INTERNATIONAL JOURNAL OF ADVANCE RESEARCH, IDEAS AND INNOVATIONS IN TECHNOLOGY

ISSN: 2454-132X
Impact Factor: 6.078
(Volume 7, Issue 3 - V7I3-1215)
Available online at: https://www.ijariit.com

An integrated approach for the smart grid using the data compression and encryption algorithm

Sukhjinder Singh
rinkuvirdi321@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 network continuously monitors the electricity demand and usage through various smart appliances. Continuous monitoring generates a large amount of redundant data. Besides that, the data is sensitive to attacks. To overcome these challenges, we have designed an integrated approach for a smart grid using the data compression and encryption algorithm. We have used the DRACO algorithm for data compression. Further, we have designed an improved chaotic cubic map algorithm by hybrid it with AES layers to enhance security. For validation purposes, the data is randomly generated and various performance metrics are calculated for it. In the last, the proposed integrated approach is compared with the existing approaches. The results show that the proposed approach is superior to the existing approaches.

Keywords: *Advanced Encryption Standard (AES), DRACO, Chaotic Cubic Map Algorithm, Smart Grid.*

1. INTRODUCTION

Smart Grid is equipped with smart appliances such as renewable energy resources, advanced metering infrastructure (AMI), smart meter, and electricity managing prediction models [1]. The AMI appliance periodically measures the real-time electricity and communicates to the Supervisory Control and Data Acquisition unit through the communication line. Smart Grid systems consist of two broad components: the traditional power grid and the high data communication layer, as shown in Figure 1 [1]. The physical part of the smart grid can be defined as:

1. Generation: The components include circuit breakers, digital control units (AGC), photovoltaic (PV) systems, and power storage systems.

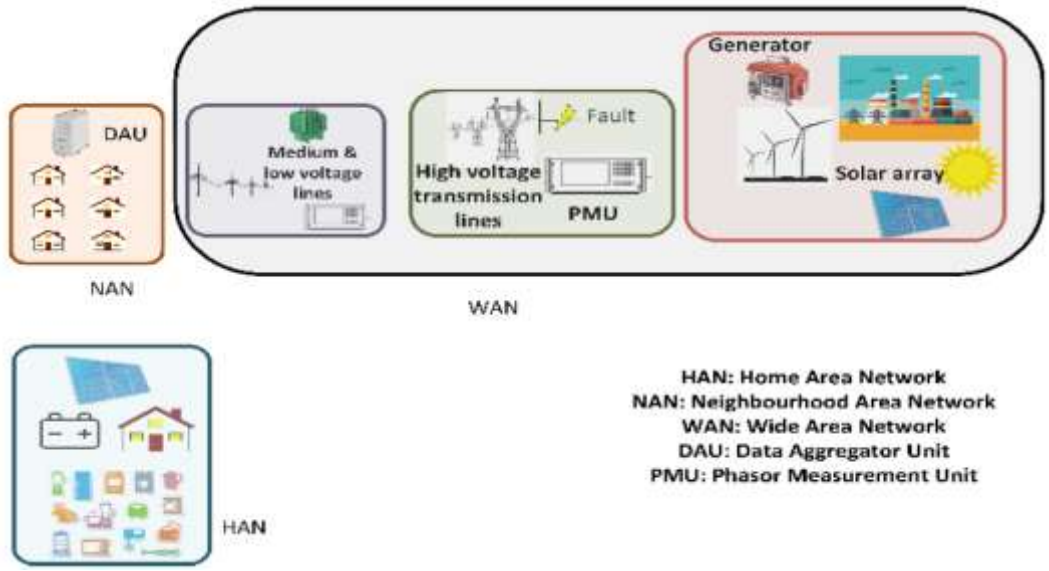

Fig.1 Smart Grid System

2. Delivery and Distribution: Equipment includes unit measurement units (PMUs).
3. Meter: Smart meter.
4. Communication: Connection of device configuration using wireless communication technologies such as Zigbee, WiMAX, LTE, and IEEE PMU standards of communication C37.118 [2].

Grid maintenance is required so that the power supply, which is the main purpose of the power company, is not interrupted. The security of the entire grid and cybersecurity are less important to many utilities [3]. Power system cybersecurity is witnessing the rapid and rapid adoption of technologies related to computers, wireless communications, Internet of Things (IoT) devices, and many applications that support the real-time, trouble-free operation of a present-day smart energy system. Next, we explained the smart grid challenges.

1.1 Redundant Data Generation due to Continuous Monitoring

In the smart grid, Advanced meter Infrastructure (AMI) is continuously monitoring the smart meter and send the electricity usage to the supervisory control and data acquisition (SCADA) unit. Continuous monitoring generates a large amount of redundant data. Therefore, data compression is required before data communication.

1.2 Attacks in the Smart Grid

In general, as shown in Figure 2, there are four systems in which malicious runner attacks and controls a system: reconnaissance, scanning, exploitation, and maintaining access [4]. In the early stages of the investigation, attackers collect information about their motives. In the second step, the probe, the attacker attempts to detect weaknesses in the system. These activities are to identify open ports and identify the capabilities and weaknesses of each port. During exploitation, he/she tries to weaken and has complete control over his intent. When an attacker gets the opportunity to control and quarantine, he saves that opportunity, the last step. This process is accomplished by installing an undetectable program. As a result, he/she can easily recover to the target system later.

Fig. 2 Attacking cycle followed by hackers to get control over a system [5]

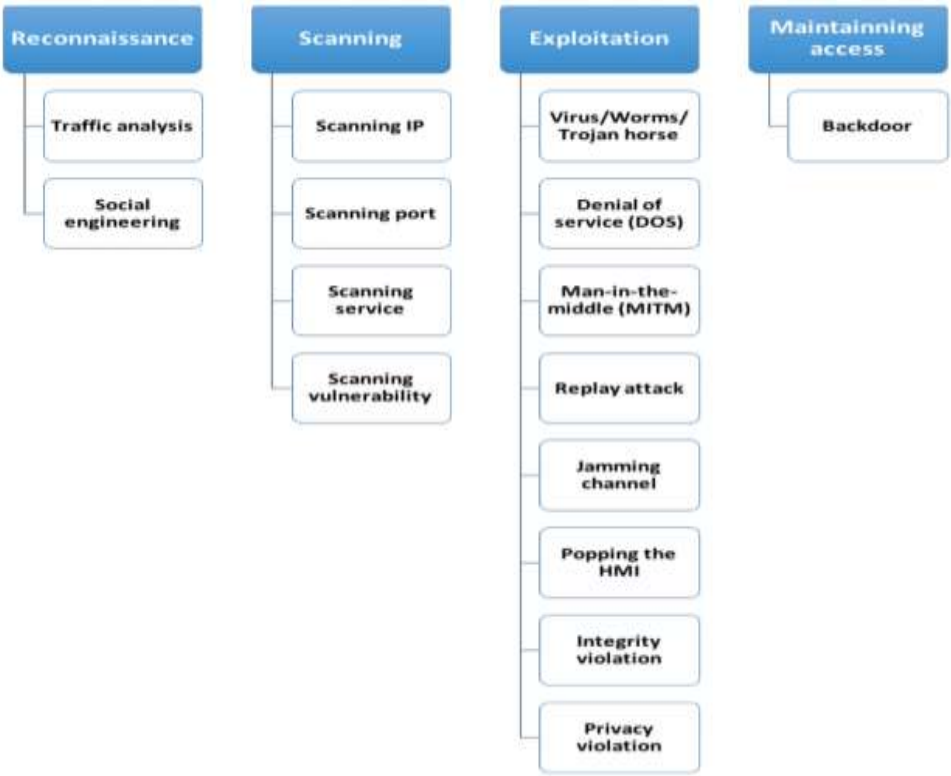

Fig. 3 Classification of Cyber-attacks in the Smart Grid [5]

In the smart grid, an attacker follows a series of steps to compromise security standards [5]. In each case, they seized it, despite obstacles that we could hardly imagine. "Therefore, you can launch an attack based on these techniques. Figure 3 shows the type of attack at each point in time.

1.3 Security System

To overcome these attacks, security systems have been designed using cryptography algorithms. Cryptography algorithms scramble the secret data using a private key. In the literature, the most preferred cryptography algorithms are used in the smart grid are Advanced Encryption Standard (AES) [6], homomorphic encryption [7], and chaotic map [8-9]. Out of these, chaotic map algorithm takes lesser execution time for data encryption as compared to the other algorithms. However, it provides lesser security in terms of the avalanche effect. The avalanche effect is a security parameter of cryptography. It calculates the number of bits changed in the encrypted data with changing one-bit in the secret data. In our work, we have enhanced the security of the chaotic map algorithm.

1.4 Main Contribution

The main contribution of this paper is to design an integrated approach by hybrid the data compression and encryption algorithm. In our work, we have used the latest data compression algorithm, namely, DRACO for data compression. Further, the compressed data is encrypted using the improved chaotic cubic map algorithm. In the improved chaotic cubic map algorithm, the compressed data is encrypted using XOR operation. After that, AES two layers-sub-byte and shift row are used to provide better security in terms of avalanche effect. The experimental results are performed on the standard dataset and various performance parameters are calculated for it. The results show that the proposed method is superior as compared to the existing methods.

The rest of the paper is as follows. Section 2 gives an overview of the DRACO, chaotic map, its types, and the Advanced Encryption Standard (AES) algorithm. Section 3 presents the proposed methodology. Section 4 shows the experimental results. In the last, the conclusion and future scope are presented in Section 5.

2. RELATED WORK

In this section, the compression algorithm DRACO, chaotic map, its types, and the AES algorithm (diffusion and confusion layers) are explained.

2.1 DRACO Algorithm

Data Reduction Algorithm for Correlated Data (DRACO) is recently proposed by Pourmirza et al. [10]. The following steps are taken to perform compression using the DRACO algorithm.

Initially, consecutive two data values are taken. The first data original value is stored and the second consecutive data value is compressed by performing the XOR operation between them. The process is repeated for other data values to achieve compression, as shown in Table 1. If the correlation between the data value is high then very superior compression is achieved by this algorithm. Besides that, if the magnitude of the data value is needed to send it separately.

Table 1 DRACO Algorithm based Data Compression

Measured Value	Binary Value	XOR Value	Output Value
97	1100001	1100001	97
98	1100010	11	3
99	1100011	01	1
100	1100100	11	3
101	1100101	01	1

On the receiver side, in the same fashion, the consecutive data values are read. The first data value represents the original value whereas the second value represents the compressed data. After that, an XOR operation is performed between them to determine the original data value.

2.2 Chaotic Map and its Types

Next, we have discussed the types of chaotic maps [11].

- **Logistic Map:** Logistic logos depicting a behavior disorder are considered to be one of the most common types of non-concussion disorder (DCS) systems. It is 1DCS that can be described as follows.

$$X_{n+1} = \mu X_n(1 - X_n) \qquad (1)$$

- **Tent Map:** The second map we used was our tent map. In mathematics, tent mapping [1-2-2.24] is a repetitive task, in the form of tents, forming a unique time-varying process. It takes the Xn head and the line really and lists it in another key,

$$X_{n+1} = \begin{cases} \mu X_n & \text{for } X_n < 0.5 \\ \mu(1 - X_n) & \text{for } X_n > 0.5 \end{cases} \qquad (2)$$

- **Cubic Map:** cubic map is one of the unique systems that modestly does not line up chaotic map that shows chaos. It is explained

$$X_{n+1} = f(X_n) = \mu X_n^3 + (1 - \mu)X_n \quad (3)$$

where μ is the chaotic factor and n is the number of iterations, and $\mu \in [0, 4]$, $X \in [0, 1]$ in which the chaotic behavior is realized when $\mu \in [3.57, 4]$.

2.3 Advanced Encryption Standard (AES) Algorithm (Diffusion and Confusion Layer)

The AES algorithm was developed by two researchers, Vincent Rijmen and Joan Daemen. The AES algorithm comes under a symmetric algorithm. The symmetric algorithm uses the same key for encryption for decryption purposes. Also, the symmetric

algorithm relies on block ciphers. AES has a 128-bit blockchain, 128/192/256-bit different paths, and a total of 10/12/14 surround for data storage and destruction [12]. The AES algorithm consists of four layers of each circle (sub-bytes, row switching, column merging, and circle key addition) for encryption. This is explained below.

- **Sub-Byte Layer:** Text and key input with the AES algorithm. The display and keys are 128 bits long. Therefore, it is constructed using a 4X4 matrix on both sides of an 8-bit long matrix. Therefore, the value of the element matrix varies from 0 to 255. An XOR function is executed between a level and a key. It then passed through a repair box called the sub byte area. The variable box replaces the original matrix material with another item, as shown in Figure 4.

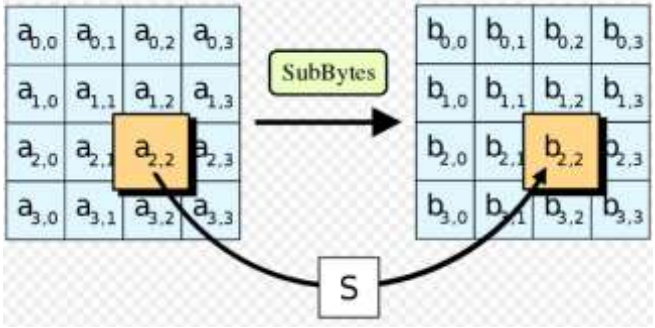

Fig. 4 Sub-Byte Step

It is a subtle strategy. The meditative painting to do is work one-on-one with no work. Therefore, the s-box has a 2 ^ 8 ratio. These mixtures are stored in a visible table.

- **Shift Row Layer:** After finishing a small process, it passed the shift row line. The shifting line distributes the damage according to the linear regression line, as shown in Figure 5. The first line was changed to 0 bytes, the second line was changed to 1 byte, the third line was changed to 2 bytes, and the 4th line was changed to 3 bytes.

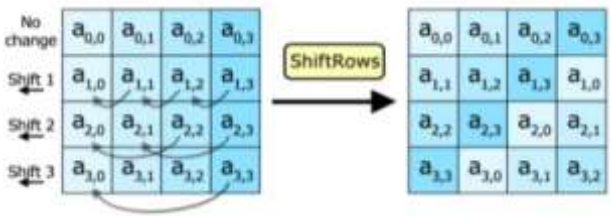

Fig. 5 Shift Row Step

3. PROPOSED METHOD

The proposed algorithm is simple and provides better data compression and security as compared to the existing algorithms. The flowchart for the proposed algorithm is shown in Figure 3.1. In the proposed algorithm, initially, the secret data is read and compressed using the DRACO algorithm. After that, the compressed data is encrypted using the XOR operation with a key. The key is random generated using the chaotic cubic map algorithm. To generate the key, the initial population (x) and control parameter (μ) is inputted to the cubic map algorithm. After that, on the encrypted data, the AES algorithm two layers (diffusion and confusion layer) applied to get final encrypted data. In the diffusion layer, the encrypted data matrix is circular rotated based on the matrix row index. Next, in the confusion layer, the rotated matrix is given to the substitution box (s-box) to transform the bits.

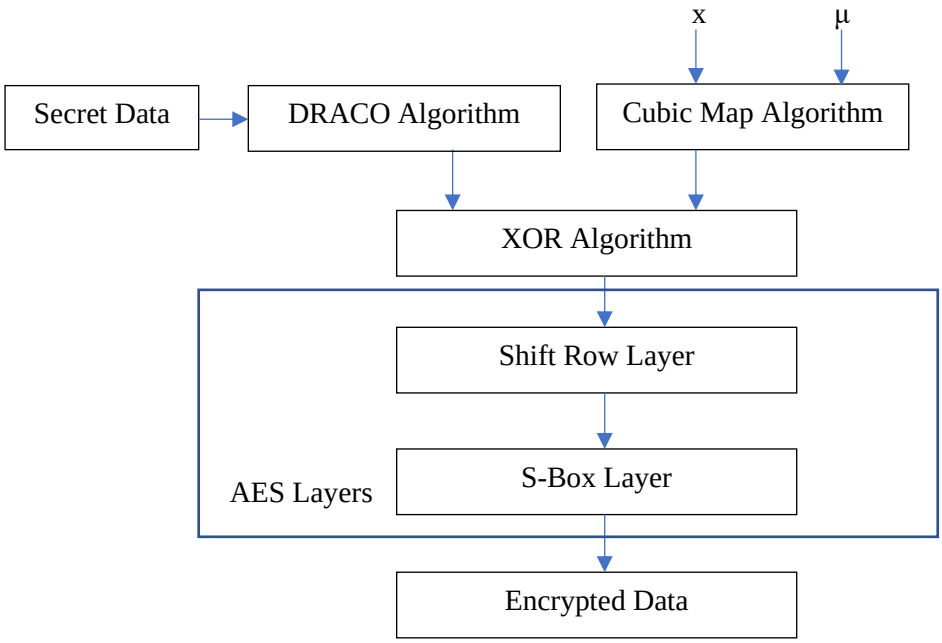

Fig. 3.1 Block Diagram of the Proposed Algorithm

4. EXPERIMENTAL RESULTS

In this section, the experimental results for the proposed algorithm are shown. The secret data is randomly generated. The algorithm is written and simulated in MATLAB. We have measured the various performance parameters for it [13].

4.1 Data Compression

The data compression is calculated using Eq. (4).

$$DC = \frac{Originalfile - Compressed\ file}{Original\ file}\% \quad (4)$$

Table 2 shows the data compression of the DRACO algorithm The results show the DRACO algorithm provides approximately 37% compression in the practical scenario.

Table 2 Data Compression for the DRACO Algorithm

Original File (in bits)	Compressed File	DRACO Algorithm
4096	2563	37.42%
8192	5123	37.46%
16384	10243	37.48%

4.2 Mean Square Error (MSE)

MSE parameter measures the error between original and encrypted data. The higher value of MSE represents a significant change in the data value after data encryption [13]. It is calculated using Eq. (5).

$$MSE = \frac{\sum_{ij}(P_{ij} - E_{ij})^2}{M \times N} \quad (5)$$

Table 3 shows the comparative analysis based on the MSE parameter and found that the proposed algorithm provides higher MSE as compared to the existing algorithms.

Table 3 Comparative Analysis based on the Mean Square Error (MSE) with the Existing Algorithms

Data	Cubic Map [12]	Proposed Algorithm
File1	0.81	8.80
File2	2.5977	18.27
File3	6.1621	7.5840
File4	1.7813	6.4141
File5	3.113	6.3652

4.3 Peak Signal to Noise Ratio (PSNR)

PSNR parameter calculates how much noise addition in the original data after encryption. It is measured in decibels. A small value of PSNR indicates low noise is added due to the encryption process. It is calculated using Eq. (6).

$$PSNR = 10 \log_{10} \frac{P^2}{MSE} \quad (6)$$

Table 4 shows the comparative analysis based on the PSNE parameter. The results show that the proposed algorithm provide lesser PSNR as compared to the existing algorithms.

Table 4 Comparative Analysis based on the Peak Signal to Noise Ratio (PSNR) (in dB) with the Existing Algorithms

Data	Cubic Map [12]	Proposed Algorithm
File1	49.04	38.68
File2	43.98	35.51
File3	40.23	39.33
File4	45.62	40.05
File5	43.20	40.09

4.4 Correlation Coefficient (CC):

The correlation coefficient parameter measures the correlation between the original and encrypted data. Its value varies from -1 to 1. In the ideal scenario, the correlation coefficient value for data encryption is required to be 0. It is calculated using Eq. (7).

$$r = \frac{\sum_i (x_i - x_m)(y_i - y_m)}{\sum_i \sqrt{\sum_i (x_i - x_m)^2} \sqrt{\sum_i (y_i - y_m)^2}} \quad (7)$$

Table 5 shows the comparative analysis based on the correlation coefficient parameter. The results show that the proposed algorithm provide lesser CC as compared to the existing algorithms.

Table 5 Comparative Analysis based on the Correlation Coefficient (CC) with the Existing Algorithms

Data	Cubic Map [12]	Proposed Algorithm
File1	0.0985	-0.0012
File2	0.0346	-0.0384
File3	0.0836	0.0541
File4	0.0558	0.0046
File5	0.0226	0.0599

4.5 Avalanche Effect: This parameter measures the security of the encryption algorithm [14]. In the ideal scenario, if a 1-bit change in the plaintext then 50% of ciphertext bits should be changed. Table 6 shows the comparative analysis based on the avalanche effect parameter. The results show that the proposed algorithm provides a higher avalanche effect as compared to the existing algorithms.

Table 6 Comparative Analysis based on the Avalanche Effect with the Existing Algorithm

Data	Cubic Map [12]	Proposed Algorithm
File1	4%	48%

5. CONCLUSION AND FUTURE SCOPE

In this paper, we have designed an integrated approach for a smart grid in which data compression and encryption algorithm is hybrid. Initially, the data is compressed using the DRACO algorithm. After that, data is encrypted using the chaotic cubic map algorithm by performing the XOR operation. Next, the XOR output is passed through two layers of the AES algorithm to provide final encryption. To validate the performance of the proposed method over the existing algorithms, various performance parameters calculated for it. The results show that the proposed method provides better compression, lower peak signal to noise ratio, correlation coefficient, and high avalanche effect as compared to the existing algorithms. In the future, data error correction code is hybrid in the proposed method to make it robust against channel attacks.

6. REFERENCES

[1] Islam, S. N., Baig, Z., & Zeadally, S. (2019). Physical layer security for the smart grid: Vulnerabilities, threats, and countermeasures. *IEEE Transactions on Industrial Informatics*, *15*(12), 6522-6530.

[2] Bou-Harb, E., Fachkha, C., Pourzandi, M., Debbabi, M., & Assi, C. (2013). Communication security for smart grid distribution networks. *IEEE Communications Magazine*, *51*(1), 42-49.

[3] Alcaraz, C., & Zeadally, S. (2015). Critical infrastructure protection: Requirements and challenges for the 21st century. *International journal of critical infrastructure protection*, *8*, 53-66.

[4] Engebretson, P. (2013). *The basics of hacking and penetration testing: ethical hacking and penetration testing made easy*. Elsevier.

[5] El Mrabet, Z., Kaabouch, N., El Ghazi, H., & El Ghazi, H. (2018). Cyber-security in smart grid: Survey and challenges. *Computers & Electrical Engineering*, *67*, 469-482.

[6] Yang, C., Wu, J., Wang, L., Zhang, X., Li, L., & Liu, S. (2020). Smart Grid Monitoring Systems based on Advanced Encryption Standard and Wireless Local Area Network. In *IOP Conference Series: Materials Science and Engineering* (Vol. 719, No. 1, p. 012056). IOP Publishing.

[7] Mohammadali, A., & Haghighi, M. S. (2021). A Privacy-Preserving Homomorphic Scheme with Multiple Dimensions and Fault Tolerance for Metering Data Aggregation in Smart Grid. *IEEE Transactions on Smart Grid*.

[8] Tur, M. R., & Ogras, H. (2021). Transmission of Frequency Balance Instructions and Secure Data Sharing Based on Chaos Encryption in Smart Grid-Based Energy Systems Applications. *IEEE Access*, *9*, 27323-27332.

[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] Pourmirza, Z., Walker, S., & Brooke, J. (2021). Data reduction algorithm for correlated data in the smart grid. *IET Smart Grid*.

[11] Yousif, B., Khalifa, F., Makram, A., & Takieldeen, A. (2020). A novel image encryption/decryption scheme based on integrating multiple chaotic maps. *AIP Advances*, *10*(7), 075220.

[12] Rijmen, V., & Daemen, J. (2001). Advanced encryption standard. *Proceedings of Federal Information Processing Standards Publications, National Institute of Standards and Technology*, 19-22.

[13] Mondal, B., & Mandal, T. (2020). A secure image encryption scheme based on genetic operations and a new hybrid pseudo random number generator. *Multimedia Tools and Applications*, 1-24.

[14] Bansod, G., Pisharoty, N., & Patil, A. (2017). BORON: an ultra-lightweight and low power encryption design for pervasive computing. *Frontiers of Information Technology & Electronic Engineering*, *18*(3), 317-331.

