iJRASET
International Journal For Research in Applied Science and Engineering Technology

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

Volume: 7 **Issue:** III **Month of publication:** March 2019

DOI: http://doi.org/10.22214/ijraset.2019.3454

www.ijraset.com

Call: 08813907089 | E-mail ID: ijraset@gmail.com

International Journal for Research in Applied Science & Engineering Technology (IJRASET)
ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor: 6.887
Volume 7 Issue III, Mar 2019- Available at www.ijraset.com

Design Development and Performance Evaluation of Low Complexity Cryptographic Algorithm for Security in IOT

Neha Parashar[1], Rajveer Singh[2]
[1, 2]*Rajasthan College of Engineering for Women*

Abstract: ***Internet of Things (IoT) is promising future technology is expected to connect billions of devices. Expected to produce more communication Data peaks and data security can be a threat. This The size of the device in this architecture is basically small, Low power consumption. Traditional encryption algorithm in general Due to its complexity and requirements, it is computationally expensive Many rounds of encryption are basically a waste of constraints Gadget energy. Less complicated algorithm, however, possible Compromise required integrity. It is a 64-bit block password that requires a 64-bit key to encrypt data. The architecture of the algorithm is a mixture of feistel and a uniform replacement - to replace the network Simulation. The results show that the algorithm provides just a substantial security five rounds of encryption.***
Index Terms**: *IoT, Security; Encryption; Wireless Sensor Network, WSN,***

I. INTRODUCTION

Internet of Things (IoT) is turning into one Emerging research and practice areas of discussion in recent years of implementation. Internet of Things is a model including the general ability to perceive entities Communicate with other devices using the Internet [1]. Due to Broadband Internet is now generally available at its cost the connection is also reduced, with more gadgets and sensors connecting to it [2]. Such conditions are being provided Suitable for the development of the Internet of things. There are many because we want to approach the complexity of the Internet of Things Every object from all over the world [3]. Exquisite
Chip and sensor embedded in the physical things Around us, everyone passes a valuable number of processes Sharing so much data starts with the device they must themselves communicate securely with the Internet of Things platform. This platform consolidates data from many devices and applies analytics to share the most valuable data application. Internet of Things is using the traditional Internet, sensors Network and mobile network to another level will connect to the internet. Must pay attention to the problem what has always been considered is the assurance of the related issues Confidentiality, data integrity and authenticity based on security and privacy [4]. Modern Progress in Communication and Communication Computer networks add to the network's challenge Security, scalability and reliability [16], [17]. Like all the others Communication networks are also wireless sensor networks Prone to safety problems. The WSN may contain multiple sensors Nodes and each node consists of a processor, a limited battery Power, and memory and communication skills. Make sure Security in wireless sensor networks can provide the best algorithm Resource constraints for WSN nodes are secure need. Traditional cryptographic algorithms are not suitable Because of the distinctive features of WSN [3]. Key The problem with designing a wireless sensor network cryptographic algorithm is Deal with the trade-offs of security, memory, power, and security performance. In order to meet the high safety requirements, Much effort has been made in assessing passwords Algorithm and proposed energy efficiency password [4], [5] . To use IoT technology, it is necessary to establish such a system Confirm the user's security and privacy It does not pose any serious threat to its data integrity, Confidentiality and authority. In essence, the Internet of Things is vulnerable various security threats, if necessary, security measures did not take information leaks or threats may damage the economy [17], [18]. Such a threat may be is considered as one of the major obstacles in the Internet of Things [19], [20].The Internet of Things is very open to attack [21], [22] the possibility of a physical attack on its components is high Because they are out of surveillance for a long time. Second, thanks For wireless communication media, eavesdropping is very simple. Finally, IoT members assume a low level of abilities in terms of the energy they are in also in terms of computing power carried out the traditional calculation of expensive security algorithms Obstacles to energy performance can result restricted equipment. It is estimated there will be a considerable amount of data Generated when IoT is used for monitoring purposes maintaining the unity of the data is crucial [23]. Exactly, the data integrity and certification are issues of concern. At a high level, the Internet of Things consists of

three levels components are hardware, middleware and demos [1]. Hardware consists of sensors and actuators, middle ware Provide storage and calculation tools and presentations Different interpretation tools are provided Platform. It is not feasible to process the collected data Billions of sensors, context-aware middleware solutions It is recommended to help the sensor determine the most important data Processing [24]. IoT architecture is not in essence Provide enough margins to complete the necessary actions Participate in the process of certification and data integrity. These IoT devices such as RFID are questionable including the basic requirements of the certification process Constant communication with servers and switches messages and nodes. In the security system, the confidentiality of the data is maintained and make sure the mail is in progress Exchange data to retain its originality unchanged the invisible IoT is made up of many small ones Devices such as RFID are still unmanned to extend Second, adversaries have easier access to stored data In memory [25]. Provides immunity to Sybil Attacks in RFID Tags, Received Signal Strength Indication (RSSI)A method-based approach was used in [26], [27], [28] and [29].Many solutions have been proposed for wireless sensors The network that views sensors as part of the Internet Connect via nodes [30]. However, the sensor nodes in the Internet of Things itself is considered a node of the Internet The certification process is even more important. Integrity The data also becomes crucial and needs special attention maintain its reliability.

II. CRYPTOGRAPHIC ALGORITHMS

DWT Demand for lightweight cryptography has been growingExtensive discussions [32], [33], also have short comings Emphasized IoT on constrained devices. There There are actually some lightweight cryptographic algorithms It is not always a safe and effective trade-off. Among Block ciphers, stream ciphers and hash functions, blocks the password has shown quite good performance. Proposed a new grouping password m crypton[34]. Password with 64-bit, 96-bit and 128-bit options Bit key size. Follow the architecture of this algorithm by crypton [35] however the function of each component is Simplify to enhance its performance on restricted hardware. The successor to Hummingbird 1 [37] is [36] Proposed as Hummingbird-2 (HB-2). With a 128-bit key and A 64-bit initialization vector Hummingbird-2 was tested to stay not affected by all previously known attacks. However the cryptanalysis of HB-2 [38] underscores the weakness the algorithm and the initial key can be recovered. [39]Studied different traditional encryption algorithms, including RC4, IDEA and RC5, and measure their energy consumption. The computational costs of RC4 [40] and IDEA [41] have been calculated, and RC5 password on different platforms. However, various Existing algorithms were omitted during the study. TEA [42], Skipjack [43] and RC5 algorithms Implemented on Mica 2 hardware platform [44]. Measuring Password energy consumption and memory utilizationMica2 is configured in a single dust. Including several group password AES [45], XXTEA [46], Skipjack and RC5Implementation [47], energy consumption and implementation time Measured. The results show that in the AES algorithm, the size of the key on the encryption, decryption and key settings have a great impact on the stage, the longer the key length, Expand the implementation process. RC5 offers a variety of parameters Key size, number of cycles, and word size can be was changed. The author has made many combinations Find it takes longer if this word is executed Increase in size. Since the key setup phase is not involved XXTEA and Skipjack, they reduce energy but their safety less powerful than AES and RC5. [48]

III. METHODOLOGY

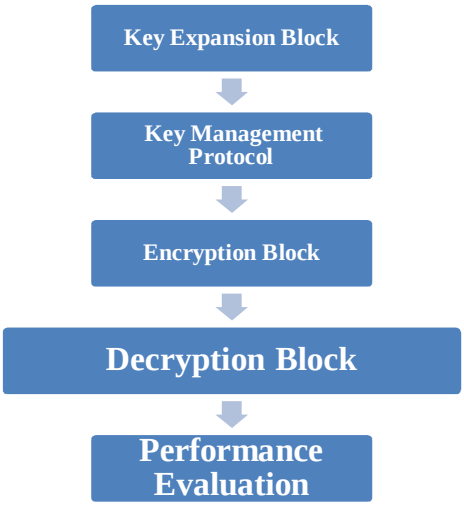


Fig2.1Steps Involved in Cryptographic Algorithm

ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor: 6.887
Volume 7 Issue III, Mar 2019- Available at www.ijraset.com

A. Key Expansion Block

It is the main process used to generate different keys for encryption and Decrypt. In order to perform different operations cause confusion and proliferation. This is to reduce weak key possibilities as well as adding the key strength. Wheel key (Kr) is derived from the input Key scheduling through the key. this process Consists of two parts: key expansion and round key select. Key expansion performs logical operations (XOR, XNOR), left (LS), matrix multiplication Use fixed matrix (FM), use P tables and arrange Use the T table for transposition.

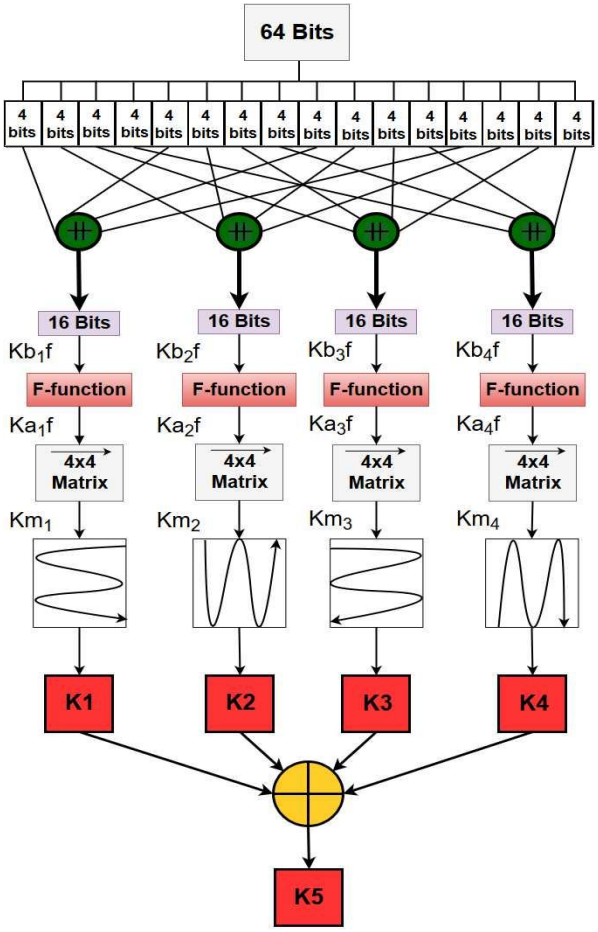


Fig2.2 Steps Involved in Cryptographic Algorithm

The architecture of the key expansion block is shown in Fig.2.2 . The block uses an f -function which is influenced by tweaked Khazad block cipher [64]. Khazad is not a feistel cipher and it follows wide trial strategy. The wide trial strategy is composed of several linear and non-linear transformations that ensures the dependency of output bits on input bits in a complex manner [65].

B. Key Management Protocol

The key can be securely sent to the encoder with the aid of LEAP [18].It is a simple and energy efficient protocol designed for large scale WSN, which allows secure key establishment through the use of four types of keys. They are known as the individual key, group key, cluster key, and pair wise shared key.

C. Encryption Block

The encryption process is started once The key generated by the key expansion block is safe Encoder receives via secure communication Channels are created by the LEAP protocol. Encryption Process, simple operation, including AND, OR, XOR,XNOR, LS (Left), Substitute (S) and Swap The operation is to create confusion and proliferation.

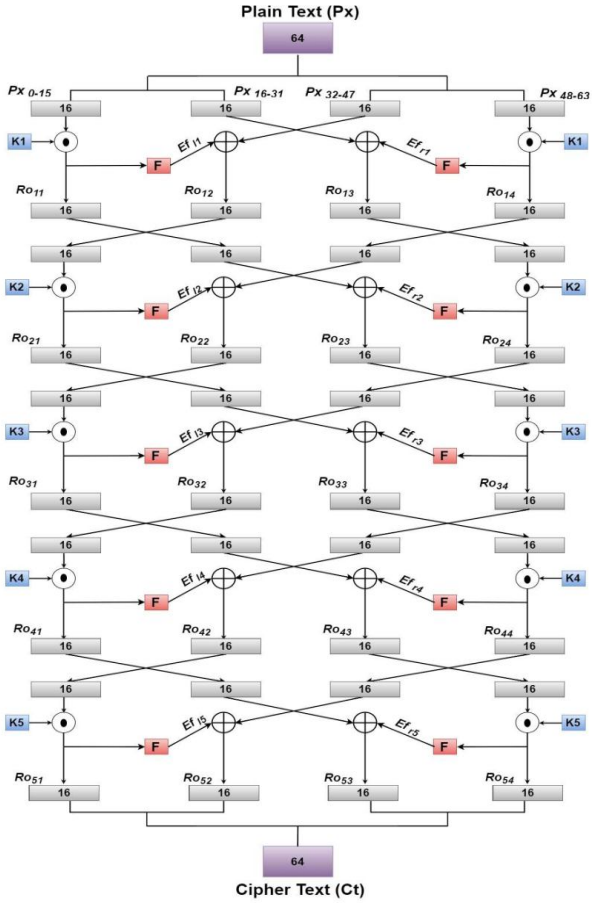


Fig2.2 Steps Involved in Cryptographic Algorithm

D. Decryption Block

Decryption is the process of taking encoded or encrypted text or other data and converting it back into text that you or the computer can read and understand. This term could be used to describe a method of un-encrypting the data manually or with un-encrypting the data using the proper codes or keys.

IV. PERFORMANCE ANALYSIS

In order to test the security strength of the proposed algorithm, The algorithm is based on the following criteria.

Key Sensitivity, Effect of Password on Entropy, Histogram

And the relevance of the image. We further tested the algorithm Used to calculate resource utilization and calculation complex. To this end, we observe the memory utilization and this algorithm is used for the total calculation time that k represents, encrypt, and decrypt.

1) *Key Sensitivity:* The encryption algorithm must be sensitive to the key. This means that if there is a slight difference between the key and the key, the algorithm cannot recycle the original data the original key. The avalanche test is used to evaluate the amount Change in cipher text by changing a key or plain text. According to strict avalanche standards SAC [66] if 50% of the bits change as a result of a change, the test is considered perfect. Visual observation of this the effect, we use a differentiated key to decrypt the image only one key from the right key
2) *Execution Time:* one of the basic parameters the evaluation of this algorithm is the amount of time it takes to encode and decode specific data. The proposed algorithm is designed for the IoT environment must consume the least Time and provide considerable security
3) *Memory Utilization:* memory utilization is the main focus on resource constrained IoT devices. One encryption the algorithm consists of several calculation wheels may consume significant memory, making it unsuitable for use in the Internet of Things.

Therefore, the proposed algorithm is evaluated in terms of memory usage. The amount of memory is small interaction will facilitate its deployment in the Internet of Things.

4) *Image Histogram:* A method to observe visual effect of the cipher is to encrypt an image with the proposed algorithm and observe the randomness it produces in the image. To evaluate the generated randomness, histogram of the image is calculated. A uniform histogram after encryption depicts appreciable security.

5) *Image Entropy:* The encryption algorithm adds extra information to the data so as to make it difficult for the intruder to differentiate between the original information and the one added by the algorithm. We measure the amount of information in terms of entropy, therefore it can be said that higher the entropy better is the performance of security algorithm.

V. RESULTS

The simulation of the algorithm is done to perform the standard tests including Avalanche and image entropy and histogram on Intel Core i5-4200U@2.30 GHz processor using MATLAB-2017a.

The Internet of Things (IoT) is a promising future technology that promises to connect billions of devices. It is expected that more communication data peaks and data security may pose a threat. The device size in this architecture is basically small and the power consumption is very low. The traditional general encryption algorithm is expensive because of its complexity and requirement. Many rounds of encryption are basically a waste of constraint Gadget energy. Less sophisticated algorithms, however, may compromise the required integrity. In this article, we propose a lightweight encryption algorithm called Secure Internet of Things (SIT). It is a 64-bit block cipher that requires a 64-bit key to encrypt the data. The work done in this research can be classified into following points-

A. Implementation of Light Weight Cryptography system for IOT compatible system.
B. Implementation of Image encryption and decryption system.
C. Implementation of algorithm for multiple platforms (JPEG-2000, JPEG, BMP,PNG,GIF).
D. Performance Analysis of simulated technique on basis of number of changing pixel rate (NPCR) and the unified averaged changed intensity (UACI).
E. Analysis of wrong key encryption.
F. Analysis of execution time and memory allocation of the proposed system.
G. Development of graphical user interface (GUI) for the overall process

Correlation Analysis

Image	Format	Correlation Original	Correlation Encrypted
Relax	JPEG	0.9624	0.0019
Relax	JPEG-2000	0.9564	0.0016
Relax	GIF	0.9464	0.0027
Relax	PNG	0.9624	0.0002
Relax	BMP	0.9624	0.0002

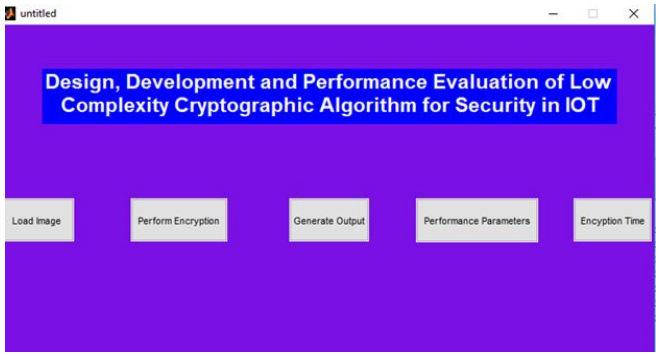
Entropy Analysis

Type of Image	Entropy	Entropy Decrypted
JPEG	7.9970	7.4747
JPEG-2000	7.9971	7.4927
PNG	7.9976	7.4771
BMP	7.9976	7.4771
GIF	7.9974	7.2564

Performance Analysis of simulated technique on basis of number of changing pixel rate (NPCR) and the unified averaged changed intensity (UACI).

Type of Image	NPCR	UACI
JPEG	99.6414	26.3742
JPEG-2000	99.5865	26.3577
PNG	99.6277	26.3999
BMP	99.6277	26.3998
GIF	99.5499	29.7076

Development of GUI-



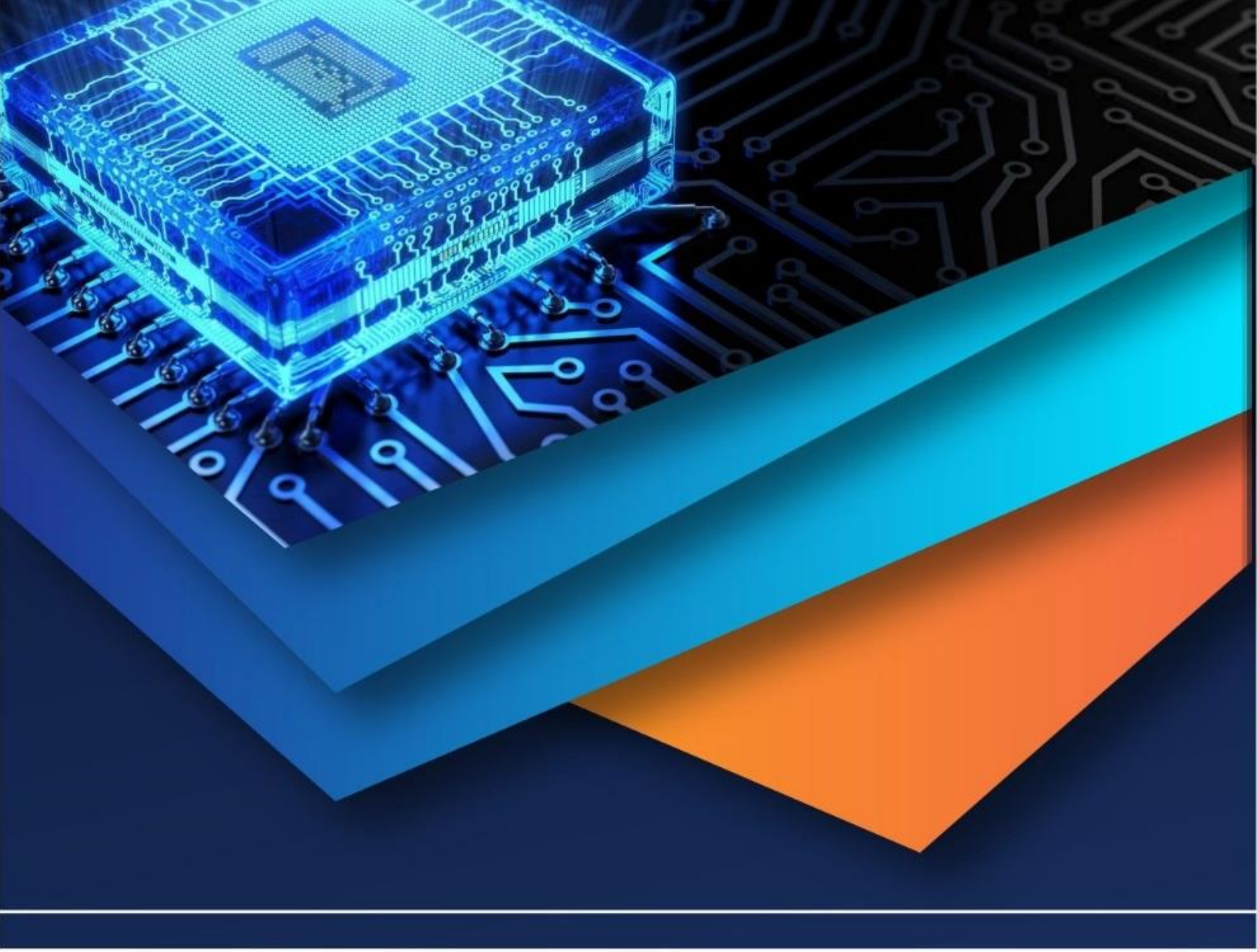
IV CONCLUSION

The Internet of Things will become an indispensable part of our daily lives in the near future. The energy is limited to the devices and the sensors will constantly communicate with each other and they should not compromise. The result makes the algorithm a suitable candidate in IoT applications. We are interested in the near future. Detailed performance evaluation and cryptanalysis algorithms run on different hardware and software platforms to prevent possible attacks. Power-constrained networks such as wireless sensor networks (WSNs) and IOTs require an algorithm that can provide reliable security at an affordable computational cost. In this article, we implemented the SF architecture on the MATLAB® platform and performed various standard tests on image and text data. Test results show that it performs well in terms of computational time and randomness.

REFERENCES

[1] Usman, Muhammad, et al. "Sit: A lightweight encryption algorithm for secure internet of things." arXiv preprint arXiv:1704.08688 (2017).
[2] R. Want and S. Dustdar, “Activating the internet of things [guest editors’introduction],” Computer, vol. 48, no. 9, pp. 16–20, 2015.
[3] J. Romero-Mariona, R. Hallman, M. Kline, J. San Miguel, M. Major, and L. Kerr, “Security in the industrial internet of things,” 2016.
[4] 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.
[5] G. Ho, D. Leung, P. Mishra, A. Hosseini, D. Song, and D. Wagner, “Smart locks: Lessons for securing commodity internet of thingsdevices,” in Proceedings of the 11th ACM on Asia Conference onComputer and Communications Security. ACM, 2016, pp. 461–472.
[6] 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.
[7] D. Miorandi, S. Sicari, F. De Pellegrini, and I. Chlamtac, “Internet of things: Vision, applications and research challenges,” Ad Hoc Networks,vol. 10, no. 7, pp. 1497–1516, 2012.
[8] L. Da Xu, “Enterprise systems: state-of-the-art and future trends,” IEEE Transactions on Industrial Informatics, vol. 7, no. 4, pp. 630–640, 2011.
[9] P. Zhao, T. Peffer, R. Narayanamurthy, G. Fierro, P. Raftery, S. Kaam, and J. Kim, “Getting into the zone: how the internet of things canimprove energy efficiency and demand response in a commercialbuilding,” 2016.
[10] Y. Li, M. Hou, H. Liu, and Y. Liu, “Towards a theoretical frameworkof strategic decision, supporting capability and information sharingunder the context of internet of things,” Information Technology andManagement, vol. 13, no. 4, pp. 205–216, 2012.
[11] Z. Pang, Q. Chen, J. Tian, L. Zheng, and E. Dubrova, “Ecosystemanalysis in the design of open platform-based in-home healthcareterminals towards the internet-of-things,” in Advanced CommunicationTechnology (ICACT), 2013 15th International Conference on. IEEE,2013, pp. 529–534.
[12] S. Misra, M. Maheswaran, and S. Hashmi, “Security challenges andapproaches in internet of things,” 2016.
[13] M. C. Domingo, “An overview of the internet of things for people withdisabilities,” Journal of Network and Computer Applications, vol. 35,no. 2, pp. 584–596, 2012

[14] W. Qiuping, Z. Shunbing, and D. Chunquan, "Study on key technologiesof internet of things perceiving mine," Procedia Engineering, vol. 26,pp. 2326–2333, 2011.
[15] H. Zhou, B. Liu, and D. Wang, "Design and research of urban intelligenttransportation system based on the internet of things," in Internet ofThings. Springer, 2012, pp. 572–580.
[16] B. Karakostas, "A dns architecture for the internet of things: A casestudy in transport logistics," Procedia Computer Science, vol. 19, pp.594–601, 2013.
[17] H. J. Ban, J. Choi, and N. Kang, "Fine-grained support of securityservices for resource constrained internet of things," InternationalJournal of Distributed Sensor Networks, vol. 2016, 2016.
[18] S. Khan, M. Ebrahim, and K. A. Khan, "Performance evaluation ofsecure force symmetric key algorithm," 2015.
[19] P. L. L. P. Pan Wang, Professor SohailChaudhary, S. Li, T. Tryfonas,and H. Li, "The internet of things: a security point of view," InternetResearch, vol. 26, no. 2, pp. 337–359, 2016.
[20] M. Ebrahim, S. Khan, and U. Khalid, "Security risk analysis in peer2 peer system; an approach towards surmounting security challenges,"arXiv preprint arXiv:1404.5123, 2014.
[21] M. A. SimplicioJr, M. V. Silva, R. C. Alves, and T. K. Shibata,"Lightweight and escrow-less authenticated key agreement for theinternet of things," Computer Communications, 2016.



10.22214/IJRASET

45.98

IMPACT FACTOR: 7.129

IMPACT FACTOR: 7.429

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY