An Analysis of Block Ciphers And Algorithms Used In IOT

Prof. Vijay Swaroop[1], Prof. Rajendra M[2], Indira.R.Somannavar[3], Rakshitha C[4]
[1, 2] Professor, Dept of Computer Science
[3, 4]Dept of Computer Science
[1, 2] Atria Institute of Technology, Bengaluru

Abstract- *In today's world, everything is being connected to the internet. This terminology is referred to as Internet of Things (IoT). Majority of IoT devices are low resource devices. Conventional encryption methods are not appropriate for such devices. To encrypt data on these devices we make use of lightweight block ciphers. These smart devices are characterized by low computing power, small memory size, limited battery supply and small memory size. The internet of things, within the border domains of security requires algorithms that are secure and are able to protect the devices connected to the internet. There are problems associated with these algorithms in terms of its strength and performance related to security. So, we need to enhance its strength and performance by using avalanche effect. This paper provides a brief analysis on both block ciphers and also algorithms being used in internet of things.*

Keywords- Avalanche effect; Internet of Things (IoT); Cryptographic Algorithms; Security, Block cipher;

I. INTRODUCTION

Things which are interconnected within the network of networks is called the Internet of Things (IoT).[3]**Holdowsky et al**. states that flaws such as Denial of Service (DOS) frequently occurs on machines connected to the IOT. Kouns [1] indicated that by 2020 there will be over 26 billion connected devices.
We need to use best algorithm which has high security and performance. So we need to compare the strength of the algorithm to know which one is best. Avalanche effect is one of the method to compare the strength of an algorithm.

Zibideh [5] showed that the avalanche effect is a desirable property for traditional algorithm like AES, DES and other well-known algorithms used on the IoT. this method can be used to compare the strength of different algorithms. We can say that it is a property of some cipher systems in which a small change in the input results in a very large change in the output. The algorithm which gives high avalanche effect are best in performance speed and security.

The input for a block cipher is a block of plaintext bits and generates a block of ciphertext bits as output which is generally

of the same size as input[6]. A block cipher in general is depicted as follows:

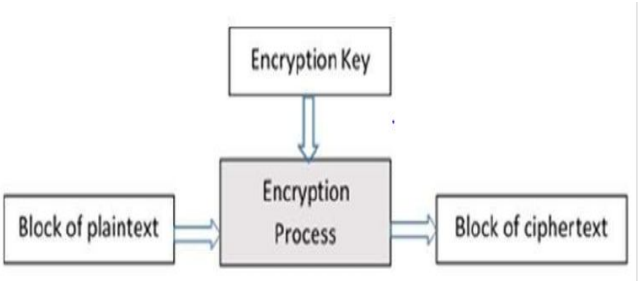

Fig 1: BLOCK CIPHER

The size of the block will be fixed priory. The strength of encryption scheme is unaffected by the choice of the block size. Key Length is the major factor on which the strength of cipher depends. They have fixed block size and key size. Two major operations used in block cipher for encryption are Confusion and Diffusion. Confusion makes complex relationship among encryption key and cipher text. Diffusion is used to propagate influence of each bit in the block of plain text over a number of bits in cipher text block making cipher text oversensitive to statistical attacks.

IoT is now required to apply implementation of data protection to sensor devices in environments with various restrictions that have not previously been subject to such implementation[8]. Encryption is used as an effective countermeasure.

In this paper we considered effects on ten algorithms that are mostly used on IoT domain for encryption. Also these algorithms are: AES algorithm, Camellia algorithm, CAST-128 algorithm, Clefia algorithm, DES algorithm, Blowfish algorithm, Modular Multiplication based Block Cipher (MMB), Rivest Cipher 5 (RC-5)-32/32/16 algorithm, Serpent algorithm and Skipjack algorithm.

Also we have few relevant lightweight block ciphers optimized for software implementations. Block ciphers considered in this paper are CLEFIA [8], SIMON[12],PICCOLO[11],TWINE[9],SPECK[7], XTEA [6], AES [13], PRESENT [11], KLEIN [10], LED [9], mCrypton etc.

II. METHODOLOGY

In this section we consider types of block ciphers, Avalanche effect of some algorithms. Block cipher can be of type: Substitution Permutation Network(SPN) and Feistal based network. Feistal networks can be further classified as Classical Feistal Networks and Generalized Feistal Networks.

1. Feistel structures:

In this section, a Feistel cipher, the block of plain text to be encrypted is split into two equal-sized halves. The round function is applied to one half, using a subkey, and then the output is XORed with the other half. The two halves are then swapped[13].The encryption process uses the Feistel structure consisting multiple rounds of processing of the plaintext, each round consisting of a "substitution" step followed by a permutation step. Decryption function in the Feistel type structure do not require much implementation cost as Feistel structure use same program code for both encryption and decryption operations in order to decreases the memory requirements.

Some popular Feistel networks are CLEFIA [8], SIMON [9], PICCOLO [11], TWINE [9], SPECK [8], and XTEA [10].Feistel networks are further classified into Classical Feistel Structures (CFS) and Generalized Feistel structures (GFS).
One advantage of the Feistel model compared to a substitution permutation network is that the round function does not have to be invertible.

2. Substitution Permutation Networks (SPN):

SPN has a chain of linked mathematical operations. A combination of substitution layer with permutation layer along with key mixing constitutes a round of SPN. A substitution function or confusion function provides confusion and constitutes a substitution/confusion layer. This layer constitutes non-linear operations provided by S-boxes (Lookup-Tables based) or by using bit-slice implementation. Permutation layer has P-box and is also called diffusion layer. Permutation layer constitutes invertible linear transformations or simple fixed permutations(bit-wise or word wise). It has extra inherent parallelism for confusion and diffusion and it requires S-box to be invertible. AES[7], PRESENT[6], KLEIN[12], LED[11], mCRYPTON [12] are some latest and widely used SPN block ciphers by researchers against the number of publications mentioned in this paper.

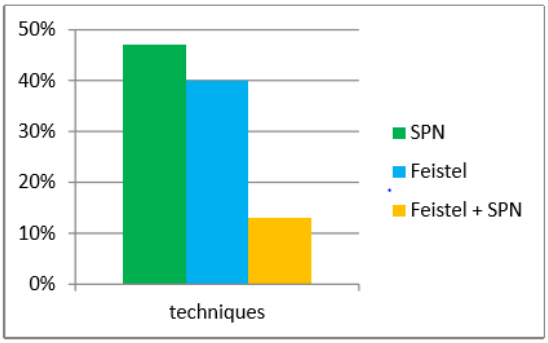

Fig 2: Comparative Use of Various Techniques in Lightweight Block Ciphers

Weuse Avalanche effect using initial vector XORed with plaintext and final vector XORed with cipher text. In this paper we will use initial vector XORed with plaintext and final vector XORed with cipher text and test the avalanche effect of all the algorithm.

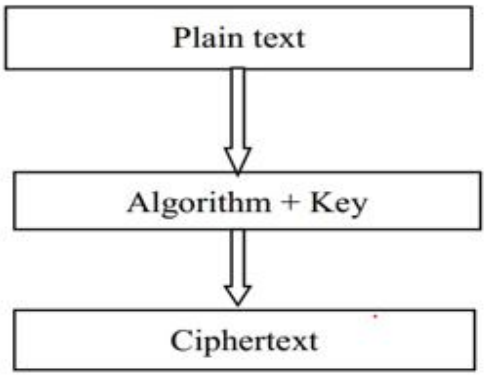

Fig. 3: The model of well-known algorithms

Fig 3 shows standard well known model for encryption .After that, an analysis of avalanche effect of our proposed algorithm was done as shown Fig 4.

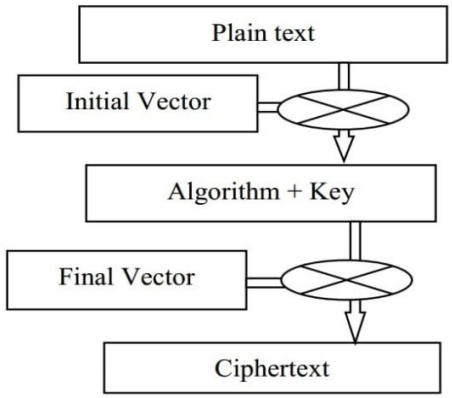

Fig 4: Model of our proposed work, where initial and final vectors are implemented.

We calculated the avalanche effect at different positions of cipher texts. If two cipher text were not the same in any of the positions, then the avalanche effect was calculated as that number of different positions divided by total number of position of the cipher text. The dividend was multiplied by hundred to give percentage.

The main characteristics that differentiated one encryption algorithm from another was its ability to encrypt data when its time and speed were also measured [4].

Some of the available ciphers are not fully optimized and can be explored further. All these ciphers have some kind of weaknesses like:

a) Weak substitution box
b) Weak permutation layer
c) Weak key scheduling
d) Susceptibility to some kind of attacks
e) Computationally complex and expensive
f) Low resource utilization

III. RESULTS AND ANALYSIS

1.BLOCK CIPHERS:

Table below shows few relevant lightweight block ciphers optimized for software implementations.

Cipher	Year	Technique	Key Size (bits)	Block Size (bits)	No. of Rounds
Improved Lilliput [15]	2017	SDPN	80	64	30
GIFT [65]	2017	SPN	128	64/128	28/40
SIT [16]	2017	Feistel + SPN	64	64	5
DLBCA [67]	2017	Feistel	80	32	15
LiCi [66]	2017	Feistel	128	64	31
SKINNY [17]	2016	SPN	64-384	64/128	32-56
MANTIS [17]	2016	SPN	128	64	10/12
SPARX [33]	2016	SPN with ARX-based S-Boxes	128/256	64/128	24-40
LAX [33]	2016	SPN with ARX-based S-Boxes	128/256	64/128	24-40
FeedFunnel [14]	2016	Feistel	80/128	64	10/12
PICO [12]	2015	SPN	128	64	32
RECTANGLE [7]	2015	SPN	80/128	64	25
Chaskey [45]	2014	SPN with ARX-based S-Boxes	128	128	8
DLBCA [66]	2014	SPN	80	64	22
ITUBee [54]	2014	Feistel	80	80	20
HISEC [13]	2014	Feistel	80	64	15
LAC [43]	2014	Feistel	80	64	16
SIMON [8]	2013	Feistel	64/ 72/ 96/ 128/ 144/ 192/ 256	32/48/64/96/128	32/36/42/44/52/ 54/68/69/72
SPECK [8]	2013	Feistel	32/ 64/ 72/ 96/ 128	64/ 72/ 96/ 128/	22/ 23/ 26/ 27 28/ 29/ 32/ 33
				144/ 192/ 256	34
HeW [58]	2013	Feistel-M	80/128	64	32
LEA [41]	2013	SPN with ARX-based S-Boxes	128/192/256	128	24/28/32
SCREAM [36]	2012	SPN	128	128	10/12
PRINCE [34]	2012	SPN	128	64	12
Hummingbird-2 [10]	2011	SPN+Feistel	128	64	4
TWINE [9]	2011	SPN	80/128	64	36
LED [21]	2011	SPN	64/128	64	32/48
LBlock [32]	2011	Feistel+SPN	80	64	32
PICCOLO [11]	2011	SPN	80/128	64	25/31
KLEIN [19]	2011	SPN	64/80/96	64	12/16/20
CLEFIA [16]	2007	Feistel	128/192/256	128	18/22/26
PRESENT [6]	2007	SPN	80/128	64	31
SEA [29]	2006	Feistel	96	96	93
mCrypton [22]	2005	SPN	64/96/128	64	12
TOEA [27]	2004	Feistel	64	64	48
Camellia [26]	2000	Feistel + SPN	128/192/256	128	18/24/24
KHAZAD [25]	2000	SPN	128	64	8

Block Size and Key Size is in number of bits; Feistel-M (Balanced GFN + SPN); Extended Generalized Feistel Network (EGFN)

2. ALGORITHMS:

Out of ten algorithms 6 algorithms failed to increase the avalanche effect and 4 algorithms that passed the avalanche effect when proposed method wused when key was fixed.

Number of algorithm failed to increase avalanche effect	6	AES, Blowfish , Clefia, DES,MMB, Serpent
Number of algorithm passed to increase avalanche effect	4	Camellia, RC5 , Skipjack, Cast-128

Out of ten algorithms 3 algorithms failed to increase the avalanche effect and 7 algorithms passed the avalanche effect when proposed method was used when plain text was fixed.

Number of algorithm failed to increase avalanche effect	3	Camellia, Clefia, Blowfish
Number of algorithm passed to increase avalanche effect	7	AES,DES,RC5, MMB, Serpent, Skipjack,Cast-128

IV. CONCLUSION

All the ten algorithms that are currently used on the internet of things (IoT) failed to give the highest avalanche effect when compared to our modified algorithm on both fixed key and plaintext variation.

we managed to increase the avalanche effect to 60% of the algorithms tested when the key was fixed and 70% when plaintext was fixed

Block ciphers are one of the main primitives for cryptographic applications. In this paper, we discussed various lightweight block ciphers suitable for IoT applications. These are generally categorized as either hash functions, stream ciphers or block ciphers. A number of cryptanalysts showed that there exist numerous attacks on ciphers for which the ciphers must provide good resistance. IoT being emerging field requires lightweight cipher designs having rich encryption standards, robust architecture, less complexity, less execution time, lower power consumption, low resource utilization and good resistance against possible attacks. As a result, the design of lightweight block ciphers has fascinated attention of many researchers', especially in the last 5 years. Through our extensive literature survey over lightweight block ciphers, we found that available ciphers are not fully optimized and can be explored further. The search continues for a lightweight cipher which should fulfill the requirements of a good lightweight cipher.

REFERENCES

[1] J. Kouns, "Bring Your Own Internet of Things BYO-IoT" 2015 RSA Conference, pp 4-5.

[2] B. Johnson, "How the Internet of Things Works"

[3] J. Holdowsky, M. Mahto, M. E. Raynor and M. Cotteleer, "Inside the Internet of Things.

[4] Bourke, "CSCE 477/877", 2015 Cryptography and Computer Security Department of Computer Science & Engineering University of Nebraska—Lincoln, NE 68588, 2015, pp 5-138.

[5] D. D. Moskovich. "An Overview of the State of the Art for Practical Quantum Key Distribution", Vol. 4, 2015.

[6] Madakam, S., Ramaswamy, R. and Tripathi, S., 2015. Internet of Things (IoT): A literature review. Journal of Computer and Communications, 3(05), p.164. {a}

[7] Hafsa Tahir, A.K. and Junaid, M., 2016. Internet of Things (IoT): An Overview of Applications and Security Issues Regarding Implementation. {b}

[8] Xu, Q., Ren, P., Song, H. and Du, Q., 2016. Security enhancement for IoT communications exposed to eavesdroppers with uncertain locations. IEEE Access, 4, pp.2840-2853. {c}

[9] Kaur, A., 2016. Internet of Things (IoT): Security and Privacy concerns. International Journal of Engineering Sciences & Research Technology. (pp. 161-165). DOI: 10.5281/zenodo.51013.

[10] Daemen, J. and Rijmen, V., 1999. AES proposal: Rijndael.

[11] Bogdanov, A., Knudsen, L.R., Leander, G., Paar, C., Poschmann, A., Robshaw, M.J., Seurin, Y. and Vikkelsoe, C., 2007, September. PRESENT: An ultralightweight block cipher. In CHES (Vol. 4727, pp. 450466).

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

[13] Beaulieu, R., Shors, D., Smith, J., Treatman-Clark, S., Weeks, B. and Wingers, L., 2013. The SIMON and SPECK Families of Lightweight Block Ciphers. Cryptol ogy ePrint Archive, Report 2013/404.

[14] Suzaki, T., Minematsu, K., Morioka, S. and Kobayashi, E., 2011, November. Twine: A lightweight, versatile block cipher. In ECRYPT Workshop on Lightweight Cryptography (Vol. 2011).

[15] Engels, D.W., Saarinen, M.J.O., Schweitzer, P. and Smith, E.M., 2011. The Hummingbird-2 Lightweight Authenticated Encryption Algorithm. RFIDSec, 11, pp.19-31.

[16] Shibutani, K., Isobe, T., Hiwatari, H., Mitsuda, A., Akishita, T. and Shirai, T., 2011, September. Piccolo: An

ultra-lightweight blockcipher. In CHES (Vol. 6917, pp. 342-357).

[17] Bansod, G., Pisharoty, N. and Patil, A., 2016. PICO: An Ultra Lightweight and Low Power Encryption Design for Ubiquitous Computing. Defence Science Journal, 66(3).

[18] AlDabbagh, S.S.M., Shaikhli, A., Taha, I.F. and Alahmad, M.A., 2014, September. Hisec: A new lightweight block cipher algorithm. In Proceedings of the 7th International Conference on Security of Information and Networks (p. 151). ACM.

[19] Baysal, A. and Şahin, S., 2015, September. Roadrunner: A small and fast bitslice block cipher for low cost 8-bit processors. In International Workshop on Lightweight Cryptography for Security and Privacy (pp. 58-76). Springer, Cham.

[20] Mumthaz Pookuzhy Ali, Geethu T George, 2017. "Optimised Design of Light Weight Block Cipher Lilliput with Extended Generalised Feistal Network (EGFN)." International Journal of Innovative Research in Science, Engineering and Technology, Vol. 6, Issue 4. Website: www.ijirset.com.