IJARIIT INTERNATIONAL JOURNAL OF ADVANCE RESEARCH, IDEAS AND INNOVATIONS IN TECHNOLOGY

ISSN: 2454-132X
Impact Factor: 6.078

(Volume 7, Issue 2 - V7I2-1317)
Available online at: https://www.ijariit.com

Authentication encryption scheme using leopard and chaotic tent map algorithm for smart grid

Ravi Duddi
raviduddi1@gmail.com
Adesh Institute of Engineering and Technology, Faridkot, Punjab

Puneet Jain
puneetjain988@gmail.com
Adesh Institute of Engineering and Technology, Faridkot, Punjab

ABSTRACT

Smart Grid (SG) has gain popularity due to reliability, efficiency, and sustainability. They transmit periodically collected reading. The reading contains very sensitive data such as personal information and geometric locations. Therefore, transmission and storage of data have many security challenges such as eavesdropping and tampering attacks. This proposes a novel authentication encryption scheme that provides confidentiality, integrity, and authentication of the data. To achieve these objectives, we have hybrid the LEOPARD and chaotic tent map algorithm. The LEOPARD algorithm provides confidentiality and the chaotic tent map algorithm gives the authentication tag to verify the data integrity and authentication. The algorithm is simulated in MATLAB. The experimental results show that the proposed algorithm provides better results as compared to the existing algorithms in terms of PSNR, execution time, and security.

Keywords: *Chaotic Tent Map, LEOPARD, AES, Smart Grid, Security.*

1. INTRODUCTION

Smart Grid (SG) enhances the existing power grid by providing the multi-directional information flow between any two or more units in the system. It collects the appropriate data from the smart meters and communicates the information to substations. This data is used for load forecasting, load balancing, and bill generation [1]. However, the smart grid infrastructure is faced with various security threats such as data attacks, natural disasters, theft, and terrorism [2]. Thus, any violation in the data due to these threats negatively impacts the smart grid network. In this paper, we have worked on data attacks. To overcome data attacks, cryptography and steganography algorithms are used [3]. The cryptography algorithms encrypt the secret data using a private key to secure it. On the other side, steganography algorithms hide the secret data in the cover media to secure it [4]. In this work, we have worked on cryptography algorithms due to less overhead as compared to steganography (steganography algorithm required cover media and limited embedding capacity). Cryptography algorithms are classified into symmetric and asymmetric algorithms based on the key. In symmetric algorithms, the same key is used for encryption and decryption purposes whereas, in asymmetric algorithms, a key pair (public and private key) is used to encrypt and decrypt the secret data. Further, based on the block size, the symmetric algorithm is classified into block cipher and stream cipher. In the last, a block cipher is sub-classified into substitution-permutation network and Feistel network [5].

In the literature, various security algorithms are used to provide data security in the smart grid. The most popular algorithms are AES [6], Blowfish [7], 3DES [8], chaotic map [9], ChaCha [10], Homomorphic encryption [11], and RSA [12]. Out of these algorithms, AES, Blowfish, and 3DES are block cipher that processes the secret data in the fixed block and provides confidentiality, encrypts a large amount of data. Further, the ChaCha algorithm comes under stream cipher in which XOR operation is performed between data and key to encrypt the secret data. The security of the stream cipher depends on the randomness of the key and suitable for encrypting a small amount of data. In the last, Homomorphic encryption and RSA algorithm comes under asymmetric algorithms that provide confidentiality, authentication but take long execution time to achieve it. Further, various hybrid approaches are proposed in order to enhance security. Reza et al. [10], hybrid the ChaCha, chaotic map, and asymmetric algorithm to provide encryption and authentication but this approach consumes large execution time due to bit-level operation, multiplication, and modular operation. In order to overcome these limitations, in this paper, we have designed an authentication encryption scheme that provides confidentiality, integrity, authentication, and takes lesser execution time. To achieve this goal, we have used the LEOPARD and Chaotic Tent Map algorithm in our work.

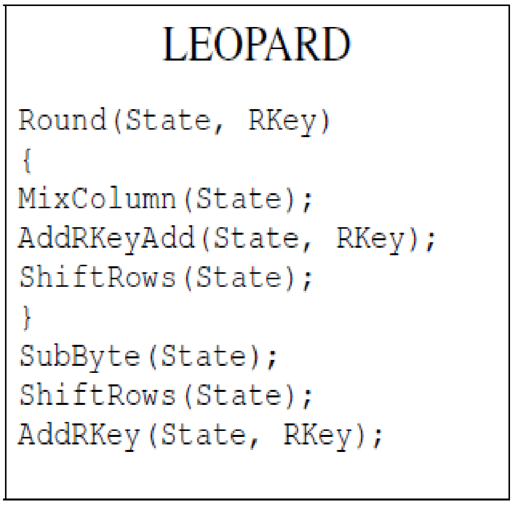
The rest of the paper as follows. Section 2 gives an overview of the LEOPARD algorithm and chaotic map algorithm. Section 3 explains the proposed algorithm. Section 4 shows the experimental results performed for the proposed algorithm. In last, a conclusion is drawn in Section 5.

2. LEOPARD AND CHAOTIC TENT MAP ALGORITHM

In this section, we have explained the LEOPARD and chaotic tent map algorithm to understand the proposed authentication encryption scheme.

2.1 LEOPARD Algorithm

Lightweight Encryption Operation Permutation Addition Rotation and Diffusion (LEOPARD) is a Permutation-Substitution network (PSN) algorithm [13]. It is based on the standard cryptography algorithm AES. The LEOPARD algorithm is 128-bit block size. It requires a 128-bit key and 10 rounds for encrypt a single block. The pseudocode for the LEOPARD algorithm is shown in Figure 2.1.



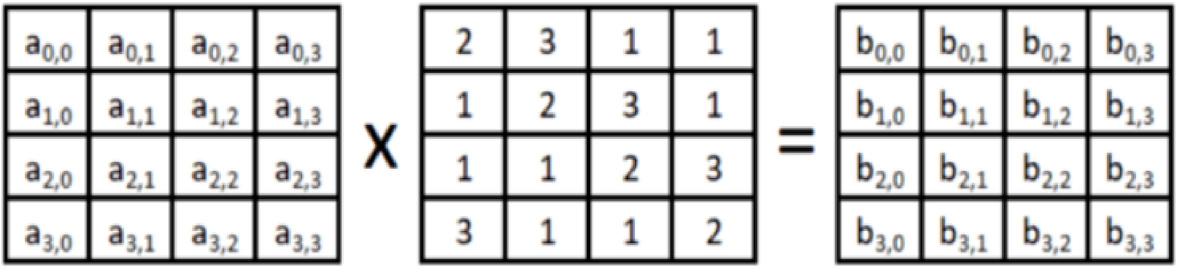
```
LEOPARD

Round(State, RKey)
{
MixColumn(State);
AddRKeyAdd(State, RKey);
ShiftRows(State);
}
SubByte(State);
ShiftRows(State);
AddRKey(State, RKey);
```

Fig. 2.1: Pseudocode for the LEOPARD Algorithm

LEOPARD algorithm processes the input data into blocks. If the data is lesser than block size then zero padding is done. Initially, the data and key are read and XOR Operation is performed on it. After that, for 9 rounds three-layer operation is performed known as Mix column, Add round key and shift row. In the last round (10th), sub-byte, shift row, and add round key operation performed to encrypt the secret data. The 128-bit data and key is represent in 4 × 4 matrix for the perform the operations. Next, we have explained the layers of LEOPARD algorithm [14].

- Mix Column Layer

In this step, the secret data matrix is multiplied with constant 4X4 matrix, as shown in Figure 2.2. This step is also providing the avalanche effect in the encryption scheme. The constant matrix contains 4 elements such as [2 3 1 1]. The multiplication with 2 and 3 required 2 look-up table with each table has 256 elements



$$\begin{array}{|c|c|c|c|}\hline a_{0,0} & a_{0,1} & a_{0,2} & a_{0,3} \\ \hline a_{1,0} & a_{1,1} & a_{1,2} & a_{1,3} \\ \hline a_{2,0} & a_{2,1} & a_{2,2} & a_{2,3} \\ \hline a_{3,0} & a_{3,1} & a_{3,2} & a_{3,3} \\ \hline \end{array} \times \begin{array}{|c|c|c|c|}\hline 2 & 3 & 1 & 1 \\ \hline 1 & 2 & 3 & 1 \\ \hline 1 & 1 & 2 & 3 \\ \hline 3 & 1 & 1 & 2 \\ \hline \end{array} = \begin{array}{|c|c|c|c|}\hline b_{0,0} & b_{0,1} & b_{0,2} & b_{0,3} \\ \hline b_{1,0} & b_{1,1} & b_{1,2} & b_{1,3} \\ \hline b_{2,0} & b_{2,1} & b_{2,2} & b_{2,3} \\ \hline b_{3,0} & b_{3,1} & b_{3,2} & b_{3,3} \\ \hline \end{array}$$

Fig. 2.2: Mix Column Layer

- Add Round Key Layer

In the add round key step, in each round the key is updated and generated on the fly. The key matrix 4th column is passed from the s-box and XOR operation is done with a constant with original first column of the key which produced first column of the new key matrix. Further, new key matrix first column XOR with original second column to generate second column of the new key matrix and this process executed for the remaining column.

- Shift Row Layer

In this step, the data matrix rows are circular shifted according to the index of the row. For example, the first row 0 times, second row 1 byte, third row 2 byte and, fourth row 3byte left circular rotated as shown in Fig. 2.2.

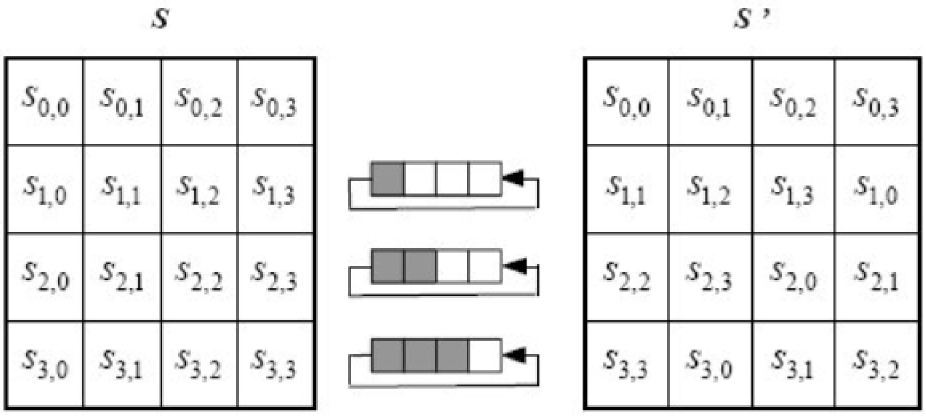

S
S '
$s_{0,0}$ $s_{0,1}$ $s_{0,2}$ $s_{0,3}$
$s_{1,0}$ $s_{1,1}$ $s_{1,2}$ $s_{1,3}$
$s_{2,0}$ $s_{2,1}$ $s_{2,2}$ $s_{2,3}$
$s_{3,0}$ $s_{3,1}$ $s_{3,2}$ $s_{3,3}$
$s_{0,0}$ $s_{0,1}$ $s_{0,2}$ $s_{0,3}$
$s_{1,1}$ $s_{1,2}$ $s_{1,3}$ $s_{1,0}$
$s_{2,2}$ $s_{2,3}$ $s_{2,0}$ $s_{2,1}$
$s_{3,3}$ $s_{3,0}$ $s_{3,1}$ $s_{3,2}$

Fig. 2.2: Shift Row Layer

- Sub-Byte Layer

In the sub-byte step, each element 8 bits are substitute with other 8 bits and this should be bijective mapping (one to one mapping) as shown in Fig. 2.3. The original 8 bits are multiplied with a constant polynomial and further affine transformation is taken. In the software level, 2^8=256 combination look-up table is formed for substitute the data.

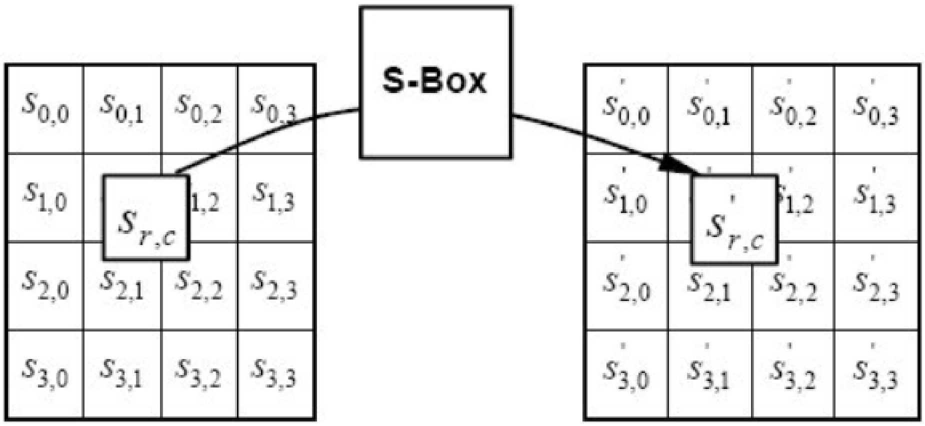

S-Box
$s_{0,0}$ $s_{0,1}$ $s_{0,2}$ $s_{0,3}$
$s_{1,0}$ $s_{r,c}$ $s_{1,2}$ $s_{1,3}$
$s_{2,0}$ $s_{2,1}$ $s_{2,2}$ $s_{2,3}$
$s_{3,0}$ $s_{3,1}$ $s_{3,2}$ $s_{3,3}$
$s'_{0,0}$ $s'_{0,1}$ $s'_{0,2}$ $s'_{0,3}$
$s'_{1,0}$ $s'_{r,c}$ $s'_{1,2}$ $s'_{1,3}$
$s'_{2,0}$ $s'_{2,1}$ $s'_{2,2}$ $s'_{2,3}$
$s'_{3,0}$ $s'_{3,1}$ $s'_{3,2}$ $s'_{3,3}$

Fig. 2.3: Sub-Byte Step

In the proposed algorithm, the LEOPARD algorithm is used for data encryption. The LEOPARD algorithm execution time is reduced using the table splitting method. In the table splitting method, the sub-byte look-up table split into two halves. The first halve contains the data entry from 0 to 127 and second halve contains the data entry from 128 to 255. This method reduces the searching complexity from O(n) to O(n/2).

2.2 Chaotic Tent Map Algorithm

A chaotic system is a deterministic nonlinear dynamical system whose states change with iterations in a deterministic way [15]. The chaotic tent map is determined using Eq. (1).

$$x_{n+1} = \begin{cases} rx & x > 0.5 \\ r(1-x) & x \le 0.5 \end{cases} \qquad (1)$$

where $x_n \in (0, 1)$ and r ∈ (0, 2). r is known as the control parameter or bifurcation parameter. Here x_n is the state of the system at time n. x_{n+1} denotes the next state and n denotes the discrete-time.

3. PROPOSED ALGORITHM

The proposed algorithm provides encryption, authentication, and takes less execution time as compared to the existing algorithms. To achieve this goal, the encryption algorithm works under CCM mode that provides encryption and authentication. In addition, software optimization algorithms are used to reduce the execution time. The block diagram of the proposed encryption is shown in Figure 3.1. In the proposed algorithm, the secret data and key is read and given to the encryption algorithm that gives the encrypted data in the output. In the proposed algorithm, the LEOPARD algorithm is used for data encryption. After that, to generate the authentication tag, a 128-bit random key generated using the chaotic tent map algorithm. Next, an XOR operation is performed between secret data and random key. After that, the encrypted data works as a random key for the next block to perform XOR operation. The whole process is repeated for all blocks to generate a 128-bit authentication tag. The encrypted data and authentication tag is communicated from the transmitter side.

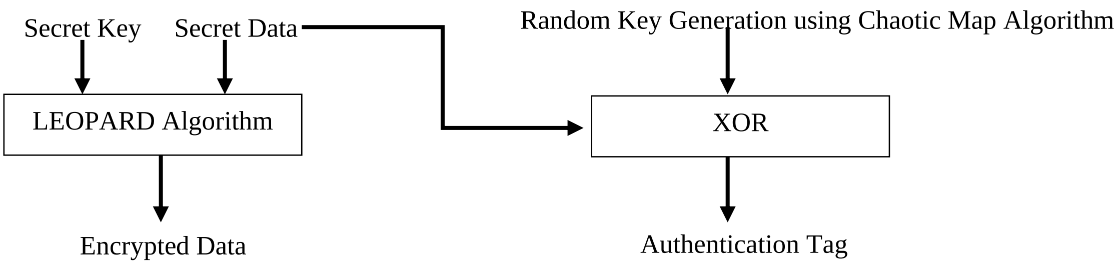


Fig. 3.1: Block Diagram of Data Encryption and Generate Authentication Tag

On the receiver side, the encrypted data and secret key is read and given to the decryption algorithm to determine the original secret data. After that, XOR operation performed between secret data and random key (the random key that generated on the transmitter side using the chaotic tent map algorithm) to generate the authentication tag on the receiver side. In last, authentication tags compared with transmitter authentication tag. If the tag value same then secret data authentication and integrity passed else failed. The block diagram for the decryption algorithm is shown in Figure 3.2.

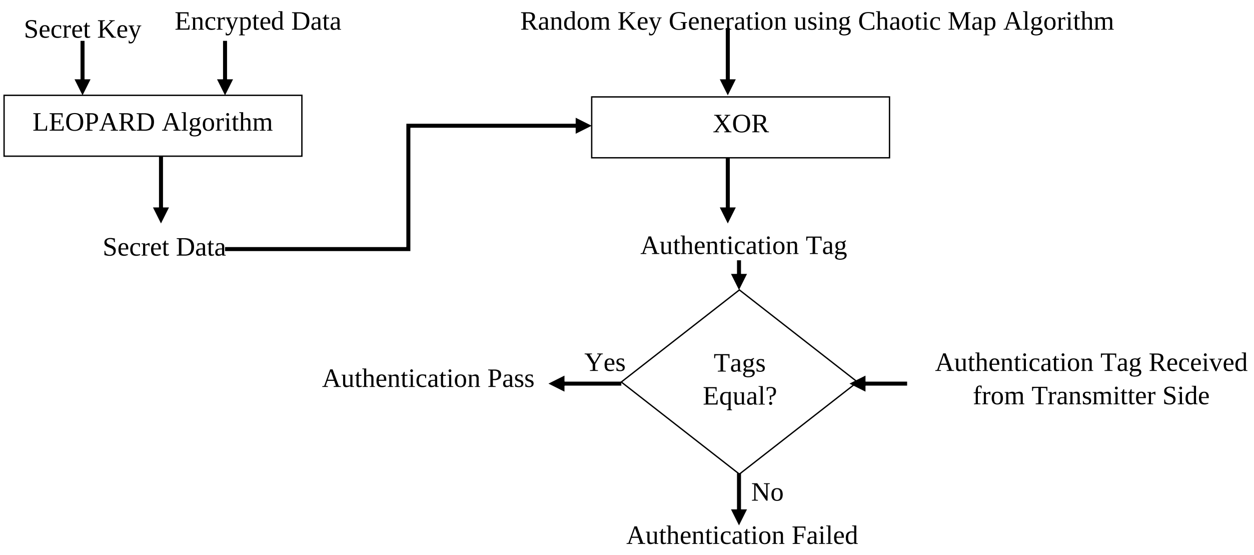


Fig. 3.2: Block Diagram of Data Decryption and Verification

4. EXPERIMENTAL RESULTS

This section shows the experimental results are performed for the proposed algorithm to validate it over the existing algorithms. The secret data is randomly generated. The algorithm is simulated in MATLAB and measured the various performance parameters for it.

4.1 Peak Signal to Noise Ratio (PSNR)

This parameter is used to measure the distortion in the encrypted data. In the ideal case, low value of PSNR gives better for the encrypted image and calculated using Equation (4.1-4.2) and measured in decibel [6].

$$PSNR = 10 \times \log_{10} \frac{Peak^2}{MSE} \qquad (4.1)$$

Here, Peak is peak value in the secret data and MSE is Mean Square Error and it is calculated using Eq. (4.2).

$$MSE = \frac{1}{J \times K} \sum_{m=1}^{J} \sum_{n=1}^{K} (X_{m,n} - Y_{m,n})^2 \qquad (4.2)$$

Here, J, and K defines as the row and column of the secret data. Table 4.1 shows the minimum PSNR between original and encrypted data.

Table 4.1: PSNR for the Proposed Algorithm

File	PSNR (in dB)
File1	12.61
File2	13.91

File3	14.60
File4	12.93
File5	13.09

4.2 Correlation Coefficient (CC)

This parameter measures the demographic changes between original and encrypted data. The CC is varies -1 to 1. The 1 value represents the original and encrypted data is same and -1 value represents the original and encrypted data are complement to each other. It is determined using Eq. (4.3)

$$CC=\frac{\sum_{m=1}^{J}\sum_{n=1}^{K}(A_{mn}-A_{mean})(B_{mn}-B_{mean})}{\sqrt{\sum_{m=1}^{J}\sum_{n=1}^{K}((A_{mn}-A_{mean})^2)\sum_{m=1}^{J}\sum_{n=1}^{K}(B_{mn}-B_{mean})^2}} \qquad (4.3)$$

whereas, AB denotes the original and encrypted data. JK represents the row and column of the data. In the last, mn denotes the subscripted variables. Table 4.2 shows that the proposed algorithm provides minimum correlation between original secret data and encrypted data.

Table 4.2: Correlation Coefficient for the Proposed Algorithm

File	Correlation Coefficient
File1	0.0036
File2	0.0123
File3	0.024
File4	0.036
File5	0.0045

4.3 Entropy

Entropy is simply the average (expected) amount of the information from the data. Information entropy is an important feature of randomness. Here, the entropy value is calculated by the equation (4.4).

$$E=-\sum_{i=1}^{n} p_i \log_2 p_i \qquad (4.4)$$

Where n number of different data values, p_i is probability of occurring the data value i. Table 4.3 shows that the proposed algorithm provides approximate similar entropy after encryption.

Table 4.3: Entropy for the Proposed Algorithm

File	Entropy for Secret Data	Entropy for Encrypted Data
File1	7.4105	7.9887
File2	7.3641	7.9880
File3	7.1303	7.9901
File4	7.5497	7.9899
File5	7.0238	7.9904

4.4 Execution Time

The total time spent for data encryption and to generate authentication tag. In the MATLAB, the execution time of the code is determined using the tic and toc command. Table 4.4 shows the execution time for the proposed algorithm. The results show that the proposed algorithm takes very less time for data encryption and to generate authentication tag.

Table 4.4: Execution Time for the Proposed Algorithm

File	Execution Time (in Seconds)
File1	1.31
File2	1.93
File3	1.30
File4	1.74
File5	1.31

4.5 Comparative Analysis

In this section, we have compared the proposed algorithm with the existing algorithms based on the various performance parameters in Table 4.5. The proposed algorithm provides lesser execution time with better security in terms of confidentiality and authentication.

Table 4.5: Comparative Analysis with the Existing Algorithms

Parameters	AES [6]	Proposed Algorithm
Execution Time (in Seconds)	2.42	1.52
PSNR (in dB)	12.84	12.64

Confidentiality	Yes	Yes
Authentication	No	Yes

5. CONCLUSION AND FUTURE SCOPE

The communication of the data in the smart grid network makes it prone to various attacks in the communication channel. The most popular attacks are eavesdropping, tempering, and denial of service. To overcome these attacks, cryptography algorithms are used. In this paper, an encryption authentication scheme is designed for the smart grid using the LEOPARD and chaotic tent map algorithm. The proposed algorithm provides encryption-authentication and takes less execution time as compared to the existing algorithms.

6. REFERENCES

[1] Otuoze, A. O., Mustafa, M. W., & Larik, R. M. (2018). Smart grids security challenges: Classification by sources of threats. *Journal of Electrical Systems and Information Technology*, *5*(3), 468-483.

[2] Goel, S., & Hong, Y. (2015). Security challenges in smart grid implementation. In *Smart Grid Security* (pp. 1-39). Springer, London.

[3] Mishra, R., & Bhanodiya, P. (2015, March). A review on steganography and cryptography. In *2015 International Conference on Advances in Computer Engineering and Applications* (pp. 119-122). IEEE.

[4] Kumar, A., & Raghava, N. S. (2019). Chaos-based steganography technique to secure information and integrity preservation of smart grid readings using wavelet. *International Journal of Computers and Applications*, 1-7.

[5] Rani, S., & Kaur, H. (2017). Technical review on symmetric and asymmetric cryptography algorithms. *International Journal of Advanced Research in Computer Science*, *8*(4).

[6] Rajdeep Kaur, Puneet jain, and Navdeep Kaur Jhajj (2020) Data and key encapsulation for the smart grid using improved AES and difference expansion algorithm**.** *International Journal of Advance Research, Ideas and Innovations in Technology*, 6(5).

[7] Menon, D. M., & Radhika, N. (2015). Design of a secure architecture for last mile communication in smart grid systems. *Procedia Technology*, *21*, 125-131.

[8] Metke, A. R., & Ekl, R. L. (2010). Security technology for smart grid networks. *IEEE Transactions on Smart Grid*, *1*(1), 99-107.

[9] Zhang, L., Zhu, Y., Ren, W., Wang, Y., Xiong, N. N., & Zhang, Y. (2020). An Energy Efficient Authentication Scheme using Chebyshev Chaotic Map for Smart Grid Environment. *arXiv preprint arXiv:2008.11366*.

[10] Reza, S. S., Ayob, A., Arifeen, M. M., Amin, N., Saad, M. H. M., & Hussain, A. (2020). A lightweight security scheme for advanced metering infrastructures in smart grid. *Bulletin of Electrical Engineering and Informatics*, *9*(2), 777-784.

[11] Li, F., Luo, B., & Liu, P. (2010, October). Secure information aggregation for smart grids using homomorphic encryption. In *2010 first IEEE international conference on smart grid communications* (pp. 327-332). IEEE.

[12] Abood, O. G., Elsadd, M. A., & Guirguis, S. K. (2017, December). Investigation of cryptography algorithms used for security and privacy protection in smart grid. In *2017 Nineteenth International Middle East Power Systems Conference (MEPCON)* (pp. 644-649). IEEE.

[13] Sparrow, R. D., Adekunle, A. A., & Berry, R. J. (2016, December). LEOPARD: Lightweight Encryption Operation Permutation Addition Rotation and Diffusion. In *2016 10th International Conference on Signal Processing and Communication Systems (ICSPCS)* (pp. 1-5). IEEE.

[14] Daemen, J., & Rijmen, V. (2002). *The design of Rijndael* (Vol. 2). New York: Springer-verlag.

[15] Zhang, X., & Cao, Y. (2014). A novel chaotic map and an improved chaos-based image encryption scheme. *The Scientific World Journal*, *2014*.