Comparison of Image Selectivity in Compression Techniques for Light Weight Cryptography in IOT

Neha Parashar
Rajasthan College of Engineering for Women

Rajveer Singh
Rajasthan College of Engineering for Women

Abstract: As IOT is coming out as an emerging technology from the last few decades and the demand for the devices based on IOT are also increasing. So, the dependency on this technology is increasing side by side. This requires the proper encryption method which is cost effective, reliable, size effective and requires a small key size. Many of the encryption methods are proposed till now for the same but still we always can have improvement, in this paper we present an effective algorithm which provides security for the IOT based devices as well as meet the specifications which are mentioned above. Simulation and results compare the image compression techniques to provide security with cost and size effective design.

Keywords: **IOT security, WSN, Encryption, Decryption**

I INTRODUCTION

Internet of things is abbreviated as IOT. Internet of Things is a very important topic of technical and social significance. Consumer products, goods, cars and vehicles, industrial and basic components, sensors, and other day to day objects are merged with connectivity of internet and powerful data capabilities which assure to transform the way we work and live. The impact of IOT on the Internet and economy are attractive, with some 100 billion devices connected to IOT and a global economic impact of almost $11 trillion by 2025. The concept of merging computers, sensors, and networks to control the devices has existed for many years. The technology for this process includes common connectivity, widespread adoption of IP-based networking, computing the economics, miniaturization of the devices, 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 own characteristics. The four common communications models described includes Device-to-Device, Device-to-Cloud, Device-to-Gateway, and Back-End Data-Sharing models. These models show the flexibility in such a manner that IOT devices can provide Importance to the user. Above all this, a matter of concern is that we need improve the security of the devices which are internet based. Normal cryptographic algorithms perform perfectly in these kind of devices and hence these kind of platforms do not require light weight algorithm for the security purpose .On the other end of the spectrum the devices like embedded systems and the sensor networks require a light weight cryptographic algorithm for the security purpose. Light weight cryptography focuses upon the highly- compelled devices which are found at this part of the whole community of devices. Microcontrollers bear a huge and large range of performance characteristics. We know that the 16-bit and 32-bit microcontroller is famously common still for the ultra-low-cost applications the demand of lower bit microcontroller is very huge. The type of instruction available now a day's consists of very less amount of codes, which results in a huge number of cycles of a common cryptographic algorithm, which results in making the processor slower or power-consuming for the intended application. This becomes a huge problem when we need more power to run real time applications. These types of devices need low weight cryptographic algorithms not only to use a very small number of gates, but also to achieve the low timing and low power requirements. Thus, the above examples shows that how the light weight cryptography As lightweight encryption technology is uniquely aimed for the devices which are low-end devices but it is important that lightweight algorithms are also required at the high end of the device community. So the environment and applications need to decide if the low weight cryptography can be acceptable in every field for the maximum results. Lightweight cryptography becomes important for the security of the Internet of Things. Usually the developers get really confused to choose in between constrains of the security while designing the light weight cryptography. The particular requirements for the security are safety, cost and the productivity.

II. Light weight cryptography for IOT

Light weight cryptography is basically the type of encryption and decryption which refers to the consumption of less power, size and memory consumption. The basis of light weight cryptography is low cost and minimizing the size. We have terms like size of the key, number of encryption rounds, cost that are related to the performance of the algorithm. If we need to achieve a design which is cost effective, good in performance and also minimum in size than all these qualities in one go is difficult to achieve. For example if we implement this kind of algorithm than it would require a big area which results in high cost, and if we need to achieve a design with high reliability and of minimum cost than we need to compromise with the capacity. Among all these there is a basic component which is used for the light weight cryptography that is GE gate equivalent. This defines about the production's complexity. GE plays important part in the field of hardware implementations. Most of the algorithms used today are a part of software without hardware usage. In today's era we are in a need of hardware implementations too which demands less number of GE. Most of the algorithms used

today are a part of software without hardware usage. Due to this the already existing algorithms are impossible to implement on the devices which are having a limited processing power, less volume and the less amount of power consumption. The basis of the light weight cryptography is the reduction in cost for overall process. The developers of this type of cryptosystem have to focus on the performance, cost and the security. The new approaches are trying to solve the cost issues and are creating the methods to understand the cryptosystem and its importance some of these can be the usage of the traditional cryptographic protocols, modification of the previously used algorithms on the basis of hardware implementations, cost and limitations and the modification in the methodology to generate the algorithm The aim is to get a reliable and cost effective system. The main focus is the reduction of size of the encryption key, block encrypted data and the algorithms internal state, and because of this the algorithm would become light weight.

III Proposed Methodology

The methodology used for developing the algorithm for light weight encryption consists of some of the steps which need to be followed. While doing the development for the security algorithm for IOT based devices we need to take care of some constrains like memory space used, cost effectiveness, size of key, number of gates used and the measure of efficiency. The steps include key expansion followed by the key management protocol then the encryption after which the decryption of the codes finally is followed by the evaluation of the performance. Following flow chart shows the flow chart for the steps described above.

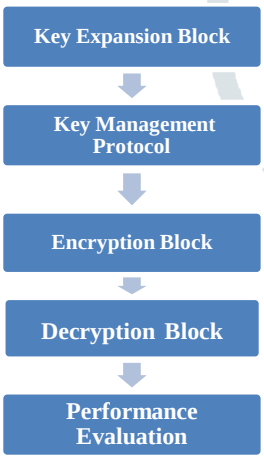

Fig 1.1 Flow Chart of the steps required to develop the algorithm

Key Expansion: Key expansion is the main process for generating unique keys for encryption and decryption. If the separate operations are performed then it leads to confusion and proliferation and this is done to minimize the probability of weak keys and maximize the advantages of key. Key expansion uses the logical operations like (XOR, XNOR), left (LS), matrix multiplication and fixed matrix (FM) also the P tables and permutations use T tables for transposition. The block architecture of key expansion is shown in the following figure.

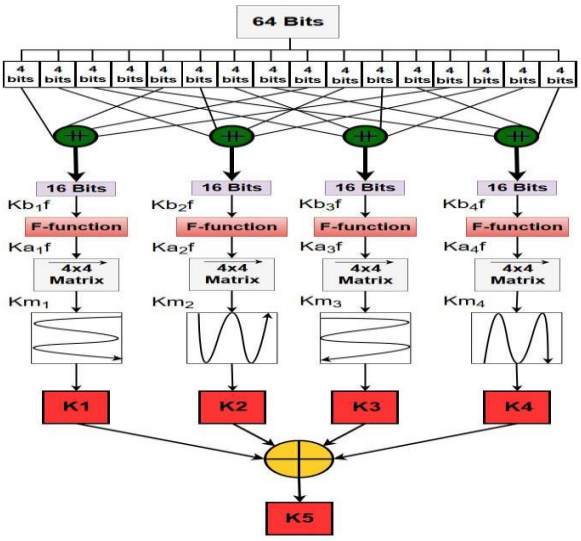

Fig1.2 Block architecture of key expansion

Key Management Protocol-The key can be securely sent to the encoder via LEAP which is again a light weight algorithm used for cryptography in IOT base devices. It is very simple and energy-saving protocol that is designed for some large-scale wireless sensor networks. It confirms the balance of security keys through four types of different keys which are the personal keys, group keys, cluster keys, and pair wise judicious shared keys. This protocol basically deals with the storage, exchange, destruction and the replacement of keys. Key managing is done at the level of user, which basically means that it handle the keys inside the operation done by the cipher.

Encryption Protocol: The encryption process is usually known as the coding in easy language and the process of encryption starts as soon as the key is generated by key expansion block. It is safely send to through and is received by the encoder. The secure communication channels are formed by the LEAP protocol. Encryption Process turns out to be a very simple operation which includes AND, OR, XOR, XNOR, LS (Left), Substitute (S) and Swap operations, the operation is to create confusion and proliferation which in turn enhance the security of the system. Encryption block is the very important block in the series of the security enhancement of the IOT devices.

Decryption Block: Decryption is the process of taking encoded or encrypted text to convert it back into the readable text which computer can read and understand. This describes a method to decrypt the data manually or via using the proper codes or keys. In this process the system takes out the information and converts it into the form that is understandable not only by the user nut also by the system. The whole procedure is done to enhance the security of the system and if the coded form is send via the channel it would be less prone to the attacks and hence to decode the data again for the real information we get the safe and secure data back at the output side.

IV. Experimental Results

To test the security of the studied algorithm, the algorithm is evaluated as per the mentioned parameters. These

parameters are key sensitivity, effect of cipher on entropy, histogram and correlation of the image.

Key Sensitivity: An encryption algorithm must be sensitive to its key. It means that the algorithm should not extract the original data if the key even has a minute difference from the original key.

Image	Entropy	Entropy Decrypted
Relax.JPEG	7.9970	7.4747

Execution Time: One of the fundamental parameter for evaluation of the algorithm is the amount of time that it takes to encode and decode a particular given data.

Memory Utilization: Memory utilization is major concern in resource constrains IOT devices. An encryption algorithm consists of many computational rounds which occupy good memory making it unsuitable to get utilized in IOT.

Image Entropy: The encryption algorithm adds extra information to the data which makes it difficult for the attacker to differentiate between the original information and the one added by the algorithm. It is measured that the amount of information in terms of entropy, therefore it is believed that higher the entropy better the performance of security algorithm is.

Correlation: The correlation between two values is a relationship which depicts the dependency of one value on another. Data points that hold substantial dependency has a significant correlation value. A good cipher removes the dependency of the cipher text from the original message.

B Results

Using the MATLAB we have successfully studied about the encryption and decryption of an image. Implementation via MATLAB code is done to understand the basic concept behind. The results are compared and analyzed further. The code is implemented on the various formats of the images like JPEG, GIF, and PNG etc. also the results are analysed over performance parameters. The effectiveness and accuracy is also checked on the same platform to get a better algorithm that provides a security as well as meet the requirement of other parameters also.

Correlation Analysis

For various images and their JPEG format we have tested the correlation of the original as well as the encrypted images. The following table shows the correlation between the original and the encrypted images of JPEG format.

Table 1.1 Correlation analyses

Image	Correlation Original	Correlation Encrypted
Relax.JPEG	0.9564	0.0016

Entropy Analysis

The following table shows the entropy of the JPEG image format for decrypted and encrypted image.

Table 1.2 Entropy analysis

Execution Time and Memory Usage

Table 1.3 Analysis of execution time and memory usage

Image	Execution Time	Memory Usage (Byte)
Relax.JPEG	26.32 Sec	894791680

The table shows the execution time and the memory usage for JPEG image format and which is again showing the efficiency of the algorithm proposed.

All above parameters are tested on MATLAB to check out the efficiency of the algorithm studied over here.

V. FUTURE WORK

IOT platform faces many of these challenges like those of power, the bandwidth, scalability, security and privacy. Security and privacy is the most dedicated challenge need to be resolved to preserve the faith in the users of IOT based devices. Predefined security solutions at each layer are still prone to attacks related to security. So the existing cryptography algorithms can be used to assure security. But the conventional heavy weight algorithms are not applicable for IOT due to their harsh environment. Hence lightweight cryptography solutions which are symmetric as well as asymmetric can be used. So much cost effective, lightweight security algorithm can be developed in future which use less number of block size and key size with a cost effective nature and providing a better security for the IOT based devices

VI. CONCLUSION

Since the idea of combining computers, sensors, and networks to judge and control devices has been there for many decades, the current flow of key technology and the market trends is indulging in a new reality of the “Internet of Things’’. IOT promises to follow up a revolutionary, fully interconnected and world, with relationship between different objects and their surroundings and objects with people becoming more closely connected. The idea of the Internet of Things as an array of devices which are related to the Internet might fundamentally change about what people think to be “online”.

Even the potentials are significant, a large number of challenges stand in the path of the vision – basically in the areas of security; privacy; interoperability and the standards; legal and rights issues; and this includes the emerging economies. 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] Maria Almulhim, Noor Zaman, "Proposing secure and the lightweight authentication scheme for IOT based E health applications" *International* conference on advance communication technology; 2018.

[2] Muhammad Naveed Aman, Kee Chaing Chua, "A light weight mutual authentication protocol for IOT system,2017.

[3] 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.

[4] Gaurav Bansod, Abhijit Patil, "An Ultra light weight design for security in pervasive computing" IEEE second international conference on big data security cloud, 2016.

[5] 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.

[6] Ayaz Hassan moon, Ummer Iqbal, "Light weight authentication framework for WSN" International conference on Electrical, Electronics and Optimization techniques, 2016.

[7] 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.

[8] D Jamuna Rani, "Light weight cryptographic algorithm for medical internet of things", Online international conference on Green Engineering and Technology, 2016.

[9] Sudhir Satpathy, Sanu Mathew, "Ultra low energy security circuits for IOT applications", IEEE 34th international conference on computer design, 2016.

[10] Sainandan Bayya Vankata, Prabhkar Yellai, " A new light weight transport method for secured transmission of data for IOT", international journal of electrical, electronic engineering, 2016.

[11] Amber Sultan, Xuelin Yang, "Physical layer data encryption using chaotic constellation rotation in OFDM-PON" Proceedings of 15th international Bhurban conference on applied science and technology Islamabad Pakistan, 2018.

[12] Xuelin Yang, Zanwei Shen, "Physical layer encryption algorithm for chaotic optical OFDM transmission against chosen plaintext attacks", in ICTON 2016.

[13] Han Chen, Xuelin Yang, "Physical layer OFDM data encryption using chaotic ZCMT precoding matrix", IEEE, ICTON 2017.

[14] Gao Baojian, Luo Yongling, Hou Aiqin, "New physical layer encryption algorithm based on DFT-S-OFDM system" International Conference on Mechatronic Sciences, Electric Engineering and Computer, Shenyang, China, 2013.

[15] Meihua Bi, Xiaosong Fu, "A key space enhanced Chaotic encryption scheme for physical layer security in OFDM-PON", IEEE photonics Journel", 2017.

[16] Pan Cao, Xiaofeng Hu, Jiayang Wu, "Physical layer encryption in OFDM-PON employing time variable keys from ONUs, IEEE photonics journal, 2 April 2014.

[17] Amber Sultan, Xuelin Yang, "Chotic Constellation Mapping for Physical Layer Data Encryption in OFDM-PON, IEEE Photonics Technology, vol.30, no.4, 2018.

[18] Yaoqiang Xiao, Zhiyi Wang, "Time Frequency Domain Encryption with SLM scheme for Physical Layer security in OFDM-PON system, J.OPT. Communication NETW./VOL..10, NO. 1, 2018.

[19] Xuelin Yang, Xiaonan Hu, Zanwei Shen, "Physical Layer Signal Encryption using Digital Chaos in PFDM-PON, IEEE ICICS 2015.

[20] Wei Zhang, Chongfu Zhang, "Brownian Motion Encryption for Physical layer security improvement in CO-OFDM-PON, IEEE Photonics Technology Letters, 2016.

[21] Dana Halabi, Salam Hamdan, "Enhance the security in smart home applications based on IOT-CoAP protocol.

[22] Jongsoek Choi, Yongtae Shin, "study on information security sharing system among the industrial IOT service and product provider, IEEE ICOIN, 2018.

[23] Jin Hyeong Jeon, Ki-Hyung Kim, "Block chain based data security enhanced IOT server platform, IEEE ICOIN, 2018.

[24] Muhammet Zekeriya Gunduz, Resul Das, "A comparision of cyber security oriented testbeds for IOT based smart grids, IEEE 2016.

[25] Himanshu Gupta, Garima Varshney, "A security Framework for IOT devices against wireless threats, second

international conference on telecommunication and networks, 2017.

[26] Thomas Maurin, Lurent, George Caraiman, "IOT security assessment through the interfaces P-SCAN test bench platform, 2018 EDAA.

[27] Israr Ahmed, Saleel A.P., Babak Beheshti, "Security in the Internet of things, 4th HCT information technology trends, Dubai, 2017.

[28] Peter Bull, Ron Austin, "Flow based security for IOT devices using an SDN gateway, 4th International conference on future internet of things and clouds, 2016.

[29] Iqra Hussain, Mukesh Chandre Negi, "A secure IOT based power plant control using RAS and DES encryption techniques in data link layer", International conference on Infocom technologies and unmanned systems, 2017.

[30] Nuzhat Khan, Nazmus Sakib, "Performance analysis of security algorithm for IOT devices", IEEE region 10 Humanitarian technology conference, Dhaka, 2