Evaluating the Security of Wireless Networks using Artificial Intelligence

Sirwan Ahmed Mohammed
CNS/ATM Manager
Sulaimaniyah International Airport

Evaluating the Security of Wireless Networks using Artificial Intelligence

Sirwan Ahmed Mohammed
CNS/ATM Manager
Sulaimaniyah International Airport
Sirwan@sulairport.krd

Abstract

The main propose of this paper is to show of security evaluation of the wireless Telecommunication network. Information security helps users feel more confident and trust the network by making sure their sensitive information is kept confidential, intact, and accessible.

This paper aims to simplify the understanding of securing wireless networks against hacking attempts. The model's assessment was conducted using an Artificial Intelligence program, specifically employing a fuzzy logic tool and code. This is because cryptography stands as a pivotal element in the system responsible for safeguarding information. Given the heavy reliance of many organizations on information systems for their day-to-day operations, ensuring their security is a paramount concern. As no information system can be entirely impervious to breaches, it becomes imperative to assess and ascertain the level of security information enjoys on the Wireless network.

This study introduces a methodology for evaluating the security of cryptography algorithms by employing a fuzzy logic system. To achieve this, the system necessitates well-defined fuzzy sets that capture various expressions of information security objectives. These sets are instrumental in accurately assessing the inputs. The process of defuzzification was executed through the Centroid technique. The results showcase an effective system for analyzing the security level.

Keywords: Cryptography algorithms, RC5 algorithm, Blowfish algorithm, DES algorithm, AES algorithm, information security, Fuzzy logic, Artificial Intelligent.

1. INTRODUCTION

This paper focuses on the assessment of wireless network security using artificial intelligence. It emphasizes the significant assets inherent in a wireless communication system that are pivotal to safeguard for optimal system performance. Additionally, the paper conducts a comparative analysis of various security algorithms, specifically categorizing them into symmetric (private) and asymmetric (public) key encryption. For this study, symmetric key encryption was employed, which involves using a single key for both encrypting and decrypting data in the symmetric algorithm [2,3 ,4 ,6 , 9, 10, 12].

Numerous instances of both robust and vulnerable cryptographic keys can be found in algorithms like RC5, Blowfish, DES, and AES. DES relies on a singular 64-bit key, whereas Blowfish employs a range of keys (32-448 bits), and RC5 employs a 2040-bit key. This paper delves into a methodology for assessing the security level of chosen symmetric encryption algorithms. Cryptographic algorithms consume considerable computational resources, including factors such as block size, number of rounds, and key size [7, 8, , 15, 18].

This research assesses four distinct encryption algorithms: DES, Blowfish, RC5, and AES. The evaluation encompasses varying data types such as text, documents, audio, and video data, along with alterations in packet size and key size for the specified cryptographic algorithms [1, 21, 23]. This chapter comprises three sets of experiments. Initially, AES, RC5, Blowfish, and DES algorithms are appraised using artificial intelligence, and the findings of this assessment will be presented. Subsequently, the outcomes of the DES algorithm, which serves as a case study for the evaluation of wireless networks, will be expounded employing the Fuzzy logic tool. Finally, a comparative analysis of AES, RC5, Blowfish, and DES will be conducted based on their respective security levels [2,5,7,8,9,10,12,14, 16,17,20,24].

2. Symmetric algorithm

2.1 RC5 algorithm

The RC5 encryption algorithm can be characterized by the following parameters [19]:

-Block Size (b): The algorithm operates on plain text data blocks of variable length, which can be either 16, 32, or 64 bits.

-Key Length (k): RC5 employs a key of selectable length, which can vary from 0 to 2040 bits, corresponding to 0 to 255 bytes.

-Number of Rounds (r): The algorithm is organized into a series of iterations known as "rounds." The number of rounds, denoted as 'r,' can take values within the range of 0 to 255.

2.2 Blowfish algorithm

Blowfish, conceived in 1993 by Bruce Schneier, is a symmetric block cipher employing a variable-length key. It is widely integrated into numerous encryption products and cipher suites. This 64-bit cipher functions through two main components: a key expansion phase and a data encryption phase. The key expansion component transforms a key, potentially up to 448 bits long, into various subkey arrays, summing up to 4168 bytes. Subsequently, data encryption is executed using a 16-round Feistel network. [1,11,22].

2.3 DES algorithm

DES is a block cipher that processes data in 64-bit blocks. For every 64 bits of plain text given to DES, it generates a corresponding 64-bit block of cipher text. The key is 64 bits long, the block size is 64 bits, and the algorithm undergoes 16 rounds of processing. [1, 12, 18,22]

2.4 AES algorithm

The U.S. National Institute of Standards and Technology (NIST) established the Advanced Encryption Standard (AES) in 2001 to safeguard electronic data. AES has become widely adopted due to its superior strength compared to DES and triple DES, despite being more challenging to configure. It operates on data in blocks and employs a key that can be 128, 192, or 256 bits in length. The data blocks that AES encrypts are uniformly 128 bits in size. [12,13, 18, 22].

3. Characteristics of Cryptography algorithms

While certain crucial traits may not be easily measurable, there is an intuitive notion that certain features of cryptographic algorithms can be described using either objective, numerical measures or subjective, descriptive assessments. These metrics can serve as a means to assess and contrast cryptographic algorithms, as well as to gauge the inferred level of confidentiality provided by products incorporating such algorithms. The attributes of encryption algorithms that were taken into account in formulating these metrics [1,2,4,11,12,16,18,19]:

1- **Type of algorithm** (symmetric, Asymmetric, and hash).
2-Key size: The Key Length Metric proposed in this white paper is intended to provide this comparative value.
3-Rounds: Rounds were considered but may not be an important metric because rounds, like word and block size, are not universal characteristics and may not have great value in specifying meaningful thresholds.
4-Complexity: (Algorithm complexity for encryption, decryption, and key setup.)
5.Strength: An assessment of the strength of the algorithm, based on key length, algorithm complexity and the best methods of attack.

4. Assessing Cryptographic Algorithms through Fuzzy Logic

In this segment, the cryptographic algorithm will undergo assessment employing fuzzy logic. The process of fuzzifying input variables revolves around three key components (namely, variable block size (w), variable number of rounds (r), and variable key size (B)) integrated into the model's decision-making layer. The model's structure adheres to the Mamdani style inference system, renowned for its adeptness in emulating human reasoning and facilitating thorough analysis. The implementation leverages both a fuzzy logic tool and MATLAB code. The objective of this endeavor is to evaluate the security readiness level of the cryptographic algorithm, employing fuzzy logic as a means of decision-making, rather than relying solely on human judgment [14,20,24].

4.1 The fuzzy Model

Fuzzy logic-based evaluation modeling architecture is given in figure 1:

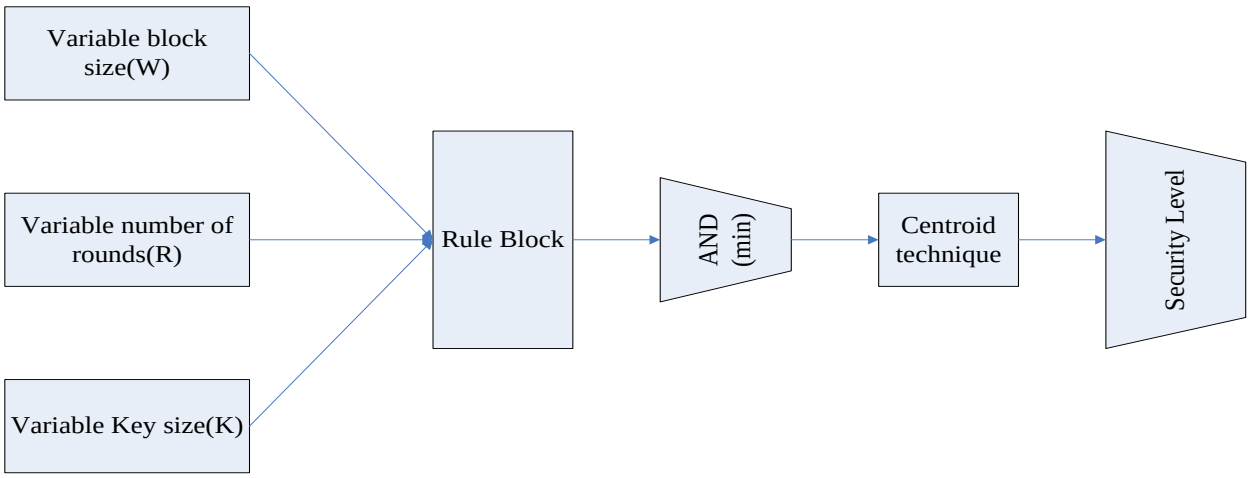

Figure 1 Architecture for fuzzy logic-based evaluation modeling

Fuzzification → Rule Evaluation→ Aggregation→Defuzzification →Output

a-Fuzzification*:* Fuzzification involves assigning membership values to a fuzzy variable through membership functions. Initially, crisp inputs (Block Size, Number of Rounds, and Key Size) are taken, and their degree of belongingness to the

relevant fuzzy sets is determined. These crisp inputs are always numerical values within the defined range. After obtaining the crisp inputs, they are then processed against the corresponding linguistic fuzzy sets.

For Block Size and Number of Rounds, linguistic values are categorized as Low, Medium, and High. Meanwhile, for Key Size, linguistic values are classified as Bad, Good, Very Good, and Excellent. The output, Security Level, is also described using the linguistic values Bad, Good, Very Good, and Excellent.

The input variables' universe of discourse for the RC5 algorithm spans from 0 to 6 for Block Size, from 0 to 12 for Number of Rounds, and from 0 to 12 for Key Size. In the case of the Blowfish algorithm, the universe of discourse ranges from 0 to 8 for Block Size, from 0 to 4 for Number of Rounds, and from 0 to 10 for Key Size.

For the DES algorithm, the input variables' universe of discourse spans from 0 to 8 for Block Size, from 0 to 4 for Number of Rounds, and from 0 to 10 for Key Size.

The Security Level output for all three algorithms falls within the universe of discourse of 0 to 30.

b. Rule evaluation*:* In this phase, the fuzzified inputs are employed in the antecedents of the fuzzy rules. As the fuzzy rule involves multiple antecedents, a fuzzy operator (either AND or OR) is employed to produce a singular value representing the outcome of the antecedent evaluation. A total of 20 rules were generated in this assessment, achieved by linking three inputs to one output through the use of the conjunction operator (AND).

c. Aggregation of the rule outputs: The aggregation process takes the set of trimmed output functions generated by the implication process for each rule as input. It produces a single fuzzy set for each output variable as its output.

d. Defuzzification: For the process of defuzzification, the aggregate output fuzzy set serves as the input, and the outcome is a numerical value. The centroid technique was employed in this step, as it is the widely adopted method for defuzzification.

5 Implementation

The design has been executed using the MATLAB fuzzy logic toolbox and code. The interfaces for this implementation are outlined below:

a. **FIS editor*:*** Figure 2 provides details regarding the FIS editor for decision-making. It illustrates the labels of both input and output variables.

b. **Membership function editor*:*** Figure 3 depicts the interface for modifying the membership functions of either the model's input or output.

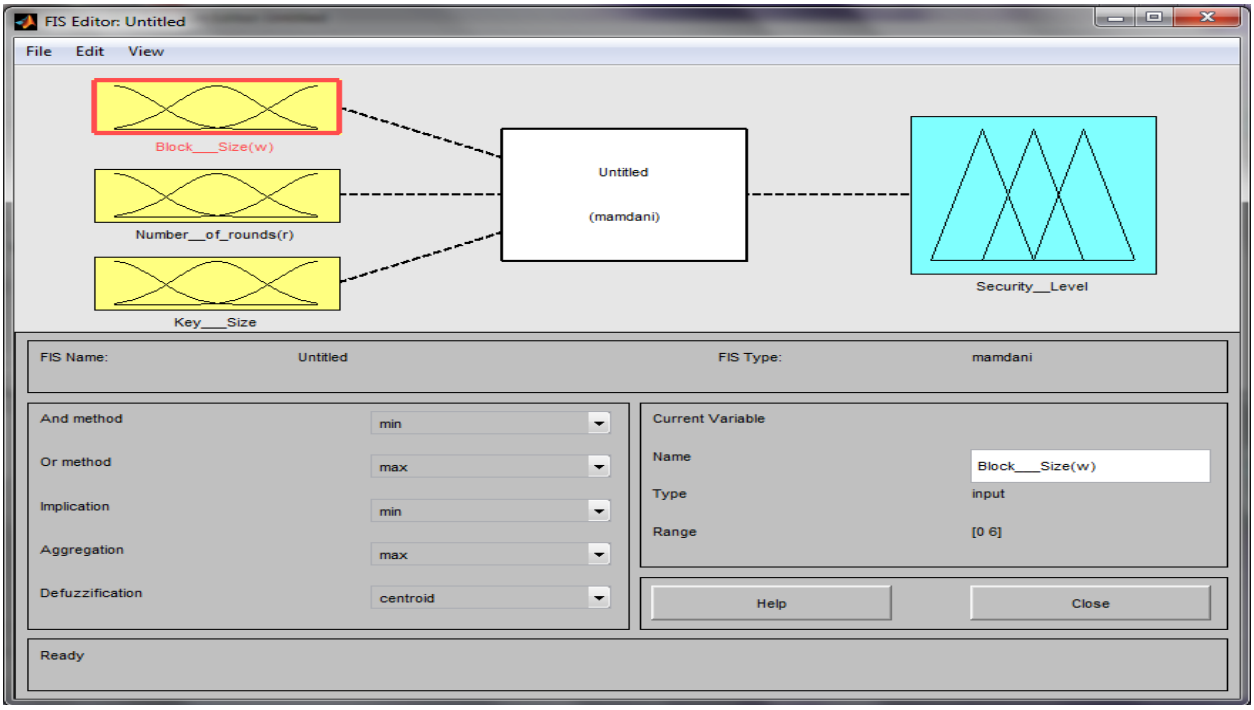

Figure 2 FIS editor (decision)

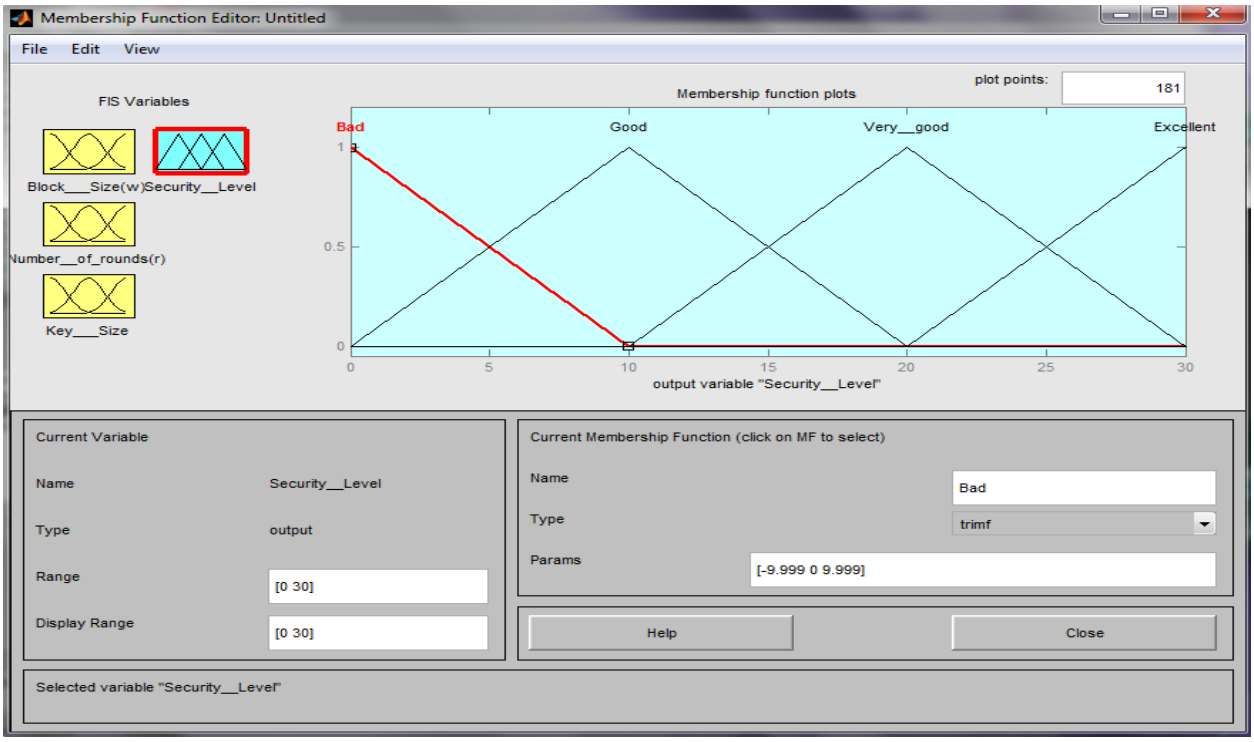

Figure 3 Membership functions of the model

c. **Rule editor*:*** Figure 4 to RC5 algorithm are used to add, change or delete rules.

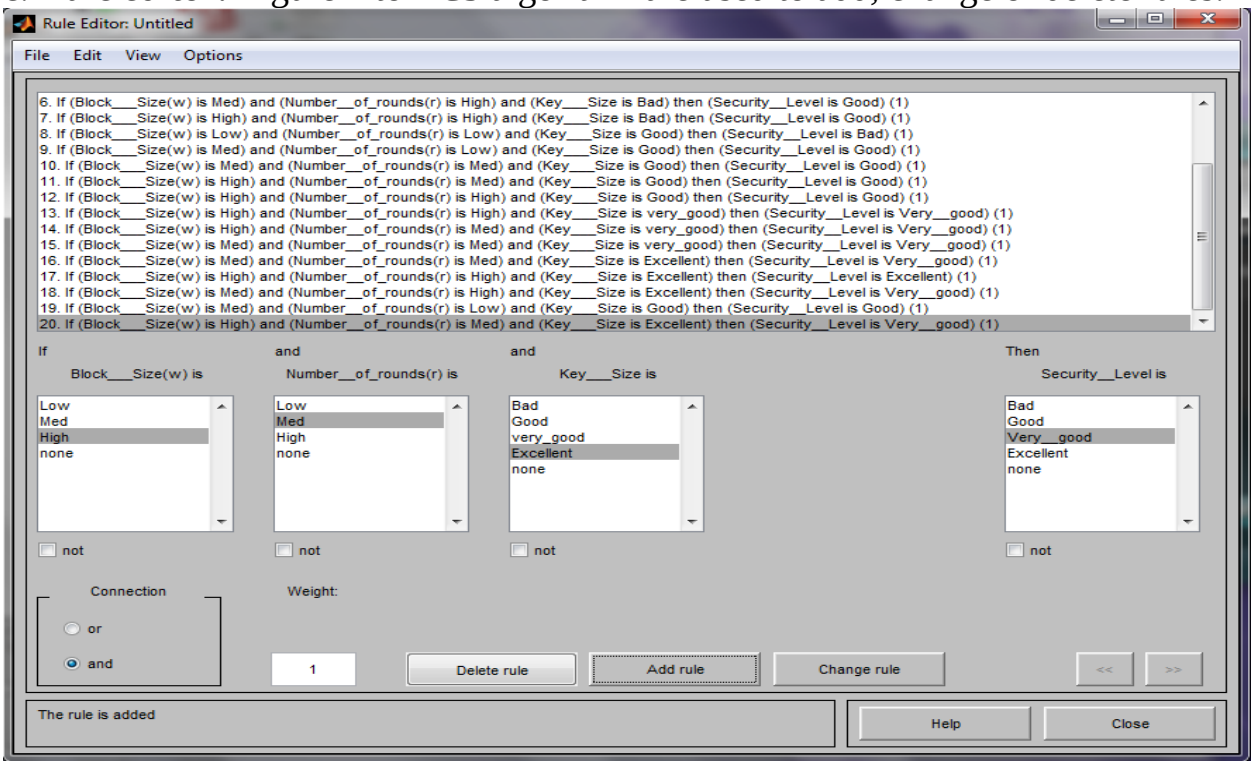

Figure 4 Rules Editor

d. **Rule viewer**: The RC5's rule viewer, as seen in Figure 5, presents a visual representation of all the variables across the rules, a combined view of the rules, and the defuzzification output. Additionally, it provides the precise value for the system's output. Each rule corresponds to a row of plots, while each variable is represented in columns.

e**. Model Structure:** Figure 6 illustrates the model structure for RC5, providing a graphical depiction of inputs, outputs, and their interconnections. The established rules are then converted into the structure of a fuzzy model. This model is primarily defined by the rules and the associated fuzzy sets pertinent to the underlying issue. The fuzzy perception encapsulates the interplay between the variables during and post evaluation of the output, presenting a streamlined representation of the rules in the form of a condensed fuzzy model.

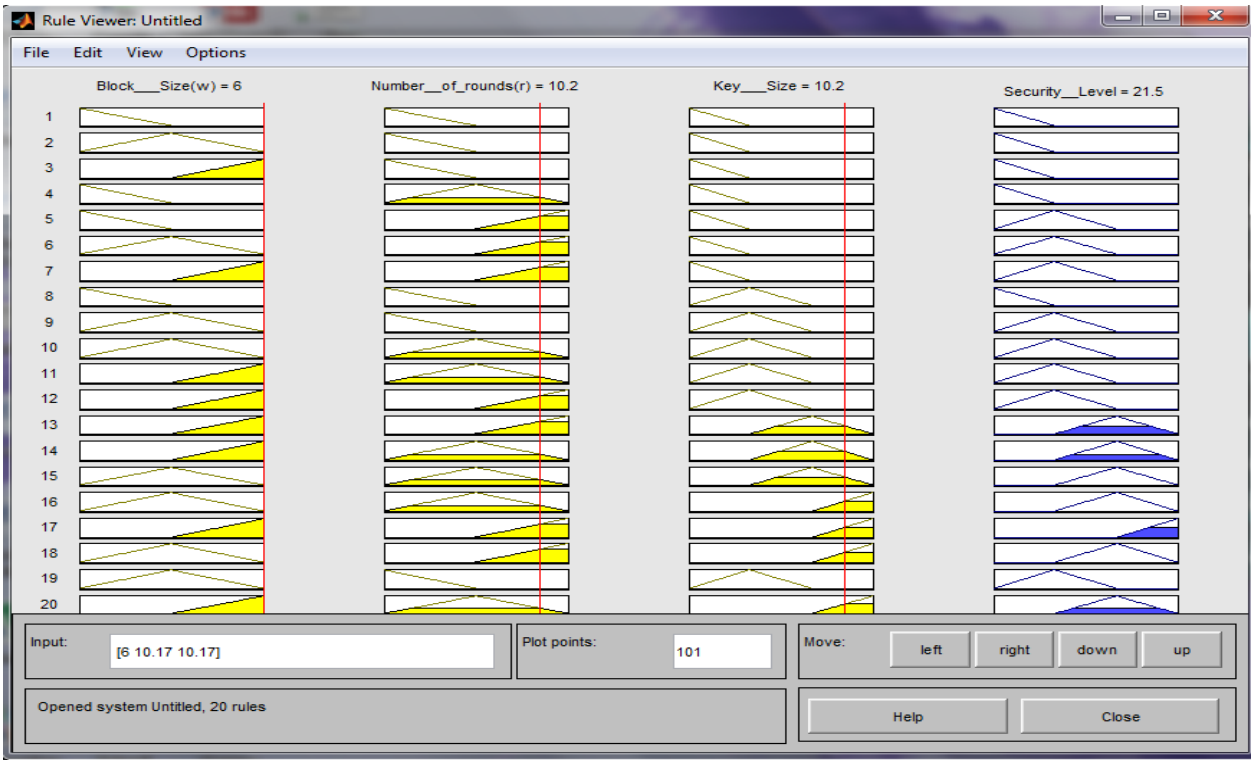

Figure 5 Rule viewer

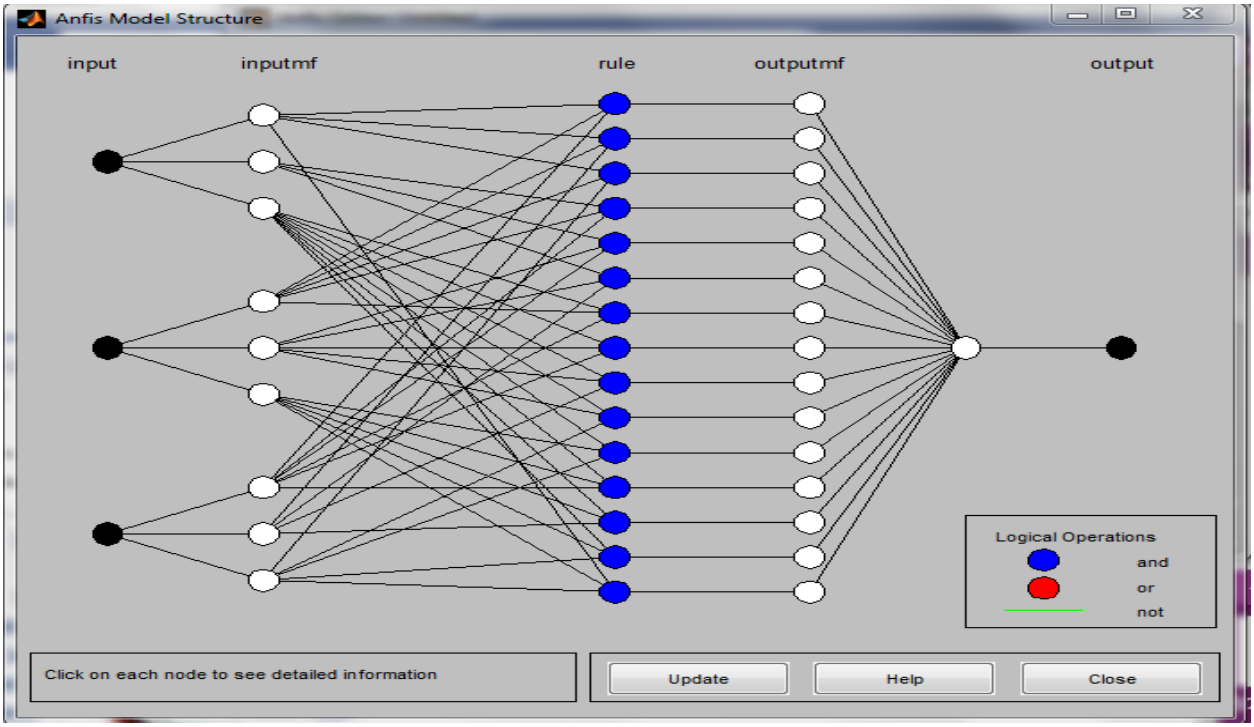

Figure 6 Model Structure

The flow chart for the proposed cryptography algorithm evaluation is shown in the Figure 7

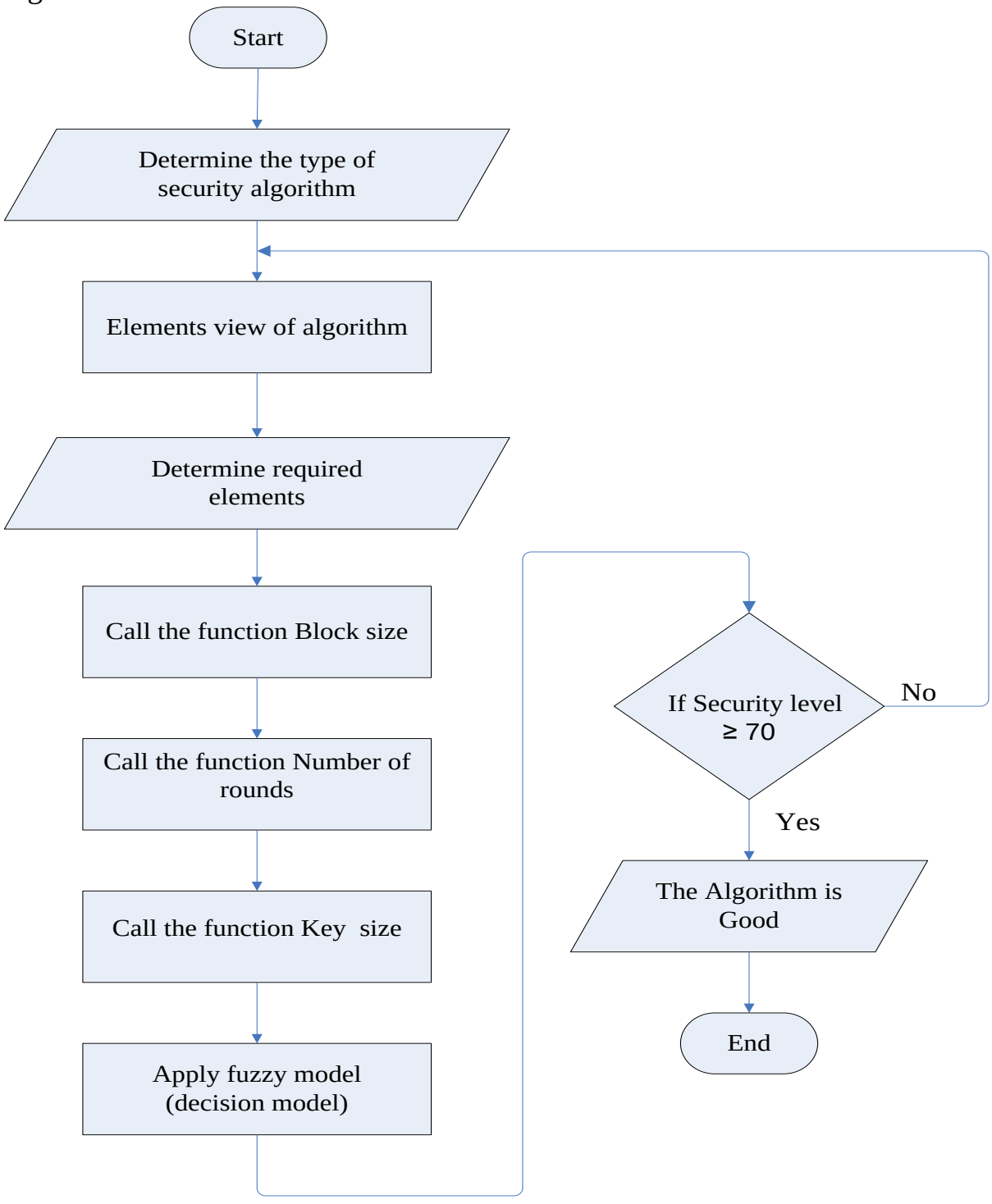

Figure 7 Flow chart to evaluation of cryptography algorithm

5. Results

5.1 Results of RC5 algorithm Evaluation

This is accomplished by invoking elements that possess three inputs and one output, employing 20 sets of input states, and obtaining the corresponding output (Security Level). Table 1 displays these input values along with their corresponding output results. It highlights the relationship between the number of rounds and security level, block size and security level. Furthermore, Figure 8 illustrates the impact of these three parameters on the security level.

Table 1 Security level percentage value of RC5 algorithm

Number States	Block Size %	Number of rounds%	Key size%	Security level%
1	13.67	12.1	8.98	23.83
2	33.33	16.8	8.98	24.36
3	33.33	16.8	17.57	29.56
4	33.33	16.8	20.7	30.9
5	33.33	26.95	20.7	31
6	33.33	26.95	24.6	31.2
7	33.33	26.95	24.6	31.9
8	66.66	30.07	28.51	32.86
9	66.66	35.55	33.98	34.33
10	66.66	38.67	37.1	38.66
11	66.66	39.45	39.45	41.33
12	66.66	58.2	46.48	47
13	66.66	63.67	49.6	49.66
14	66.66	67.57	52.73	52.33
15	66.66	71.48	58.2	55.66
16	66.66	73.82	65.23	64
17	66.66	81.64	74.6	68.33
18	66.66	84.75	80.07	69.33
19	100	86.33	84.75	71.66
20	100	100	100	89.33

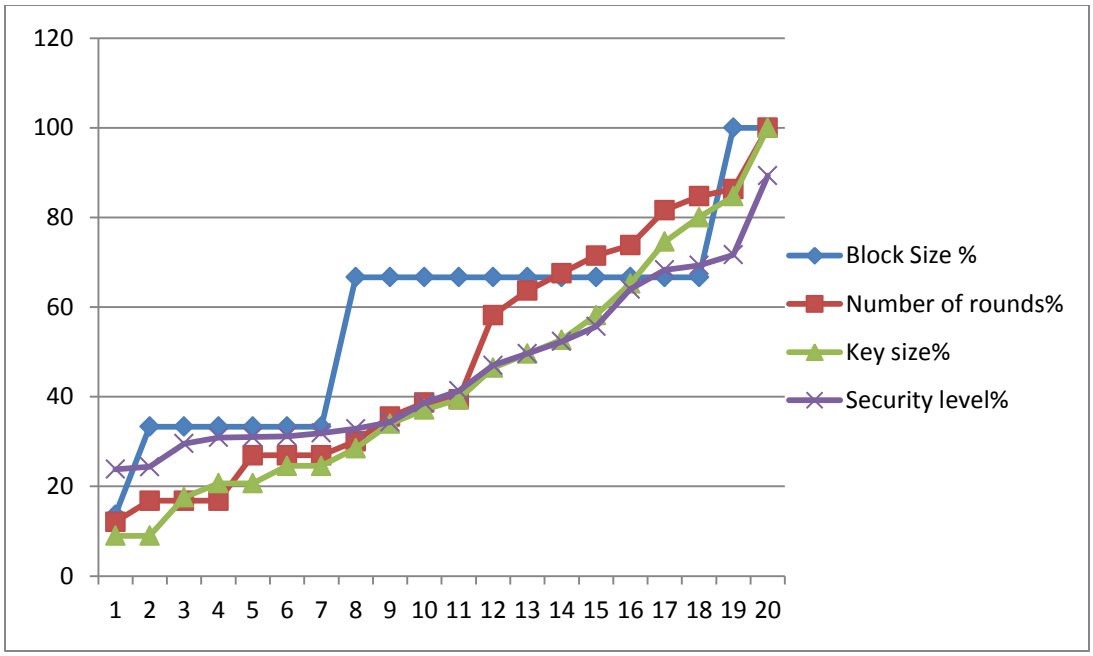

Figure 8 Block size, Number of rounds, key size and security level of RC5 algorithm

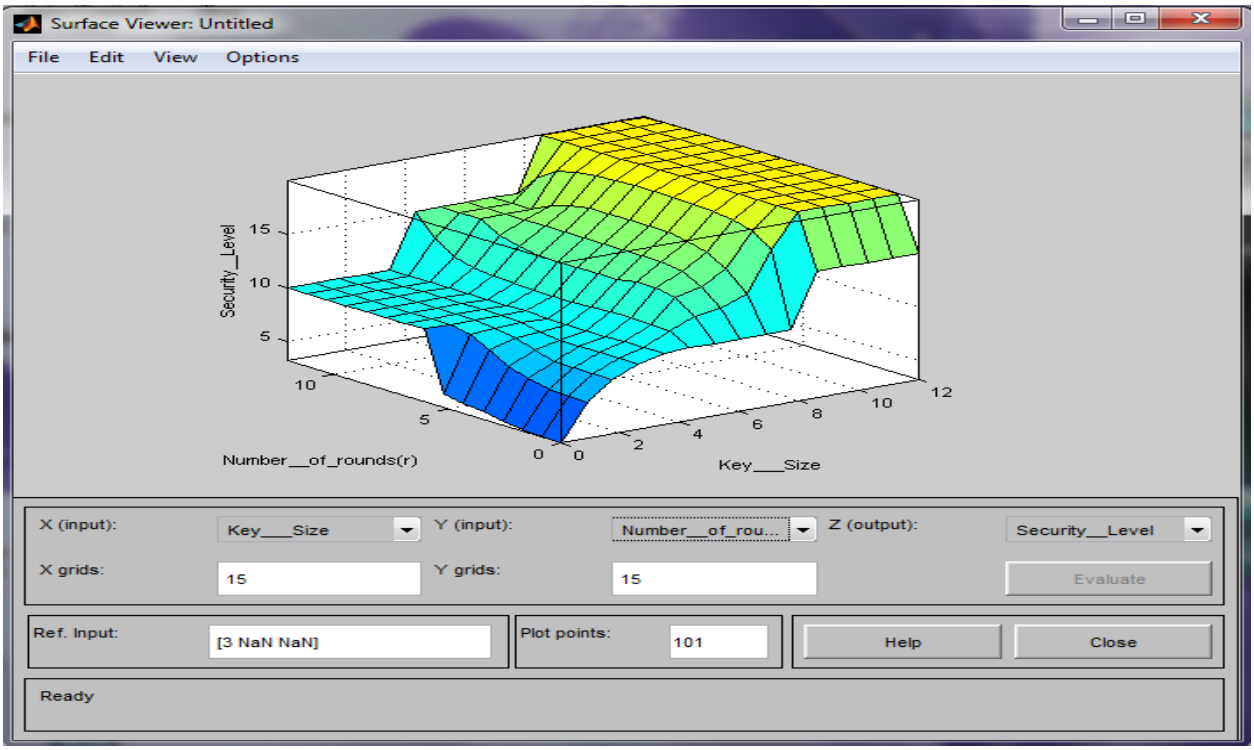

Figure 9 surface viewer

5.2 Result of Blowfish algorithm

For the assessment of the Blowfish algorithm considering three evaluation criteria, Table 2 illustrates the input-output pairs, demonstrating the influence of inputs on the output (security level).

Table 2 Security level percentage value of Blowfish algorithm

No.	Block Size %	Number of round%	Key size%	Security level%
1	o.6	3.012	9.03	11.3
2	6.62	5.4	10.24	11.9
3	11.44	9.025	11.45	14.23
4	12.56	9.025	11.45	14.43
5	12.56	12.56	15.06	20.03
6	18.67	12.56	15.06	21.03
7	18.67	17.74	22.29	27.9
8	28.31	23.49	28.31	30.96
9	31.92	28.32	31.93	32.33
10	42.77	33.125	42.77	33.33
11	52.41	53.62	60.84	34.33
12	59.63	58.42	66.87	41.33
13	63.25	62.05	69.28	44
14	68.07	65.67	71.69	47.33
15	68.07	65.67	71.69	53
16	76.5	71.5	75.3	53.33
17	82.52	76.5	77.71	60
18	88.55	82.52	81.33	69
19	94.57	93.73	92.17	72.33
20	100	100	100	72.66

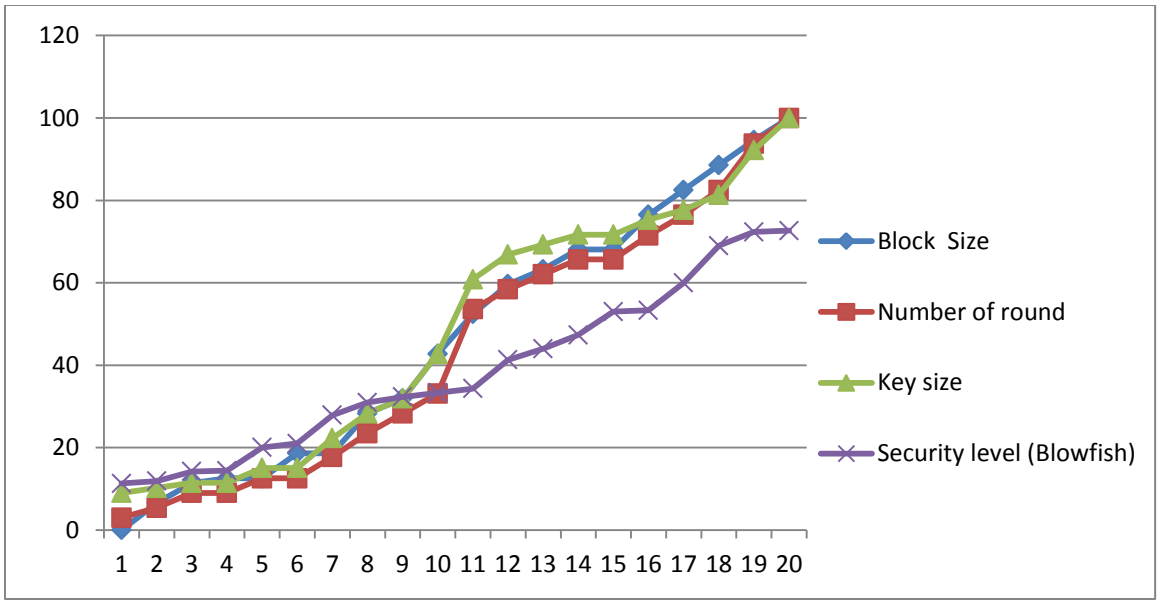

Figure 10 relations block size ,number of rounds ,key size and security level of Blowfish algorithm

5.3 Result of DES algorithm

5.3.1 Case Study

To validate the efficacy of the fuzzy logic approach and assess its capability in determining security levels for wireless networks, experiments were conducted within the network. The process involved applying the fuzzy logic method initially to establish input parameter factors (training dataset). Subsequently, the output from the FIS was employed as the target output (security level). The outcomes are presented in Table 3.

Table 3 Security level percentage value of DES algorithm

No.	Block Size %	Number of round%	Key size%	Security level%
1	9.03	18.67	6.62	12.5
2	13.85	18.67	6.62	12.5
3	13.85	21.08	6.62	12.86
4	13.85	21.08	10.24	13.46
5	23.5	21.08	10.24	13.93
6	23.5	27.1	10.24	13.93
7	23.5	27.1	13.85	21.13
8	29.51	31.92	19.87	25.9
9	36.75	37.95	24.7	29.83
10	37.95	43.97	28.31	31.43
11	40.36	47.6	37.95	33.26
12	43.97	52.4	46.38	33.33
13	53.61	65.67	57.22	40
14	64.46	72.9	59.63	47.66
15	69.82	77.025	59.63	52
16	70.11	79.72	73.42	53.66
17	70.86	85.12	77.92	54.66
18	77.025	87.85	85.13	59.33
19	84.23	90.55	86.03	61.
20	100	100	100	66.66

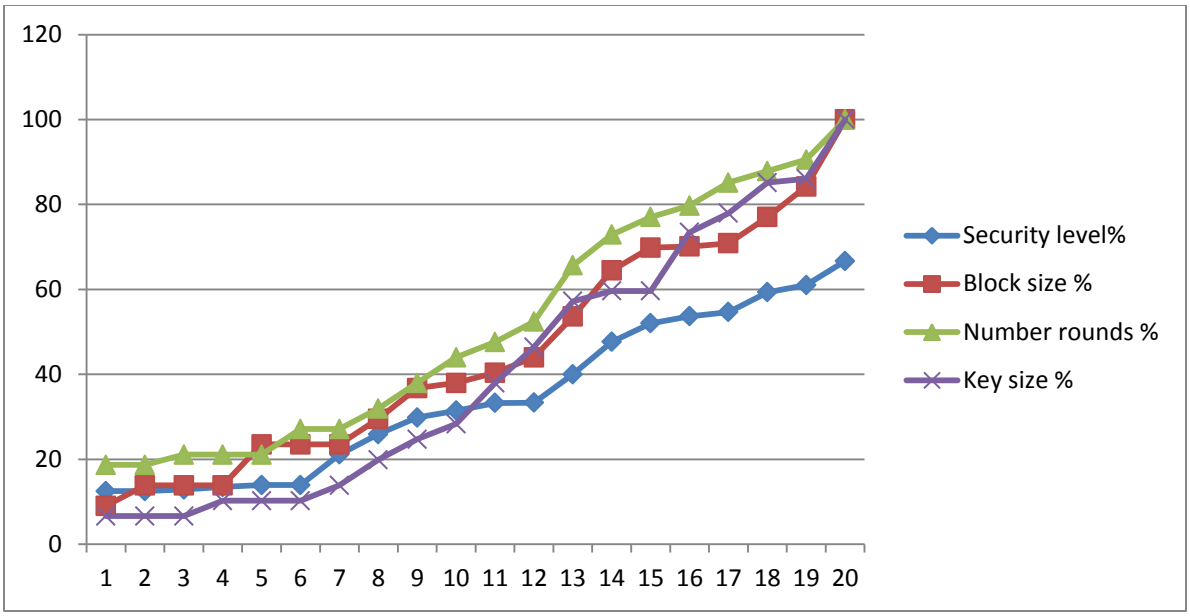

Figure 11 relations among of block size, number of rounds, key size and security level of DES algorithm

5.4 Results of AES algorithm Evaluation

This is accomplished by utilizing elements with three inputs and one output in 20 different input states, yielding the output (Security Level). Table 4 provides these input-output pairs, showcasing the relationship between the number of rounds and security level, block size and security level. Additionally, Figure 12 depicts the impact of these three parameters on the security level.

Table 4 Security level percentage value of AES algorithm

No.	Block Size %	Number of round	Key size%	Security level%
1	5	1	5	35.4
2	10	2	10	42
3	15	3	15	51.1
4	20	4	20	55.2
5	25	5	25	58.3
6	30	6	30	60.7
7	35	6	35	68.5
8	40	7	40	70.6
9	45	7	45	72.1
10	50	8	50	75.4
11	55	9	55	77.2
12	60	10	60	79
13	65	10	65	81.2
14	70	11	70	83.6
15	75	12	75	85.2
16	80	12	80	88.9
17	85	13	85	91.4
18	90	13	90	92.7
19	95	14	95	95
20	100	14	100	96.8

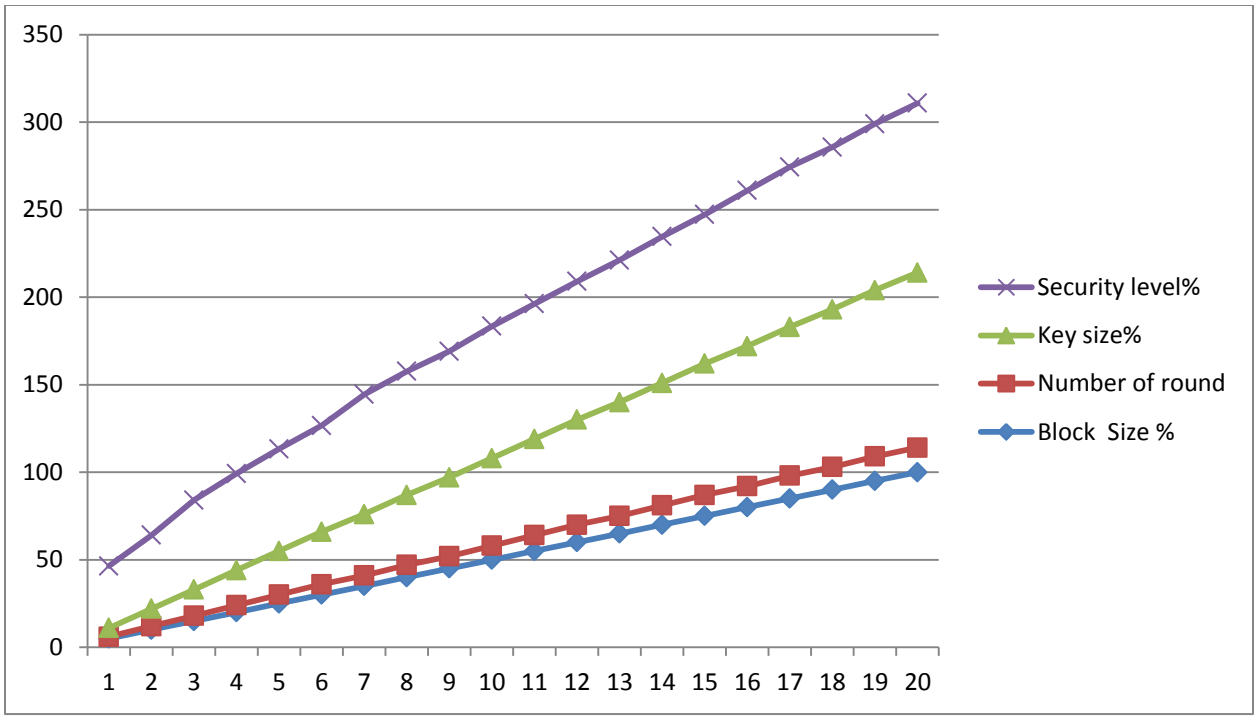

Figure 12 relations among of block size, number of rounds, key size and security level of AES algorithm

5.5 Result of comparisons of RC5, Blowfish, DES and AES algorithm

Case study:

For the purpose of comparing the algorithm results in terms of security levels, Table 5 and Figure 13 present the findings. Based on these outcomes, it is evident that AES emerges as the most secure option and is highly recommended for utilization in Wireless Telecommunication Networks.

Table 5 comparison of algorithms

No.	Security level% DES algorithm	Security level% Blowfish algorithm	Security level% RC5 algorithm	Security level% AES algorithm
1	12.5	11.3	12.5	35.4
2	12.5	11.9	12.5	42
3	12.86	14.23	12.86	51.1
4	13.46	14.43	13.46	55.2
5	13.93	20.03	13.93	58.3
6	13.93	21.03	13.93	60.7
7	21.13	27.9	21.13	68.5
8	25.9	30.96	25.9	70.6
9	29.83	32.33	29.83	72.1
10	31.43	33.33	31.43	75.4
11	33.26	34.33	33.26	77.2
12	33.33	41.33	33.33	79
13	40	44	40	81.2
14	47.66	47.33	47.66	83.6
15	52	53	52	85.2
16	53.66	53.33	53.66	88.9
17	54.66	60	54.66	91.4
18	59.33	69	59.33	92.7
19	61.	72.33	61.	95
20	66.66	72.66	66.66	96.8

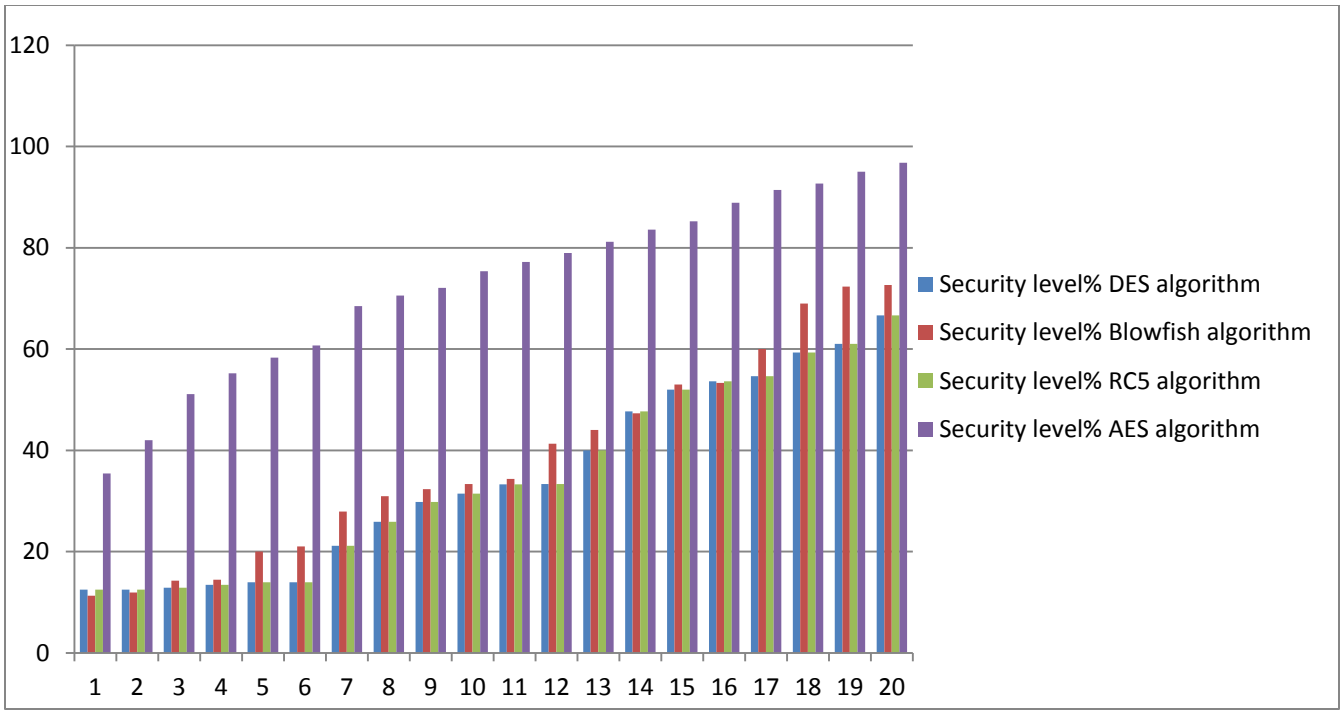

Figure 13 comparisons of RC5, Blowfish, DES and AES algorithm

6. Conclusions and Suggestions for Future Work

6.1- Conclusions

The research paper compared the RC5, Blowfish, DES and AES block cipher algorithms using Artificial Intelligence. The performance assessment was conducted on a system with a 3GHz core, 4GB RAM, and Windows 7 Professional Version 2012.

The study evaluated the algorithms based on criteria such as block size, number of rounds, and key size. It then analyzed the modeling duration and security level as the output. The results indicated that AES (96.8%) had the highest security level, followed by Blowfish (86.9%), RC5 (81.7%), and DES (48%). RC5 was deemed more favorable than the others due to certain reasons.

The use of security block cipher algorithms in networks is a complex process that requires periodic evaluation. Establishing a secure wireless network system necessitates a comprehensive security model.

Various metrics, including block size, number of rounds, and key size, impact the security information in the network. The study observed that the structure of cryptographic algorithms significantly influenced the security level, as demonstrated in Tables 1, 2, 3 and 4.

Fuzzy logic was employed to evaluate the complexity of block cipher algorithms. Parameters such as key size, block work size, number of rounds, and modeling duration were considered to choose more secure algorithms and select a secure structure.

The selected AES encryption algorithm was compared with RC5, Blowfish and DES. It was discovered that DES exhibited the lowest encryption security level and lacked flexibility compared to AES, which was found to be superior for evaluation based on fuzzy logic tools. Blowfish demonstrated a high security level under specific conditions (key size 7.5, block size 4.5, and one round).

6.2- Future Work

1- Comparison between symmetric and asymmetric algorithms to security level.

2- Comparison between single cryptography algorithms with hybrid cryptography algorithm to security level.

3- Comparison between security levels of Cryptography algorithm by different technics.

7- References

1.Landgrave T.Simith ”Cryptography algorithm metrics” January 1997.

2. P. Ruangchaijatupon, and P. Krishnamurthy, “Encryption and power consumption in wireless LANs- N”,The Third IEEE Workshop on Wireless LANs, pp. 148-152, Newton, Massachusetts, Sep. 27-28, 2001.

3. Hardjono,” Security In Wireless LANS And MANS”, Artech House Publishers, 2005.

4. K. McKay, “Trade-of between Energy and Security in Wireless Networks”, Thesis, Worcester Polytechnic Institute, Apr. 2005.

5. R. Chandramouli, \Battery power-aware encryption,” ACM Transactions on Information and System Security (TISSEC)”, vol. 9, no. 2, pp. 162-180, May 2006.

6. P. Ding, \Central manager: “A solution to avoid denial of service attacks for wireless LANs”, International Journal of Network Security”, vol. 4, no. 1, pp. 35-44, 2007.

7. Wei Xie;Mingbo Xiao;Felix Zhao;Yan Yao “Implementation and Evaluation of Channel Assignment Tool for Multi-Radio Multi-Channel Wireless Mesh Networks” IEEE Wireless Communications and Networking Conference 2007.

8. Yuan Lingyun;Wang Xingchao “Study on performance evaluation method based on measurement for wireless sensor network” IEEE International Conference on Communications Technology and Applications 2009.

9. Diaa Salama Abd Elminaam, Hatem Mohamed Abdual Kader, and Mohiy Mohamed Hadhoud” Evaluating The Performance of Symmetric Encryption Algorithms” International Journal of Network Security, Vol.10, No.3, PP.213,219, May 2010.

10. Runfu Zhang;Lianfen Huang;Mingbo Xiao "Security Evaluation for Wireless Network Based on Fuzzy-AHP with Variable Weight" IEEE Second International Conference on Networks Security, Wireless Communications and Trusted Computing 2010.

11. "Blowfish Algorithm" Available : http://www.schneier.com/blowfish. November 2012.

12. Akash Kumar Mandal;Chandra Parakash;Archana Tiwari" Performance evaluation of cryptographic algorithms: DES and AES" IEEE Students' Conference on Electrical, Electronics and Computer Science 2012.

13. Daniel F. García "Performance Evaluation of Advanced Encryption Standard Algorithm" Second International Conference on Mathematics and Computers in Sciences and in Industry (MCSI) 2015.

14. Sun Yi, Gu Wei, J. Lu and Zenghui Yang, "Fuzzy clustering algorithm-based classification of daily electrical load patterns", 12th International Conference on Fuzzy Systems and Knowledge Discovery (FSKD), pp. 50-54, 2015.

15. Vaibhav Garg;Kotaro Kataoka;Siva Subramanya Rohith Talluri "Performance evaluation of wireless ad-hoc network for post-disaster recovery using Linux Live USB nodes" IEEE 11th International Conference on Wireless and Mobile Computing, Networking and Communications (WiMob) 2015.

16. Lulu Liang;Yanzhao Liu;Yuangang Yao;Tianshi Yang;Yuening Hu and Chen Ling "Security challenges and risk evaluation framework for industrial wireless sensor networks" IEEE 4th International Conference on Control, Decision and Information Technologies (CoDIT) 2017 .

17. L. Xiao, X. Wan, X. Lu, Y. Zhang, and D. Wu, ''IoT security techniques based on machine learning: How do IoT devices use AI to enhance security?'' IEEE Signal Process. Mag., vol. 35, no. 5, pp. 41–49, Sep. 2018.

18. Arpit Kubadia;Drishti Idnani;Yash Jain " Performance Evaluation of AES, ARC2, Blowfish, CAST and DES3 for Standalone Systems : Symmetric Keying Algorithms" 3rd International Conference on Computing Methodologies and Communication (ICCMC) 2019.

19. Jayvee Christopher N. Vibar and Ruji P. Medina "ERC5a – An Enhanced RC5 Algorithm on Bit Propagation in the Encryption Function" IEEE 4th International Conference on Computer and Communication Systems (ICCCS) 2019.

20. XIAOYING QIU, ZHIGUO DU and XUAN SUN "Artificial Intelligence-Based Security Authentication: Applications in Wireless Multimedia Networks" IEEE Access November 28, 2019.

21. Jiming Yao; Peng Wu; Yang Wang; Zhihui Wang and Yize Tang "Research on Power Wireless Network Quality Evaluation Method Based on Multi-dimensional Index" 14 December 2020.

22. Hasan Dibas;Khair Eddin Sabri "A comprehensive performance empirical study of the symmetric algorithms:AES, 3DES, Blowfish and Twofish" IEEE International Conference on Information Technology (ICIT) 2021.

23. Marina Talaat Rouaf;Adil Yousif "Performance Evaluation of Encryption Algorithms in Mobile Devices" International Conference on Computer, Control, Electrical, and Electronics Engineering (ICCCEEE) 2021.

24. Qichao Xu; Zhou Su; Ruidong Li "Security and Privacy in Artificial Intelligence-Enabled 6G" IEEE Network (Volume: 36, Issue: 5, PP 188 - 196 25 November 2022).