Indian Journal of Science and Technology, Vol 10(39), DOI: 10.17485/ijst/2017/v10i39/119856, October 2017
ISSN (Print) : 0974-6846
ISSN (Online) : 0974-5645

A Choice of Symmetric Cryptographic Algorithms based on Multi-Criteria Analysis Approach for Securing Smart Grid

Raja Mouachi*, Addi Ait-Mlouk, Fatima Gharnati and Mustapha Raoufi

Laboratory of Intelligent Energy Management and Information Systems, Faculty of Sciences Semlalia, Cadi Ayyad University, Marrakech, Morocco; mouachiraja@gmail.com, aitmlouk@gmail.com, gharnati@uca.ac.ma, raoufi@uca.ma

Abstract

In order to optimize production, consumption and distribution of energy, the different devices of a Smart Grid (SG) exchange daily increasing flows of information. Moreover, SG produces much more data stream than the traditional network. In addition to the large volume, the data of the SG are characterized by their diversity. However, securing these data flows is essential. Indeed, a single failure or attack could compromise the safety of the whole electrical network, the malfunction of which could have serious repercussions. Therefore, cryptography as a solution is necessary for SG to become realizable and secure. Being able to classify and to make a good choice of symmetric cryptographic algorithms for security of SG, we proposed to use an approach based on multi-criteria analysis.

Keywords: Confidentiality, Cryptography, Security, Smart Grid, Multi-criteria Analysis, PROMETHEE GAIA

1. Introduction

The use of the SG has huge economic benefits, privacy concerns and critical security. SG is based on the idea of a two-way digital communication control device in the consumer's home. It is a joint electrical grid, increased power from suppliers to consumers[1,2]. Further advantages of the SG must be protected to improve the reliability, efficiency, economy and national security as an improved easier to control and monitor.

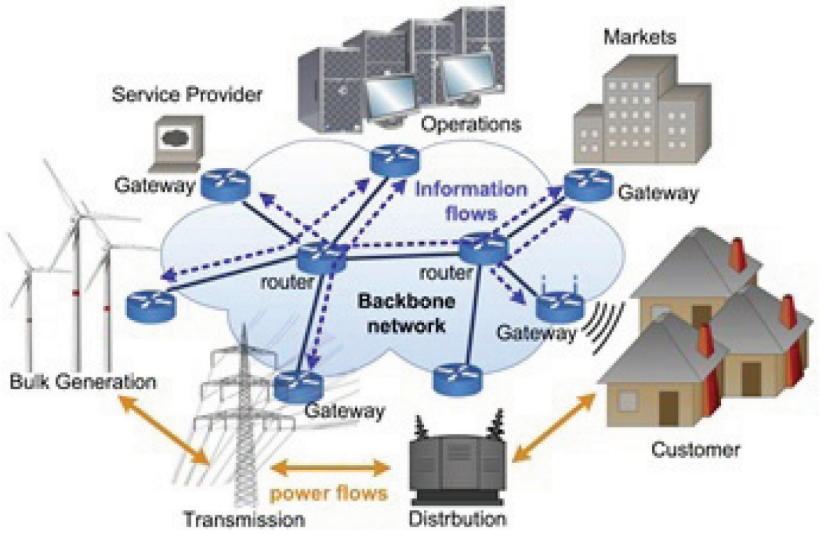


Figure1. The network architecture in the SG: backbone and local-area networks.

*Author for correspondence

With the transformation of the current power system to the SG, many advantages, for customers as well as providers, arise like stability, reliability, easier integration of "green" energy and reduction of costs are just a few of them. Also, the SG offers energy efficient solutions for both customers and providers[3]. But with the complexity that enables these advantages, the SG also becomes vulnerable to attacks and failure. Risks to security like hacking attacks or data theft are as much a problem as privacy[4]. The collected consumption data is very detailed which is very dangerous when in the wrong hands, for both companies and customers. Not only can malicious attackers get valuable information about the customers from this data, but also the power company itself or third parties, like the customer's employer, can use the information for advertisements or surveillance.

It is essential to understand what are the security objectives before providing a comprehensive treatment of cyber security in the SG. Here, we describe the security objectives for the SG:

- **Availability**: Accessing information in a timely in the SG. Loss of availability could affect the power delivery since access to authorized individuals might be denied.
- **Integrity**: Only the authorized party is allowed to modify the transmitted information[5]. Loss of integrity in the SG might modify sensors values and products recipes, which in turn can affect the power management.
- **Confidentiality**: it means protecting against unauthorized disclosure of information. It may be applied to whole messages, parts of messages, and even existence of messages[6].
- **Authentication**: It ensures the reliability of the message by checking the origin of a message what it claims to be [7]. Authentication of humans and machine is crucial, and a weakness in it can lead to an illegitimate device making use of the SG resources or an attacker gaining access to private information.

The security issues in SG is a very active area of research. Moreover, it is in this context that our work dedicated to the comparison and choice of symmetric cryptography algorithms for securing SG based on multiple analysis approaches.

2. Related Work

2.1 Type of Cryptography

One way to guarantee the security objectives in the SG is the use of cryptography. The objective of cryptography is not only encrypting and decrypting process but it is also about solving real-world problems that require information security[8]. In fact, cryptographic techniques are being recommended in the Roadmap and NIST Framework for the SG.

Asymmetric and symmetric encryption are the two basic encryption technique in cryptography.

2.1.1 Asymmetric Encryption

This method operates with a pair of keys, consisting of a public key and a private key. It brings security in a wide range of applications that cannot be solved using only symmetric techniques.

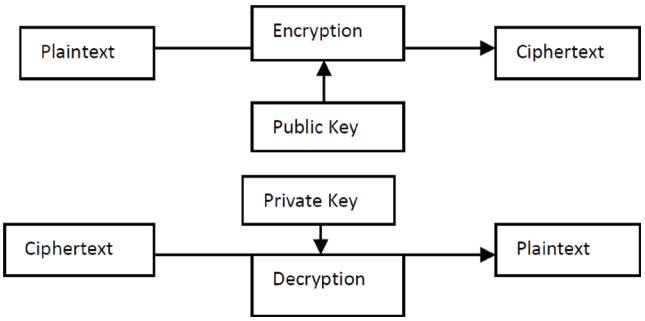


Figure 3. Asymmetric encryption.

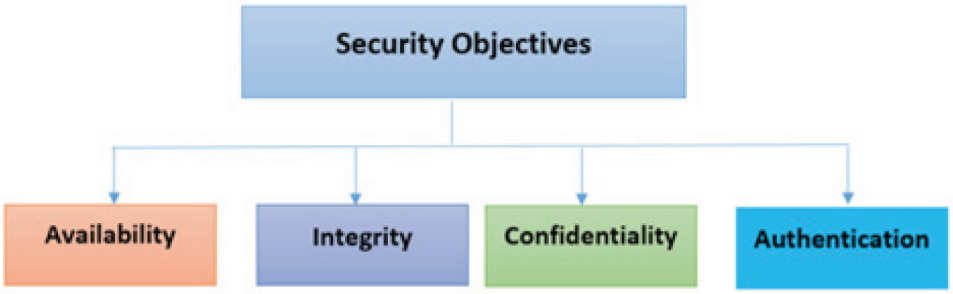


Figure 2. Four high-level security objectives for the Smart Grid.

2.1.2 Symmetric Encryption

Involved two parties who share a joint secret or key. This exclusive knowledge of the key enables private and secure communications between the two parties.

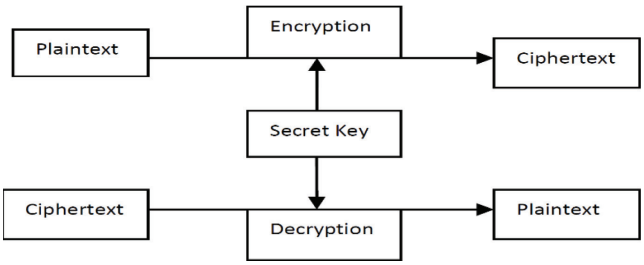


Figure 4. Symmetric encryption.

2.2 Compared Symmetric Cryptography Algorithms

The symmetric cryptography algorithms that will be implemented and analyzed are as follows:

Blowfish: It is a symmetric block cipher that takes block size of 64 bits with variable length key and it was developed by Schneier[9]. It is slowly gaining popularity as a robust encryption algorithm[10].

DES: DES is a symmetric block cipher, with a 64-bit block size and a 56- bit key. It consists of a16-round series of substitutions and permutations. In each round, data and key bits are shifted, permitted, XORed, and sent through, 8 s-boxes, a set of lookup tables that are essential to the DES algorithm. The decryption is the same operation, operated in reverse[11].

3DES: Triple DES is also called Triple Data Encryption Algorithm, which is a block cipher. It is based on the DES algorithm. The key length is 112 bits or 168 bits and block size is 64-bit length. 3DES was developed to provide a relatively uncomplicated method of increasing the key size of DES to protect against such attacks[12].

AES: Advance Encryption Standard (AES) was designed by Vincent Rijmen and Joan Daemen and it is one of the Symmetric key block cipher that is identical key is used for both encryption and decryption. In this block cipher algorithm, the Key length: 128, 192, or 256 bit and Block length: 128 bit which is very big in size[13]. Each round of AES uses permutations and substitution network, and is suitable for both hardware and software implementation[14]. The Table 1 shows the theoretical comparison between DES, AES, 3DES, BLOWFISH algorithms.

3. Methodology

3.1 Choice of MCDA Method

MCA is a sub-field of operational research, and management science, dedicated to the development of decision support tools in order to solve multi-criteria problems. When modeling a real decision problem using multi-criteria analysis, three types of problematic, choice, sorting and ranking are distinguished. The multi-criteria analysis provides the ability to rank the symmetric cryptography algorithms according to a set of proposed criteria.

3.2 Description of PROMETHEE Method

This method developed by Brans[15,16] has been applied in several situations thanks to its ability to simplify and solve multi-criteria problems by following the given steps[17,18]:

First of all, it is necessary to determine the matrix of k criteria according to the n different alternatives, Let A= {a1,…,an} the set of n alternatives, and j={f1,…,fq} the set of q criteria, (see Table 2).

Table 1. Characteristics of algorithms

Algorithms	*Year of use*	*Key Size*	*Size of block*	*No. Of Rounds*	*Structure*	*Feature*	*Flexible*
DES	*1977*	*64 bits*	*64-bits*	*16*	*Feistel*	*Not structure Enough*	*No*
AES	*2000*	*128, 192 or 256 bits*	*128-bits*	*10, 12, 14*	*Substitution, Permutation*	*Replacement for DES,Excellent Security*	*Yes*
3DES	*1978*	*112 or 118 bits*	*64-bits*	*48*	*Feistel*	*Adequate Security*	*Yes*
BLOWFISH	*1993*	*32-448 bits*	*64-bit*	*16*	*Feistel*	*Excellent Security*	*Yes*

Table 2. Evaluation table

	F_1	F_2	...	F_k	...	F_q
A_1	$f_1(a_1)$	$f_2(a_1)$	...	a	...	$f_q(a_1)$
A_2	$f_1(a_2)$	$f_2(a_1)$	...	a	...	$f_q(a_2)$
...	...	...	...	...	...	...
A_n	$f_1(a_n)$	$f_2(a_n)$	...	a	...	$f_q(a_n)$

$$\forall a_i, a_j \in A : d_k(a_i, a_j) = f_k(a_i) - f_k(a_j) \quad (1)$$
$$\pi(a_i, a_j) = P_k\left[d_k(a_i, a_j)\right]$$

The alternative a is better than alternative b according to criterion f, if f (a) > f (b). The preference function can take values on the scale from 0 to 1.

When the function of preference has been associated to each criterion by the decision maker, all comparisons between all pairs of actions can be performed for all criteria. A degree of preference is then calculated for each couple of action by the formula (2).

$$\pi(a,b) = \sum_{k=1}^{q} P_k(a,b).w_k \quad (2)$$

where, wj are weights associated with criteria (the importance of the criterion in percentages, close to 1 if very important, close to 0 if very little significant).

$$w_k \geq 0 \quad And \quad \sum_{k=1}^{q} w_k = 1$$

Compute preference matrix:

$$\forall a_i, a_j \in A : \pi(a_i, a_j) = \sum_{k=1}^{q} w_k \pi_k(a_i, a_j) \quad (3)$$

As a consequence:

$$\pi(a_i, a_i) = 0$$
$$\pi(a_i, a_j) \geq 0$$
$$\pi(a_i, a_j) + \pi(a_j, a_i) \leq 0$$

Compute flow scores:

$$\phi^+(a_i) = \frac{1}{n-1}\sum_{b \in A} \pi(a_i, b)$$
$$\phi^-(a_i) = \frac{1}{n-1}\sum_{b \in A} \pi(b, a_i)$$
$$\phi(a_i) = \phi^+(a_i) - \phi^-(a_i) \quad (4)$$

As a consequence:

$$\phi(a_i) \in [-1;1] \text{ And } \sum_{a_i \in A} \phi(a_i) = 0$$

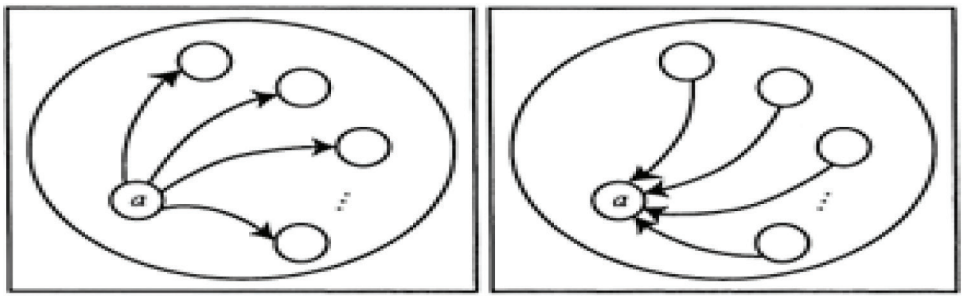
Complete rankings based on the net flow score.

$$a_i P a_j \Leftrightarrow \phi(a_i) \succ \phi(a_j)$$
$$a_i I a_j \Leftrightarrow \phi(a_i) = \phi(a_j)$$

The Partial ranking are:

$$a_i P a_j \Leftrightarrow \left[\phi^+(a_i) \succ \phi^+(a_j)\right] \wedge \left[\phi^-(a_i) \leq \phi^-(a_j)\right]$$
$$a_i P a_j \Leftrightarrow \left[\phi^+(a_i) \geq \phi^+(a_j)\right] \wedge \left[\phi^-(a_i) \prec \phi^-(a_j)\right]$$
$$a_i I a_j \Leftrightarrow \left[\phi^+(a_i) = \phi^+(a_j)\right] \wedge \left[\phi^-(a_i) = \phi^-(a_j)\right]$$
$$a_i J a_j otherwise$$

PROMETHEE GAIA (Geometrical Analysis for Interactive Aid) the Promethee and Gaia method helps decision makers find the alternative that best suits their goal and their understanding of the problem, Figure 5.



(a) The $\phi^+(a)$ outranking flow. (b) The $\phi^-(a)$ outranking flow.

Figure 5. The PROMETHEE outranking flows.

Plan GAIA (geometrical analysis for interactive aid)
We have:

$$\Phi(a_i) = \frac{1}{n-1}\sum_{b\in A}\sum_{k=1}^{q} w_k \pi(a_i,b) - \frac{1}{n-1}\sum_{b\in A}\sum_{k=1}^{q} w_k \pi_k(b,a_i)$$

$$= \sum_{k=1}^{q} w_k \frac{1}{n-1}\sum_{b\in A} \pi_k(a_i,b) - \pi_k(b,a_i) = \sum_{k=1}^{q} w_k \phi_k(a_i)$$

where,

$$\Phi_k(a_i) = \sum_{b\in A} \pi_k(a_i,b) - \pi_k(b,a_i)$$

Every alternative can be represented by a vector in a space to q dimensions.

$$\vec{\phi}(a_i) = \left[\phi_1(a_i),\ldots,\phi_q(a_i)\right]$$

3.3 Analysis of Symmetric Cryptography Algorithms

Each of the encryption techniques has its own strong and weak points. In order to apply a suitable cryptography algorithm to Smart Grid, we should have knowledge regarding performance, strength and weakness of the algorithms. Therefore, these algorithms must be analyzed based on several features.

This section aims at comparing symmetric cryptographic algorithms in terms of a number of parameters to choose the best one for Smart Grid:

- Memory used
- Encryption time
- Decryption time
- Battery energy consumed
- Simulation time

For the implementation of the algorithms, MATLAB is used. The Table 3 shows the Comparison between AES-128, AES-192, AES-256, DES, 3DES, BlOWFISH.

To classify symmetric cryptography algorithms and to choose the best one for SG in terms of different criteria previous described we choose to apply the multi-criteria analysis approach named PROMETHEE. The following section details this comparative approach.

3.4 Application of PROMETHEE Method

In this section, we will apply the proposed approach to classify symmetric cryptography algorithms and to choose the best one for SG in terms of different criteria.

Based on the decision maker's preferences, the Table 3 gives the evaluation table as a list of values in rows and columns that allows the analyst to identify the performance of relationships between sets of rules and measures. The evaluation table is used to describe a multi-criteria decision analysis problem where each alternative need to be evaluated on N criteria. The Table 4 represents weights of relative importance of different criteria.

The next step is the computation of preference between pairwise, this function expressing with which degree algorithm_i is preferred to algorithm_j over all criterion, and algorithm_j is preferred to algorithm_i.

Next, we compute the partial and global outranking flow Table 5 then we present the final result of association rules ranking over all criteria used by the decision makers see Table 5.

The graphic illustration of result processing is obtained by using PROMETHEE in Figure 7, and by using GAIA plan Figure 8.

Table 3. Comparison between AES-128, AES-192, AES-256, DES, 3DES, BlOWFISH

	Memory used (KB)	Encryption time (ms)	Decryption time (ms)	Battery energy consumed	Simulation time (ms)
AES-128	10.7	750	480	50	1300
AES-192	12.9	880	520	55	1420
AES-256	14.7	990	630	60	1670
DES	18.2	1001	900	68	2000
3DES	20.7	1150	800	75	1970
BLOWFISH	9.38	710	622	55	1410

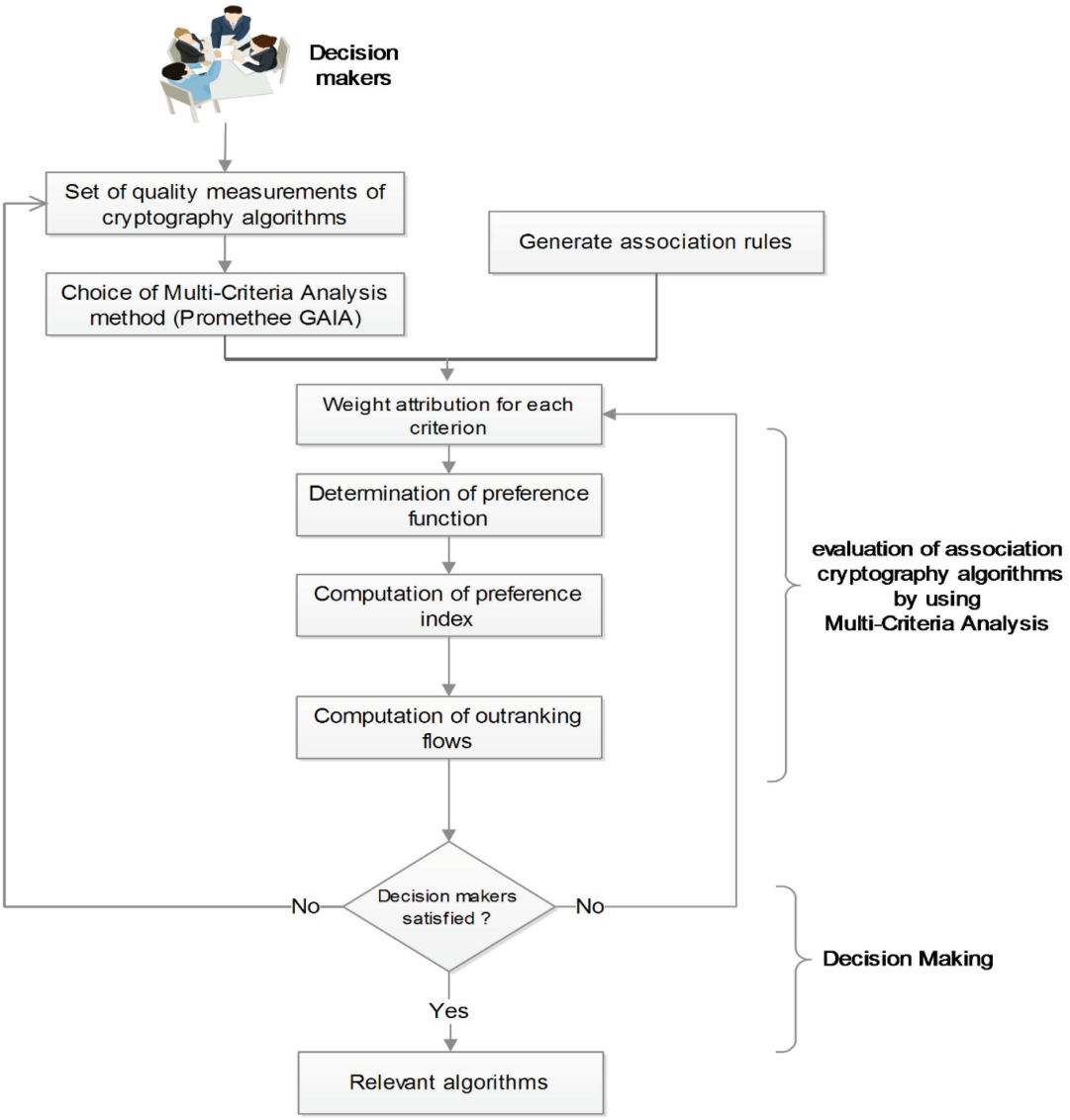


Figure 6. Multi criteria analysis process.

Table 4. Weights of relative importance

Criteria	Memory used (KB)	Encryption time(ms)	Decryption time(ms)	Battery energy consumed	Simulation time (ms)
weight	5.00	3.00	3.00	2.00	1,00

Table 5. Preference flow

	Memory used	Encryption time	Decryption Time	Battery	Simulation time
AES-128	0,6000	0,6000	1,0000	1,0000	1,0000
AES-192	0,2000	0,2000	0,6000	0,4000	0,2000
AES-256	-0,2000	-0,2000	-0,2000	-0,2000	-0,2000
DES	-0,6000	-0,6000	-1,0000	-0,6000	-1,0000
3DES	-1,0000	-1,0000	-0,6000	-1,0000	-0,6000
Blowfish	1,0000	1,0000	0,2000	0,4000	0,6000

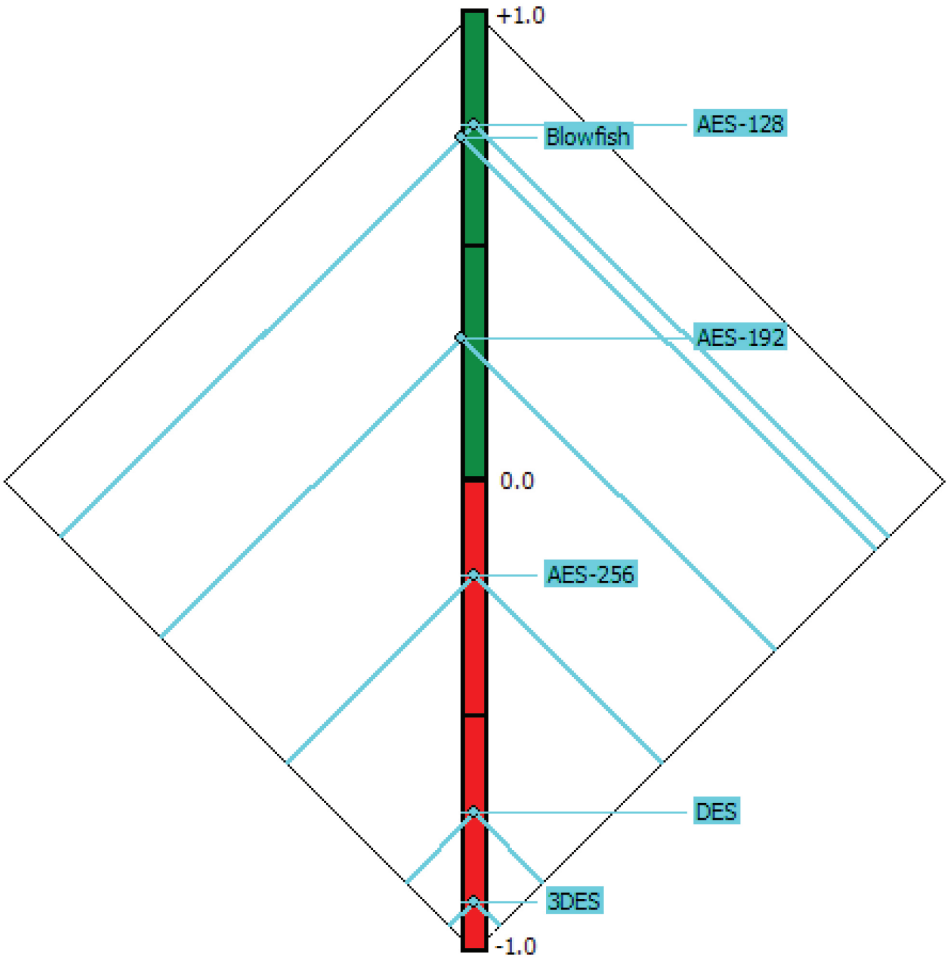


Figure 7. PROMETHEE rankings of algorithms.

Reading the results obtained by the PROMETHEE method, it is graphically confirmed that algorithm AES-128, has the strongest flow index, so it is the most relevant one, concluded, the interesting algorithms according to the decision maker's preferences are presented by order in Table 6 from Orders 1 to 6.

Table 6. weights of relative importance

	action	Phi	Phi+	Phi-
1	AES-128	0,7600	0,8800	0,1200
2	Blowfish	0,7333	0,8533	0,1200
3	AES-192	0,3067	0,6400	0,3333
4	AES-256	-0,2000	0,4000	0,6000
5	DES	-0,7067	0,1467	0,8533
6	3DES	-0,8933	0,0533	0,9467

4. Conclusion and Future Work

Cryptography plays a vital role in securing communication for SG. To secure communication in SG, various cryptography methods are used. These methods are based on symmetric or private key-based encryption and asymmetric or public key based encryption. Each of the cryptography methods has its own strong and weak points. So it is important to use correct encryption method. In this paper, we presented different symmetric cryptographic algorithms and their characteristics. Compared by using a multi-criteria approach in which we proposed the use of PROMETHEE method. In fact, the application of this method confirmed that AES-128 is the appropriate selected algorithm according to the preference of decision makers. In the future work, we will

Figure 8. GAIA plan for algorithms rankings.

implement a new approach based on the results found in this work in order to propose a solution to secure the flow of data that circulates in SG network.

5. References

1. Sajjad H, Zafar RO. Key management scheme and cryptography in smart grid elements. International Journal of Advanced Research in Computer Science and Software Engineering. 2015; 5(8).
2. Flick T, Morehouse J. Securing the Smart Grid: Next generation power grid security: Elsevier Science; 2010.
3. Amin SM, Wollenberg BF. Toward a smart grid: power delivery for the 21st century. Power and Energy Magazine, IEEE. 2005; 2:34–41. Crossref.
4. Cavoukian CWA, Polonetsky J. Smartprivacy for the smart grid: Embedding privacy into the design of electricity conservation. Technical report, Information and Privacy Commissioner (IPC), Ontario, Canada; 2009.
5. Pethe HB, Pande SR. Comparative study and analysis of cryptographic algorithms AES and RSA. International Journal of Advance Research in Computer Science and Management Studies. 2017 Jan; 5(1).
6. Thakur J, Kumar N. DES, AES and Blowfish: Symmetric key cryptography algorithms simulation based performance analysis. The International Journal of Emerging Technology and Advanced Engineering. 2011 Dec; 1(2).
7. Sasi SB, Dixon D, Wilson J. A general comparison of symmetric and asymmetric cryptosystems for WSNs and an overview of location based encryption technique for improving security. IOSR Journal of Engineering. 2014 Mar; 4(3).
8. Vijayakumar P, Indupriya S, Rajashree R. A hybrid multilevel security scheme using DNA computing based color code and elliptic curve cryptography. Indian Journal of Science and Technology. 2016 Mar; 9(10).

9. Schneier B. The Blowfish Encryption Algorithm [Internet]. [cited]2008 Oct 25. Available from: http://www.schneier.com/blowfish.html.
10. Mandal PC. Superiority of blowfish Algorithm. 128X International Journal of Advanced Research in Computer Science and Software Engineering. 2012 Sep; 2(9).
11. AbdElminaam DS, Kader HMA, Hadhoud MM. Evalution the performance of symmetric encryption algorithms. International Journal Of Network Security. 2010 May; 10(3):216–22.
12. Karthik S, Muruganandam A. Data encryption and decryption by using triple DES and performance analysis of crypto system. 2014 Nov; 2(11):2347–3878.
13. Pahal R, Kumar V. Efficient implementation of AES. International Journal of Advanced Research in Computer Science and Software Engineering. 2013 Jul; 3(7).
14. Soumya D, Ramesha K, Guruprasad SP. A survey on cryptography algorithms for network communication. International Journal of Engineering Science and Computing. 2016; 6(5).
15. Brans JP, Mareschal B, Vincke P. How to select and how to rank projects: The PROMETHEE method. European Journal of Operational Research. 1986; 24(2):228–38. Crossref.
16. Brans JP, Mareschal P. The PROMETHEEGAIA decision support system for multicriteria investigations. Investigation Operativa. 1994; 4(2):107–17.
17. Ait-Mlouk A, Gharnati F, Agouti T. Multi-criteria decisional approach for extracting relevant association rules. International Journal of Computational Science and Engineering. 2017; 15(314). Crossref.
18. Ait-Mlouk A, Gharnati F, Agouti T. An improved approach for association rules mining using multi-criteria decision support system: A case study in road safety. European Transport Research Review. 2017; 9(3). Crossref.