INTERNATIONAL JOURNAL OF ADVANCE RESEARCH, IDEAS AND INNOVATIONS IN TECHNOLOGY

ISSN: 2454-132X
Impact factor: 6.078
(Volume 6, Issue 4)
Available online at: https://www.ijariit.com

Lightweight privacy-preserving scheme for the smart grid data using ANU and Perturbation Algorithm

Ravinderpal Singh
ravindersk15@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 collects the data of smart meter and communicates the data to electricity generation, pricing, and billing departments. The departments used this information for electricity forecasting, real-time pricing, and generate electricity bills. The smart grid data contains customer personal information as well as electricity consumption details. Thus, sharing all information with the departments violates customer privacy. In addition, if no security mechanism provided for the data makes it prone to the attacks. In this paper, we have proposed a privacy-preserving algorithm for smart grid data security. The algorithm has two-phase. In the first phase, customer personal information and electricity consumption details separated. In the second phase, the customer's personal information is secured using a lightweight algorithm ANU and electricity consumption details are secured using noise addition on the data by applying the perturbation algorithm. The algorithm is coded and simulated in the MATLAB 2013a. The experimental results show that the proposed technique consumes less memory and provides better security as compared to the existing algorithms.

Keywords: *Smart Grid, Privacy-Preserving, ANU, Perturbation*

1. INTRODUCTION

The smart grid is an advanced power grid that combines modern information and control technologies with the traditional power grid. Further, it provides two-way communication between users and the control centers. Moreover, it balances loads, adjusting prices, and planning the electricity forecasting [1]. The smart grid provides stable electricity to the users and gives the load management information to the users that help in saving electricity bills. However, the smart grid also brings users the risk of leakage of privacy [2]. The attackers can spy privacy by eavesdropping the communication is happened between users and the control center. For example, users have different electricity consumption during peak and non-peak hours. The attackers based on this information determine when users available or not in the home [3]. In addition, the control center based on the user's electricity consumption forecast the electricity generation required. Thus, if the attacker temper the data that communicating to the control center then based on wrong information electricity forecasting is done that un-balance the electricity load on the network. To overcome these challenges, security algorithms are required to preserve the privacy of the users.

In the literature, various cryptography and data perturbation algorithms have been used to preserve the privacy of the users [4-5]. The cryptography algorithms scramble the secret data using the key and give the encrypted data in the output. In cryptography, the Advanced Encryption Standard (AES) and Homomorphic encryption algorithm are most preferred [6-7]. The AES algorithm provides better security but consumes large memory. The Homomorphic encryption algorithm takes long execution time for data encryption due to the long key size. On the other side, the data perturbation algorithms add noise to the original data and give noisy data in the output. The data perturbation algorithms take less time as compared to the cryptography algorithms but less secure. In data perturbation, noise addition and noise multiplication are the most preferred algorithms [7-10]. The major limitation of the existing data perturbation algorithm is that the noise parameter needs to communicate to the receiver.

To overcome all these challenges, we have proposed a lightweight privacy-preserving scheme by hybrid the cryptography and data perturbation algorithm. The data communicates to the control center contains the user's information as well as their electricity consumption data. Thus, the user's information that is sensitive data is encrypted using the cryptography ANU algorithm. On the other side, the data perturbation algorithm is applied to the electricity consumption data to make it noisy. Thus, difficult for the attacker to spy the data. In addition, the noise generated and added such a way no need to communication noise parameter to the receiver. The experimental results show that the proposed technique consumes less execution time, memory and provide better security.

The rest of the paper as follows. Section 2 shows that related work is done privacy-preserving. Section 3 explains the proposed technique in detail. Section 4 shows the experimental results. Conclusion and future scope are drawn in Section 5.

2. RELATED WORK

In this section, cryptography and data perturbation algorithms used in the literature are discussed. Section 2.1 explains the most preferred cryptography algorithms. Section 2.2 explains the data perturbation algorithms.

2.1 Cryptography Algorithms

The Advanced Encrypted Standard (AES) is used for encrypting a large amount of data in the smart grid. The detail description is given below.

2.2.1 Advanced Encryption Standard (AES): AES algorithm is based on the substitution-permutation network. AES contains one substitution layer (s-layer) and 2 permutation layers (shift row and mix column) [6]. The block diagram of AES is shown in Figure 1. AES algorithm process the data in the block size of $128 - bit$, supports three key sizes $128/192/256$bits, and total $10/12/14$ rounds according to the key size. Initially, add round key operation performed between plaintext and key. Thereafter, it passed to the first round. Each round performs substitution and permutation operation on the data. In addition, generate the sub-key from the original key in each round. The plaintext 128-bit is processed into 8-bit chunks when passed through the substitution layer. The s-layer contains a look-up table that contains $2^8 = 256$ combinations. Further, permutation layer, mix column required 2 look-up table that contains the same combination as s-layer contains. Thus, the AES algorithm consumes a large amount of memory.

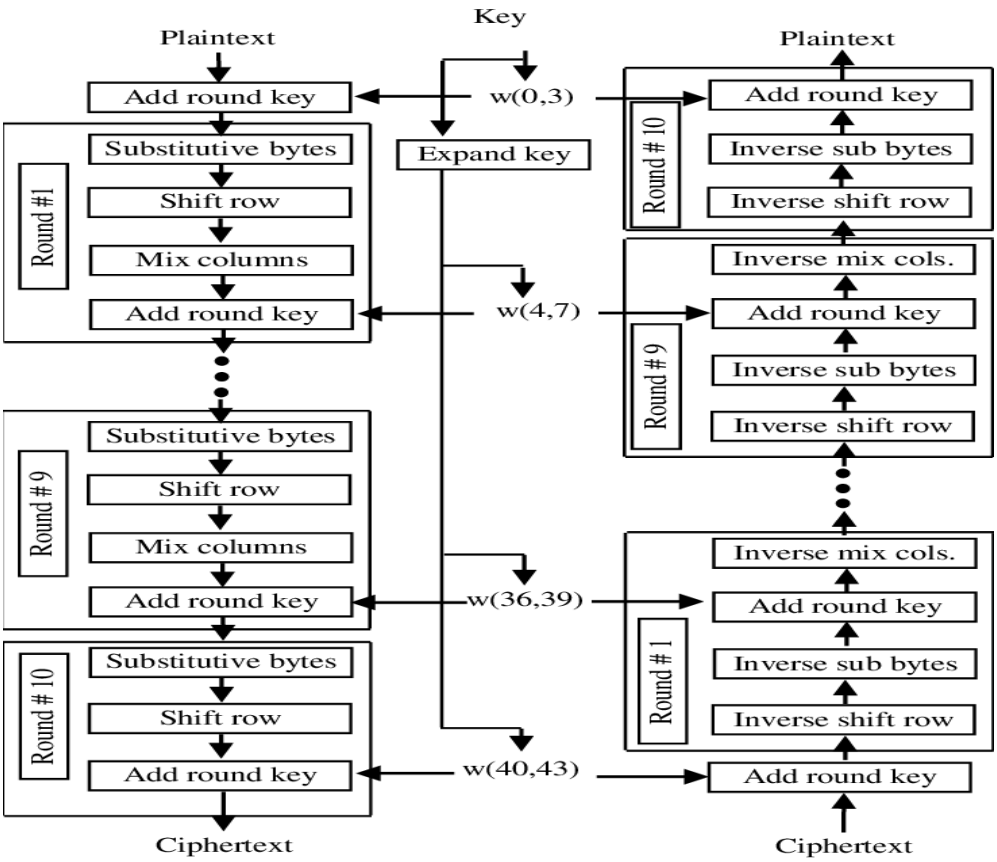

Fig. 1: Block Diagram of AES Algorithm

2.2 Perturbation Algorithms

The data perturbation algorithm makes the data noisy to preserve the privacy of the user. In the literature, the data perturbation is divided into two parts, data-oriented and context-oriented [10]. In the data-oriented approach, the user information is made noisy to protect it from the external attacks like eavesdropping attack. In the context-oriented approach, the user location and timing information is secured. The most popular data perturbation algorithm noise addition and multiplication are performed on the data using Eq. (1-2).

$$Output_{noisy} = Input\ Data + Noise \quad (1)$$

$$Output_{noisy} = Input\ DataXNoise \quad (2)$$

The noise parameter needs to send to the receiver.

3. PROPOSED TECHNIQUE

In the given paper, an algorithm is proposed intended for the preservation of privacy in the smart meter. Security method, say, data encryption and also anonymization algorithm are utilized. The encryption algorithm utilized here is the ANU algorithm, which has the benefit of low memory consumption and better security. On the other side, the anonymization algorithm utilized

here is noise addition, which has the benefit of simple operations and defends data privacy. The flowchart of the privacy-preserving algorithm for the smart meter is shown in figure 2. The detail description is given below.

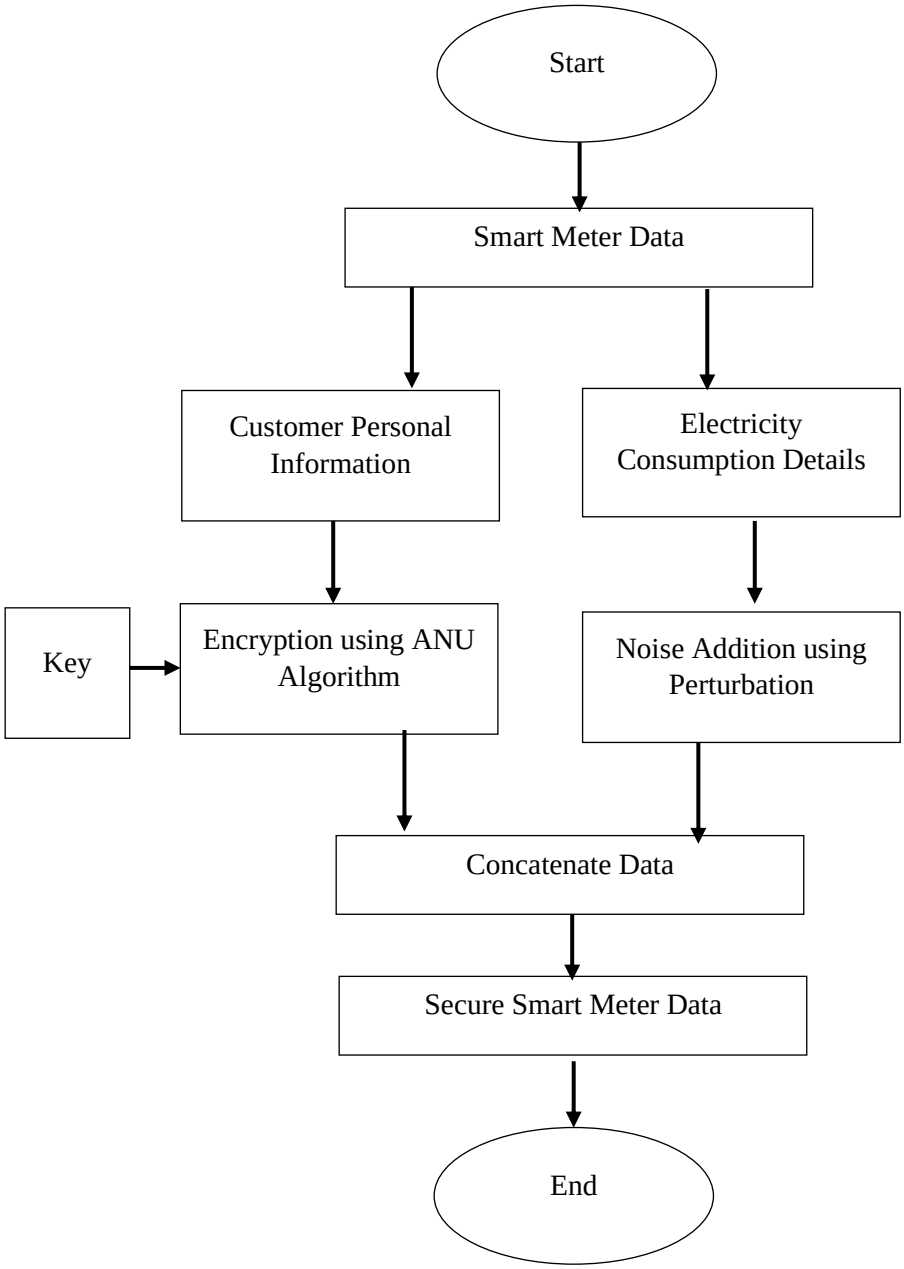

Fig. 2: Architecture of Privacy-Preserving Algorithm for the Smart Meter

3.1 Smart Meter Data

The smart meter contains a number of customer information and electricity attributes. The customer information attributes are $\{Customer\ Name, Smart\ Meter\ ID, Mobile\ Number, Address\}$ and electricity attributes are $\{Total\ Electricity\ Consumption, Smart\ Meter\ Rent, Load\ Information\}$.

3.2 Data Encryption and Anonymization Algorithm

Initially, the customer information and electricity attributes are split because encrypting all information takes long execution time and increases the latency for processing the data for different departments. Thus, customer information is encrypted using lightweight algorithm ANU and electricity information altered using noise addition perturbation algorithm. The detail description is given below.

3.2.1 ANU Algorithm: ANU algorithm comes under the category of lightweight algorithm and proposed by Bansod et al. in 2016 [11]. The algorithm is based on Feistel Network (FN) that comes under the category of the symmetric algorithm. Thus, the same key required for encryption and decryption purposes. The algorithm has a block size $64-bit$, two key sizes $80/128bit$ and required 25 rounds for data encryption. The data encryption process is explained below. Initially, the $64-bit$ data is read and split into two parts known as (P_i^L) and (P_i^R). On the left part, the function (F) is applied. The function contains two sub-functions (F_1) and (F_2). The function (F_1) shuffles the bits of the left part by performing the left circular shifting by 3-bits and passing through its substitution box known as s-box. Thereafter, XOR operation performed between the shuffled bits and the right part (P_i^R). Next, again on the left part function (F_2) applies and bit shuffle by performing the right circular shifting by 8-bit and passing through s-box. The shuffle bits XOR operation performed with the previously generated shuffle bits and key as shown in Fig. 3.

In the last, the left and the right part bits interchanged by performing bit-level permutation. The whole process is performed 25 times for data encryption. The detail description of circular shifting, S-box, permutation, and key scheduling is given below.

- **Circular Shift**: The circular shift operation changes the bit position of the data stream.
- **S-Box**: The substitution box is based on the bijective mapping. Bijective mapping is basically one to one mapping. The data bits are transformed from one form to another and vice versa on the receiver side. The data 64-bits are processed in a 4-bit chunk. Thus, 2^4 combinations generated in the s-box as shown in Table 1. The 4-bits are represented in the hexadecimal form. The hexadecimal value varies from 0- F.

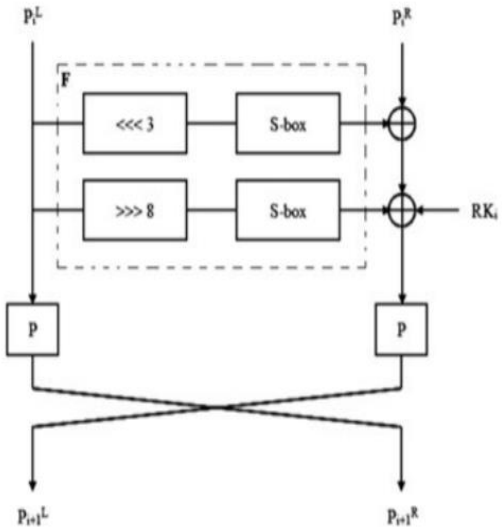

Fig. 3: Block Diagram of ANU Cipher

Table 1: S-Box

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

- **Permutation**: The permutation layer shuffles the data bits at a bit level. The permutation is done on the basis of table 2 in the ANU algorithm.

Table 2: Permutation- Layer

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

- **Key Scheduling**: The key scheduling algorithm generates the sub-keys for each round. The key scheduling algorithm for 80/128-bit is shown in Table 3.

Table 3: Key Scheduling for the ANU Cipher

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

3.2.2 Noise Addition Perturbation Algorithm: To secure the electricity data noise addition perturbation algorithm is applied to the electricity consumption details. The detail description of the noise addition is given below.

$$Z = X + \sigma \quad (3)$$

whereas, Z, X denotes the transformed and original data. σ is the standard deviation of the data attributes that work as noise in our work. The advantage of the proposed noise addition method is that we don't have to communicate the standard deviation parameter to the smart grid. But, on the other side, there is a high correlation between original and noisy data. Thus, we have passed the noisy data through the permutation layer of the ANU algorithm that reduces the correlation between them. On the receiver side, the inverse permutation is applied that gives the noisy data. Thereafter, the standard deviation of noisy data is calculated and subtracted from it that gives the original data in the output using Eq. (2).

$$X = Z - \sigma \quad (4)$$

4. EXPERIMENTAL RESULTS

In this section, the proposed technique simulation, performance analysis, and comparative analysis with existing techniques are done to validate the results. The code is written and simulated in MATLAB 2013a. The system configuration is $i7$ processor, 8GB RAM. We have calculated various parameters correlation, execution time, memory consumption, avalanche effect for the proposed technique as explained below.

- **Correlation:** This parameter measures the correlation between original and encrypted data. In the MATLAB corr2 command available that gives the correlation between data. In the ideal case, the correlation near zero value for the data encryption algorithm. In Table 4, the correlation for the different datasets. The ANU algorithm achieves better correlation as compared to the data perturbation algorithm. Thus, the customer information is highly secure.

Table 4: Correction between Original and Encrypted data

Original Data	ANU Algorithm Correlation	Data Perturbation Correlation
Dataset1	-0.0687	-0.6074
Dataset2	-0.1574	-0.6090
Dataset3	-0.0662	-0.6079
Dataset4	-0.1505	-0.6108
Dataset5	-0.1276	-0.6089

- **Execution Time:** The total time taken by the ANU algorithm for data encryption and noise addition by data perturbation is measured in seconds. In the MATLAB, tic and toc command available to achieve this goal. We have taken a number of the dataset on that proposed technique applied. The execution time for the different datasets is shown in Table 5.

Table 5: Execution Time for the Proposed Technique

Original Data	Execution Time (Seconds)
Dataset1	0.41
Dataset2	0.40
Dataset3	0.42
Dataset4	0.48
Dataset5	0.41

- **Memory Consumption:** In the cryptography algorithms, the substitution layer consumes maximum memory in the form of the look-up table. Thus, the memory consumed by the ANU algorithm is 64-bit.
- **Avalanche Effect:** Avalanche effect is the security parameter of the cryptography algorithm. In the avalanche effect, we measure how many bits are changed in the ciphertext with changing 1-bit in the key. In the ideal case, a 50% probability is required. It is calculated using Eq. (5).

$$Avalanche\ Effect: \frac{Number\ of\ Bits\ Changed}{Block\ Size} X100 \quad (5)$$

Table 6: Avalanche Effect for the ANU Algorithm

Plaintext: $[0000\ 0000\ 0000\ 0000]_{Hex}$	Plaintext: $[0000\ 0000\ 0000\ 0000]_{Hex}$
Key: $[0000\ 0000\ 0000\ 0000\ 0000]_{Hex}$	Key: $[0000\ 1000\ 0000\ 0000\ 0000]_{Hex}$
Ciphertext:$[\ 53b4\ 6545\ 6af0\ 3349]_{Hex}$	Ciphertext:$[96e9\ 6b2d\ d117\ 76b8]_{Hex}$
Avalanche Effect: $\frac{35}{64}X100$=54%	

In last, we have done the comparative analysis of the proposed technique with the existing technique in Table 7. The results show that the proposed technique gives better results as compared to the existing AES algorithm.

Table 7: Comparative Analysis with the Existing Technique

Parameters	AES [6]	Proposed Technique
Execution Time	2.97	0.42
Memory Consumption	16384	64
Avalanche Effect	50%	54%

5. CONCLUSION AND FUTURE SCOPE

In this paper, we have designed a lightweight privacy-preserving technique. We have deployed a lightweight algorithm ANU to secure the sensitive information of the customer and the perturbation noise addition algorithm to secure the electricity consumption. The experimental results show the proposed technique achieves better correlation, consumes less memory and execution time, and provide better security as compared to the existing algorithm. In the future, we will do hardware implementation of the proposed technique to improve the performance in terms of throughput. In addition, explore other lightweight privacy-preserving techniques.

6. REFERENCES

[1] Chen, Hanchun, and Yongjie Yang. "A Practical Scheme of Smart Grid Privacy Protection." In *IOP Conference Series: Materials Science and Engineering*, vol. 394, no. 4, p. 042058. IOP Publishing, 2018.

[2] McDaniel, Patrick, and Stephen McLaughlin. "Security and privacy challenges in the smart grid." *IEEE Security & Privacy* 7, no. 3 (2009): 75-77.

[3] Chen, Hanchun, and Yongjie Yang. "A Practical Scheme of Smart Grid Privacy Protection." In *IOP Conference Series: Materials Science and Engineering*, vol. 394, no. 4, p. 042058. IOP Publishing, 2018.

[4] Iyer, Swapna. "Cyber security for smart grid, cryptography, and privacy." *International Journal of Digital Multimedia Broadcasting* 2011 (2011).

[5] Savi, Marco, Cristina Rottondi, and Giacomo Verticale. "Evaluation of the precision-privacy tradeoff of data perturbation for smart metering." *IEEE Transactions on Smart Grid* 6, no. 5 (2015): 2409-2416.

[6] Li, Shaohua, Kaiping Xue, David SL Wei, Hao Yue, Nenghai Yu, and Peilin Hong. "SecGrid: A Secure and Efficient SGX-Enabled Smart Grid System With Rich Functionalities." *IEEE Transactions on Information Forensics and Security* 15 (2019): 1318-1330.

[7] Li, Fengjun, Bo Luo, and Peng Liu. "Secure information aggregation for smart grids using homomorphic encryption." In *2010 first IEEE international conference on smart grid communications*, pp. 327-332. IEEE, 2010.

[8] Chen, Yuwen, José-Fernán Martínez, Pedro Castillejo, and Lourdes López. "A privacy-preserving noise addition data aggregation scheme for smart grid." *Energies* 11, no. 11 (2018): 2972.

[9] Chen, Keke, and Ling Liu. "A survey of multiplicative perturbation for privacy-preserving data mining." In *Privacy-Preserving Data Mining*, pp. 157-181. Springer, Boston, MA, 2008.

[10] Mert, Dilan, Mehmet Ulvi Şimşek, and Suat Özdemir. "Privacy Preserving Metering Protocol in Smart Grids." In *IFIP International Conference on Artificial Intelligence Applications and Innovations*, pp. 467-477. Springer, Cham, 2015.

[11] 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.

