IJARIIT
International Journal Of Advance Research, Ideas And Innovations In Technology

ISSN: 2454-132X
Impact factor: 4.295
(Volume 5, Issue 3)
Available online at: www.ijariit.com

Improving quality of service in the smart grid using data compression and encryption technique

Simrandeep Singh
simargill51@gmail.com
Adesh College of Engineering and Technology, Faridkot, Punjab

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

Ravinder Kumar
ravinderkr@gmail.com
Adesh College of Engineering and Technology, Faridkot, Punjab

ABSTRACT

In this paper, to improve the quality of service in terms of embedding capacity and resource utilization of the database has done using data compression and lightweight encryption technique for the smart grid. In the proposed technique, the run-length encoding technique used for data compression and ANU lightweight algorithm has been used for data encryption. The algorithm has designed and simulated in MATLAB 2013a. The experimental results show that the proposed technique has taken fewer resources and consume less file size as compared to conventional AES techniques.

Keywords— *Smart grid, Security, Compression, Quality of service*

1. INTRODUCTION

Smart Grid is the next generation power grid which provides the reliable, efficient, and uninterrupted power supply to the customers [1]. The smart grid conceptual model is divided into various categories such as bulk generation, energy transmission, energy distribution, domestic and non-domestic customers, and service provider.

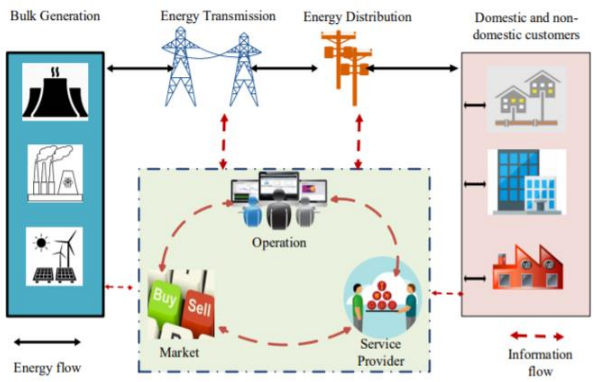

Fig. 1: Conceptual model of the smart grid [1]

The service provider manages, control the energy distribution and provide two-way communication with customers. Thus, a large amount of sensitive information is communicated on the network. Therefore, a large amount of storage devices and security algorithms are required to store and secure the database. Next, to improve the quality of service in the smart grid compression, attacks and its countermeasure techniques are studied.

1.1 Compression techniques for smart grid

In the smart grid, smart meter plays an important role which monitors the data continuously using various sensors and communicate data periodically. Thus, a large amount of raw data available in the smart grid database. To manage the raw data in the database, it is compressed using a compression technique. The compression technique is classified as lossy and lossless compression [2]. In the lossless compression, all raw data is recovered back after de-compression. In our proposed technique, we have worked on lossless compression technique.

1.2 Attacks in the smart grid

In the smart grid, sensitive information is communicated between the smart meter and smart grid. Thus, the communication line is prone to a number of attacks. These attacks are

1.2.1 Eavesdropping: Wireless signals are carried in open space, and are susceptible to eavesdropping by an adversary. Sensitive information from a smart meter can easily be observed and assessed through such an attack. Low-cost eavesdroppers exist in the market, to convenience launch of such attacks. Data encryption is an approach towards protecting sensitive information from revelation to the adversary. However, if a certain pattern is depicted by the transmitted data, an intelligent adversary may still be able to decipher the message content. For instance, if a household is unoccupied, the electricity usage will dwindle. If the smart meter is programmed to communicate with the data concentrator unit only when a certain threshold of energy usage is crossed, or if the message length to be transmitted is directly proportional to energy consumption, then a pattern of activity of the household may be construed.

1.2.2 Jamming: The main goal of this attack is to prevent the smart meters from communicating with the utility provider, through jamming of the wireless medium with noise signals. Such attacks can be classified into two types: i) Proactive jamming, wherein the jammer can emit noise signals continuously to completely block a wireless channel, and (ii) Reactive jamming, wherein the jammer first eavesdrops on the radio channel and launches the attack only when signals are sensed on the channel. Because of such an attack, the legitimate smart meter can be affected into two ways: (i) the channel will be tagged as "busy" for any carrier sensing done by a legitimate smart meter, and (ii) the smart meter may be prevented from receiving packets. It is non-trivial to differentiate between reactive jammer attacks that may result from routine communication signals and from adversary-initiated signals.

1.2.3 Injecting Requests/ Restricting Access: The main goal of this attack is to disrupt the routine operations at the MAC layer of the smart meter. The attacker prevents the smart meters from initiating legitimate MAC operations alternatively, causes packet collision. This attack is highlighted as follows:

(a) It is similar to reactive jamming; in which the attack is launched based on the intent to block the communication channel,
(b) It targets a multi-user access channel, and
(c) The attacker sets its own back off timer to be very short in length, so that the channel prioritizes access to the adversary each time it wishes to communication, denying access to legitimate smart meters of the smart grid.

To secure the sensitive information from these attacks, the security goals for the smart grids required. These are [4]

- **Confidentiality:** Confidentiality parameter shows that only authenticated users encrypt/decrypts the message using their private key.
- **Integrity:** Integrity assures that the data is not modified between the transmitter and receiver during the exchange.
- **Privacy:** Privacy parameter is the ability to protect private information such as identity, location of the smart grid and gateways.
- **Authentication:** In the smart grid network, authentication is required to identify the identity of the users. These security goals can be achieved using cryptography algorithms are used. Cryptography algorithms provide data security, integrity, and authentication. The cryptography algorithms encrypt the message such a way only authenticated parties encrypt/decrypts the data [5]. The block diagram for the encryption is shown in figure 2. The cryptography algorithms are divided into three types [6].
- **Symmetric Cryptography:** In symmetric cryptography, the same key is deployed for encryption and decryption purposes. The symmetric algorithm consumes fewer resources as compared to asymmetric and used for encrypting a large amount of secret data. Some examples of symmetric algorithms are DES, AES, and Blowfish.

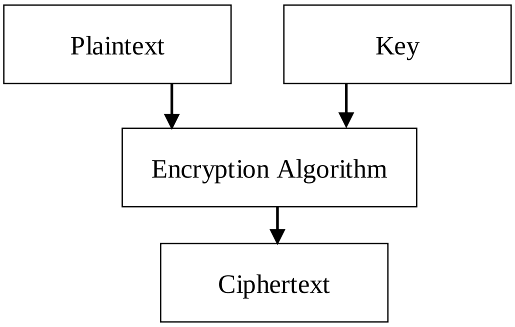

Fig. 2: Block diagram of cryptography

- **Asymmetric Cryptography:** In asymmetric cryptography, different keys public and private key used for data encryption and decryption purposes. Asymmetric algorithms are preferred for data authentication where opportunity to agreeing on the private key is not possible. Some examples of asymmetric algorithms are Diffie Hellma, El-Gamal, RSA, and Elliptic Curve Cryptography.

In this paper, the database data is compressed using Mutated Huffman Coding. Next, the compressed data is encrypted using the lightweight encryption algorithm ANU. Further, the performance analysis of the proposed technique is done using compression as well as security analysis parameters.

The rest of the paper is as follows. Section II defines the related work has done in the field of compression as well as security for the smart grid. Section III explains the proposed technique. Section IV shows the experimental results. In the last conclusion is drawn in section V.

2. LITERATURE SURVEY

In this section, the smart grid compression, as well as security algorithms, have studied.

X. Li, X. Liang, R. Lu et.al 2012 [7] According to smart meters privacy, the major benefit of the smart grid is collecting a huge amount of readings data for various appliances in the household. However, this advantage could turn to privacy concern, as the information about the house energy usage can reveal personal habits and daily activities for householders. To address the privacy of smart meters, several protection approaches have been proposed, such as employing homomorphic encryption during data reading aggregation process, compressing the readings and adding random sequences, or deploying anonymization schemes to conceal the real identity of smart meters.

Spiegel, et al. [8], in this paper, comparative analysis of the various compression technique is done for the smart meter. Further, to achieve a better trade-off between compression ratio and computational cost, they have usedthe binary run-length encoding algorithm.

Ochoa, et al. [9], this work presents a simulation model for point to-point transmission of encrypted data using the application layer of Open Smart Grid Protocol (OSGP). The simulation aims to verify the integrity of the data transmitted from one point to another using Power Line Communication (PLC). The simulation model was developed in MATLAB and uses RSA, AES, RC-6, and 3-DES cryptographies to encode data. Data transmission uses PLC technique with Gaussian Minimum Shift Key (GMSK) modulation. Results demonstrate that it is possible to use the OSGP protocol in the application layer with different criteria, which can be used according to the data size. It was applied an Additive White Gaussian Noise (AWGN) in the transmission to simulate the effects that exist in a real network. The experiments demonstrate that RC-6 outperforms the other cryptographic algorithms, presenting the smallest execution time, with low memory requirements.

Aarti Agarkar and Himanshu Agarwal [10], this paper review the various authentication and privacy scheme for smart grid security. They have explored various encryption techniques such as homomorphic encryption, elliptic curve cryptography, and lattice cryptography. Further, defined the tradeoff issues, and future research direction such as privacy enhancement using blockchain and lightweight cryptography.

In the literature, various compression techniques such as Huffman coding, JPEG 2000, run length encoding and cryptography techniques AES, Homomorphic Encryption has used. Existing cryptography technique consumes a large number of resources. Therefore, in our work lightweight compression as well as encryption technique are explored.

3. PROPOSED TECHNIQUE

In this section, the proposed technique is explained in detail. The block diagram is shown in Fig. 3. Initially, the smart grid database data is read and encoded using run-length encoding. Next, the encoded data and key are input to the lightweight encryption algorithm which generates the ciphertext. The components have explained below.

3.1 Run-length Encoding

Run Length Encoding (RLE) is a lossless compression technique and based on interpixel redundancy [11]. In this encoding scheme, two values are required to store the information. One value contains the original value and second value contains the information on how many times the original sequence is repeated. To understand run length encoding in detail explained with the example below.

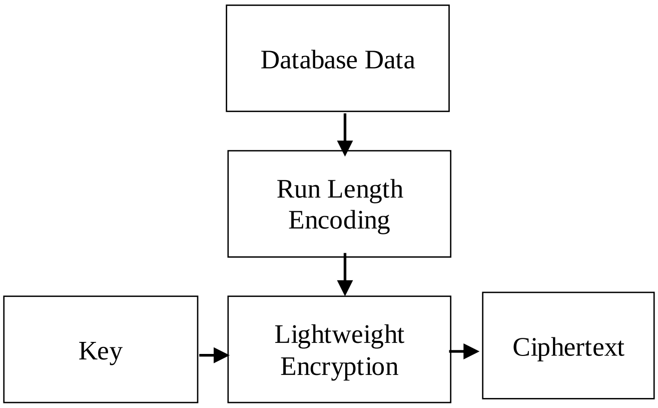

Fig. 3: Block Diagram of the Proposed Technique

Original Sequence
1110000011110000111111
Compressed Form using Run Length Encoding
{111} = {1,3}
{00000} = {0,5}
{1111} = {1,4}
{0000} = {1,4}
{111111} = {1,6}

3.2 ANU Algorithm

The lightweight algorithm ANU invented in 2016 by Gaurav Bansod and their group [12]. ANU is Feistel network-based block cipher.

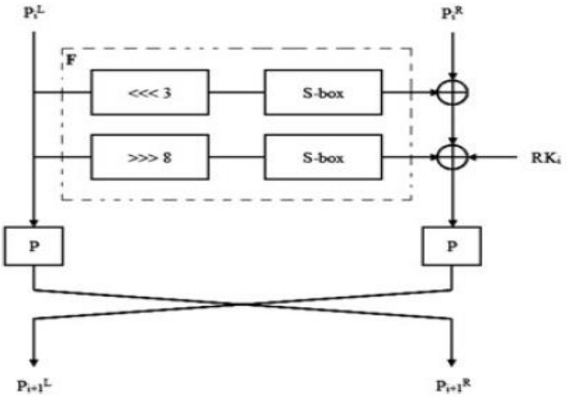

Fig. 4: Block Diagram of ANU Algorithm [ref]

This cipher has 64-bit block size, 80/128-bit key, and 25 rounds. The block diagram of ANU cipher is shown in figure 4. The substitution box (s-box) and permutation table are shown in table 1 and 2.

Table 1: Substitution Box

X	S-Box(X)
0	2
1	9
2	7
3	E
4	1
5	C
6	A
7	0
8	4
9	3
A	8
B	D
C	F
D	6
E	5
F	B

Table 2: Bit Permutation

i	0	1	2	3	4	5	6	7
BP(i)	20	16	28	24	17	21	25	29
I	8	9	10	11	12	13	14	15
BP(i)	22	18	30	26	19	23	27	31
i	16	17	18	19	20	21	22	23
BP(i)	11	15	3	7	14	10	6	2
i	24	25	26	27	28	29	30	31
BP(i)	9	13	1	5	12	8	4	0

The pseudocode for the ANU algorithm encryption as well as key scheduling is shown in Table 3.

Table 3: Pseudo code for the ANU Algorithm

```
Encryption Algorithm
For k is 0 to 24 rounds
{
        Data Split ($State_{63-0}$)
        Left Circular Shift ($State_{31-0}$, 3)
        Right Circular Shift ($State_{31-0}$, 8)
XOR($State_{31-0}$, $State_{63-32}$)
        XOR Operation($State_{31-0}$, $State_{31-0}$, $key_{63-0}$)
 }
```

```
Key Scheduling Algorithm
For 80-Bit Key
         Left Circular shift(Key, 13)
         S-Box Layer($Key_{0-3}$)
          XOR Operation ($Key_{63-59}$, $Round\_Counter$)
For 128-bit Key
        Left Circular shift(Key, 13)
        S-Box Layer($Key_{0-7}$)
        XOR Operation ($Key_{63-59}$, $Round\_Counter$)
```

4. EXPERIMENTAL ANALYSIS OF THE PROPOSED TECHNIQUE

In this section, the simulation results and performance analysis of the proposed technique are done. The algorithm is designed and simulated in MATLAB 2013a. In our work, smart grid data taken as secret data for compression and encryption purposes. The performance analysis of the proposed technique is done using the following parameters.

4.1 Compression Ratio

Compression Ratio (CR) is defined as the ratio between uncompressed and compressed data [11]. The compression ratio for smart data is shown in Table 4.

Table 4: Compression Ratio

Secret Data	Original Size	Compressed Size	Compression Ratio
Baboon	65536	102753	0.64
Brabara	65536	36243	1.81
Cameraman	65536	56988	1.15
Pepper	65536	23049	2.84
Rice	65536	34893	1.88
House	65536	70002	0.94

The table shows that maximum compression ratio achieves in pepper image and minimum compression in baboon image.

4.2 Avalanche Effect

This parameter measures the security of encryption algorithm [12]. In the ideal scenario, if a 1-bit change in the plaintext than half of the cipher text bits should be changed.

Table 5: Avalanche effect

Plaintext	[0000 0000 0000 0000] $_{hex}$
Key	[0000 0000 0000 0000 0000] $_{hex}$
Key	[0000 0000 0000 2000 0000] $_{hex}$
Avalanche Effect	54%

4.3 Memory consumption for look-up table combination

This parameter is used to determine how much memory is consumed for storage the look-up table as shown in table 6. The table shows that ANU consumes minimum and AES consumes maximum memory for s-boxes.

Table 6: Memory Consumption for the S-Boxes

Algorithm	Memory Consumption for S-Box
DES	8 S-boxes (6-bit Input and 4-bit Output) ~=512bits
AES	1 S-Box (8 bits input and 8 bits output)~=2048
Blowfish	4 S-Box (256 Entry in Each)
ANU	64 bit

4.4 Computation time

This parameter is used to determine how much time is spent on data compression as well as encryption. In the MATLAB, tic and toc command available which tells the overall time consumption of the technique. The computation time for the different dataset images is shown in table 7. The table shows that baboon image takes maximum computation time and pepper image take minimum computation time for compression as well as encryption.

Table 7: Computation Time for the Different Dataset Images

Dataset Images	Computation Time (Seconds)
Baboon	18.38
Brabara	7.0287
Cameraman	10.26
Pepper	4.84
Rice	7.19
House	12.60

4.5 Comparative Analysis with the Existing Technique

In this section, the file size of the proposed technique after data compression and encryption is compared with the existing technique in Table 8. In our work, we have compared our proposed technique with the existing algorithm with AES. The results show that the proposed technique has better file size as compared to the AES algorithm due to a small block size. The table shows that pepper image is consumed minimum file size and baboon image consumes maximum file size.

Table 8: Comparative analysis with the existing techniques based on the file size after compression and encryption

Dataset Images	Original Size	Compressed Size	Run Length Encoding + AES	Proposed Technique
Baboon	65536	102753	102912	102848
Brabara	65536	36243	36352	36288
Camera man	65536	56988	57088	57024
Pepper	65536	23049	23296	23168
Rice	65536	34893	35072	34944
House	65536	70002	70144	70080

5. CONCLUSION

In this paper, initially, an overview of the smart grid, its architecture and its advantages over conventional power grid explained. Next, the smart grid raw data compression, attacks, and its countermeasure techniques are discussed. Further, a literature review on smart grid architecture, data compression, as well as attacks and countermeasure techniques has done and found that Huffman coding, JPEG 200, AES, RSA, 3DES, ECC are the most preferred compression and encryption technique. These algorithms resource consumption high. Therefore, in this thesis, various lightweight compression and encryption techniques are explored and run length encoding and ANU lightweight cryptography algorithm have selected for the proposed technique. Next, the proposed technique is designed and simulated in the MATLAB 2013a. The performance analysis is done on the basis of computation time, resource consumption, and the avalanche effect. The results show that pepper image provides better compression, minimum file size and takes minimum computation as compared to the other images. Next, the comparative analysis of the proposed technique is done with the existing technique and found that the proposed technique takes less file size as compared to the existing work.

6. REFERENCES

[1] Kumar, Pardeep, Yun Lin, Guangdong Bai, Andrew Paverd, Jin Song Dong, and Andrew Martin. "Smart Grid Metering Networks: A Survey on Security, Privacy and Open Research Issues." IEEE Communications Surveys and Tutorials (2019).

[2] Spiegel, Julien, Patrice Wira, and Gilles Hermann. "A Comparative Experimental Study of Lossless Compression Algorithms for Enhancing Energy Efficiency in Smart Meters." In 2018 IEEE 16th International Conference on Industrial Informatics (INDIN), pp. 447-452. IEEE, 2018.

[3] Baig, Zubair A., and Abdul-RaoofAmoudi. "An analysis of smart grid attacks and countermeasures." Journal of Communications 8, no. 8 (2013): 473-479.

[4] Ferrag, Mohamed Amine, Leandros A. Maglaras, Helge Janicke, and Jianmin Jiang. "A survey on privacy-preserving schemes for smart grid communications." arXiv preprint arXiv: 1611.07722 (2016).

[5] Kamil, Samar, MasriAyob, Siti Norul Huda Sheikh Abdullah, and Zulkifli Ahmad. "Challenges in Multi-Layer

Data Security for Video Steganography Revisited." Asia-Pacific Journal of Information Technology and Multimedia 7, no. 2-2 (2019).

[6] Tripathi, Ritu, and Sanjay Agrawal. "Comparative study of symmetric and asymmetric cryptography techniques." International Journal of Advance Foundation and Research in Computer (IJAFRC) 1, no. 6 (2014): 68-76.

[7] X. Li, X. Liang, R. Lu, X. Shen, X. Lin, and H. Zhu, “Securing smart grid: cyber-attacks, countermeasures, and challenges,” Communications Magazine, IEEE, vol. 50, no. 8, pp. 38–45, Aug. 2012.

[8] Spiegel, Julien, Patrice Wira, and Gilles Hermann. "A Comparative Experimental Study of Lossless Compression Algorithms for Enhancing Energy Efficiency in Smart Meters." In 2018 IEEE 16th International Conference on Industrial Informatics (INDIN), pp. 447-452. IEEE, 2018.

[9] Ochôa, Iago Sestrem, Valderi RQ Leithardt, Cesar AlbenesZeferino, and Jorge Sa Silva. "Data Transmission Performance Analysis with Smart Grid Protocol and Cryptography Algorithms." In 2018 13th IEEE International Conference on Industry Applications (INDUSCON), pp. 482-486. IEEE, 2018.

[10] Agarkar, Aarti, and Himanshu Agrawal. "A review and vision on authentication and privacy preservation schemes in smart grid network." Security and Privacy 2, no. 2 (2019): e62.

[11] Husseen, A. H., S. Sh Mahmud, and R. J. Mohammed. "Image compression using proposed enhanced run length encoding algorithm." Ibn AL-Haitham Journal for Pure and Applied Science 24, no. 1 (2017).

[12] Bansod, Gaurav, Abhijit Patil, Swapnil Sutar, and Narayan Pisharoty. "ANU: an ultra-lightweight cipher design for security in IoT." Security and Communication Networks 9, no. 18 (2016): 5238-5251.