RESEARCH ARTICLE OPEN ACCESS

Implementation of Lightweight Encryption Algorithm for use in IoT

Shruti Kumbhare[1], Nehal Behare[2],Bhushan Jawade[3]Suyog Gupta[4]

1(Department of Electronics & Telecommunication Engineering , SRPCE, Nagpur Email: shrutikumbhare44@gmail.com)
2(Department of Electronics & Telecommunication Engineering , SRPCE, Nagpur Email: beharenehal@gmail.com)
3(Department of Electronics & Telecommunication Engineering , SRPCE, Nagpur Email: bjawade94@gmail.com)
4(Department of Electronics & Telecommunication Engineering , SRPCE, Nagpur Email: suyog@srpce.ac.in)

Abstract:

The Internet of Things (IoT) being a promising innovation without bounds is relied upon to interface billions of gadgets. The expanded number of correspondence is required to produce piles of information and the security of information can be a risk. The gadgets in the design are basically smaller in size and low powered. Traditional encryption algorithms are generally computationally expensive because of their multifaceted nature and requires numerous rounds to encode, basically squandering the compelled vitality of the devices. Less perplexing calculation, nonetheless, may trade off the coveted integrity.In this paper we propose a lightweight encryption algorithm which is a 64-bit block cipher and requires 64-bit key to encrypt the data. The architecture of the algorithm is a mixture of feistel and a uniform substitution-permutation network. Simulations result shows the algorithm provides substantial security in just five encryption rounds.

***Keywords*— IoT,Security, Encryption, Wireless Sensor Network ,WSN, Lightweight Encryption algorithms.**

I. INTRODUCTION

The Internet of Things (IoT) is turning out to be an emerging discussion in the field of research and practical implementation in the recent years. IoT is a model that incorporates customary entities with the aptitude to detect and speak with kindred gadgets utilizing Internet. As the broadband Internet is currently for the most part available and its cost of network is likewise decreased, more devices and sensors are getting associated with it. Such conditions are giving reasonable ground to the development of IoT. There is incredible arrangement of complexities around the IoT, since we wish to approach each question from anyplace on the planet.

The sophisticated chips and sensors are embedded in the physical things that surround us, each transmitting valuable data. The way toward sharing such huge measure of information starts with the gadgets themselves which should safely communicate with the IoT stage. This stage coordinates the information from numerous gadgets and apply analytics to impart the most significant information to the applications.

The IoT is taking the conventional internet, sensor network and mobile network to another level as everything will be connected to the internet.

A matter of concern that must be kept under consideration is to ensure the issues related to confidentiality, data integrity and authenticity that will emerge on account of security and privacy [1].

A. Applications of IoT:

With the progression of time, an ever increasing number of gadgets are getting associated with the Internet. The houses are destined to be outfitted with smart locks [2], the PCs, tablets, advanced mobile phones, smart TVs, computer game consoles even the refrigerators and air conditioners have the ability to convey over Internet. This pattern is expanding outwards and it is assessed that by the year 2020 there will be more than 50 billion items associated with the Internet [3]. This gauges for every individual on earth there will be 6.6 items on the web. The earth will be covered with a huge number of sensors gathering data from physical questions and will transfer it to the Internet.

It is proposed that use of IoT is yet in the beginning period yet is starting to advance quickly.

A review of IoT in building computerization framework is given in [4]. It is suggested in [5] that different ventures have a developing enthusiasm towards utilization of IoT. Different utilizations of IoT in medicinal services ventures are talked aboutin [6], the improvement opportunities in healthcare brought in by IoT will be enormous [7].

It has been anticipated that IoT will contribute really taking shape the mining production more secure [8] and the determining of calamity will be made conceivable. It is normal that IoT will change the car administrations and transportation frameworks [9]. As more physical items will be furnished with sensors and RFID labels transportation organizations will have the capacity to track and screen the question development from beginning to goal [10], along these lines IoT indicates promising conduct in the logistics business also.

B. Security Challenges in IoT IoT:

To receive the IoT innovation it is important to fabricate the certainty among the clients about its security and protection that it won't make any genuine risk their information uprightness, privacy and specialist. Inherently IoT is defenceless against different kinds of security dangers, if important safety efforts are not taken there will be a risk of data spillage or could demonstrate a harm to economy. Such dangers might be considered as one of the major hindrance in IoT.

IoT is to a great degree open to attacks, for the reasons that there is a reasonable chance of physical attack on its parts as they stay unsupervised for long time. Also, because of the remote correspondence medium, the eavesdropping is extremely simple. In conclusion the constituents of IoT bear low competency regarding vitality with which they are worked and furthermore as far as computational capability. The execution of conventional computationally extensive security algorithms will bring about the deterrent on the execution of the energy constrained gadgets.

It is anticipated that considerable amount of data is relied upon to be produced while IoT is utilized for monitoring purposes and it is essential to protect unification of data. Precisely, data integrity and authentication are the matters of concern.

From a high level perspective, IoT is made out of three segments to be specific, Hardware, Middleware and Presentation. Hardware comprises of sensors and actuators, the Middleware gives storage and computing tools and the Presentation gives the understanding apparatuses available on various stages. It isn't plausible to process the information gathered from billions of sensors, setting mindful Middleware arrangements are proposed to enable a sensor to choose the most essential information for processing [24]. Inalienably the architecture of IoT does not offer adequate edge to achieve the vital activities associated with the procedure of authentication and data integrity. The gadgets in the IoT, for example, RFID are faulty to accomplish the crucial prerequisites of validation process that includes consistent correspondence with the servers and exchange messages with the nodes

In secure frameworks the privacy of the information is kept up and it is ensured that amid the procedure of message exchange the information holds its creativity and no modification is inconspicuous by the framework. The IoT is made out of numerous little gadgets, for example, RFIDs which stay unattended for broadened times, it is simpler for the enemy to get to the information put away in the memory [11]. To give the invulnerability against Sybil assaults in RFID tags, received signal strength indication(RSSI) based techniques are utilized as a part of [12], [13], [14] and [15].

Numerous arrangements have been proposed for the wireless sensor networks which consider the sensor as a piece of Internet associated by means of nodes. In any case, in IoT the sensor node themselves are considered as the Internet nodes influencing the authentication process considerably more critical. The integrity of the information additionally ends up essential and requires uncommon consideration towards retaining its reliability.

C. Addressing the Security Challenges :

As of late an investigation by HP uncovers that 70% of the gadgets in IoT are helpless against attacks [16]. An attack can be performed by detecting the correspondence between two hubs which is known as a man-in-the-middle attack. No dependable arrangement has been proposed to provide cater such attacks. Encryption however could limit the measure of harm done to the information integrity. To guarantee information unification while it is put away on the centre product and furthermore amid the transmission it is important to have a security instrument. Different cryptographic algorithms have been created that address the said matter, however their usage in IoT is flawed as the equipment we bargain in the IoT are not reasonable for the execution of computationally extensive encryption algorithms. An exchange off must be done to satisfy the necessity of security with low computational cost.

In this paper, we proposed a lightweight cryptographic algorithm tobe used in IoT networks. The proposed algorithm is intended for IoT to manage the security and resource utilization challenges specified in section I-B.

II. PROPOSED ALGORITHM

The architecture of the proposed algorithm provides a simple structure suitable for implementing in IoT environment. Some well-known block cipher use Substitution-Permutation (SP) network. Several alternating rounds of substitution and transposition satisfies the Shannon's confusion and diffusion properties that ensues that the cipher text is changed in a pseudo random manner. Other popular ciphers including SF [17] and DES [18], use the feistel architecture. One of the major advantage of using feistel architecture is that the encryption and decryption operations are almost same. The proposed algorithm is a hybrid approach based on feistel and SP networks. Thus making use of the properties of both approaches to develop a lightweight algorithm that presents substantial security in IoT environment while keeping the computational complexity at moderate level.

Proposed algorithm is a symmetric key block cipher that constitutes of 64-bit key and plain-text. In symmetric key algorithm the encryption process consists of encryption rounds, each round is based on some mathematical functions to create confusion and diffusion. Increase in number of rounds ensures better security but eventually results in increase in the consumption of constrained energy. The cryptographic algorithms are usually designed to take on an average 10 to 20 rounds to keep the encryption process strong enough that suits the requirement of the system. However the proposed algorithm is restricted to just five rounds only, to further improve the energy efficiency, each encryption round includes mathematical operations that operate on 4 bits of data. To create sufficient confusion and diffusion of data in order to confront the attacks, the algorithm utilizes the feistel network of substitution diffusion functions. Details of the entire process are as discussed below :

A. Generation of Key :

Another vital process in symmetric key algorithms is the generation of key. The key generation process involves complex mathematical operations. In WSN environment these operations can be performed wholly on decoder, on the contrary in IoT the node themselves happens to serve as the Internet node, therefore, computations involved in the process of key generation must also be reduced to the extent that it ensures necessary security.

The most fundamental component in the processes of encryption and decryption is the key. It is this key on which entire security of the data is dependent, should this key be known to an attacker, the secrecy of the data is lost. Therefore necessary measures must be taken into account to make the revelation of the key as difficult as possible. The feistel based encryption algorithms are composed of several rounds, each round requiring a separate key. The encryption/decryption of the proposed algorithm is composed of five rounds, therefore, we require five unique keys for the said purpose

The proposed algorithm is a 64- bit block cipher, which means it requires 64-bit key to encrypt 64-bits of data. A cipher key (Kc) of 64-bits is taken as an input from the user. This key shall serve as the input to the key expansion block. The block upon performing substantial operations to create confusion and diffusion in the input key will generate five unique keys. These keys shall be used in the encryption/decryption process and are strong enough to remain indistinct during attack.

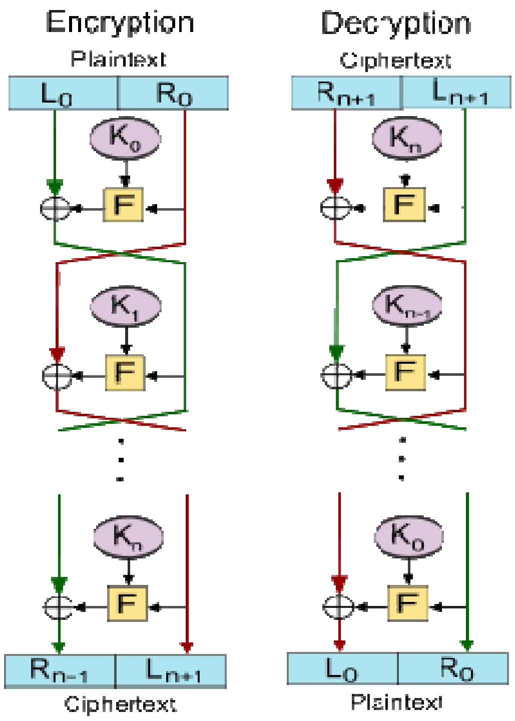

Fig. 1Process of Encryption & Decryption

B. Generation of Key :

After the generation of round keys the encryption process can be started. For the purpose of creating confusion and diffusion this process is composed of some logical operations, left shifting, swapping and substitution. The process of encryption is illustrated in Fig. 1.

III. RESULTS

The simulation of the algorithm is performed Intel Core i3-3770@3.40 GHz processor using MATLAB(R2017a). The results in Fig. 4 show that the accurate decryption is possible only if the correct key is used to decrypt image, else the image remains non recognizable. For a visual demonstration of avalanche test, the wrong key has a difference of just bit from the original key, the strength of the algorithm can be perceived from this result.

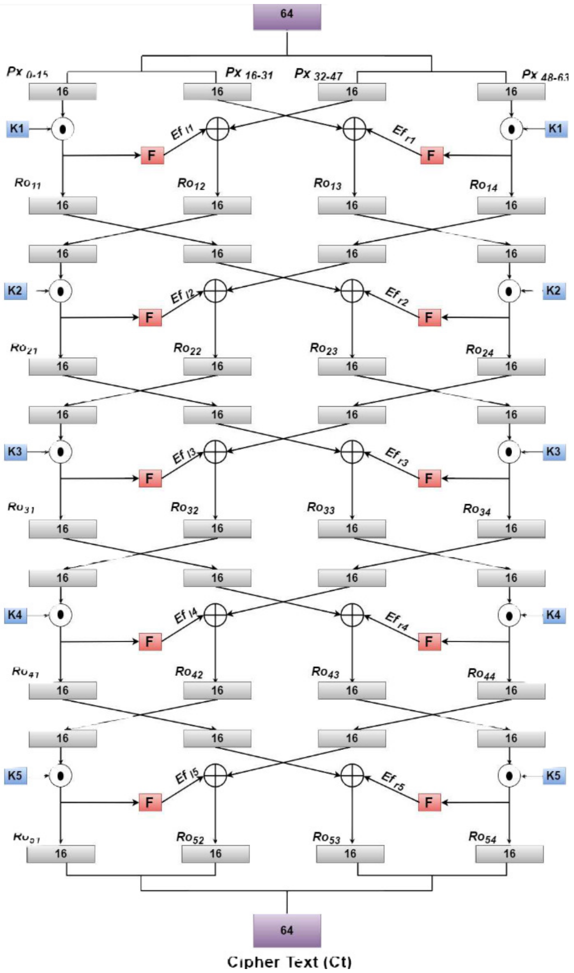

Fig. 2: Encryption Process

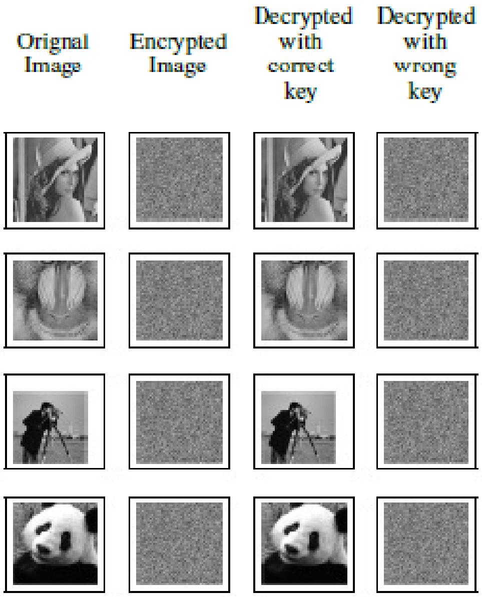

Fig. 3: Decryption Process

IV. CONCLUSIONS

In the near future Internet of Things will be an essential element of our daily lives. Numerous energy constrained devices and sensors will continuously be communicating with each other the security of which must not be compromised. For this purpose a lightweight security algorithm is proposed in this paper named as SIT. The implementation show promising results making the algorithm a suitable candidate to be adopted in IoT applications. In the near future we are interested in the detail performance evaluation and cryptanalysis of this algorithm on different hardware and software platforms for possible attacks.

REFERENCES

1. *H. Suo, J. Wan, C. Zou, and J. Liu, "Security in the internet of things: a review," in Computer Science and Electronics Engineering (ICCSEE), 2012 International Conference on, vol. 3. IEEE, 2012, pp. 648–651.*
2. *G. Ho, D. Leung, P. Mishra, A. Hosseini, D. Song, and D. Wagner, "Smart locks: Lessons for securing commodity internet of things devices," in Proceedings of the 11th ACM on Asia Conference on Computer and Communications Security. ACM, 2016, pp. 461–472.*
3. *D. Airehrour, J. Gutierrez, and S. K. Ray, "Secure routing for internet of things: A survey," Journal of Network and Computer Applications, vol. 66, pp. 198–213, 2016.*
4. *P. Zhao, T. Peffer, R. Narayanamurthy, G. Fierro, P. Raftery, S. Kaam, and J. Kim, "Getting into the zone: how the internet of things can improve energy efficiency and demand response in a commercial building," 2016.*
5. *[10] Y. Li, M. Hou, H. Liu, and Y. Liu, "Towards a theoretical framework of strategic decision, supporting capability and information sharing under the context of internet of things," Information Technology and Management, vol. 13, no. 4, pp. 205–216, 2012.*
6. *[11] Z. Pang, Q. Chen, J. Tian, L. Zheng, and E. Dubrova, "Ecosystemanalysis in the design of open platform-based in-home healthcare terminals towards the internet-of-things," in Advanced Communication Technology (ICACT), 2013 15th International Conference on. IEEE, 2013, pp. 529–534.*
7. *M. C. Domingo, "An overview of the internet of things for people with disabilities," Journal of Network and Computer Applications, vol. 35, no. 2, pp. 584–596, 2012.*
8. *W. Qiuping, Z. Shunbing, and D. Chunquan, "Study on key technologies of internet of things perceiving mine," Procedia Engineering, vol. 26, pp. 2326–2333, 2011.*
9. *H. Zhou, B. Liu, and D. Wang, "Design and research of urban intelligent transportation system based on the internet of things," in Internet of Things. Springer, 2012, pp. 572–580.*
10. *B. Karakostas, "A dns architecture for the internet of things: A case study in transport logistics," Procedia Computer Science, vol. 19, pp. 594–601, 2013.*
11. *T. Karygiannis, B. Eydt, G. Barber, L. Bunn, and T. Phillips, "Guide- lines for securing radio frequency identification (rfid) systems," NIST Special publication, vol. 80, pp. 1–154, 2007.*
12. *J. Wang, G. Yang, Y. Sun, and S. Chen, "Sybil attack detection based on rssi for wireless sensor network," in 2007 International Conference on Wireless Communications, Networking and Mobile Computing. IEEE, 2007, pp. 2684–2687.*
13. *[27] S. Lv, X. Wang, X. Zhao, and X. Zhou, "Detecting the sybil attack co- operatively in wireless sensor networks," in Computational Intelligence and Security, 2008. CIS'08. International Conference on, vol. 1. IEEE, 2008, pp. 442–446.*
14. *Y. Chen, J. Yang, W. Trappe, and R. P. Martin, "Detecting and localizing identity-based attacks in wireless and sensor networks," IEEE Transactions on Vehicular Technology, vol. 59, no. 5, pp. 2418–2434, 2010.*
15. *S. Chen, G. Yang, and S. Chen, "A security routing mechanism against sybil attack for wireless sensor networks," in Communications and Mobile Computing (CMC), 2010 International Conference on, vol. 1. IEEE, 2010, pp. 142–146.*
16. *S. A. Kumar, T. Vealey, and H. Srivastava, "Security in internet of things: Challenges, solutions and future directions," in 2016 49th Hawaii International Conference on System Sciences (HICSS). IEEE, 2016, pp. 5772–5781.*
17. *M. Ebrahim and C. W. Chong, "Secure force: A low-complexity cryptographic algorithm for wireless sensor network (wsn)," in Control System, Computing and Engineering (ICCSCE), 2013 IEEE Interna- tional Conference on. IEEE, 2013, pp. 557–562.*
18. *D. Coppersmith, "The data encryption standard (des) and its strength against attacks," IBM journal of research and development, vol. 38, no. 3, pp. 243–250, 1994.*