected works in information encryption for IoT applications. Writing shows concentrates on power utilization, handling speed, parcel size, information types, and torrential slide impact in information encryption for IoT applications.

According to Gartner report (Stamford 2013), IoT can deliver in excess of a 300 billion US dollar income in 2020, barring cell phones, tablets, and PCs. Furthermore, by 2020, measures of cell phones and tablets arrived at over 7.3 billion units. For countless information correspondence over the organization, a perplexing and enormous organization will be made. Numerous web based applications have been presented, like internet shopping, moment installment, and electronic bill installment. Other than web applications, a few new ideas are arising in Cryptocurrency, Blockchain, and the Internet of Things (IoT).

In an IoT climate, the interest for utilizing the fitting cryptographic arrangement is expanding. By the by, on account of the restricted battery duration, low power calculation, little memory, restricted power supply, and little size of the edge gadgets endure impediments in applying cryptography. An ordinary cryptographic crude may not be reasonable for these low-fueled edge gadgets. For example, a RFID tag can't utilize a 1204-piece RSA calculation because of an absence of assets [13]. The ongoing savvy industry requires a smart cryptographic arrangement that can give satisfactory security execution in unavoidable registering and just asset restricted edge gadgets.

The assessment of lightweight codes, Software Implementation for remote sensor networks is finished, the creators produce an execution of lightweight block figures including KLEIN-80, TWINE-80, Piccolo-80, SPECK (64,96) and SIMON(64,96) are carried out on the Atmega128 processor in re-enactment climate of AVR studio 5.1.The assessment shows that the SPECK(64,96) figure has been the best worth according to the point of view of energy and is suitable for remote sensor organization (WSN) with the fundamental necessity of energy [10].

A light-weight cryptographic calculation for the web of thing (IoT) named as the safe web of thing SIT. The proposed calculations are intended for the web of thing to think about the wellbeing and assets use difficulties. The engineering of proposed calculation presented simple construction appropriate for executing on the web of thing climate. A great deal of notable block figure including AES (Rijndael), 3-Wa, SAFER, SHARK, Grasshopper PRESENT, and Square use Substitution Permutation SP NW. different elective rounds of replacement and rendering fulfill Shannon's disarray in addition to dispersion properties which guarantee that the code text is changed in a pseudo irregular manner. Other normal codes including SF, Blowfish, Camelia, and information encryption standard utilize the Feistel engineering. One of the fundamental benefits of utilizing Feistel engineering is that the encryption in addition to unscrambling methods is practically equivalent. A proposed calculation is a crossover approach based Feistel in addition to Substitution-Permutation SP organizations. In this manner, making utilization of properties of the two ways to deal with further develop a light-weight calculation that presents significant security in the web of thing climate while keeping the computational intricacy at the gentle level [11].

The authors **Abebe Abeshu Diro ,Yunyoung Nam and Naveen Chilamkurti** proposed a Proxy re-encryption utilizing Eliptic bend cryptography to address the security difficulties of asset obliged IOT gadgets by offloading cryptographic computations at Fog hubs. In disseminated climate as IoTs ,Proxy re-encryption, presented by Bleumer, Strauss and Blaze , is a new encipher strategy to give security. In this encryption method, a middle of the road or facilitator hub, for instance, haze hub is outfitted with some key K1,K2 .These keys enables the haze hubs to decipher unique message PT encoded with the public key PUK1 of a client into an encryption of a similar message PT under an alternate public key PUK2 without releasing the items in message to the moderate haze hub and mystery key to any of the conveying substances. This method helps in settling stockpiling limitations and key administration issues. There are five principal methodology of intermediary re-encryption like Key age, Client encryption, Fog re-encryption, Fog unscrambling and Client decoding. The security plot is executed by the creators in JAVA utilizing nics-crypto and probed a laptop(Intel® Core of

32GB RAM) .It expects to carry out on genuine stages ,for instance, Arduino and raspberry[12].

To give start to finish security to any correspondence fundamental three security i.e, CIA (C-secrecy, I-Integrity, A-Authentication) prerequisites ought to be satisfied. **Nadeem Abbas, Muhammad Asim, Noshina Tariq, Thar Baker, and Sohail Abbas** ,the authors in [14], proposed an original FSS-Fog security administration utilizing two cryptographic plans, Identity based computerized mark and Identity based encryption .It has been expected by the creators that all IoT gadgets are doled out some info security boundaries ,for instance, particular ID,username and secret word. The verifier at the haze layer, validates, the shipper by these boundaries (IDrec). A little size key Ksmall of 128 bit is produced by the IoT gadget, who needs to speak with haze layer. The creators utilized hilter kilter encryption (RSA public key calculation) for the public key encryption. The gadget encodes the critical Ksmall with the assistance of haze layer public key and consolidates both enciphered IDrec alongside nonce and Ksmall. Thus, the IoT gadget sends the code message C to the haze layer for the verification [14].

5. LIGHTWEIGHT CRYPTOGRAPHY ALGORITHMS FOR IOT SECURITY ANLYSIS [2]:

Ref.	**Algorithm**	**Key Size (bits) Block Size (bits)Rounds**			**Structure**	**Performance**				**Merits**	**Attacks/Analysis**
						Tech. (⍰M)	Power (⍰W)	Area (GE)	Throughput At 100Khz (Kbps)		
[16]	AES	128	128	10	SPN	0.13	2.48	2400	56.64	Upholds bigger key sizes, quicker in both equipment and programming.	Related key assault, Boomerang, Biclique cryptanalysis
[17]	PRESENT	80	64	32	SPN	0.18	1.54	1030	12.4	Ultra Lightweight code, Energy proficient.	Necessary, Bottleneck assaults, shortened differential cryptanalysis, Side-channel assaults
		128				0.18	2.00	1339	12.12		
[18]	RECTANGLE	128	64	26	SPN	0.13	1.78	1787	246	Quick executions utilizing bit cut strategies	slide assault, related-key cryptanalysis, measurable Saturation Attack
[19]	HIGHT	128	64	32	FN	0.25	5.48	3048	188.20	Super lightweight, gives high security, great for RFID labeling.	Unimaginable differential assault on 26th round,Biclique cryptanalysis
[20]	CLEFIA	128	128	18	FN	0.13	2.48	2488	39	Has quick encryption and unscrambling, lesser rounds, energy productive	Key Recovery Attack on tenth round, Saturation Cryptanalysis

[21]	CAMELLIA	128	128	18, 24	SPN	-	1.54	6511	290.1	Protection from savage power assault on keys, security levels similar to AES.	Reserve timing assaults , Impossible differential assault
[22]	TWINE	80, 128	64	36	FN	0.09	1.30	1866	178	Great for little equipment, productive programming execution	Compromise assaults, Saturation Attack
[23]	SIMON	128	128	64	SPN	0.13	1.32	1317	22.9	Upholds a few key sizes, performs well in Hardware	Differential shortcoming assaults, Attacks on diminished variants
[23]	SPECK	128	128	32	SPN	0.13	1.40	1396	12.1	Performs better in programming	Key Recovery, Boomerang assault

6. CONCLUSION:

The objective of lightweight cryptography (LWC) is to give security and protection in asset compelled applications, implanted frameworks, Internet-of-Things (IoT), and digital actual frameworks, including Radio Frequency Identification (RFID) frameworks, remote sensor organizations, vehicle specially appointed organizations, and medical care. Web of Things has been quickly tracking down its way through our current life and is planning to work on the personal satisfaction by associating us with many savvy gadgets, innovations, and applications. The IoT will have total computerization of everything around us. Albeit a lot of assessment has been done in the IoT, yet there is another thing to research in it. The rising thought of adventures and lawmaking bodies in this development has provoked a wide spread research and achieved various successful errands. A piece of the challenges in IoTs like the general designing, security and assurance concerns surely stick out, while others concern like openness, constancy, execution of the sagacious devices really require more thought. Likewise this paper presented an outline of light-weight cryptography execution and had drawn about the different very lightweight block calculates whose goal is to programme and gear successful.

7. FUTURE SCOPE:

From the overview and relative investigation, the accompanying examination issues are found on which further work should be possible.

1. In IoT, information security and verification is a major concern so quantities of methods are proposed in which cross breed models of encryption and validation calculations are made (like hybridization of AES and RSA strategy) yet this causes expansion in the memory necessity on the gadgets. To counter this issue, the encryption calculations are worked in CCM mode which gives security as well as confirmation.

2. In the lightweight code to give similar degree of safety as in ordinary code, the quantity of rounds expanded. The huge number of rounds debases the presentation. Thus, the future exploration bearing is plan lightweight code, for example, way that it gives quick disarray and dispersion in less number of rounds.

3. The RSA and ECC calculations numerical displaying in light of discrete logarithm and particular number juggling. These demonstrating incorporate enormous number of duplication activity. Thus, research heading is to utilize Vedic Multiplier (like UT and NDD Vedas) instead of ordinary multiplier for quick reaction.

8. REFERENCES:

[1] Hassan, A. (2021).Lightweight Cryptography for the Internet of Things. Advances in Intelligent Systems and Computing,1290,780–795. https://doi.org/10.1007/978-3-030-63092-8_52

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

[3] S. B. Sadkhan and A. O. Salman, "A survey on lightweight-cryptography status and future challenges," *2018 International Conference on Advance of Sustainable Engineering and its Application (ICASEA)*, 2018, pp. 105-108, doi: 10.1109/ICASEA.2018.8370965.

[4] Usman, Muhammad, Irfan Ahmed, M. Imran Aslam, Shujaat Khan, and Usman Ali Shah. "SIT: a lightweight encryption algorithm for secure internet of things." arXiv preprint arXiv:1704.08688 (2017).

[5] N. A. Gunathilake, W. J. Buchanan and R. Asif, "Next Generation Lightweight Cryptography for Smart IoT Devices: : Implementation, Challenges and Applications," 2019 IEEE 5th World Forum on Internet of Things (WF-IoT), 2019, pp. 707-710, doi: 10.1109/WF-IoT.2019.8767250.

[6] I. K. Dutta, B. Ghosh, and M. Bayoumi, "Lightweight cryptography for internet of insecure things: A survey," 2019 IEEE 9th Annu. Comput. Commun. Work. Conf. CCWC 2019, no. January, pp. 475–481, 2019, doi: 10.1109/CCWC.2019.8666557.

[7] S. Chandra, S. Paira, S. S. Alam, and G. Sanyal, "A comparative survey of symmetric and asymmetric key cryptography," 2014 Int. Conf. Electron. Commun. Comput. Eng. ICECCE 2014, pp. 83–93, 2014.

[8] Mouha N. The design space of lightweight cryptography. NIST Light Cryptogr Work. 2015;2015:1–19.

[9] R. Roman et al., "Securing the Internet of Things," in IEEE Computers, 2011, vol. 44(9), pp. 51–58

[10] J. Hosseinzadeh, A. Ghaemi, "Software Implementation And Evaluation of Lightweight Symmetric Block Ciphers Of The Energy Perspectives And Memory," INTERNATIONAL JOURNAL OF ENGINEERING EDUCATION (IJEE) ISSN: 0949-149X www.sweetmaxwell.org March- April 2017 Vole 9, No 2017.

[11] M. Usman., I. Ahmed , M. Imran , S. Khan, U. Ali , "SIT: A Lightweight Encryption Algorithm for Secure Internet of Things," (IJACSA) International Journal of Advanced Computer Science and Applications, Vol. 8, No. 1, 2017.

[12] Abebe Abeshu Diro , Naveen Chilamkurti ,Yunyoung Nam, :Analysis of Lightweight Encryption Scheme for Fog-to-Things Communication, IEEE Access, Volume 6 (2018).

[13] B. Padmavathi and S. Ranjitha Kumari, "A survey on performance analysis of DES, AES and RSA algorithm along with LSB substitution," International Journal of Science and Research, vol. 2, no. 4, pp. 170–174, 2013.

[14] Nadeem Abbas, Muhammad Asim, Noshina Tariq, Thar Baker, and Sohail Abbas , :A Mechanism for Securing IoT –enabled Applications at the Fog Layer, Journal of Sensor and Actuator Networks(JSAN), Volume 8, Issue 1 (2019)

[15] R. Hassan, A. S. Ahmed, and N. E. Osman, "Enhancing security for IPv6 neighbor discovery protocol using cryptography," American Journal of Applied Sciences, vol. 11, no. 9, pp. 1472–1479, 2014.

[16] A. Moradi et al., "Pushing the Limits: A Very Compact and a Threshold Implementation of AES," in Advances in Cryptology – EUROCRYPT 2011 Lecture Notes in Computer Science, Springer, 2011, vol. 6632, pp. 69-88.

[17] A. Bogdanov et al., "PRESENT: An Ultra-Lightweight Block Cipher," in Cryptographic Hardware and Embedded Systems - CHES 2007 Lecture Notes in Computer Science, Springer, 2007, pp. 450-466.

[18] W. Zhang et al., "RECTANGLE: a bit-slice lightweight block cipher suitable for multiple platforms," in Science China Information Sciences, 2015, vol. 58(12), pp. 1-15.

[19] D. Hong et al., "HIGHT: A New Block Cipher Suitable for Low- Resource Device," in Cryptographic Hardware and Embedded Systems - CHES 2006 Lecture Notes in Computer Science, 2006, pp. 46-59.

[20] T. Akishita and H. Hiwatari, "Very Compact Hardware Implementations of the Blockcipher CLEFIA," in Selected Areas in Cryptography Lecture Notes in Computer Science,Springer, 2012, pp. 278-292.

[21] A. Satoh and S. Morioka, "Hardware-Focused Performance Comparison for the Standard Block Ciphers AES, Camellia, and Triple-DES," in Lecture Notes in Computer Science Information Security, Springer, 2003, pp. 252-266.

[22] P. Kumarkushwaha et al., “A Survey on Lightweight Block Ciphers,” inInternational Journal of Computer Applications, 2014, vol. 96(17), pp. 1-7.

[23] R. Beaulieu et al., “The SIMON and SPECK lightweight block ciphers,” in Proceedings of the 52nd Annual Design Automation Conference, 2015, pp. 1-6.

[24] Kumar, S.A., Vealey, T. and Srivastava, H., 2016, January. Security in internet of things: Challenges, solutions and future directions. In 2016 49th Hawaii International Conference on System Sciences (HICSS) (pp. 5772-5781). IEEE.

[25] Shamala, Mary & Godandapani, Zayaraz & Vivekanandan, Kaniappan & Vijayalakshmi, V.. (2021). Lightweight Cryptography Algorithms for Internet of Things enabled Networks: An Overview. Journal of Physics: Conference Series. 1717. 012072. 10.1088/1742-6596/1717/1/012072.

[26] Alaba, F.A., Othman, M., Hashem, I.A.T. and Alotaibi, F., 2017. Internet of Things security: A survey. Journal of Network and Computer Applications, 88, pp.10-28.