THE PERFORMANCE ANALYSIS OF THE PROPOSED PRESENT ALGORITHM WITH LMLA ENCRYPTION TECHNIQUE FOR CYBER SECURITY

R. Nithya
Department of Computer Science and Engineering,
Bannari Amman Institute of Technology, Erode, India.
nithyarangasamy03@gmail.com

T. Savithadevi
Department of Computer Science and Engineering,
*Dr.N.G.P Institute of Technology,*Coimbatore, India.
csesavi@gmail.com

S. Suresh kumar
Department of Computer Science and Engineering,
Kalasalingam Academy of Research and Education,
Krishnankoil,India.
sureshhkumar.ssk@gmail.com

Dr. K. Chandraprabha
Department of Information Technology,
Bannari Amman Institute of Technology, Erode, India.
knaprabha@gmail.com

A. Indirani
Department of Artificial Intelligence and Machine Learning,
Bannari Amman Institute of Technology, Erode, India.
indirania@bitsathy.ac.in

Abstract

Cyber security has become a salvation for many wireless communication systems and technologies in the wake of cyber criminals and attacks. These cyber intruder's impairments wreak havoc for both commercial corporations and federal agencies. The attackers attack the system and personal data by employing various tricks and valuable resources like tools that break the security keys and become a demurrer for security administrators. These cyber-attacks potentially result in the collapse of wireless equipment, blackouts, and the exposure of national security information. The attackers will obtain valuable confidential data and disrupt the network. It also paralyzes the systems and renders data inaccessible for the authorized users in the network. Many advanced techniques are being explored to counteract these cyber threats. In this backdrop, the article examines the several distinct cyber-attacks and the advanced encryption mechanisms for thwarting the attacks from the intruders. This paper proposes a new hybrid encryption scheme for furnishing the security during communication in the network. The performance analysis of the proposed Logistic Map and 3D Chaotic Multi-Scroll Lorenz attractor (LMLA) with PRESENT Algorithm shows that it outperforms the traditional encryption techniques by furnishing 58.064% lower in storage space, 51.162% lower in dynamic memory during encryption. The throughput of the proposed the LMLA encryption is 16.276% increased than the traditional encryption standards and the encryption time of the proposed PRESENT algorithm with LMLA is 29.906% lower than the traditional encryption algorithms.

Keywords:* *Attack, Storage, Security, Data, Throughput, Logistic Map, Communication.

I. Introduction

The Internet is becoming a more common feature of (online) information and services. The Internet is a global network comprising millions of interconnected computers, networks, and other devices. The internet aids in the transportation of data over the network from a source to other nodes. The intelligent systems, computers, networks and mobile have increased the internet usage that made the cybercriminals and adversaries to turn their attention over the Internet [3, 17]. For designing and executing the cyber-attacks the cyber criminals require only a computer and the internet connection. Henceforth the cyber threats are becoming more accessible, less affordable and far less hazardous than the physical threats. As cyberspace has grown, cyber threats have become far more focussed, powerful and complex in posing difficulties. It not only creates complications for the states but also for the political parties, criminals, individuals and terrorist groups. In real time cyber security is required for identifying the threats, evaluating or analysing the threats and defending against the threat [4].

Confidentiality of the messages, availability of the services and resources, and integrity of the message ensures the security for the system or the network [2]. The illegal penetration of the individuals or programmes into the network will intent to disrupt the regular flow of activities and endanger the security and integrity of the system [1, 18]. Assaults on individuals, property, organisations, and society are the four distinct categorizations of cyber-attacks as depicted in Fig. 1.Assaults on the individual incurs spoofing Email, defamation and stalking of cyber. Assaults on property include credit_card fraud, theft on internet time and crimes based on intellectual property. Assaults against organization incurs Denail_of_Service attack, attack on virus, bombing on Email and logic bomb. Assault against society incurs forgery on documents, web jacking and cyber terrorism. The ransomware, Wannacry, Petya, BSNL Malware attack, Breaches on data, mirai botnet malware and heist on union bank are the other assault incidents that occurred in India [5, 11].

Fig. 1 Various Attacks by the Cyber Intruders

The two key characteristics of the encryption algorithms are: the potential to prevent breaches from several types of threats and the processing speed and if the threats doesn't exist then the mechanism is known to be secure so that they can share the original information without acquiring keys. The cryptographic encryption mechanism are broadly classified into symmetric employs the secret key for transmission of messages and asymmetric encryption that utilizes the public key for the transmission of information. The asymmetric algorithms consumes "higher storage space and higher energy efficiency which becomes demurrer in employing for processing huge amounts of individual data. Therefore the symmetric encryption mechanism is employed for processing higher individual data with lower operation time and energy efficiency. The several distinct symmetric encryption mechanisms are Advanced_Encryption_ Standard, Data_Encryption_Standard, RC4, Blowfish etc [6, 12]. These traditional techniques have lower throughput and larger storage space when compared with the PRESENT algorithm. Hence the proposed Logistic Map and 3D Chaotic Multi-Scroll Lorenz attractor (LMLA) algorithm hybrids the PRESENT algorithm with the logistic map and lorenz attractor that reduces the dynamic memory space along with the storage space.

This paper is organized as follows: The related work has been elaborated in Section 2. The several distinct cyber-attacks has been deliberated in Section 3. Section 4 demonstrates the proposed encryption scheme and Section 5 analysis the performance based on the resource utilization and throughput with the existing traditional models. Finally, this paper is concluded in Section 6.

II.RELATED WORK

Mahalakshmi.J et.al [7] introduces a block_cipher-based_cryptographic_algorithm are employed for encryption to enhance the security of the data. The plain text of the sender is encrypted by utilizing the mode of cipher_block_chaining that manipulates the block for the process of decryption as well. To empower the encryption algorithm the pseudo_random_ generator is pursued which furnishes multiple keys for processing the distinct ciphers at a time. This cipher encryption algorithm occupies lesser storage as well as the speed for both decryption and encryption is higher. This algorithm fails to furnish the through for both the process of decryption and encryption.

Abid Murtaza et.al [6] proposes a new –symmetric encryption mechanism for furnishing the security with lower complexity and processing time. It mainly uses the data coding technique for compressing the data and the data can be encoded with a secret table. Generating the random number, formulating the encoding table, shuffling the input data and encoding the information are the four distinct processes involved in the encryption technique. Decryption of the information is carried out by using the table in the reverse substitution process. The algorithm achieves higher security with higher speed in both encryption and decryption process along with various levels of flexibility in terms of distinct sizes of the key. This algorithm also serves the compression of data inherently without any complexity as it employs the 128 ASCII codes. The strike of this technique failed to analyse the throughput along with the traditional encryption mechanisms.

Jaime Raigoza et.al [8] compares the performance of two symmetric_encryption_mechanism in terms of the execution time. Advanced_Encryption_Standard and the Blowfish are the symmetric_encryption_mechanism that have a similarity of demanding the strings in multiples of the bit size. The difference between the two Encryption techniques is in execution time that is based on the ASCII value. In terms of speed, the experimental results demonstrate that the AES algorithm is 200 to 300 milliseconds faster than Blowfish. But based on the size of data disparities across the algorithms evaluated and the result is both AES and Blowfish algorithms tended to be about the same length. Henceforth the performance must be analysed based on the storage of data and resources for both the process of decryption and encryption.

Owen Lo [10] designs the PRESENT algorithm that furnishes the lower consumption of power than the traditional symmetric_encryption mechanisms. This algorithm is one of the light_weigt_encryption techniques that holds the operation of 31 rounds for decrypting and encrypting a single data block. Scheduling of keys, adding the function of round key, substitution S-box and permutation are the distinct operations that are carried out in each round of the process. The storage space for the PRESENT algorithm is higher henceforth Ameer .N.Abdulraheem [9] introduces the hybrid from Cat and Henon chaotic maps in combination with the PRESENT algorithm. This algorithm utilizes the proposed chaotic keys generator along with the PRESENT algorithm for optimizing the storage and dynamic memory. The process of the PRESENT algorithm is similar but the author integrates the 2D cat and 2D henon maps that also increases the throughput when compared with the PRESENT algorithm. This proposed mechanism improves the security with a higher level of encryption for transmitting the data in the communication network.

The proposed Logistic Map and 3D Chaotic Multi-Scroll Lorenz attractor (LMLA) that incurs the PRESENT algorithm for making the data more secure during the transmission. It also utilizes a lesser amount of resources in the process of decryption and encryption. This hybrid LMLA produces higher throughput than the existing traditional encryption standards.

III. CATEGORIZATION OF DISTINCT CYBER-ATTACKS

The cyber-attacks are broadly categorized into assault against the person, property, agencies and society. This section furnishes the detailed description of the several cyber-assaults as depicted in Fig. 2.

A. *Attack against Individual*

This type of attack incurs the spoofing of email, defamation and stalking. Spoofing of mail is the method of constructing email messages by impersonating the identity of a correspondent. It depicts the email's origin as being different from where it actually came from. The senders of this email are always anonymous. Defamation is accusing someone with the intention of lowering that person's standing among other people in society, causing him to be ignored or or subjecting him to hatred, scorn, or ridicule. When an assailant stalks a victim around the internet, sending threatening messages to the victim on multiple social media platforms that the victim frequents [5].

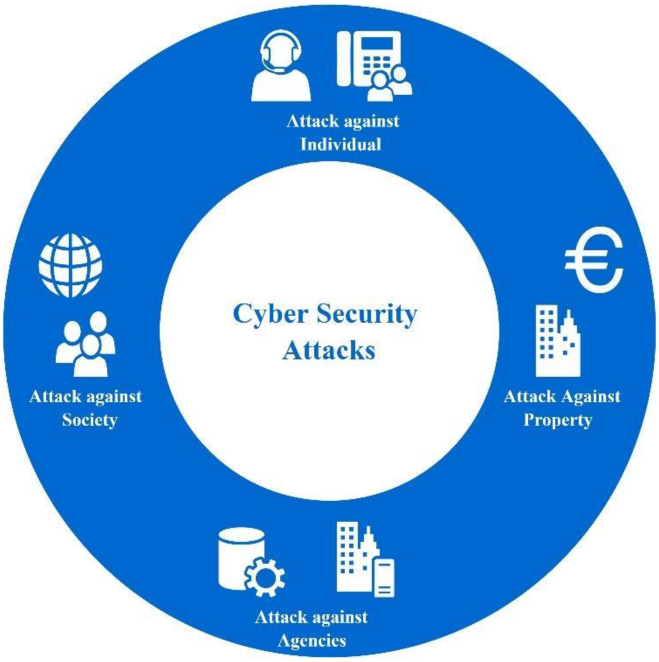


Fig. 2 Categorization of cyber assault

B. *Attack against property*

The assault against property incurs fraud in credit card, crimes in intellectual property and theft of internet time. Credit card fraud refers to the electronic fraud and deceit, which are the most lucrative transactions. A crime is any illegal conduct that deprives the owner of all or part of his human rights. Software piracy, copyright infringement, trademark and service mark infringement, and computer source code theft are examples of this sort of crime. It essentially falls under the heading of hacking. It is exploited by an unofficial user of internet hours that have been paid for by another user [5].

C. *Attack against agencies*

The assault against agencies incurs Denial_of_Service attack, assault by viruses and logic bomb. Denial_of_service is the act of restricting access over a service for the authorized user due to the intruders. A computer virus is a sort of malware that replicates itself by inserting copies of itself into other computer programmes, data files, or the hard drive's boot sector when it is run. A logic bomb is a piece of code that has been deliberately placed into a system. The code is activated when certain criteria are met, and it performs various nefarious actions [5].

D. *Attack against agencies*

A forgery is indeed a crime committed when a perpetrator distorts a document saved in electronic form. Computer systems are the target of criminal activity in this example, but they can also be employed as tools for committing forgery [5].

IV. PROPOSED METHODOLOGY

This section furnishes the detailed description of the PRESENT algorithm, general algorithm for implementation that incurs adding round key, substitution box, permutation box and the scheduling of key, chaotic encryption includes 3D Multi Scroll Chaotic System and logistic maps and finally the experimental setup.

A. *PRESENT Algorithm*

PRESENT algorithm is a kind of symmetric key cypher that uses a block cypher algorithm. In 2007, it flourished in Orange Laboratories. Then, in 2012,. "[Ultra-lightweight block cipher].suitable for lightweight cryptography, which is intended for deployment in resource-limited situations" [13] said the International Standards Organization.

The technique is employed in devices with limited memory and low power requirements (such as the Internet of Things devices). Data and keys are used to implement this technique. The algorithm for encryption and decryption accepts 64-bit blocks of data as input. An 80-bit or a 128-bit key is utilised to perform an action. Some researchers utilised the 80-bit key and predicted that the 128-bit key would be impractical in actual applications, therefore it was prioritised above the 128-bit key [14]. If the degree of security needed by the applications is high enough, academics have suggested that a larger key size should be used. Since its introduction in 2007 with several lightweight models, the PRESENT method has been a major step forward for lightweight cryptography [16].

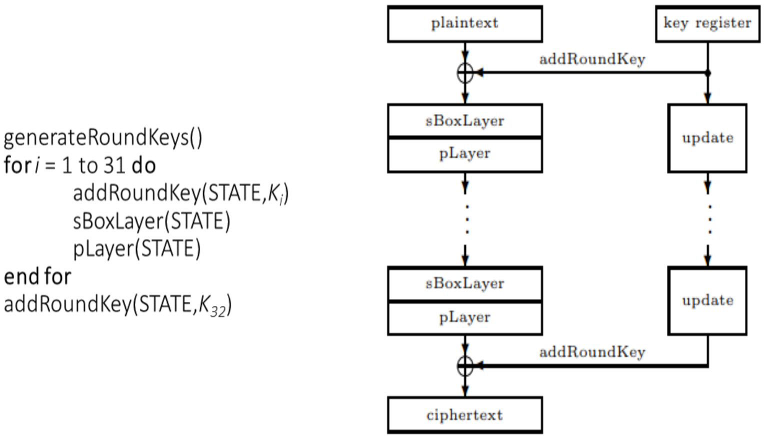
B. *General algorithm implementation*

There are 31 rounds of operations in the PRESENT algorithm that must be completed in order to achieve 64-bit data encryption or decryption, each round containing multiple difficult fundamental processes as illustrated in Fig. 3 [9].

*1) Add a Round Key:*The XOR operation for a 64-bit data

a block with 64 bits of a key for each round is called adding the Round key. First, an 80-bit user-defined key is utilised in the method whereas future rounds use key values assigned by Key Scheduling. Adding a circular key is shown in equation 1 [9].

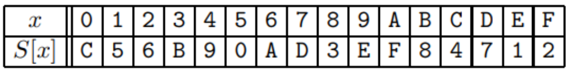
$$b_j \rightarrow b_j \oplus k_j^i \qquad (1)$$



```
generateRoundKeys()
for i = 1 to 31 do
        addRoundKey(STATE,$K_i$)
        sBoxLayer(STATE)
        pLayer(STATE)
end for
addRoundKey(STATE,$K_{32}$)
```

Fig. 3 Process of PRESENT algorithm [9]

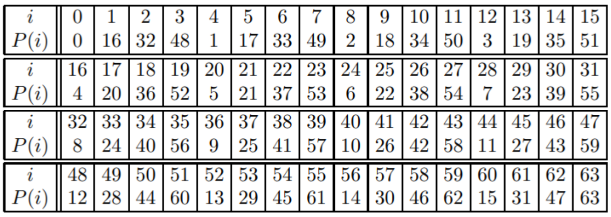
2) *Substitution-box Layer:* PRESENT's.algorithm's S-Box table stores the results of a 4-bit replacement of inputs after the Add Round Key procedure. Data blocks of 64 bits are separated into sixteen values each consisting of four bits, and each value is decided by the addition round its output. The S-Box table replaces the value of the 16-segment block with the S-Box table's value. As an example, if (C) is input as (C) in hexadecimal, the S-Box table will return (C) (4). Fig. 4 [9] depicts the inputs and outputs of a single S-box.



x	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F
$S[x]$	C	5	6	B	9	0	A	D	3	E	F	8	4	7	1	2

Fig. 4 Inputs and outputs of S-box [9]

3) *Permutation box:* The S-box is immediately followed by the P-box. The Permutation feature is utilised to reorder the data sections in this procedure. Those bits of the mixed output data that have been rearranged are encrypted again in the next step of processing. The construction of the P function is seen in Fig. 5 [9].



i	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
$P(i)$	0	16	32	48	1	17	33	49	2	18	34	50	3	19	35	51
i	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31
$P(i)$	4	20	36	52	5	21	37	53	6	22	38	54	7	23	39	55
i	32	33	34	35	36	37	38	39	40	41	42	43	44	45	46	47
$P(i)$	8	24	40	56	9	25	41	57	10	26	42	58	11	27	43	59
i	48	49	50	51	52	53	54	55	56	57	58	59	60	61	62	63
$P(i)$	12	28	44	60	13	29	45	61	14	30	46	62	15	31	47	63

Fig. 5 Construction of P function [9]

4) *Scheduling the Key:* The PRESENT Algorithm Accepts either 80-bit or 128-bit key lengths for its inputs. In any case, the 80-bit key variant is what we're concentrating on. The user-supplied key (k79,k78... k0) is stored in the key (K). There are 64 leftmost bits in the current K register contents in round i's round key of 64-bit = 63,62...0. So,in round I XORing the Round Counter Countdown with the intermediate bits from the process of extracting Ki, which represents the round key, updates a key register every round as depicted in Fig. 6 [9]. After that, a random selection of 64 bits from the entire value is used to generate the round key [9].

$$[\mathtt{k}_{79}\mathtt{k}_{78}\ldots\mathtt{k}_{1}\mathtt{k}_{0}] = [\mathtt{k}_{18}\mathtt{k}_{17}\ldots\mathtt{k}_{20}\mathtt{k}_{19}]$$

$$[\mathtt{k}_{79}\mathtt{k}_{78}\mathtt{k}_{77}\mathtt{k}_{76}] = S[\mathtt{k}_{79}\mathtt{k}_{78}\mathtt{k}_{77}\mathtt{k}_{76}]$$

$$[\mathtt{k}_{19}\mathtt{k}_{18}\mathtt{k}_{17}\mathtt{k}_{16}\mathtt{k}_{15}] = [\mathtt{k}_{19}\mathtt{k}_{18}\mathtt{k}_{17}\mathtt{k}_{16}\mathtt{k}_{15}] \oplus \mathtt{round\_counter}$$

Fig. 6 Process of Key scheduling [9]

The PRESENT method generates keys by using unique round keys on each round. In the beginning, it rotates left by 61 bits for the first time. Using S-boxes, the leftmost key is sent 4 bytes for an 80-bit key, but if the key is 128 bits, the leftmost key is provided 8 bytes for a 128-bit key.

C. *Chaotic Encryption*

Dynamic systems have been an exciting topic of study for researchers as technology has progressed. It is highly regarded in the field of message authentication and security. Dynamic systems make it impossible for attackers to anticipate the output of their attacks. High-dimensional dynamic systems using chaos-based functions have been developed to improve security. The data encryption technique relies on a high-dimensional chaotic map. In terms of invariant measure, dynamical and security without period doubling, the high-dimensional chaotic maps performed well [15].

Chen system and Lorentz system are two examples of three-dimensional chaotic systems. It is argued that the system is in disarray when the values of the parameters are 20 (a), 14 (b), 10.6 (c), and 2.8 (h). When compared to other systems like the Lorenz (1.497) and Chen (1.0742) systems, the Lyapunov exponent is the highest at 2.355. At a large Lyapunov exponent, the paths separated rapidly.

1) 3D Multi Scroll Chaotic System: The dynamics of 3D multi-scroll chaotic systems may be more complicated than those of ordinary chaotic systems with mono-scroll attractors.

$x = a(y - x)$ (2) $y = bx + cy - xz$
(3)
$z = x2 - hz$ (4)

The general equation (2-4) [9] is changed by the derivative characteristics to produce Multi scroll 3D fractional/integer order chaotic systems. The equation (5-7) [9] is the chaotic system that may show multi-scroll features.

$$\frac{d^q x_1}{dt^q} = -ax_1 + bx_2x_3 \quad (5)$$

$$\frac{d^q x_2}{dt^q} = -cx_2^3 + dx_1x_3 \quad (6)$$

$$\frac{d^q x_3}{dt^q} = ex_3 - fx_1x_2 + p_1 tanh(x_2 + g) \quad (7)$$

2) Logistic maps: Initial sensitivity, randomness, and extreme unpredictability are all characteristics of chaotic systems. Equation (8) [9] provides the mathematical formula for logistic chaotic maps.

$Xn + 1 = \mu Xn(1 - Xn)$ *(8)*

Hyper-chaotic multi-scroll attractors and Logistic maps are only two examples of the chaotic processes that go into this essential generation. It is important to follow the sequence of the innovative hybrid chaotic key generation in order.

Algorithm for proposed Logistic Map and 3D Chaotic Multi-Scroll Lorenz attractor (LMLA):
Input a=10;b=14, c=10.6 ,h= 2.8.
[X_1(0)] = 0.1; [X_2(0)] = 0.1; [X_3(0)] = 0.6
***Output**: (32) secret key with (128) bit length*

```
Begin
// 32 Round Key for PRESENT algorithm
// Logistics map

$Xn + 1 = \mu Xn(1 - Xn)$

// 3D Multiscroll chaotic map
$\frac{d^q x_1}{dt^q} = -ax_1 + bx_2x_3$
```

```
$\frac{d^q x_2}{dt^q} = -cx_2^3 + dx_1x_3$
$\frac{d^q x_3}{dt^q} = ex_3 - fx_1x_2 + p_1 tanh(x_2 + g)$

// apply Concatenate process

//apply XOR Process

//Generate the Key

END for

End
```

D. *Experimental Setup*

ESP32 Microcontroller with 40 MHz maximum operating frequency, 520 kilobytes of SRAM, 32-bit architecture, 3.3V operating voltage, and two cores is utilised in our experiment to apply cryptography on gathered data and prove which approach is more efficient. The ESP32 Microcontroller has a PRESENT lightweight algorithm and a proposed chaotic key generator LMLA technique. Data from the (IoT) model is encrypted or decrypted by this Microcontroller. An algorithm's performance will be optimised by thoroughly testing the implementation of cryptography in this experiment [9].

A Proposed key is then used to test the PRESENT Algorithm implementations. Using globally accepted performance measures, we can evaluate the effectiveness of our implementation efforts.

1) Resources employed for Implementation: The term "resources used" refers to the quantity of logical resources that will be consumed by the implementation. These resources may vary depending on the device. The microcontroller in this project is 32-bit. For example, the resources are given by the quantity of storage and RAM required in that process. Microcontroller parameters that are critical for analysis are listed below [9].

Special function registers are stored in a 520 KiB SRAM on the ESP32 microcontroller [9].

Data storage: The ESP32 microcontroller includes an inbuilt flash memory of 4MB, which is used to store information [9].

V. PERFORMANCE ANALYSIS

The performance of the proposed PRESENT Algorithm with LMLA is analysed based on the utilization of resources, time of execution in ms and the throughput in bps. The volume of conceptual resources that the implementation will employ is alluded to as the resource utilization. These resources may vary depending on the device. A 32-bit microcontroller has been used. The amount of Memory space (storage) and RAM required in that process provides the resources for that process. The execution period is the amount taken for completing the decryption and encryption processes.

By evaluating the performance of algorithm design over time, throughput is a critical factor to examine. It determines the amount of data that the algorithm will process and the number of bits per second that the digital system will process. The throughput can be evaluated by the equation 9 [9].

$$Throughput = number\ bits \cdot frequency \qquad (9)$$

Fig. 7 depicts that during the process of encryption, the memory allocation of the proposed PRESENT Algorithm with LMLA is lower compared to the traditional encryption techniques.

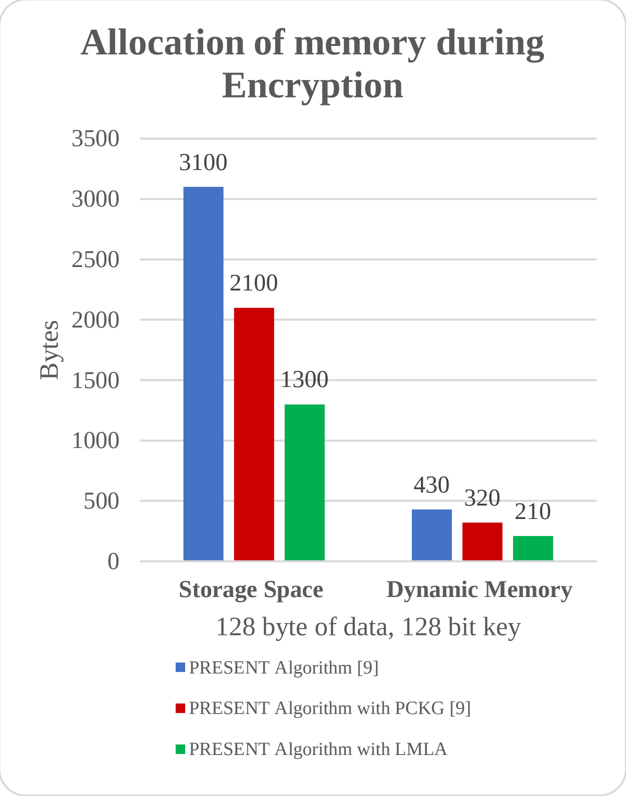


Fig. 7 Allocation of memory during Encryption

The storage space of the proposed PRESENT LMLA algorithm is 58.064% lower compared to the PRESENT Algorithm and 38.095% lower compared to the PRESENT Algorithm with PCKG. The dynamic memory of the proposed PRESENT LMLA algorithm is 51.162% lower compared to the PRESENT Algorithm and 34.375% lower compared to the PRESENT Algorithm with PCKG.

Fig. 8 depicts that during the process of decryption, the memory allocation of the proposed PRESENT Algorithm with LMLA is lower compared to the traditional techniques. The storage space of the proposed PRESENT LMLA algorithm is 54.884% lower compared to the PRESENT Algorithm and 40.594% lower compared to the PRESENT Algorithm with PCKG. The dynamic memory of the proposed PRESENT LMLA algorithm is 56.25% lower compared to the PRESENT Algorithm and 53.571% lower compared to the PRESENT Algorithm with PCKG.

The Fig. 9 depicts the execution time for both decryption and encryption process of the proposed PRESENT algorithm with LMLA is lower compared to the traditional encryption techniques. The time of execution of the proposed PRESENT LMLA algorithm during encryption is 29.906% lower compared to the PRESENT Algorithm and 23.217% lower compared to the PRESENT Algorithm with PCKG. The time of execution of the proposed PRESENT LMLA algorithm during decryption is 33.752% lower compared to the PRESENT Algorithm and 16.203% lower compared to the PRESENT Algorithm with PCKG.

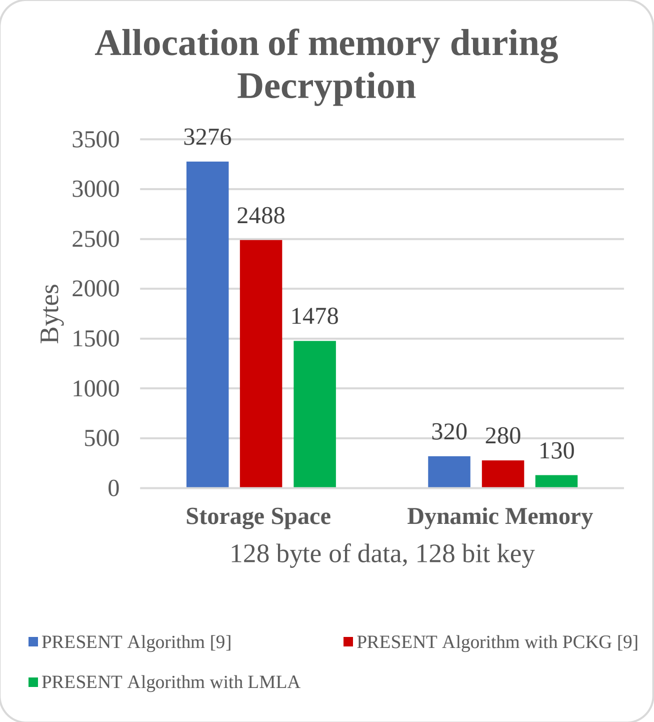


Fig. 8 Allocation of memory during decryption

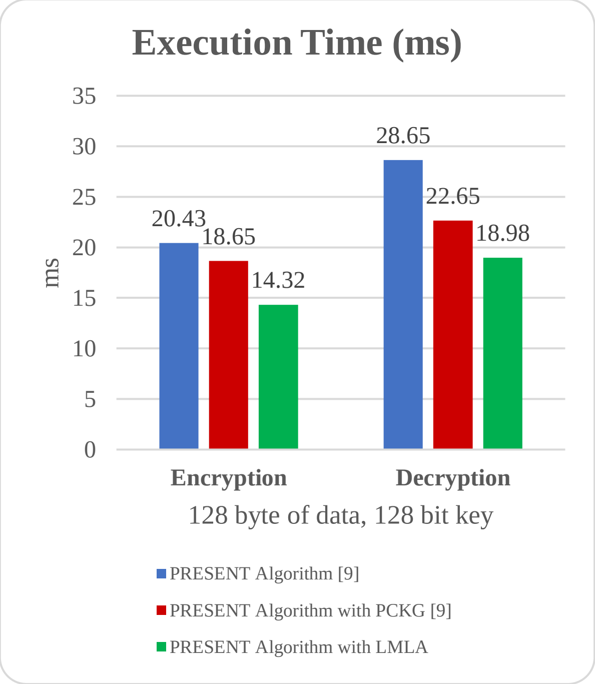


Fig. 9 Execution time for Encryption and Decryption

The Fig. 10 depicts the execution throughput for both decryption and encryption process of the proposed PRESENT algorithm with LMLA is higher compared to the traditional encryption techniques. The throughput of the proposed PRESENT LMLA algorithm during encryption is 16.276% higher compared to the PRESENT Algorithm and 8.285% higher compared to the PRESENT Algorithm with PCKG. The throughput of the proposed PRESENT LMLA algorithm during decryption is 35.763% higher compared to the PRESENT Algorithm and 18.737% higher compared to the PRESENT Algorithm with PCKG.

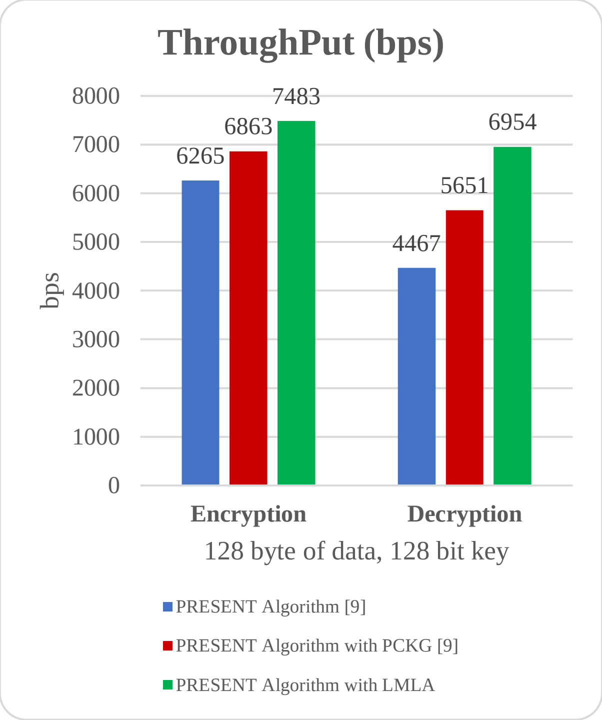


Fig. 10 Throughput for Encryption and Decryption

VI. CONCLUSION

In this research, a technique for creating chaos keys (LMLA) that combines a three-dimensional chaos system (logistic maps and 3D Multi-Scroll Lorenz Attractor) with the PRESENT algorithm to enhance its security and offer a high degree of encryption in Internet of Things (IoT) devices that transfer data. In addition, it is compared to the original PRESENT in terms of throughput, processing time, memory use, and storage space utilization. In comparison to other algorithms tested by NIST, the PRESENT Algorithm with a (LMLA) technique performed better and yielded greater randomness outcomes. The storage space of the proposed PRESENT LMLA algorithm during encryption is 58.064% lower compared to the traditional encryption standards and in the process of decryption the LMLA technique produces 54.884% lower compared to the existing algorithms. The dynamic memory of the proposed LMLA scheme furnishes 51.162% and 56.25% lower compared to the traditional encryption standards for both encryption and decryption. The execution time of the proposed LMLA scheme furnishes 29.906% and 33.752% lower compared to the traditional encryption standards for both encryption and decryption. The throughput of the proposed LMLA scheme furnishes 16.276% and 35.763% higher compared to the traditional encryption standards for both encryption and decryption.

REFERENCES

[1] Jagpreet Kaur, K .R. Ramkumar, “The recent trends in cyber security: A review”, Journal of King Saud University - Computer and Information Sciences, 2021, DOI:10.1016/j.jksuci.2021.01.018.

[2] Yuchong Li, Qinghui Liu, “A comprehensive review study of cyber-attacks and cyber security; Emerging trends and recent developments”, Energy Reports, Vol.7, pp. 8176-8186, 2021, DOI: 10.1016/j.egyr.2021.08.126.

[3] K. Shaukat, S. Luo, V. Varadharajan, I. A. Hameed and M. Xu, "A Survey on Machine Learning Techniques for Cyber Security in the Last Decade," in IEEE Access, vol. 8, pp. 222310-222354, 2020, doi: 10.1109/ACCESS.2020.3041951.

[4] S. Z. Sajal, I. Jahan and K. E. Nygard, "A Survey on Cyber Security Threats and Challenges in Modem Society," 2019 IEEE International Conference on Electro Information Technology (EIT), 2019, pp. 525-528, doi: 10.1109/EIT.2019.8833829.

[5] A. S. Choudhary, P. P. Choudhary and S. Salve, "A Study On Various Cyber Attacks And A Proposed Intelligent System For Monitoring Such Attacks," 2018 3rd International Conference on Inventive Computation Technologies (ICICT), 2018, pp. 612-617, doi: 10.1109/ICICT43934.2018.9034445.

[6] A. Murtaza, S. J. Hussain Pirzada and L. Jianwei, "A New Symmetric Key Encryption Algorithm With Higher Performance," 2019 2nd International Conference on Computing, Mathematics and Engineering Technologies (iCoMET), 2019, pp. 1-7, doi: 10.1109/ICOMET.2019.8673469.

[7] Mahalakshmi.J, K.Kuppusamy, “A Block Cipher based Cryptographic Algorithm to enhance the Data Security”, International Journal of Applied Engineering Research, Vol. 10 No.55, 2015.

[8] J. Raigoza and K. Jituri, "Evaluating Performance of Symmetric Encryption Algorithms," 2016 International Conference on Computational Science and Computational Intelligence (CSCI), 2016, pp. 1378-1379, doi: 10.1109/CSCI.2016.0258.

[9] A. N. Abdulraheem and B. M. Nema, "Secure IoT Model Based on PRESENT Lightweight Modified and Chaotic Key Generator," 2020 1st. Information Technology To Enhance e-learning and Other Application (IT-ELA, 2020, pp. 12-18, doi: 10.1109/IT-ELA50150.2020.9253079.

[10] Owen Lo, William J. Buchanan, and Douglas Carson, “Correlation Power Analysis on the PRESENT Block Cipher on an Embedded Device”, In Proceedings of the 13th International Conference on Availability, Reliability and Security ARES, Association for Computing Machinery, New York, USA, Article. 21, pp. 1–6. DOI:10.1145/3230833.3232801.

[11] V. A. Greiman, "Cyber attacks: the fog of identity," 2016 International Conference on Cyber Conflict (CyCon U.S.), 2016, pp. 1-13, doi: 10.1109/CYCONUS.2016.7836617.

[12] M. B. Yassein, S. Aljawarneh, E. Qawasmeh, W. Mardini and Y. Khamayseh, "Comprehensive study of symmetric key and asymmetric key encryption algorithms," 2017

International Conference on Engineering and Technology (ICET), 2017, pp. 1-7, doi: 10.1109/ICEngTechnol.2017.8308215.

[13] “INTERNATIONAL STANDARD ISO / IEC Information technology — Security techniques — Lightweight cryptography,” vol. 2012, 2012.

[14] A. Bogdanov, L. R. Knudsen, G. Leander, C. Paar, and A. Poschmann, “PRESENT: An Ultra-Lightweight Block Cipher”, In: Paillier P., Verbauwhede I. (eds) Cryptographic Hardware and Embedded Systems - CHES 2007. CHES 2007. Lecture Notes in Computer Science, vol 4727. Springer, Berlin, Heidelberg. DOI:10.1007/978-3-540-74735-2_31.

[15] Durga R, and Poovammal E,”Generation of RAESSES Hash Function for Medical Blockchain Formation Based on High Dynamic Chaotic Systems”,International Journal of Advanced Science and Technology, vol. 29, no.6, pp. 8427-8440, 2020.

[16] S. B. Sadkhan and A. O. Salman, "A survey on lightweight-cryptography status and future challenges," 2018 International Conference on Advance of Sustainable Engineering and its Application (ICASEA), 2018, pp. 105-108, doi: 10.1109/ICASEA.2018.8370965.

[17] Kothai G, Poovammal E,” Performance Analysis of Stationary and Deterministic AODV Model,” International Journal of interactive mobile technologies, vol:14, no: 17, 2020, DOI:10.3991/ijim.v14i17.16643.

[18] G. Kothai, E. Poovammal, Gaurav Dhiman, Kadiyala Ramana, Ashutosh Sharma, Mohammed A. AlZain, Gurjot Singh Gaba, Mehedi Masud, "A New Hybrid Deep Learning Algorithm for Prediction of Wide Traffic Congestion in Smart Cities", *Wireless Communications and Mobile Computing*, vol. 2021, Article ID 5583874, 13 pages, 2021,DOI : 10.1155/2021/5583874.