How to Cite:
Savima, K., & Srinath, M. V. (2022). A novel encryption technique for enhanced security performance in IoT devices and comparative algorithmic approach of lightweight block ciphers: Presopt. *International Journal of Health Sciences*, *6*(S6), 9711–9720. https://doi.org/10.53730/ijhs.v6nS6.12532

A novel encryption technique for enhanced security performance in IoT devices and comparative algorithmic approach of lightweight block ciphers: Presopt

K. Savima
Research Scholar, S.T.E.T Women's College (Autonomous), Affiliated to Bharathidasan University, Tiruchirappalli, Sundarakkottai, Mannargudi - 614016, Thiruvarur Dt., Tamil Nadu, India
*Corresponding author email: savimastet@gmail.com

Dr. M. V. Srinath
Research Supervisor, S.T.E.T Women's College (Autonomous), Affiliated to Bharathidasan University, Tiruchirappalli, Sundarakkottai, Mannargudi - 614016, Thiruvarur Dt., Tamil Nadu, India
Email: sri_induja@rediffmail.com

***Abstract*---**In recent times, security for hardware and software appliances has proved to be a quintessential extravagance that not many are able to afford or attempt to deliver. This is due to the escalated hacks and technologies that are contrived for smoother pragmatism. Internet of Things (IoT) has become a norm that caters to many quotidian difficulties faced by working class, and is considered to be the rapidly growing technology for sensor-collaborative working. The high necessitation to procure integrated platforms with virtual technologies has therefore augmented the development of IoT globally. However, while its incorporation with adept cognizance is entailed with good maintenance, adequate updations, and systematic security add- ons, there are still persisting glitches that impact the resilience and complete reliability of the devices. Cyberattacks, hacking and data pilferage are some of the common problems that can cause serious detriments when the privacy of data is high. The recent encryption methodologies entailing light-weight block ciphers have ameliorated the veracity, and authentication of devices for registered users. Vast research pertaining this field of study is articulated through encryption and decryption algorithms using AES, RES and other ciphers. Nevertheless, this study proposes a juxtapose of encryption-decryption algorithms and a novel framework 'PRESOPT' which is enhanced from a light-weight block cipher known as the

Manuscript submitted: 9 May 2022, Manuscript revised: 18 July 2022, Accepted for publication: 27 August 2022

Present algorithm. DES, ROT-13 and the Present framework is pivoted on in this paper to analyse the security and performance in comparison with the implementation result of PRESOPT. DES with block size of 64 bits, along with 56-bit key length, and 16 rounds of operation constitutes the working of the algorithm. On the other hand, ROT-13 is an enhancement of ceaser cipher, while the Present algorithm holds a sequence of steps with Near Feel Communication (NFC) Based Pairing that is compatibly embedded with IoT devices. PRESOPT is derived inorder to bolster and exceed the security performance of the existing algorithms, along with supplementing competence to fortify the cyberattack resistance of IoT devices. The simulations for the proposed study are implemented in Python, and the results are successfully procured.

***Keywords*---**decryption, encryption, internet of things (IoT), light-weight block cipher, present algorithm, DES, ROT-13, PRESOPT framework.

Introduction

The networking ecosystem is most often compromised due to cyberattacks and IoT is no different. IoT devices are interconnected [10], and data pilferage and infiltration are one of the networks can disrupt the security of the entire environment. While the dependency on IoT devices and integrated platforms have largely escalated, the need to stabilize the security rubrics is necessitated with higher priority. The security concerns do not only put the network to risk, but also the entirety of data involved, which entails the inception of encryption and decryption of the data involved. The sensors [11] and the frequency spectrum [1] associated with the technology largely enables data to be transmitted through a wireless medium. This medium could be often compromised to suit the hacker's confidence, and procure ownership of the network, thereby leading to data stream privacy mishaps. Most Often, this interfacing collaboration between the components of the IoT processes can be through different platforms and operating systems, along with varying standards of communication and privacy rubrics, which subsequently evinces high volatility and compromised functionality [2]. Lightweight block ciphers are used largely as an encryption technique that institutes an effective mechanism to encode the data bits or blocks of data through their sequential process. The devices thus connected for processing are embedded with encrypted algorithms that serve the purpose of evading cyberattacks, along with rendering higher resilience and sustainability of secure transactions [11].

The distinction of light-weight block ciphers lies with its incorporation of deterministic algorithms, that trigger efficacy in key generation to each block of data [9], [14]. The IoT incorporated devices scale from the tiniest size to machines and gadgets. The IoT implementable technology aids in fulfilling various purposes such as devices used for measuring temperature, RFID kits [3], gadgets fulfilling household chores and entertainment devices such as televisions and mobile phones. These devices predominantly connect to the internet and communicate

with the respective servers inorder to deliver data for analysis. Thus, resulting in opportunities for malware intrusion at differing degrees that may disrupt the privacy of the established communication. The motive of incorporating light-weight block ciphers is to customize the encryption efficacy to fit the constrained IoT device communications, along with parallelly improving the performance of sensors in the IoT devices. While symmetric and asymmetric key encryption and decryption methods have been used extensively, the primary challenge ofentailing these methods with IoT devices is the limitation that the key of algorithms holds whichmay not be compatible with the constraints that IoT devices delineate.

This study elaborates on comparing the working of three techniques for encryption and decryption, and their differences in terms of processing speed and security of the mechanism when potently utilized with an IoT device. DES [4], [6], ROT13 [4], and the light-weight cipheralgorithm 'Present' [3], [5], [7] is detailed in the ensuing sections, and the novel improvised technique that can be embedded in a IoT device to optimize the overall performance of security and time is explicated by the 'PRESOPT' framework. This paper is structured with the following sections detailing the juxtapose of existing algorithms that could be embedded with the IoT devise. Section III details the architecture of the proposed methodology, and sections IV and V elaborates on the results obtained, and the conclusion, along with imminent dimension of interestthat the domain could likely be moulded respectively.

A Juxtapose of Existing Algorithms

Pseudo-randomness of an encryption mechanism, and the efficacy of key-generation aidsin establishing the base for the encoding and decoding techniques in an algorithm. It is important for a researcher to analyse the type of encryption model that is necessitated, and therefore the benefits of symmetric and asymmetric must be cognized explicitly. This section details the various algorithmic approaches effectuated to understand the encryption and decryption of data prior to its inclusion into an IoT device. The Data Encryption Standard (DES) [4] is a same-key encryption-decryption algorithm,and is stratified under the symmetric [12] block cipher class of security algorithms. The algorithm takes in 64-bit blocks of data to convert them from a plain text to cipher text, and vice-versa through a combined approach of substitution and transposition. The prime criticism that this algorithm faces is the privacy constraint of the key which is shared both between the sender and the receiver, and its facileness of being hacked. The working phase of the DES algorithm is as shown in the below figure 1.

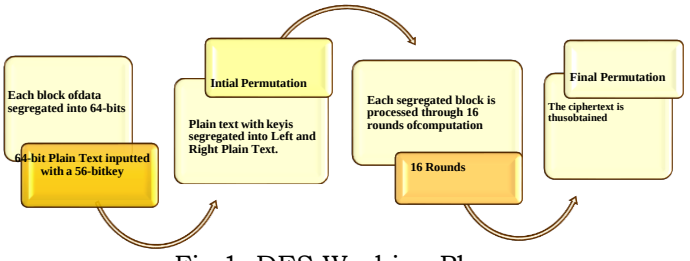

Fig 1. DES Working Phases

The DES algorithm initially allots a 64-bit key for the processing of the sequential steps, nonetheless, every 8th of the selected key is pivoted towards the working of parity checks, and hence the key is truncated to a functionable 56-bit key [6]. The 16-round process of the DES algorithm is effectuated through two phases with the initial permutation occurring only once prior to the first round of processing. The plain text inputted is bifurcated into the left and right segments and processed similarly through a permutational combination of substitution and transposition, to be finally amalgamated in the combined block of the final permutation rendering the user with the converted 64-bit cipher text. The key transformation in the DES algorithm is another significant process that enhances the security of the technique [16]. The following figure2 illustrates the transformation of the 64-bit key initially taken for processing, and its conversion through various methodologies.

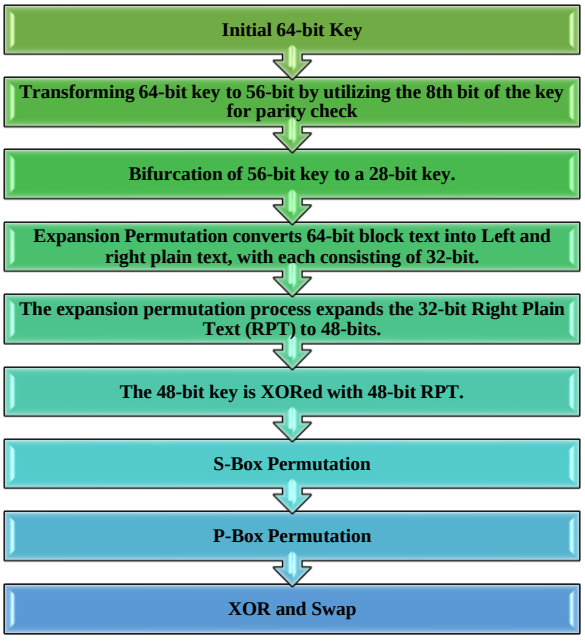

Fig 2. Key Transformation and Block processing of the Algorithm

The result of processing using the DES algorithm with respect to the lapse time and encryption-decryption security is delineated in the consecutive section of this paper. The next algorithm effectuated for this study is the ROT-13 algorithm which is optimized from the Caesar cipher with fixed rotations of 13 [17]. The working of the algorithm is by substituting every letter of the given data to the 13th data of the series [4], thereby performing the rotation of every character to its 13th place to obtain a new set of data. The working framework of the ROT13 algorithm is as given below in figure3.

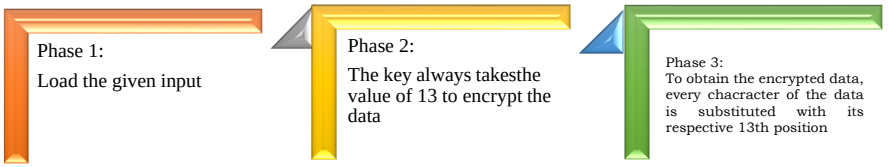

Fig 3. Working of ROT 13

The result of the implemented ROT 13 algorithm is procured to understand the time complexity involved, and the security compromises that it may evince. The Present block cipher [3], [18] is popularly utilized as an embedded program that establishes to enhance the security of IoT devices. The algorithm takes into consideration two 128-keys, and works on a 64-bit block size [5], [13]. The round size is fixed to 32, with the lastround dedicated to post whitening, and the previous rounds performing the XOR operations [7] through non-linear substitution and linear permutation layers.

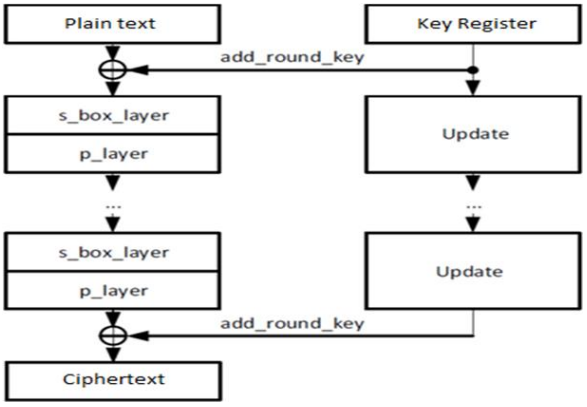

Fig 4. Main module of PRESENT Algorithm

The add_round_key performs the following operation $bj \rightarrow bj \oplus kj^{i}$ where j varies from 0to 63 and 'i' varies from 1 to 32. S_box_layer [8] performs a conversion from 4 bit to 4 bit. This is more compact than an 8-bit S Box which gives more hardware efficiency [13]. The p_layer performs the movement of bit i to a bit position P(i). The key given by the user is stored in key register K [7]. Thus, at round i, Then the key register is updated as follows.

$$K_{79}K_{78}K_{77}\ldots K_1K_0 = K_{18}K_{17}\ldots K_{20}K_{19};\ K_{79}K_{78}K_{77}K_{76} = S[K_{79}K_{78}K_{77}K_{76}];$$
$$K_i = K_{63}K_{62}K_{61}\ldots K_1K_0 = K_{79}K_{78}K_{77}\ldots K_{17}K_{16}.$$
$$K_{19}K_{18}K_{17}K_{16}K_{15} = K_{19}K_{18}K_{17}K_{16}K_{15} \oplus round\_counter.$$

The key is rotated by 61-bit positions to the left, with the left most 4 bits passed through the S_box [15], and the round counter value i is XORed with bits of K [7]. The algorithm stands resilient towards cyberattacks when embedded with IoT devices. However, the degree of sustainability fluctuation toward security when utilized with varying devices of IoT is a challenge that this algorithm encounters. The framework of the present algorithm is illustratedin the below figure5.

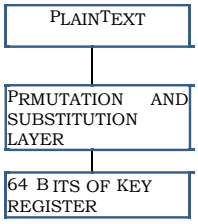

Fig 5. Flow of Present Algorithm

Working of PRESOPT

While the PRESOPT algorithm utilizes the first key for 31-rounds of encryption and the special second key for encrypting data, the odd rounds of the encryption process employ the first 128 bit key for Permutation-Substitution (P/S) and XORing the 64-bit block of data. During the even rounds of encryption, it bifurcates the data into 32-bit blocks and utilizes the 64-bit key for the P/S and XORing process on both blocks. The proposed PRESOPT algorithm is an improvisation of the existing Present algorithm, and is embedded into IoT devices that encompasses a FGPA chip [14], along with parallelly augmenting the efficiency compared to the implemented existing algorithms. To overcome the detriments of constrained utilization and device-level security observed in the Present algorithm, this novel framework is constructed as shown in Figure 6.

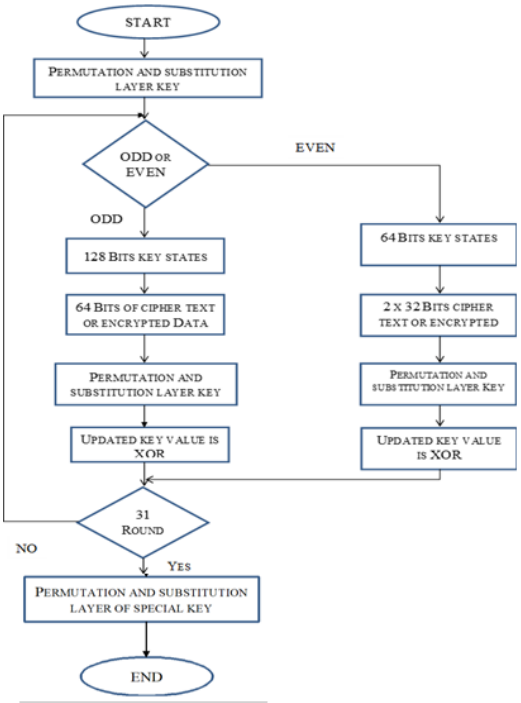

Fig 6. Proposed PRESOPT Framework

Results

The outcome of the explained cipher and implemented algorithms are presented in this section. The encryption and decryption of data, along with the security levels are measured for each of the effectuated algorithms using the Python platform. The below table1 renders the time taken, along with the relevant results for the implemented modules. While the elapsed time for the ROT13 depicts the swiftest processing speed as compared to the others, the security of the proposed PRESOPT lightweight cipher processing methodology surpasses the implemented algorithms interms of enhancing the security of the data blocks.

Table 1
Comparative output of Cipher-Algorithmic implementations

Name of Algorithm	Elapsed time	Output
ROT13	0.00200601400000088 86	Oybpx pvcure vf n xvaq bs n flzzrgevp pvcure, juvpu guebhtu pbafgnag znccvat (hfhnyyl) cebprffrf vasbezngvba oybpxf (bsgra 64 be 128 ovgf). "Yvtugjrvtug" oybpx pvcure vf qvssrerag sebz gur oybpx fb gung vg hfrf gur nytbevguzf gung erdhver yrff pbzchgvat cbjre.
Data encryption standard (DES)	0.02826936199999963	Input: 123456ABCD132536 Output: C0B7A8D05F3A829C
Present Algorithm	1651	Input: Plaintext Output: Ciphertext
Proposed Algorithm: PRESOPT	0.00281709	I/P: Block cipher is a kind of a symmetric cipher, which through constant mapping (usually) processes information blocks (often 64 or 128 bits). "Lightweight" block cipher is different from the block so that it uses the algorithms that require less computing power. O/P1: rewop gnitupmoc ssel eriuqer taht smhtirogla eht sesu ti taht os kcolb eht morf tnereffid si rehpic kcolb "thgiewthgiL" .)stib 821 ro 46 netfo(skcolb noitamrofni sessecorp)yllausu(gnippam tnatsnoc hguorht hcihw ,rehpic cirtemmys a fo dnik a si rehpic kcolB O/P2:Oerjbcatavghczbpaffryarevhdreagnugafzugvebtynar ugafrf hagvagnugabfaxpbyoa rugazbesagarerssvqafvaerucvpaxpbyoacgutvrjgutvYcaojfg voays raebauwaargsbi afxpbyoaabvgnzebsavafrffrpbecajlyynhfhiatavccnzagan gfabpau thbeugaupvujame rucvpapvegrzzlfanasbaqavxanafvaerucvpaxpbyO

Conclusion

Technology and its integrated virtual utilization are a necessitation due to the demanding nature of jobs that the current generation is adapted to. Thus, requiring thetechnological devices and modems used to be robust and hold high fault tolerance. While IoT is effectuated in almost all industries as a part of incorporating sensor modules, their adeptness to cyberattacks and hacking has been on the rise. The existing encryption models although have enhanced the impeccability of mitigating intrusion risks, their compatibility with varying devices and differing chip incorporations have been highly challenged. The proposed PRESOPT framework overcomes this obstacle, and is integrated with IoT devices holding FPGA chips, while maintaining their consistency with other versions of hardware devices with respect to rapid processing time and security augmentation. The juxtapose of existing encryption-decryption algorithms such as DES, ROT13 and the light-weight Present cipher have evinced the pros and cons, and have triggered the motivation to render consistent feasible security standards to be sustained for varying degrees of key generation and hardware models. While ROT13 yielded the fastest processing time, the security of the data was ameliorated further by PRESOPT as compared to the other existing models interms of their hacking complexity, and facileness to interrupt the encryption of data. The future work of implementation pertaining this domain could be established by pragmatically entailing real- time data integrated with IoT devices, along with commingling the proposed cipher methodology to comprehend further the optimization that may be required, and the supportive add-ons that may be required for supplemented development.

References

1. Anitha Kumari S, Mahalinga V Mandi “Implementation of Present Cipher on FPGA for IoT Applications”, International Journal of Engineering Research & Technology (IJERT), Vol. 8 Issue 08, August-2019.
2. Bogdanov, L.R. Knudsen, G. Leander, C. Paar, A. Poschmann, M.J.B. Robshaw, Y. Seurin, and C. Vikkelsoe, “PRESENT: An Ultra-Lightweight Block Cipher”, CHES 2007, LNCS 4727, pp. 450–466, 2007, Springer-Verlag Berlin Heidelberg.
3. Bogdanov, L.R. Knudsen, G. Leander, C. Paar, A. Poschmann, M.J.B. Robshaw, Y. Seurin, and C. Vikkelsoe, “PRESENT: An Ultra-Lightweight Block Cipher”, September 2007 DOI: 10.1007/978-3-540-74735-2_31
4. Daniel Dinu, Yann Le Corre, Dmitry Khovratovich, L´eo Perrin, Johann Großsch¨adl, Alex Biryukov, “Triathlon of Lightweight Block Ciphers for the Internet of Things”, Journal of Cryptographic Engineering 9(15), DOI:10.1007/s13389-018-0193-x, September 2019
5. Evans, D. (2011). The Internet of Things: How the next evolution of Internet is changing everything”, CISCO, San Jose, CA, USA, white paper, 2011, https://www.cisco.com/c/dam/en_us/about/ac79/docs/innov/IoT_IBSG_0411FINAL.pdf
6. Fatemeh Babaeian, Nemai Chandra Karmakar, “Time and Frequency Domains Analysis of Chipless RFID Back-Scattered Tag Reflection”, IoT 2020, 1(1), 109-127; doi.org/10.3390/iot1010007

7. Hillman Akhyar Damanik, Merry Anggraeni, Tomi Defisa, “Analysis Stego-Image Extraction using ROT13 and Least Significant Bit (LSB) Algorithm Method on Text Security”, November 2017, Journal Ilmiah FIFO 9(2):147, DOI:10.22441/fifo.2017.v9i2.008.
8. Lavanya R, Karpagam M, Jaikumar R, “A Comparative Study on the Implementation of Block Cipher Algorithms on FPGA”, 2017 IJSRST, Volume 3, Issue 8, ISSN: 2395-6011.
9. M. Sujitha, M. Pushpa, “An Encryption Algorithm for Improving Database Security using ROT & REA”, Indian Journal of Computer Science and Engineering (IJCSE), ISSN: 0976- 5166, Vol. 6 No.3 Jun-Jul 2015.
10. Maria Imdad, Sofia Najwa Ramli and Hairulnizam Mahdin, “An Enhanced Key Schedule Algorithm of PRESENT-128 Block Cipher for Random and Non-Random Secret Keys”,
11. Mohammed Nazeh Abdul Wahid, Abdulrahman Ali, Babak Esparham and Mohamed Marwan, “A Comparison of Cryptographic Algorithms: DES, 3DES, AES, RSA and Blowfish for Guessing Attacks Prevention”, Journal of Computer Science Applications and Information Technology, ISSN Online: 2474-9257, Aug 2018.
12. Nur, I. L., Ahmad, M., Syarif, S., & Ahmar, H. (2021). The performance of midwives in managing childbirth using a digital partograph. International Journal of Life Sciences, 5(2), 26–35. https://doi.org/10.29332/ijls.v5n2.1219
13. Prakasam P, Madheswaran M, Sujith K.P, Md Shohel Sayeed, “An Enhanced Energy Efficient Lightweight Cryptography Method for various IoT devices”, ICT Express, Volume 7, Issue 4, December 2021, Pages 487-492.
14. Qusay Idrees Sarhan, “Internet of Things: A Survey of Challenges and Issues”, January 2018, International Journal of Internet of Things and Cyber-Assurance, 1(1), DOI:10.1504/IJITCA.2018.10011246
15. Shreyank N Gowda, “Innovative Enhancement of the Caesar Cipher Algorithm for Cryptography”, DOI: 10.1109/ICACCAF.2016.7749010, Sept 2016
16. Sreeja Rajesh, Varghese Paul, Varun G. Menon and Mohammad R. Khosravi, “A Secure and Efficient Lightweight Symmetric Encryption Scheme for Transfer of Text Files between Embedded IoT Devices”, February 2019, doi:10.3390/sym11020293.
17. Suryasa, I. W., Rodríguez-Gámez, M., & Koldoris, T. (2021). The COVID-19 pandemic. International Journal of Health Sciences, 5(2), vi-ix. https://doi.org/10.53730/ijhs.v5n2.2937
18. Symmetry 2022, 14, 604, https://doi.org/ 10.3390/sym14030604
19. Welekar, R., Rajurkar, S., & Kodwani, U. (2022). A novel approach for file encryption. International Journal of Health Sciences, 6(S2), 9447–9455. https://doi.org/10.53730/ijhs.v6nS2.7474
20. Yogesh K, Rajiv M, Harsh S, “Comparison of symmetric and asymmetric cryptography with existing vulnerabilities and countermeasures”, International Journal of Computer Science and Management Studies. 2011;11(3):60-63.
21. Zaid M. Jawad Kubba1 and Haider K. Hoomod, “Modified PRESENT Encryption algorithm based on new 5D Chaotic system”, IOP Conf. Series: Materials Science and Engineering 928 (2020) 032023 IOP Publishing doi:10.1088/1757-899X/928/3/032023.

22. Zaid M.Jawad Kubba,“Developing a lightweight cryptographic algorithm based on DNA computing” Published Online: 04 December 2020