IJIREEICE

ISSN (Online) 2321-2004
ISSN (Print) 2321-5526

International Journal of Innovative Research in
Electrical, Electronics, Instrumentation and Control Engineering

Vol. 7, Issue 7, July 2019

Designing and Development of Efficient Data and Image Security System for Secure in IOT

Payal Mundra[1], Vinod Todwal[2]

Student, RCEW (RTU), IT Department, Jaipur, India[1]

Associate Professor, RCEW (RTU), IT Department, Jaipur, India[2]

Abstract: Internet of Things (IoT) is promising future technology is relied upon to interface billions of gadgets. Expected to deliver more correspondence Data pinnacles and information security can be a risk. This size of the gadget in this engineering is essentially little, low power utilization. Many rounds of encryption are essentially a misuse of requirements Gadget vitality. Less convoluted calculation, be that as it may, conceivable compromise required uprightness. It is a 64-bit square secret key that requires a 64-bit key to encrypt information. The engineering of the calculation is a blend of feistel and a uniform substitution - to supplant the system Simulation. The outcomes demonstrate that the calculation gives only a considerable security five rounds of encryption. The proposed work demonstrates the implementation of symmetric key lightweight algorithm for secured data transmission of images and text using image encryption system as well as reversible data hiding system. Proposed research have demonstrated faster computation, less complexity and higher PSNR as compared to existing algorithms. In the proposed work we have implemented symmetric key cryptography for various format of images, as well as real time image acquisition system has been designed in the form of graphical user interface. Reversible data hiding system has also been designed for secure data transmission system.

Keywords: PSNR, IOT, Encryption, MSE, Cipher, Symmetric Key, Cloud, Image Processing

I. INTRODUCTION

Internet of things is abbreviated as IOT. Today IOT is a key and overriding subject of the technical and social significance. Products of consumers, items and vehicles, industry based and basic components, sensors, and other day to day objects are merged with connectivity of internet and the strong data capabilities which assure to change the type in which we work and live. The influence of the devices based on the Internet and economy are attractive, with some 100 billion devices connected to IOT and a worldwide economic impact of mostly $11 trillion by 2025. The concept of mixing computers, the sensors, and networks to specifically command the devices that is existing for numerous years. The technology for this process includes similar connectivity, huge and wide adoption of IP-based networking, calculating the economics, minimizing the size of the devices, highly advanced data analytics and the cloud computing. The architecture has been designed so that it supports packet switching with better mobility and a better service of quality. Different technical communication models are used in IOT implementation, each follow its characteristics. The four common communications models which exist include Device-to-Device, Device-to-Cloud, Device-to-Gateway, and Back-End Data-Sharing models. The 4G network uses the concept of best connected which mean the terminal will always select the best possible available access. 4G uses the IPV6 address scheme; this will allow each mobile to use its own IP address. [Muhammad Usman, et-al, 2017] has proposed a light weight algorithm for the encryption; encryption is done for the security purpose. The name of the algorithm proposed in the presented paper is secure IOT that is also known as (SIT). Encryption algorithms are very expensive because of their complex nature and because they require several rounds for the encryption process after that the security is ensured. The proposed algorithm SIT is a 64 bit block cipher and it only requires 64 bit key for the process of encryption of data and hence is known as the light weight encryption. In this work we have presented an algorithm which is light weight cryptography algorithm to secure IOT. The algorithm proposed is a 64-bit block cipher which needs a 64-bit key to encrypt data. This algorithm only requires five rounds to ensure the security of the data. light weight cryptographic algorithm which shows the step by step encryption of the 64 bit plain text to convert it into a 64 bit cipher text. Whole of the procedure requires the five encryption rounds with the logical operations.

II. METHODLOGIES

The methodology used for the purpose to develop the algorithm for light weight encryption consists of some of the steps which need to be followed.

IJIREEICE

ISSN (Online) 2321-2004
ISSN (Print) 2321-5526

International Journal of Innovative Research in
Electrical, Electronics, Instrumentation and Control Engineering

Vol. 7, Issue 7, July 2019

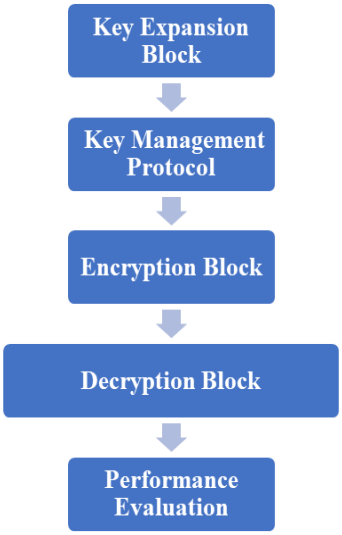


Figure 1.1 Flow chart for developing the algorithm

Any non-Critical Information called cover data (C) acts as a carrier of Critical Information (CI). A Secrete Key (K) is used by the Steganographic embedding function (f Em) to hide CI and gives Stego data (S) as an output (device at Transmitting end DT) as shown in figure-

$(DT) \rightarrow fEm(C,CI,)$

where S is Stego data, C is cover data, CI is Critical Information, and K is Secrete Key.

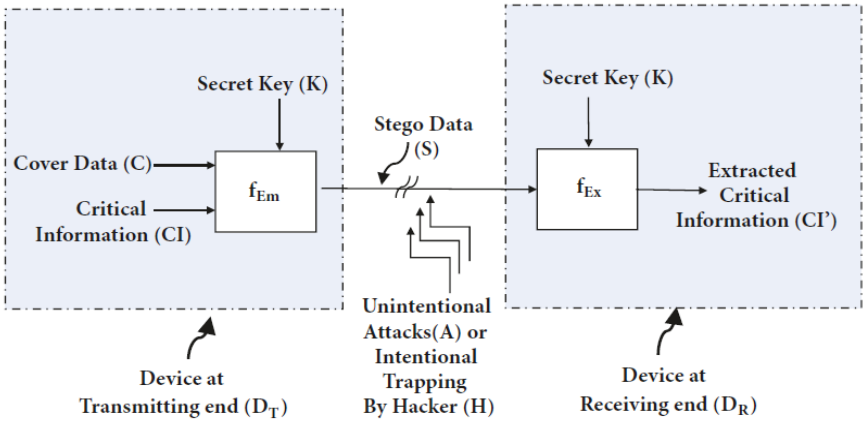


Fig 1.2 Steps Involved in Reversible Hiding Algorithm [25]

Proposed reversible data hiding system to implement data hiding system consists of both cryptographic and Steganographic approach and therefore is called Crypto- Stego System.

III. RESULTS

In this chapter we discuss about the experimental scenarios, results obtained and the performance analysis of the light weight cryptographic algorithm for IOT devices which depends on the size and geographical parameters. Energy efficiency is more important for the efficient planning and the development of algorithm which is light weight. The implementation of the code and algorithm has a motive to get the histogram analysis, graphical results and the entropy of a given data on MATLAB.

Since we have discussed in the earlier chapters that internet of things is emerging as a valuable technology for the society and also in the field of communication. This increases the dependency on the internet and hence the issue to secure the same has become more prominent in past few decades. Now the major issues which developers deal with are the size, economy, power consumption and security. If we deal with the traditional cryptography algorithms, we can see that they basically rely upon the number of encryption rounds which means as the number of encryption rounds increases the security improves but this has a demerit too, as the power consumption is also increased with the number

IJIREEICE

ISSN (Online) 2321-2004
ISSN (Print) 2321-5526

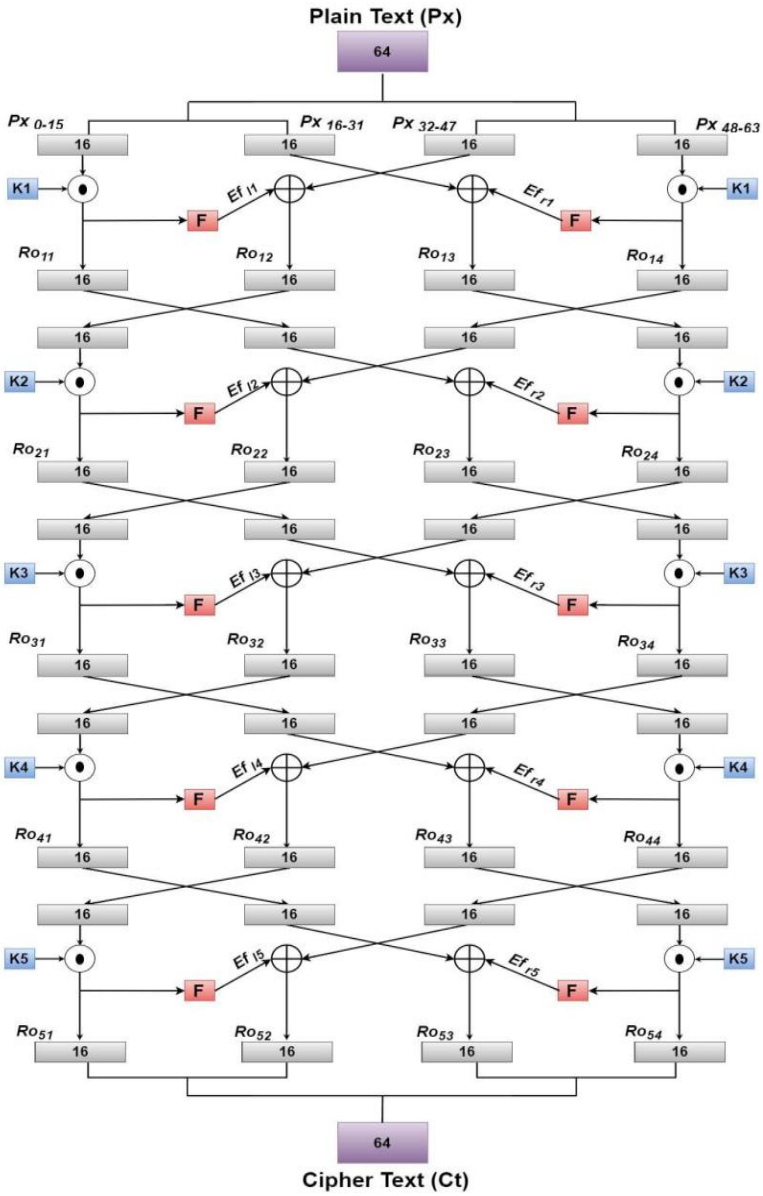
International Journal of Innovative Research in
Electrical, Electronics, Instrumentation and Control Engineering

Vol. 7, Issue 7, July 2019

of encryption rounds. The traditional kind of algorithms also uses large number of gates which also increase the size. And rest of the algorithms which are little sophisticated compromises with security. In this work we have presented an algorithm which is light weight cryptography algorithm to secure IOT. The algorithm proposed is a 64-bit block cipher which needs a 64-bit key to encrypt data. The basic idea of the research done can be classified into the points described below:

1. Implementation of Light Weight Cryptography for the system which is IOT compatible.
2. Implementation of Image encryption and decryption on the system.
3. Implementation of the algorithm on multiple platforms (JPEG-2000, JPEG, BMP, PNG, GIF).
4. Performance Analysis of simulated technique which is based on the number of changing pixel rate (NPCR) and the unified averaged changed intensity (UACI).
5. Analysis of wrong key encryption.
6. Analysis of the execution time and memory allocation of the proposed system.
7. Development of graphical user interface (GUI) for the same process

Implementation of Light Weight Cryptography system for IOT compatible system



1.3 Encryption process in light weight cryptography

IJIREEICE

ISSN (Online) 2321-2004
ISSN (Print) 2321-5526

International Journal of Innovative Research in
Electrical, Electronics, Instrumentation and Control Engineering

Vol. 7, Issue 7, July 2019

Internet of Things established itself as a promising technology for the society in future and is connecting billions of devices. The increase in number of communication devices and procedures are expected to create a huge amount of data and the also a threat to the security of data. The devices which are used in the architecture of the same are necessarily tiny in size and less in power. Conventional encryption algorithms are usually expensive to compute over and because of their complexity it requires number of rounds for encryption, which actually waste the constrained energy of the gadgets. Less complex algorithm, can compromise the essentially needed integrity. In the following work the proposed algorithm is lightweight encryption algorithm named as Secure IOT (SIT). This basically is a 64-bit block cipher also it needs a 64-bit key for the encryption of the data. The architecture of the proposed security algorithm is merger of feistel and a substitution-permutation network which is uniform. The result after the simulation shows that the algorithm is able to provide security in only five rounds of encryption.

The following diagram shows the steps which are involved in the encryption of the light weight cryptographic algorithm which shows the step by step encryption of the 64 bit plain text to convert it into a 64 bit cipher text. Whole of the procedure requires the five encryption rounds with the logical operations. The whole procedure can be analyzed below by looking at the architecture of the whole encryption process.

Correlation Analysis

Image	Format	Correlation Original	Correlation Encrypted
Relax	JPEG	1.0000 / 0.9564	1.0000 / -0.0016
Relax	JPEG-2000	1.0000 / 0.9624	1.0000 / 0.0019
Relax	GIF	1.0000 / 0.9464	1.0000 / -0.0027
Relax	PNG	1.0000 / 0.9624	1.0000 / -0.0002
Relax	BMP	1.0000 / 0.9624	1.0000 / -0.0002

Entropy Analysis

Image	Type	Execution Time	Memory Usage (Byte)
Relax.jpg	JPEG	26.32 Sec	894791680
Relax.jp2	JPEG2000	20.45 Sec	897445888
Relax.png	PNG	17.26 Sec	892973056
Relax.bmp	BMP	18.365196 Sec	898744320
Relax.gif	GIF	19.089435 Sec	894238720

Execution Time and Memory Uses

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

PSNR and MSE value analysis

Type of Image	PSNR	MSE
JPEG	60.90	0.020
JPEG-2000	65.11	0.015
PNG	62.11	0.018
BMP	64.12	0.021
GIF	60.22	0.021

IJIREEICE

ISSN (Online) 2321-2004
ISSN (Print) 2321-5526

International Journal of Innovative Research in
Electrical, Electronics, Instrumentation and Control Engineering

Vol. 7, Issue 7, July 2019

IV. CONCLUSION

The Internet of Things is very famous now, and so there is a need to accept and resolve its challenges and try to maximize its benefits simultaneously reducing the risks. Internet Society thinks about IOT as it represents a growing platform for people and institutions which can interact with each other and indulge on to the Internet and network connectivity into their personal, social, and economic lives. Solutions for maximizing the best usage of IOT with minimizing the risks can't be met by getting involved in a polarized debate that puts the promises of IOT against security threats. But it would take dedicated engagement and collaboration among the researchers and the developers to make this way towards security works.

REFERENCES

[1]. Subhash Nemani, Jayachandra Prasad Talari, Sumalatha Vangala "Reversible Data Hiding Using Secure Force Algorithm" International Journal of Pune and Applied Mathematics Volume,2018
[2]. Maria Almulhim, Noor Zaman, "Proposing secure and the lightweight authentication scheme for IOT based E health applications" International conference on advance communication technology; 2018.
[3]. Muhammad Naveed Aman, Kee Chaing Chua, "A light weight mutual authentication protocol for IOT system,2017.
[4]. Mehdi Baahrami, Dong Li, Mukesh Singhal, "Efficient parallel implementation of light weight data privacy method for cloud users; seventh international workshop on data intensive computing in clouds, 2016.
[5]. Gaurav Bansod, Abhijit Patil, "An Ultra light weight design for security in pervasive computing" IEEE second international conference on big data security cloud, 2016.
[6]. Zahid Mahmood, Huansheng Ning, "Light weight two level session key management for end user authentication in internet of things" IEEE international conference on IOT, 2016.
[7]. Ayaz Hassan moon, Ummer Iqbal, "Light weight authentication framework for WSN" International conference on Electrical, Electronics and Optimization techniques, 2016.
[8]. Muhammad Usman, Irfan Ahmed, Shujaat khan, "SIT: A light weight encryption algorithm for secure internet of things," international Journal of advanced computer science and applications, vol. 8, no.1, 2017.
[9]. D Jamuna Rani, "Light weight cryptographic algorithm for medical internet of things", Online international conference on Green Engineering and Technology, 2016.
[10]. Sudhir Satpathy, Sanu Mathew, "Ultra low energy security circuits for IOT applications", IEEE 34th international conference on computer design, 2016.