Journal of Theoretical and Applied Information Technology
31st January 2019. Vol.97. No 2

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

INCORPORATING DEOXYRIBONUCLEIC ACID IN AES SCHEME FOR ENHANCING SECURITY AND PRIVACY PROTECTION

OMAR G. ABOOD[1], MAHMOUD A. ELSADD[2], SHAWKAT K. GUIRGUIS[1]
[1] Department of Information Technology, Institute of Graduate Studies and Researches, Alexandria University, Egypt.
[2] Department of Electrical Engineering, Faculty of Engineering, Menoufia University, Egypt.

Corresponding author: omar.ghazi88@yahoo.com

ABSTRACT

This paper presents an algorithm based on AES through modifications of the system. The algorithm developed herein is based on incorporating DNA computing in AES algorithm instead of the mix-column stage. The modified algorithm enhances the process to be more secure under the communicated signals used in the smart grid especially in the self-healing process. The breaking time is increased via using two keys whilst keeping the round times. Furthermore, the encryption and decryption times are decreased which is a critical in many smart grid applications. The work carried out a comparison within the study between the modified and the conventional AES algorithms under the different methods of control employed in the fault management. The total time needed to accomplish the fault management process including the encryption and decryption times is computed and evaluated. The assessment of the presented method is done through MATLAB. The sample results are evaluated and discussed.

Keywords:- *AES, DNA, Fault management, Privacy protection, Smart grid, Self-healing.*

1. INTRODUCTION

The conventional electrical power distribution system has not had complete information about outage details and comes out with consequently inefficient responses that could be concluded. The smart grid has the ability of transmitting power with elevated efficiency and responding to a wide range of events and conditions using modern information technologies. Hence, the smart grid can be seen as an electric system relying on the use of information technologies that use two-way communications and computational intelligence in a combined system across generating, transmitting, distributing and consuming electricity to fulfill a system that can be considered clean, with safety, reliability, flexibility, and can be more efficient and sustainable [1]-[2].

Many applications of the smart grid require sharing private information over communication media assembling all agents distributed in the grid. This requires improved security as the information as the information tends to be sensitive especially those used for smart protection purposes. However, nowadays, the transmission of data suffers from attacks from a wide array of malicious users. Therefore, the demand on security is increasing at a rapid pace [**3**]. Consequently, the cryptography algorithms, combining the encrypting and decrypting processes on information is necessary to overcome these attacks. The most well-known cryptography algorithms are DES [4], RSA [5], BLOWFISH [6], T-DES [7] and AES [8]. The strength of the algorithms can be only evaluated via three factors, namely: brute force attack, key size, and block cipher [9]. They are briefly showcased in the Appendix A. According to the extensive comparative studies, AES presents the best algorithm out of the mentioned ones [10]-[11]. Hence, the trend nowadays improving AES.

Different modern encryption techniques were presented to enhance the AES algorithm. These techniques only concentrate on decreasing the required encryption time through employing different agents. In [3], a method is presented, based on the fuzzy logic principle to control

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

the reading and writing operation of the overall S-box. Additionally, the memory operations which are used as inputs to AES and the lifting scheme wavelet are employed to decrease the data transfer capacity. However, this work hasn't been employed with any smart grid application.

The work presented in [12] uses a DNA computing and round-reduced AES block cipher combined. The method used images with the dimensions of n×m = 256×256 pixels. This work also hasn't been applied to any of the smart network applications. Another work presented in [13] used an encryption method through JEX encoding/decoding combined with the proposed AES algorithm modified for encryption. This method was applied on image data file, yet it also hasn't been applied in the smart grid applications field. A high-definition image encryption scheme relying on an improved 128-bit AES (AES-128) cipher is presented in [14]. In the method, the same round role is used on a plaintext for 10 rounds to generate a cipher text with a secret key. The round function comprises of four different sub-functions, namely: Sub Byte, Shift Row, Mix Column and Add Round Key. The work presented three alterations on AES-128 to decrease the encryption and decryption speeds as it
removed the Mix Column in Rounds 2, 4, 6, 8 and 10, to decrease the amount of logic gates in hardware execution through the simplification of the s-box used in Sub Byte and to elevate the security level of AES-128 by adding Mix Column to the key schedule algorithm which is used to generate a number of round keys from a secret key.

Another work [15] presented an AES-like cipher relying on key-dependent S-boxes. The cipher was designed to meet the design standards of AES. This was implemented to increase the security level to be comparable with the AES to resist black-box attacks. Other than that, a white-box implementation for the AES-like cipher proposed should be sufficient in withstanding the existing white-box attacks. Accordingly,
[16] evaluated the main component of the image encryption scheme that the research presented. The work was a presentation of the modified AES-128 cipher. A main measure in the development of a block cipher is the security. Accordingly, the plaintext chosen should be resisted by the block cipher against any possible attacks as the attacker should have permission to a wide array of chosen-plaintext and ciphertext pairs. However, these contemporary methods do not concentrate on increasing the breaking time through complicating the key. Additionally, these contemporary methods were
not assessed under real signals of smart grid applications.

Some of the most crucial applications for smart grid happens to be self-healing. This specific application is defined as fault management which is done automatically [17]. Accordingly,
to identify and isolate the faulty segment and then restore the remainder of the gird are all done without the consent of the user in an automatic fashion. This process requires information
to be transferred between the distributed agents which are usually Intelligent Electronic Devices (IEDs). The information sequence differs depending on the control method employed within the grid. The control methods are centralized [17], decentralized [17], autonomous [18] and modified centralized [19]. Thus, the communication information between the agents should always be secured. However, the used encryption time is crucial to reduce the required
time to restore the grid.

The main contribution of this paper is presenting a modified AES algorithm through incorporating DNA computing in AES algorithm instead of the mix-column stage. The presented algorithm is more suitable for the used signals in the self-healing smart grid rather than that of the conventional AES algorithms. The presented algorithm decreases the total required time for restoring the service through the self-healing process by reducing the encryption/decryption time under any used control method compared with the traditional AES algorithm.

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

2. STRUCTURE OF AES

The AES has become the most common selection for numerous applications which has led to its adoption as the standard encryption method used by the National Institute of Standards and Technology (NIST) at the beginning of the 2000s [10]. AES presents a block cipher which is symmetric and contains data blocks of 128-bits with the use of a cipher key of varying lengths (128, 192 or 256) with number of rounds Nr =10, 12 or 14, respectively. Figure. 1 illustrates the AES algorithm. In this Figure., the data block consisting of an array of 4 × 4 bytes is called a state. In the left side of Figure. 1, the four different transformations of the encryption process are sequentially applied on the state. These transformations are Add Round Key; Sub Byte; Shift Rows and Mix Columns [9].

At first, the Add round key stage is a mixture between each value of the state and that of the round key is carried out using the XOR operation. Second, the Sub Byte stage is a non-linear substitution function. This function can be described in a substation table called s-box used to decode the state via converting each value to its corresponding in the s-box table. On the third stage, the Shift Rows cyclically shift the bytes in the final three rows of the state to the left direction. Therefore, the left shift changes from one to three bytes. The final step employs the Mix Column which is a process that is done through the use of a fixed matrix. Accordingly, the multiplication within the step is carried out as though it is polynomial instead of being numerical. Each of the rows within the transformation matrix is multiplied with the column corresponding to it. The process of decryption is done via the inverse stage of the sequence of the stages before where the function of each step is inversed. For instance, the inverse Shift Rows is cyclically shifting the bytes in the last three rows of the state to the right direction.

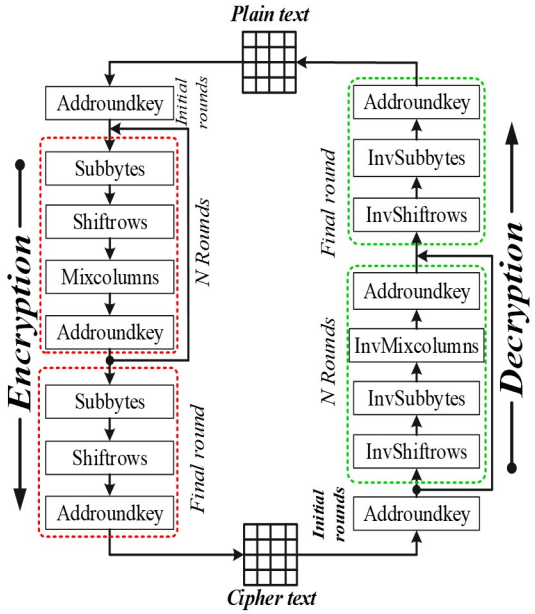

Figure. 1 Description of the AES algorithm steps [9]

3. PROPOSED ALGORITHM

Using AES algorithm on smart grid information has shown poor encryption and decryption speed. The system employs the use of AES with DNA in an incorporated algorithm in order to overcome the problem of the elevated encryption and decryption speed. This is due to the DNA coding-based cryptosystems that have shown promising results in terms of encryption due to their massive parallelism, storage and the extremely low power consumption that take [20].

The aim of incorporating DNA Computing within the AES algorithm is to achieve the highest level of security. Through the model, the key length was increased while the number of rounds remained the same 10 rounds. The aim of increasing the key length is to disable the attackers from breaking into the system while maintaining a decreased time delay for the encryption/decryption and increased complexity. Three keys were used for the development of the key to the proposed methodology. Those are presented as:

- ***First Key:***

  AES key size 2^{128} bits: this key presents the main key for the AES algorithm.

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

- ***Second Key:***
  DNA key size 2^4 bits: this key presents the DNA base where the probability of the key could be:

  - **A= 11, 10, 01, 00**
  - **T= 11, 10, 01, 00**
  - **C= 11, 10, 01, 00**
  - **G= 11, 10, 01, 00**

- ***Third Key:***

  Three different DNA bases: this base is presented as one of the following:

No. base	Encryption	Decryption
1	A=T and C=G	T=A and G=C
2	A=C and T=G	C=A and G=T
3	A=G and T=C	G=A and C=T

  - **(A=C, G=T)**
  - **(A=G, T=C)**
  - **(A=T, G=C)**

Those three keys present the developed key for the proposed system as shown in Figure. 2. In addition to obtaining a longer key in the proposed method, this system attempted to decrease the timeframe of the encryption and decryption by altering one of the stages of the AES algorithm. The stage altered is the MIX column stage where it was replaced with a DNA Helix which we named "DNA column".

The process of the DNA column is initially turning the Hex message obtained from the Shift rows step into a Binary message which is then transformed through the variable DNA computing bases into a DNA helix that is ciphered through the DNA bases to present a wholly different outcome which is returned into Binary text and thus transformed into a Hex message once again to move on to the Added round key step. DNA column used is considered a second and third keys that increase the complexity of the proposed algorithm as shown in Figure. 3. In Figure. 4 as shown flowchart to explain the methodology for the proposed algorithm.

The next example explains the contribution to the proposed system when using:

- ***Plaintext:***

"Journal of Theoretical and Applied Information Technology".

- ***Secret key:***

First Key 2^{128} bit:

"omarghaziabood88"

Second Key 2^4 bit:

A=	**11,**	**10,**	**01,**	**00.**
T=	10,	11,	00,	01.
C=	01,	00,	11,	10.
G=	00,	01,	10,	11.

Third Key 3 bit:

- ***Hex numbers:***

50 6f 6c 79 6d 65 72 73 20 66 6f 72 20 41 64 76 61 6e 63 65 64 20 54 65 63 68 6e 6f 6c 6f 67 69 65 73

- ***Binary code:***

01010000011011110110110001111001011011010110010101110010011100110010000001100110011011110111001000100000010000010100100011101100110000101101110011000110110010101100100001000000101010001100101011000110110100001101110011011110110110001101111011001110110100101100101011100111

- ***DNA bar nuclear (by second key):***

GGTTGGAAGGAGGCTAATCAGCCATCCACGTACGCGTTTATATAGACACGTGTTTCTTCATCTACATATTCAGATATGCATCCATCTGTTTCCTGCGGGCTAGCCTGCACGCAAGCATGCAAGCGAGCCGGCGGGATA

- ***Encoding DNA bar nuclear (by third key):***

CCAACCTTCCTCCGATTACTCCCTACCAGCATGCGCAAATATATCTGTGCACAAAGAAGTAGATGTATAAGACTATACGTAGGTAGACAAAGGACGCCCGATCGGACGTGCGTTCGTACGTTCGCTCGGCCGCCCTAT

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

- ***Encoding Binary code (by second key):***

101011111010000010100010100111000011 100010101000111010110110110001100110111 111001100110010000100011011101111110111 110100110111000100110011110111100011001 110010011010100110111101111110101111001 101010011100100101111001000110010000100 100111001000010001001011010011010100011 00

- ***Encoding Hex numbers:***

AF A0 A2 9C 38 A8 EB 6C 66 FC CC 84 6E FD F4 DC 4C F7 8C E4 D4 DE FD 79 A9 C9 79 19 A9 C9 79 19 93 90 89 69 9A 8C

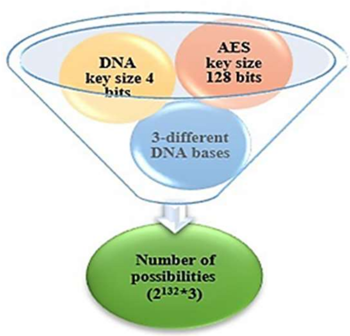

Figure. 2 Number of possibilities

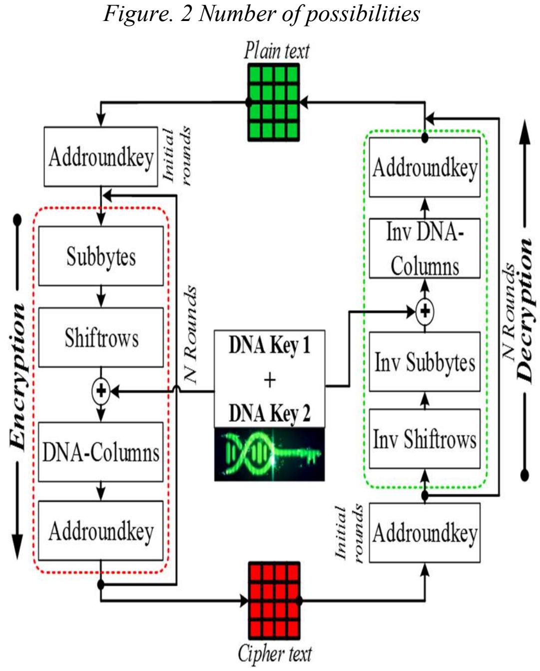

Figure. 3 Hybridization AES and DNA Computing

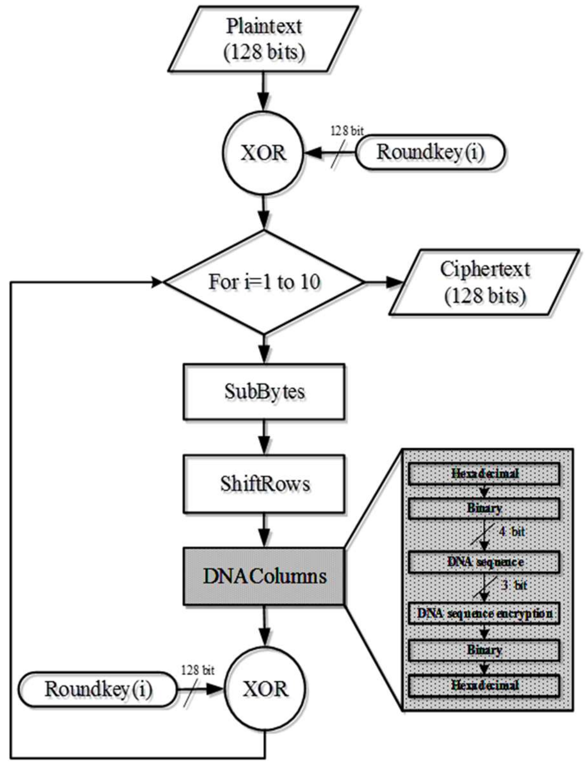

Figure. 4 flow charts for the proposed algorithm.

4. PERFORMANCE ANALYSIS OF THE PROPOSED SCHEME VERSUS THE CONVENTIONAL AES SCHEME

The performance of the proposed and conventional AES schemes is investigated in the self-healing process through the use of the IEEE 33-bus 11 kV test radial distribution feeder [19]. The performance evaluation process is done under all possible control methods that are centralized [17], decentralized [17], autonomous [18], and modified centralized control [19] strategies.

A. Self-healing Process

The world today has grown to make use of integrated protection and control schemes in order to utilize sensitive sensors and smart devices which include electronics such as Intelligent Electronic Devices (IEDs) in order to participate in self-healing of the modern distribution systems [21] [22]. The aim of those self-healing systems is to aid in obtaining a completely automated fault management system [23]. The process of fault management begins at the disconnection of the feeder and thus the disappearance of the feeder voltage in what comprises three consequences which are: Fault Management, Restoration and

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

Reparation. Those three consequences require a strategy of control in order to verify the self-healing perspective. Current control strategies are: centralized [17], decentralized [17], autonomous [18] and [24] and the modified centralized control strategies [19]. Accordingly, the control is centralized if the decision is taken at the control center level, however, if it is taken at a secondary substation level it means that the control is decentralized. Autonomous control takes another step where the decision is taken at a secondary substation initiated from the secondary substation level. For every substation, an agent is implemented to send and receive fault messages detailing the fault status.

Based on the centralized and decentralized control rules presented in [17], their implementations needed m2 + 7m +5 and 2m+2 communication hops, respectively, when the faulted segment is between substations m-1 and m. However, those communication hops need large latency, encryption and decryption times along with lowering the relatability of the fault management process as showcased in [18]. Accordingly, an autonomous strategy was introduced in [18] and [24], where it is characterized through decreasing the latency time due to a lower number of activated communication hops. Upon the disappearance of the feeder voltage, each secondary substation sensing the fault (through the indicator) to send the signal to the next substation in the downstream direction. In addition, upon not sensing the fault by the substation, then the faulted segment is recognized and then the section becomes isolated. After that, a direct connection to the primary substation is then exploited in order to update the control and restore the performed action. The strategy only requires five communication hops to restore the service and update the control centers [18]. Additionally, the reliability of the fault detection and communication are employed with the autonomous agent control to distinctively identify the fault based on two fault indicators statuses with the least number of communication hops.

While the advantages of autonomous fault management are numerous, the implementation

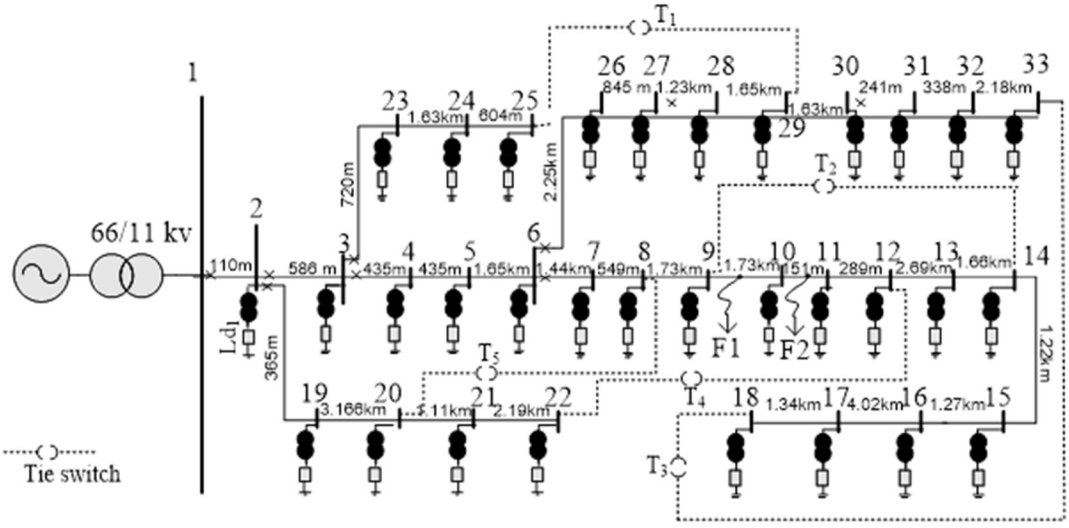

Figure. 5 IEEE 33-bus feeder with implemented agents.

requires a massive number of communication channels between each of the secondary substations and the primary one and the fault indicators (FIs). Most common FIs are based on a non-directional function may encounter mal-operations under existing Distributed Generations (DGs) [19]. To decrease the number of measuring devices, several fault location applications in the fault management strategies have been recently introduced in conjunction with the centralized

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

control strategy. Despite the fact that the control is centralized, the latency in time decreases due to the communication between the lateral substations because of the utilization of the computed fault location. The estimated fault distance at the substation is often employed in finding the faulty sections. Following that, the message is communicated up to the corresponding secondary substation for the isolation of the switches where the identification process requires communication hops' number to be equal to the lateral substations' number forward the faulty point. Then, the faulty segment is isolated through the use of control signals communicated from this panel substation to the two secondary substations upand downstream the faulted section. All previous works in this area are concentrated on reducing the restoration time improving the distribution network reliability through reducing the number of the communication hops only despite the encryption/decryption time of this signals.

B. Simulated System

The IEEE 33-bus 11 kV test radial distribution feeder has been selected as a study system; accordingly, the feeder's data is gathered from the EEE's Distribution System Analysis Subcommittee [25]. Illustrated in Figure. 5 is the feeder where 60 closed switches found at each section terminals where the sections (10-11) and (11-12) are implanted to section (12-13) as a one zone due to short lengths. Additionally, there are five open switches which are added to the system to verify system recon Figure uration [26].

C. Delay time calculation under different control methodologies

The total required time of the fault management process is calculated under all contemporary control methods. The total time is the summation of the communication latency and the encryption/decryption times. Also, it is calculated under different fault points. Supposing that the number of the required binary digits for representing all required information for verifying the fault management procedure is 11, the total number of the possible probabilities is 2^{11}.

All these probabilities are used as inputs for both the conventional AES and the proposed scheme. Then, the performance of the presented and the conventional methods are investigated. Some of the results are listed in Table 1. The results confirm that the encryption/decryption time is reduced using the presented scheme. The two right side columns illustrate the encryption/decryption time difference between both the proposed and conventional methods (Δt). Using some statistical studies for all 2^{11} cases, the summation time, average time and the minimum of the encryption/decryption time difference are obtained as shown in Table 2.

The summation of the communication latency is listed in Table 3 under different fault points using all contemporary control strategies. The delay in communication happens to be a random quantity [26] which is based on the use of the function of probability density as in (Δt= 0.168 s) for radio communication along the replacement agents. As such, the delay time is calculated by (Nch *Δt). Also, the encryption and decryption times are obtained based on the average of the encryption and decryption time, respectively under different fault points using all contemporary control strategies. As shown in Table 3, the total required time for accomplishing the fault management process is remarkably reduced under using the proposed algorithm. The reduction percentage of the total restoration time is about 30 % based on the average encryption/decryption time. Further, the total breaking time is increased via using two keys.

5. CONCLUSION

The presented modified AES algorithm is based on incorporating DNA computing in AES algorithm instead of the mix-column stage. Further, it uses three keys keeping the round times and the key length is increased. Therefore, the security process is remarkably increased where the required breaking time is increased. Further, the encryption and decryption time is decreased that are important in many smart grid applications such as the fault management process. The total required time of accomplishing the fault management process including the encryption and decryption time is calculated.

Further, in this model, DNA with complexity "N" replaces mix column with the same

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

complexity. It increases the conversion process and keeps the encryption and decryption time which as indicated in the results. In contrast, we get a system with three secret keys which multiplies the strength of the proposed system as illustrated in the results. The results provided the evidence that the modified algorithm reduced the total required time and increased the data security compared with the conventional AES algorithms.

In this context, the adversaries necessity the information about secret keys, making their selection more challenging. Therefore, it is desired to use complex secret keys, having enough larger length to resist against brute-force attacks. In the future work, the plan is to enhance encryption and decryption time by integrating Quintom computing concept with our proposed algorithm.

REFERENCES

[1] H. Gharavi and R. Ghafurian, "Smart Grid: The Electric Energy System of the Future," in Proc. of the IEEE, vol. 99, no. 6, pp. 917-921, June 2011.

[2] M. Kezunovic, "Smart Fault Location for Smart Grids," IEEE Transactions on Smart Grid, vol. 2, no. 1, pp. 11-22, March 2011.

[3] C. Sapna Kumari and K. V. Prasad, "FPGA Implementation of AES Algorithm for Image, Audio, and Video Signal," in Proc. of International Conference on Intelligent Computing and Applications. Springer, Singapore, 2018.

[4] W. Diffie and M. E. Hellman, "Special Feature Exhaustive Cryptanalysis of the NBS Data Encryption Standard," in Computer, vol. 10, no. 6, pp. 74-84, June 1977.

[5] R. L. Rivest, A. Shamir, and L. Adleman, "A Method for Obtaining Digital Signatures and Public-Key Cryptosystems," Communications of the ACM, vol. 21, no. 2, pp. 120-126, February 1978.

[6] 6- S. Bruce, "Description of a New Variable-Length key, 64-bit Block Cipher (Blowfish)," in Proc. of Cambridge Security Workshop, Fast Software Encryption. Springer-Verlag, Berlin, Heidelberg, pp.191-204, December 1993.

[7] B. Association, "Tripple Data Encryption Algorithm Modes of Operation," ANSI X9: 52-1998. Retrieved 2017-09-05. Extends ANSI X3.92-1981 Data Encryption Algorithm.

[8] FIPS, PUB. "197, Advanced Encryption Standard (AES)," National Institute of Standards and Technology, U.S. Department of Commerce, November 2001.

[9] S. William, "Cryptography and Network Security: Principles and Practice," Pearson Education, India, 2006.

[10] P. Kumar and S. B. Rana, "Development of Modified AES Algorithm for Data Security," Optik-International Journal for Light and Electron Optics, vol. 127, no. 4, pp. 2341–2345, 2016.

[11] O. G. Abood, M. A. Elsadd and S. K. Guirguis, "Investigation of Cryptography Algorithms Used for Security and Privacy Protection in Smart Grid," Proc. of IEEE 9th International Middle East Power Systems Conference, (MEPCON), Cairo, Egypt, pp.644-649, December 2017.

[12] E. Shehab, A. K. Farag and A. Keshk, "An Image Encryption Technique based on DNA Encoding and Round-reduced AES Block Cipher," International Journal of Computer Applications, vol. 107 no. 20, pp.1-6, December 2014.

[13] S.T. Sharma, M. Kantak and N. Vernekar, "Novel Approach to Image Encryption: Using a Combination of JEX Encoding-Decoding with the Modified AES Algorithm," Information and Communication Technology for Sustainable Development. Springer, Singapore, pp.201-210, 2018.

[14] S. M. Wadi and N. Zainal, "High Definition Image Encryption Algorithm based on AES Modification," Wireless Personal

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

Communications, vol. 79, no.2, pp. 811-829, 2014.

[15] B. Kunpeng and C. Wu, "An AES-Like Cipher and its White-Box Implementation," The Computer Journal, vol. 59, no.7, pp.1054-1065, 2016.

[16] Y. W. She, R. C. Phan and B.M. Goi. "Cryptanalysis of a High-Definition Image Encryption Based on AES Modification," Wireless Personal Communications, vol. 88, no.3, pp. 685-699, 2016.

[17] M. Nordman and M. Lehtonen, "An Agent Concept for Managing Electrical Distribution Networks," IEEE Trans Power Delivery, vol. 20, pp. 696-703, April 2005.

[18] N. Tarhuni, N. Elkalashy, T. Kawady and M. Lehtonen, "Autonomous Control Strategy for Fault Management in Distribution Networks," Electric Power Systems Research, vol. 121, pp. 252-59, April 2015.

[19] M. A. Elsadd, N. I. Elkalashy, T. Kawady, A. I. Taalab and M. Lehtonen, "Incorporating Earth Fault Location in Management Control Scheme for Distribution Networks," IET Generation, Transmission & Distribution, vol. 10, no. 10, pp. 2389-2398, July 2016.

[20] C. Junxin, Z. Zhi-liang, Z. Li-bo, Z. Yushu and Y. Ben-qiang, "Exploiting Self-Adaptive Permutation–Diffusion and DNA Random Encoding for Secure and Efficient Image Encryption," Signal Processing, vol. 142, pp. 340-353, January 2018.

[21] Grid 2030: "A National Vision for Electricity's Second 100 Years," Office In: Electric Transmission and Distribution, United States Department of Energy, Washington, DC, July 2003.

[22] G. Han, B. Xu, K. Fan, and G.Lv, "An Open Communication Architecture for Distribution Automation based on IEC 61850," International Journal of Electrical Power & Energy Systems, vol. 54, pp. 315-324, January 2014.

[23] C. Xia, and B. Liu, "Hierarchical Management and Control based on MAS for Distribution Grid via Intelligent Mode Switching," International Journal of Electrical Power & Energy Systems, vol. 54, pp. 352-366, January 2014.

[24] F. H. Malik, and M. Lehtonen, "Agents in Smart Grids," Electric Power Systems Research, vol. 131, pp. 71-79, 2016.

[25] V. Holkar and D. Masand, "Power Flow Analysis of RDS by Artificial Network Technique," Journal of Electrical and Electronics Engineering, vol. 2, no. 2, pp. 42-46, October 2012.

[26] S. Ghasemi and J. Moshtagh, "Radial Distribution Systems Recon Figureuration Considering Power Losses Cost and Damage Cost Due to Power Supply Interruption of Consumers," International Journal on Electrical Engineering, vol. 5, no. 3, pp. 297-315, September 2013.

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

current recommendation is to use at least 128-bit blocks.

APPENDIX

A brute force attack which is also known as a dictionary attack is a trial and error method of obtaining the private key of a specific encrypted packet of data. The trial and error process are carried out through a computer which means an elevation in the computational power in what leads to more "tries" which can be done in a short time period. When the time for computing increases, so does the performance and the capability of finding the private key. The only obstacle would be an increase in the key length.

Key size is basically the number of bits in a key which are employed through a cryptographic algorithm. Accordingly, the correct key is the only one that can decrypt the ciphertext (output) back into the original plaintext (input). While there is an increase in the computational power, there becomes another increase related to it required by the brute force to break through the key encryption. Accordingly, the key lengths increase that way in order to be more secured.

Some algorithms employ "***block ciphers***", which work on the encryption and decryption of data in blocks (fixed length groups of bits). This showcases the relation between the block-size and the data amount which can be encrypted without replicating blocks. To explain this, another work would be required in order to reach the length of information necessary for the comprehension of the topic. However, the key takeaway is that the

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

Table 1: Encryption And Decryption Time Under Different Random Signals

Signal	Encryption time (s)		Decryption time (s)		Δt	
	Conventional	Proposed	Conventional	Proposed	Encryption	Decryption
00000000001	0.085268	0.033845	0.0721	0.035126	0.051423	0.036974
00000000010	0.078724	0.039075	0.07634	0.032526	0.039649	0.043814
00000000011	0.06874	0.042576	0.0853	0.025144	0.026164	0.060156
00000000100	0.061857	0.0245	0.08252	0.030011	0.037357	0.052509
00000000101	0.05976	0.03885	0.0712	0.032233	0.02091	0.038967
00000000110	0.073587	0.039831	0.06811	0.042662	0.033756	0.025448
00000000111	0.065972	0.038245	0.0708	0.023845	0.027727	0.046955
00000001000	0.06295	0.033845	0.07318	0.029075	0.029105	0.044105
00000001001	0.06159	0.046819	0.06008	0.032576	0.014771	0.027504
00000001010	0.056901	0.0361	0.06919	0.0345	0.020801	0.03469
00000001011	0.05456	0.047306	0.0842	0.02885	0.007254	0.05535

Table 2: The Summation, Average, And The Minimum Of The Encryption/Decryption Time Difference Between The Proposed And Conventional Methods

	Encryption time		Decryption time	
	Conventional	Proposed	Conventional	Proposed
$\sum_{i=1}^{2^{11}} t$	162.1573	67.1805	165.0508	60.7182
$\frac{\sum_{i=1}^{2^{11}} t}{2^{11}}$	0.0792	0.0328	0.0806	0.0296
Min $(\Delta t)_i$	0.003506		0.013127	

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

Table 3: The Total Time Using The Average Encryption/Decryption Time

Faulty Section	Control Strat.	N_{ch}	Latency Time (s)	Encryption time (s)		Decryption time (s)		Total time (s)	
				Conventional	Proposed	Conventional	Proposed	Conventional	Proposed
1-2	centralized [17]	23	3.864	1.8216	0.7544	1.8538	0.6808	7.5394	5.2992
	decentralized [17]	6	1.008	0.4752	0.1968	0.4836	0.1776	1.9668	1.3824
	autonomous [18]	3	0.504	0.2376	0.0984	0.2418	0.0888	0.9834	0.6912
	modified centralized [19]	3	0.504	0.2376	0.0984	0.2418	0.0888	0.9834	0.6912
2-3	centralized [17]	35	5.88	2.7720	1.1480	2.8210	1.0360	11.473	8.064
	decentralized [17]	8	1.344	0.6336	0.2624	0.6448	0.2368	2.6224	1.8432
	autonomous [18]	5	0.8400	0.3960	0.1640	0.4030	0.1480	1.639	1.152
	modified centralized [19]	6	1.008	0.4752	0.1968	0.4836	0.1776	1.9668	1.3824
4-5	centralized [17]	65	10.92	5.1480	2.1320	5.2390	1.9240	21.307	14.976
	decentralized [17]	12	2.016	0.9504	0.3936	0.9672	0.3552	3.9336	2.7648
	autonomous [18]	5	0.8400	0.3960	0.1640	0.4030	0.1480	1.639	1.152
	modified centralized [19]	9	1.512	0.7128	0.2952	0.7254	0.2664	2.9502	2.0736
7-8	centralized [17]	125	21	9.9000	4.1000	10.075	3.7000	40.975	28.8
	decentralized [17]	18	3.024	1.4256	0.5904	1.4508	0.5328	5.9004	4.1472
	autonomous [18]	5	0.8400	0.3960	0.1640	0.4030	0.1480	1.639	1.152
	modified centralized [19]	10	1.68	0.7920	0.3280	0.8060	0.2960	3.278	2.304
17-18	centralized [17]	455	76.44	36.0360	14.924	36.673	13.4680	149.149	104.832
	decentralized [17]	38	6.384	3.0096	1.2464	3.0628	1.1248	12.4564	8.7552
	autonomous [18]	5	0.8400	0.3960	0.1640	0.4030	0.1480	1.639	1.152
	modified centralized [19]	10	1.68	0.7920	0.3280	0.8060	0.2960	3.278	2.304