International Journal on Recent and Innovation Trends in Computing and Communication
ISSN: 2321-8169 Volume: 9 Issue: 3
DOI: https://doi.org/10.17762/ijritcc.v9i3.5476
***Article Received**: 22 January 2021 **Revised**: 10 February 2021 **Accepted**: 23 February 2021 **Publication**: 31 March 2021*

Comparative Study and Design Light Weight Data Security System for Secure Data Transmission in Internet of Things

Abha Jadaun[a], Satish Kumar Alaria[b] ,Yashika Saini[c]
[a] *M.Tech. Scholar, Department of Computer Science &Engineering, AIET, Jaipur, India*
[b,c] *Assistant Professor, Department of Computer Science & Engineering, AIET, Jaipur, India*

ABSTRACT

Internet of things is shortened as IoT. Today IoT is a key and abrogating subject of the specialized and social importance. Results of buyers, things and vehicles, industry based and fundamental segments, sensors, and other everyday items are converged with network of internet and the solid information abilities which guarantee to change the sort in which we work and live. 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. In this paper, implemented symmetric key cryptography for various formats 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*

1. INTRODUCTION

The Internet of Things set forward the confirmation for giving the social and financial advantages to forthcoming and to the creating economy, which incorporates supported farming, water quality that is utilized, human services issues, ventures the administration of condition and so on. IoT likewise guarantees to turn into a path for accomplishing the United Nations Sustainable Development Goals. The huge extent of IoT challenges isn't novel to the nations that are industrialized. Creating districts additionally need to react towards the advantages of Internet of things. What's more needs and difficulties to execute this idea in less-created regions is to be dealt with, including frameworks, market and venture motivating forces, specialized abilities and assets of approach. The Internet of Things happening today guarantees to give a progressive, completely associated brilliant world on the grounds that the connections among items, the earth and the general population is winding up increasingly dynamic. However the test and issues worried about IoT should be considered and dealt with so as to give the potential advantages to people, society, and the economy to be figured it out. At last boosting the advantages of the Internet of Things with limiting the dangers of security can't be cultivated by getting in an endless discussion that incorporates the affirmation of IoT against its qualities. It will take committed commitment and cooperation over the gatherings of partners to give away the best routes in future. The utilization of IoT segments rise numerous lawful inquiries and gave an ascent to officially existing lawful issues about the Internet. The inquiries are gigantic in extension, and the quick change in IoT technology addresses the capacity of the related approach, legitimate and administrative zones to be adjusted. Among the arrangement of issues one is the information streams that happen when IoT gadgets gather the information of individuals in a purview and exchange it to other locale with various information security laws for progressing handling. Another is that the information gathered by IoT gadgets is some of the time inclined to abuse which causes upsetting results for the clients. Other legitimate issues with IoT gadgets involves the contention among law implementation bodies and common right bodies; information pulverization; and lawful obligation for non-required utilizations, security or protection issues. Presently the internet of things are available in light of the fact that we have the information internet associations the rise of the information and internet association has far history and age by age we have built up the speed of information over internet with the goal that the internet of things can be gotten to effectively. Following segment demonstrates the historical backdrop of age of portable information.

The objective of this work to design and simulate lightweight and symmetric block cipher based cryptographic algorithm compatible with MANET, IoT and WSN devices to implement data security with quality management. The objective of the work can be discussed as follows:-

- To understand and implement mathematical modeling of cryptographic algorithms.

International Journal on Recent and Innovation Trends in Computing and Communication
ISSN: 2321-8169 Volume: 9 Issue: 3
DOI: https://doi.org/10.17762/ijritcc.v9i3.5476
Article Received: 22 January 2021 Revised: 10 February 2021 Accepted: 23 February 2021 Publication: 31 March 2021

- To implement standard protocols compatible with WSN, MANET and IoT.
- To design and simulate data security system based on block cipher, image processing and reversible data hiding.

2. RELATED WORK

[**Mohammad ShahabGoli et.al 2017]** proposed a new method to confront cropping attack using Sudoku tables. The water marked image is scattered in this method in two sudoko tables having different solutions in which water marked is host image. Various copies of water marked images are embedded in the host image which use this two-step Sudoku method for the resistance of watermark information. The information of watermark images is increased by 98.8%. By making use of this method, watermark image is reconstructed using other segments when attacked by the attacker. Therefore, the researcher concludes that both the suduko tables are in 9X9 classic form and provides resistance to cropping attacks by 98.8%.

[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. This algorithm only requires five rounds to ensure the security of the data. The SIT algorithm showed the desirable results when tested in the paper presented and also ensures the security in the IOT applications. The architecture used in the SIT algorithm is feistel architecture, the advantage of this algorithm is that using this algorithm we can use the same architecture for both encryption and decryption process. As the number of rounds of encryption increases the security of the process increase as well.The Avalanche test is done to check the accuracy of the algorithm which shows that a single bit change in plain text brings around 49% change in the cipher bits, which is close to 50% change and 50% change is the ideal change.

[Noor Zaman, et-al, 2018] proposed a lightweight authentication model for security that offers security level against multiple attacks like Impersonation attacks, man in middle attack and unknown key sharing attacks in E-health domain based on IOT. Author presented a secure lightweight authentication scheme based on groups E-health applications based on IOT. The proposed model provides an authentication, energy efficient scheme and computation for healthcare based on IOT. This uses elliptic curve cryptography (ECC) principle that describes the features of the proposed model. The author presents lightweight authentication scheme for the people who provide healthcare and the patients. Overall the motive of the work done by the author is to design a lightweight security scheme using ECC principles for E-health application based on IOT. The author developed an authentication scheme with small key which provide good level of security, this introduced authentication scheme\model based on groups for secure data transmission for E-health application and also provided an efficient, lightweight security scheme for E-health applications based on internet of things.The suggested security model depends on RSA this is the most utilized public key cryptography algorithm. It is used in communication stacks to provide UDP/IPv6 networking for usage of low power and energy.

[Muhammad Naveed Aman, et-al, 2017] presents an efficient protocol for strong secure authentication in IOT systems. The proposed protocol uses a physical non cloned function is used to provide security. The protocol that is proposed not only protects against different attacks, but also is very efficient to deal with memory, computations, energy, and the communication.The author presented a mutual authentication protocol for the IOT system. The protocol is based upon PUFs that carry the authentication via a challenge-response mechanism. The protocol perform secure authentication and a session key is established withoutthe need to store anything in IOT device. Author demonstrated that the proposed protocol is very efficient and provides security for many different types of attacks that includes physical attacks, side-channel attacks, and the cloning attacks.One of the most important requirements for Internet-of-Things (IOT) systems is security using very less resources. IOT devices are simple and low cost and this nature makes them a target for physical, side-channel, and cloning attacks. To resolve the same issue, the author presented an efficient protocol for mutual authentication for IOT devices.

[Mehdi Bahrami, et-al, 2016] proposed the method of cloud computing this method is helpful to the users who outsource their data. If data is to be send via cloud servers then the security plays a very important role. The author proposed a light weight data privacy method which uses a pseudo random permutation method to secure the content of the original data. As far as other encryption methods are concerned they are not that much cost effective and costs too much. When the data file splits into multiple pieces then this parallel algorithm proposed will scramble the data file. If the chunks of the data files are large in the size then DPM algorithm avoids the data from attacks. Author also demonstrated the comparison results of traditional DPM and the parallel DPM. The algorithm is cost effective and also provides security for the cloud computing. This algorithm saves at least 72% over other security methods. As the encryption process consumes high battery power and hence the proposed algorithm is a savior for the battery consumption as well as an effective algorithm for cloud computing.

[GauravBansod, et-al, 2016] proposed an ultra-weight encryption design for security. Author proposed a Feistel based cipher "ANU" which possesses maximum data complexity and results in maximum number of S-boxes for some of the rounds. ANU cipher requires 934 GEs as per 128 bit of the key length and consumes a very less power of 22 mW which is very less as compared to every other scheme for the same. ANU cipher stops the basic attacks and also resists the advanced attacks like. ANU cipher which is proposed has a positive feedback in the area of lightweight cryptography, this kind of designs play a very important role in making IOT applications secure. In the block cipher, a bit permutation

International Journal on Recent and Innovation Trends in Computing and Communication
ISSN: 2321-8169 Volume: 9 Issue: 3
DOI: https://doi.org/10.17762/ijritcc.v9i3.5476
***Article Received**: 22 January 2021 **Revised**: 10 February 2021 **Accepted**: 23 February 2021 **Publication**: 31 March 2021*

shuffles all the bits in such a manner which results in a diffusion mechanism. The operation of circular shifting and permutation layer is combined together and this will increase the count in number of active S-Boxes. Author has used the algorithm to make best use of power with less complexity. The same has been demonstrated experimentally and with the numerical derivations.

3. PROPOSED WORK

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 (fEm) to hide CI and gives Stego data (S) as an output (device at Transmitting end DT) as shown in figure-

$$(DT) \rightarrow fEm\ (C, CI,) \qquad (1)$$

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

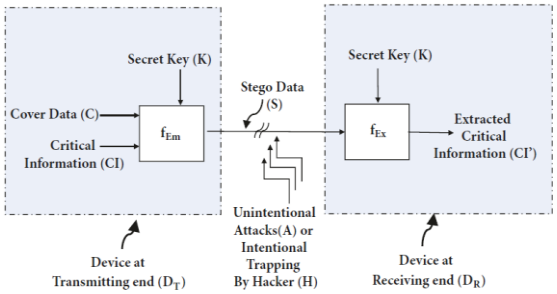

Figure 1 Steps Involved in Reversible Hiding Algorithm

The same Secrete Key (K) is used by the Steganographic extraction function (fEx) to extract CI (as a device at receiving end DR) as shown in

$$DR \rightarrow fEx\ (S,) \qquad (2)$$

where S is Stego data, CIisExtracted Critical Information, and K is Secrete Key. Typical generalized hardware Steganographic data hiding mechanism is as shown in Figure. Proposed reversible data hiding system to implement data hiding system consists of both cryptographic and Steganographic approach and therefore is called Crypto-StegoSystem. Figure outlines the proposed methodology.

As a part of cryptography As a part of cryptography, the encryption process is converting CI from plain text into unintelligible ciphertext.On the receiving side of the process, decryption is used to convert this unintelligible ciphertext back into plaintext CI as an extracted CI. If CI consists of M "Characters" in CI, stored in the Message Cache where M is number of characters in CI stored in "Message Cache" in a sequence.The process of encryption typically carried out using "Randomly Selected Set of Addresses" stored in a "LOOKUPTable" is randomly selecting any address location (Am) of Message Cache and hence, at any given time, one of the characters stored in Message Cache get selected as "Ym" and can be written as follows there is a "LOOK-UP Table"consisting of random numbers which eventually act as an addresses to locate any randomcharacter at "Message Cache". Obviously, the number of locations in "LOOK-UP Table" is 8 times more than that of the number of locations in "MessageCache", i.e., 8∗M. At any given time, one of the characters stored in "Message Cache" gets selected as "Randomly SelectedCharacter".

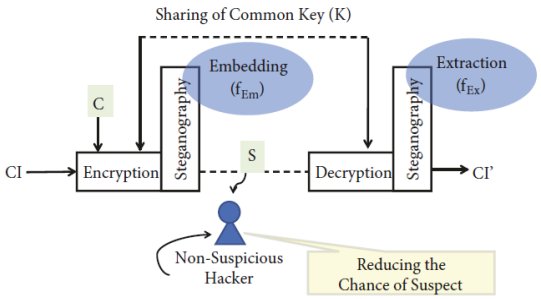

Figure 2 Steps Involved in Key Sharing in Proposed Algorithm

The overall process is explained as follows:-

1. Accept CI into Message Cache
2. Accept LOOK-UP Table as an Embedding Key (K)
3. Accept 8-byte coverdata (C)
4. Compute DWT of 8bytes of cover data
5. Randomly select byte(Y_m)from Message Cache
6. Selected it using 3LSBs of contents of selected byte LOOK-UP Table
7. Embed the selected bit at DWT coefficient C3
8. Compute IDWT of 8bytes of coverdata to get Stego data
9. Repeat Step-3 to Step-8 for all the bits of all the characters Message Cache

Stop.

4. RESULT ANALYSIS

The fundamental thought of the exploration done can be arranged into the focuses portrayed beneath

1. Implementation of low complexity symmetrical key encryption on multiple platforms (JPEG-2000, JPEG, BMP, PNG, GIF).
2. Performance Analysis of simulated technique on User defined and real time images.
3. Analysis of wrong key encryption.
4. Development of Graphical User Interface for the proposed system.
5. Analysis of the execution time and memory allocation of the proposed system.
6. Development of reversible data hiding system for image and text multiple encryption.
7. Analysis of PSNR and MSE for the proposed system.

International Journal on Recent and Innovation Trends in Computing and Communication
ISSN: 2321-8169 Volume: 9 Issue: 3
DOI: https://doi.org/10.17762/ijritcc.v9i3.5476
***Article Received**: 22 January 2021 **Revised**: 10 February 2021 **Accepted**: 23 February 2021 **Publication**: 31 March 2021*

Table 1

Analysis of Result for Reversible Data Hiding

Type of Image	PSNR	MSE
JPEG	60.91	0.021
JPEG-2000	65.13	0.016
PNG	62.12	0.019
BMP	64.13	0.022
GIF	60.21	0.022

5. CONCLUSION AND FUTURE WORK

Since consolidating PCs, sensors, and systems to pass judgment and control gadgets has been there for a long time, the present progression of key technology and the market patterns is enjoying another truth of the "Internet of Things". IOT guarantees to catch up a progressive, completely interconnected and world, with connection between various items and their environment and articles with individuals ending up more firmly associated. The possibility of the Internet of Things as a variety of gadgets which are identified with the Internet may on a very basic level change about what individuals think to be "on the web". Indeed, even the possibilities are noteworthy, countless remain in the way of the vision – essentially in the regions of security; protection; interoperability and the gauges; lawful and rights issues; and this incorporates the rising economies.

The Internet of Things is well known now, thus there is a need to acknowledge and resolve its difficulties and endeavor to boost its advantages at the same time lessening the dangers. Internet Society ponders IOT as it speaks to a developing stage for individuals and organizations which can collaborate with one another and enjoy on to the Internet and system availability into their own, social, and monetary lives. Answers for augmenting the best utilization of IOT with limiting the dangers can't be met by getting associated with a captivated discussion that sets the guarantees of IOT against security dangers. Be that as it may, it would take devoted commitment and cooperation among the specialists and the designers to make along these lines towards security works.

IOT stage faces a considerable lot of these difficulties like those of intensity, the data transfer capacity, versatility, security and protection. Security and protection is the most devoted test should be made plans to save the confidence in the clients of IOT based gadgets. Predefined security arrangements at each layer are as yet inclined to assaults identified with security. So the current cryptography calculations can be utilized to guarantee security. In any case, the regular substantial weight calculations are not appropriate for IOT because of their cruel condition. Subsequently lightweight cryptography arrangements which are symmetric just as lopsided can be utilized. So much practical, lightweight security calculation can be created in future which utilize less number of block size and key size with a financially savvy nature and giving a superior security to the IOT based gadgets.

REFERENCES

[1] Mourad Talbi and Med Salim Bouhlel, "Application of a Lightweight Encryption Algorithm to a Quantized Speech Image for Secure IoT", Preprints.org; 2018. DOI: 10.20944/preprints201802.0096.v1.

[2] Wen Zhang, Jie Men, Conglong Ma, "Research progress of applying digital watermarking technology for printing," 2018, IEEE

[3] David-Octavio Muñoz-Ramirez , VolodymyrPonomaryo , Rogelio Reyes-Reyes , VolodymyrKyrychenko , OleksandrPechenin, Alexander Totsky , "A Robust Watermarking Scheme to JPEG Compression for Embedding a Color Watermark into Digital Images," 2018, IEEE

[4] AnirbanPatra, ArijitSaha, Ajoy Kumar Chakraborty, Kallol Bhattacharya, "A New Approach to Invisible Water Marking of Color Images using Alpha Blending," 2018, IEEE

[5] Irshad Ahmad Ansari, Chang WookAhn and Millie Pant, "On the Security of "Block-based SVD image watermarking in spatial and transform domains", 2018, IEEE

[6] Alexander S. Komarov, "Adaptive Probability Thresholding in Automated Ice and Open Water Detection From RADARSAT-2 Images," 2018, IEEE

[7] Aoshuang Dong, RuiZeng, "Research and Implementation Based on Three-dimensional Model Watermarking Algorithm," 2017, IEEE

[8] EnjianBai, Yiyu Yang and Xueqin Jiang, "Image Digital Watermarking Based on a Novel Clock-controlled Generator," 2017, IEEE

[9] Oleg Evsutin, Roman Meshcheryakov,Viktor Genrikh, Denis Nekrasov and Nikolai Yugov, "An Improved Algorithm of Digital Watermarking Based on Wavelet Transform Using Learning Automata," 2017, IEEE

[10] Ritu Gill and Rishi Soni, "Digital Image Watermarking using 2-DCT and 2- DWT in Gray Images," 2017, IEEE.

[11] Mohammad ShahabGoli and AlirezaNaghsh, "Introducing a New Method Robust Against Crop Attack In Digital Image Watermarking Using Two-Step Sudoku," 2017, IEEE

[12] 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.

[13] Maria Almulhim, Noor Zaman, "Proposing secure and the lightweight authentication scheme for IOT based E health applications" *International* conference on advance communication technology; 2018.

[14] Muhammad NaveedAman, KeeChaing Chua, "A light weight mutual authentication protocol for IOT system, 2017.

[15] Mehdi Baahrami, Dong Li, MukeshSinghal, "Efficient parallel implementation of light weight data privacy method for cloud users; seventh international workshop on data intensive computing in clouds, 2016.

[16] GauravBansod, AbhijitPatil, "An Ultra light weight design for security in pervasive computing" IEEE second international conference on big data security cloud, 2016.

[17] ZahidMahmood, HuanshengNing, "Light weight two level session key management for end user authentication

International Journal on Recent and Innovation Trends in Computing and Communication
ISSN: 2321-8169 Volume: 9 Issue: 3
DOI: https://doi.org/10.17762/ijritcc.v9i3.5476
***Article Received**: 22 January 2021 **Revised**: 10 February 2021 **Accepted**: 23 February 2021 **Publication**: 31 March 2021*

in internet of things" IEEE international conference on IOT, 2016.

[18] Ayaz Hassan moon, UmmerIqbal, "Light weight authentication framework for WSN" International conference on Electrical, Electronics and Optimization techniques, 2016

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

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

[21] SainandanBayyaVankata, PrabhkarYellai, " A new light weight transport method for secured transmission of data for IOT", international journal of electrical, electronic engineering, 2016.

[22] 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.

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

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

[25] GaoBaojian, LuoYongling, HouAiqin, "New physical layer encryption algorithm based on DFT-S-OFDM system" International Conference on Mechatronic Sciences, Electric Engineering and Computer, Shenyang, China, 2013.

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

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

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

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

[30] MuhammetZekeriyaGunduz, Resul Das, "A comparision of cyber security oriented test beds for IOT based smart grids, IEEE 2016.

[31] Himanshu Gupta, GarimaVarshney, "A security Framework for IOT devices against wireless threats, second international conference on telecommunication and networks, 2017.

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

[33] Sanjay Kumar, AmbarDutta, "A Study on Robustness of Block Entropy Based Digital Image Watermarking Techniques with respect to Various Attacks," 2016, IEEE

[34] N. SenthilKumaran, and S. Abinaya, "Comparison Analysis of Digital Image Watermarking using DWT and LSB Technique," 2016, IEEE

[35] Harsha M. Patil and Prof .Baban U. Rindhe, "Study and Overview of Combined NSCT –DCT Digital Image Watermarking," 2016, IEEE