Chng Chern Wei, et. al. International Journal of Engineering Research and Applications
www.ijera.com
ISSN: 2248-9622, Vol. 12, Issue 9, September 2022, pp. 38-42

RESEARCH ARTICLE OPEN ACCESS

DNA-based Approach of Security Analysis for Cloud-based ERP System

Chng Chern Wei[1], Tadiwa Elisha Nyamasvisva[2]
[1]*Centre for Postgraduate Studies, Infrastructure University Kuala Lumpur*
[2] *Faculty of Engineering Science and Technology, Infrastructure University Kuala Lumpur*

ABSTRACT
Cloud-based ERP system is concern about the security issue of the system. To achieve more secure communication channels, computer security experts from universities and institutes around the world are still looking for better ways to improve internet security. Various cryptographic algorithms have been successfully introduced by researchers throughout the world based on the block cipher [4][5][6][7][18], fulfilling the diffusion properties and computed by several rounds to produce safe data transmission [5][6][7]. To develop to good cryptography algorithm, the research design and research methodology is an important step. The research design framework is an essential to identify the methods of DNA-based Sequencing algorithm development process and the evaluation criteria of the new proposed algorithm in Cloud-based ERP System (CBES).
Keywords – ERP, Cloud-based ERP, DNA-based, sequencing algorithm, Data Security

---

Date of Submission: 01-09-2022 Date of Acceptance: 12-09-2022

I. INTRODUCTION

This paper is focuses on the research methodology of security analysis for data security issue in cloud-based ERP System (CBES) and the development of a DNA-based Sequencing algorithm for data security in cloud-based ERP System (CBES) including the security evaluations for the proposed algorithm [3]. This paper explain in detail the entire process of the research methodology, followed by the experimental design process. Widely used of the cloud-based ERP also concern about the security issue of the system. To achieve more secure communication channels, computer security experts from universities and institutes around the world are still looking for better ways to improve internet security. To achieve this aims, cryptographic algorithm able to provide the security to ensure that insecure channels can be improve. Designing an efficient cryptographic algorithm for safe communication over the internet, the researchers need to take into account all the key aspects of digital security, especially that digital security objective is to act as a benchmark [8].

II. LITERATURE REVIEW

Enterprise Resource Planning System (ERP) is a collection of business management software applications designed to integrate and manage all business functions in an organization. The application modules contained in ERP are such as applications for human resources, finance and accounting, sales and distribution, project management, materials management, supply chain management (SCM), quality management and so on [19].

The advantages of cloud-based ERP system can provide convenience to staff in the organization to achieve more accurate and efficient information to provide the services needed by customers in order to provide a more competitive advantage with organizations that operate traditionally. According to Bjelland & Haddara in their research mentioned that, the cloud-based model is keep increasing in order to provide benefits to an organization [24].

To improve the security issue in the Cloud-based ERP system, embedded of the cryptographic algorithm into the Cloud-based ERP system is an essential. The new proposed DNA-based Block Cipher able to provide the high security to the Cloud-based ERP system. To ensure the new proposed DNA-based Block Cipher is fit and able to the provide the high security to the system, the new proposed algorithm must fulfill the Randomness Test, Avalanche Effect and the cryptanalysis as shown in the Figure 1. The Figure 1 shown the Overview of Evaluation Criteria of Cryptographic Algorithm [5][6][7][14][15]

Randomness test is a statistical analysis method for the evaluation the security of a block cipher algorithm. This test carries out the measure of confusion and diffusion properties of a new encryption algorithm. NIST Statistical Test Suite is a statistical test packages for randomness used by

NIST and has used to evaluate cryptographic algorithms. This test suite evaluate whether the new cryptographic algorithm output meet the confusion and diffusion properties of random generated outputs [5][6][7][13][10][20][11][21][22][23].

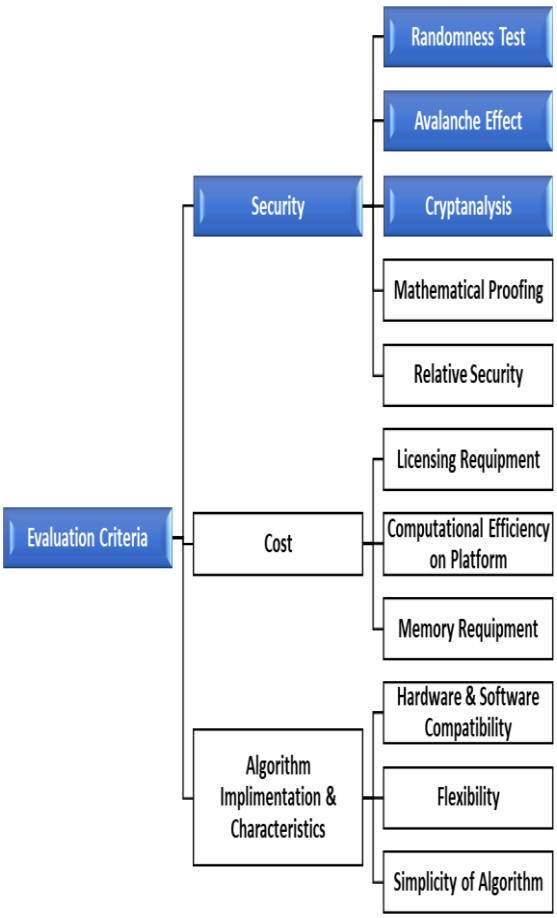

Figure 1: Overview of Evaluation Criteria of Cryptographic Algorithm [5][6][7][14][15]

III. RESEARCH METHODOLOGY PHASE:

The research methodology divided in six phase as discuss below:

3.1 Problem Identification

This phase is the first stage in conducting the research. This stage should can give a clear picture of what the researchers wish to do for the research in terms of implementation, implementing and testing.

In practice, this stage will be carried out in two phases. In the first phase, an initial system review will be conducted to help identify the area of the elements of the experiment. The next phase will focus on the literature review which is a zoom detail and in-depth study in which the introduction of requirements, constraints as well as the complication is studied.

3.2 Requirement Analysis

This phase explains the requirement for DNA-based Sequencing Algorithm. At this stage, the experimental design is set up. The type of data to be used is identified. NIST 15 statistical tests and test requirements for testing are also identified. Begin the test process after all parameters and requirements are identified.

3.3 Design and Experimental Implementation

Based on the needs of the technological era now, the creation of a new DNA-based Sequencing Algorithm is important and should be designed and implemented. This phase is named as the design phase of the system.

It is an important phase at this stage to develop a system that satisfies the cryptography criteria. The new DNA-based Sequencing Algorithm design is divided into three components which are the key scheduling, the key dependent of DNA-Based S-Box and the overall block cipher design.

There are several tools and techniques such as flowchart and data flow diagram (DFD) which can be used for designing the new DNA-based Sequencing Algorithm.

The features of each of the components are indicated. On the other hand, the costs of implementing the system specifications are estimated and other advantages have been provided in detail. While at the design stage, the use of the computer platform and also the type of the programming language in developing the DNA-based Sequencing Algorithm will be decided for this study.

Upon completion of the new design of the new DNA-based Sequencing Algorithm, the entire system is required to convert into a high-level programming language. This stage is important as all pseudo code will be coded with the use of C ++ programming language for system specification control.

Before implementing a new DNA-based Sequencing Algorithm, the pilot test algorithm will be performed by updating the code or bug error from the system's code of verification. This is an important phase in order to develop a successful and perfect system. After modifying the whole DNA-based Sequencing Algorithm, the comprehensive test must match the expected results.

3.4 Security Evaluation (Randomness)

In this phase, the NIST statistical testing will be carry out to measure the ciphertext of the

proposed algorithm satisfies the confusion and diffusion criteria under the test conditions. NIST Statistical Test Suite is a statistical package consist of 15 tests kits that were developed to test the randomness of the binary sequences produce by random number generator. All the test must satisfies the minimum requirements for the sequence length and parameter for each test.

3.5 Results and Analysis

The next stage is to run the analyzes of the results of the experiment. The decision is to fulfill the requirements and achieve the goal. If the objective is not achieved, the test and analysis should be conducted until a positive result is achieved. All displayed results are recorded using tables and graphs for visual presentation and interpretation.

3.6 Conclusion, Future Work and Document/Thesis Preparation

All the steps in carrying out this study will be carefully planned with references through literature review as well as all decisions will be recorded carefully according to scientific steps. From the results obtained, conclusions can be obtained through careful analysis steps.
Based on the results of this study, conclusions and future work will be elaborate and the first thesis can be produced.

IV. EXPERIMENTAL DESIGN

The experimental design will involve steps below as explained:

4.1 Data Preparation

For this study, the data should be pre-processed in the new DNA-based Sequencing Algorithm to obtain ciphertext. Then, this ciphertext will be used as input to the NIST configuration test 15. There are three sets of data types used in this experiment as shown in Table 1.

Table 1: Types of Data Sets

	Data 1	Data 2	Data 3
Total Block of 128 Bits	500	50,000	1,000,000
Total Bits	32,000	6,400,000	128,000,000

4.2 Performance of Randomness Test

The main objective of randomness test is to validate the new DNA-based Sequencing Algorithm in order to fit and conform to the properties of confusion and diffusion. The statistical test of NIST statistics [14][15][16] is used as a testing tool to verify whether the new DNA-based Sequencing Algorithm is meets the confusion and diffusion criteria.
NIST statistical test suite is a UNIX based software application comprising 15 tests tool implemented to test the frequency of binary cipher sequences generated based on random number of generator or cryptographic pseudorandom. The hardware specifications of the computer used for the test suite are Microprocessor Intel i7, main memory of RAM is 16GB, and 2TB SSD Hard Disk storage.

4.1.1 NIST Test Suite

This test emphasizes on a variety of non-random forms that can occur in binary sequence. Certain tests can be compressed into multiple sub-tests and the NIST Statistical Test Suite contains tests such as Table 2, below:

Table 2: List of NIST Statistical Test Suite [5][6][7] [14][15][16][17]

No.	NIST Statistical Test
1.	Frequency Test
2.	Frequency Test Within a Block Test
3.	Run Test
4.	Longest Run of Ones in a Block Test
5.	Binary Matrix Rank Test
6.	Discrete Fourier Transform Test
7.	Non-overlapping Template Matching Test
8.	Overlapping Template Matching Test
9.	Maurer's "Universal Statistical" Test
10.	Linear Complexity Test
11.	Serial Test
12.	Approximate Entropy Test
13.	Cumulative Sums Test
14.	Random Excursions Test
15.	Random Excursions Variant Test

4.1.2 NIST Test Suite Requirement for Length and Sequence Parameters

The details of the list of NIST statistical tests above discussed and the NIST has set minimum requirements for each length and sequential parameters in each test.

The NIST requirement table [5][6][7][14][15] [17] for length and sequence parameters is shown in Table 3.

Table 3: NIST Requirement for Length and Sequence Parameters [5][6][7][14][15][17]

No.	NIST Statistical Test	Minimum requirement
1	Frequency	$n \geq 100$
2	Frequency within a Block	$n \geq 100$
3	Runs	$n \geq 100$
4	Longest-Run-of-Ones in a Block	$n \geq 128$ $M = 8$
5	Binary Matrix Rank	$n \geq 38,912$
6	Discrete Fourier Transform (Spectral)	$n \geq 1,000$
7	Non-overlapping Template Matching	$n \geq 1,000,000$, $M = 13,072$, $M > 0.01 > n$
8	Overlapping Template Matching	$n \geq 1,000,000$, $n \geq M \geq N$
9	Maurer's Universal Statistical	$6 \leq L \leq 16$, $Q = 10(2L)$, $n \leq (Q+K)$ L, $n \geq 387,840$
10	Linear Complexity	$n \geq 1,000,000$, $500 \leq M \leq 5,000$
11	Serial	$M < (\log 2n) - 2$
12	Approximate Entropy	$M < (\log 2n) - 2$
13	Cumulative Sums (Cusums)	$n \geq 100$
14	Random Excursions	$n \geq 1,000,000$
15	Random Excursions Variant	$n \geq 1,000,000$

4.3 The Implementation of the Experiment

This experiment conducted by dividing it into two parts. In the first part, the experiment will test the spreading of the number of rounds for the debris block. While the second part is to test, the output frequencies cipher block or ciphertext as shown in the Figure 2.

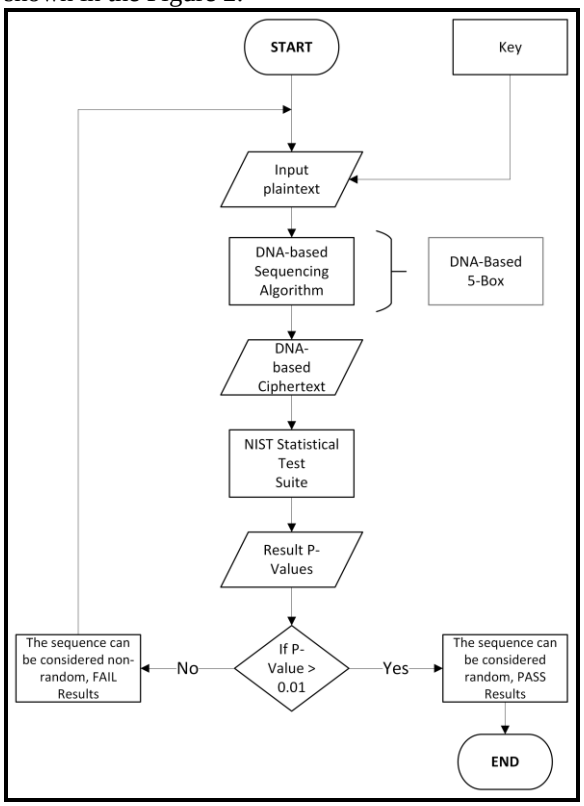

Figure 2: Experimental Flow Chat for Randomness Test

V. CONCLUSION

We have discussed the research methodology of new proposed DNA-based sequencing algorithm in order to provide the security and able to against the resistance attacks. The challenges of the research points are running of the NIST Statistical Test for the p-Values with the correct bit length and the parameters to simulate the p-values for the passing the randomness test. In the other hand, the testing environment and infrastructure is also play an important role to conduct this experiment.

REFERENCES

[1]. Global Cloud ERP Market Research Report 2022–2027. (2022). Market Data Forecast. https://www.marketdataforecast.com

[2]. Georgescu, C., Nita, A., & Toma, A. (2017). A View On NIST Randomness Tests In Dependence. International Conference of Computers and Artificial Interlligence, 9th Edition Electronics, Targoviste, Romania.

[3]. Wei, C.C., Tadiwa,E.N. (2022). A Review of Cloud-based ERP in Security Perspective. International Journal of Engineering Research and Applications (IJERA), ISSN: 2248-9622, Vol. 12, Issue 8, August 2022, pp. 66-70

[4]. Elumalai, R., & Reddy, A. R. (2011). Improving diffusion power of AES Rijndael with 8x8 MDS matrix. International Journal of Scientific & Engineering Research, 2(3).

[5]. Al-Wattar, A. H., Mahmod, R., Zukarnain, Z. A., & Udzir, N. I. (2015). Generating A New S-Box Inspired byBiological DNA. International Journal of Computer Science and Application vol. 4, p. 10.

[6]. Al-Wattar, A. H., Mahmod, R., Zukarnain, Z. A., & Udzir, N. I. (2015). A new DNA-based S-box. International Journal of Engineering & Technology IJET-IJENS, 15(04),1-9.

[7]. Al-Wattar, A. H., Mahmod, R., Zukarnain, Z. A., & Udzir, N. I. (2015). A New DNA-Based Approach of Generating Key-dependent ShiftRows Transformation. arXiv preprint arXiv:1502.03544

[8]. Saravanan, T., & Venkatesh Kumar, S. (2018). A Review Paper on Cryptography-Science of Secure Communication. International Journal of Computer Science Trends and Technology 6(4), Jul-Aug 2018.

[9]. Mara, U. T. (2017). Randomness Analysis on 3D-AES Block. 2017 13th International Conference on Natural Computation, Fuzzy Systems and Knowledge Discovery (ICNC-FSKD), 331–335.

[10]. Rukhin, A., Soto, J., et al. (2008). A Statistical Test Suite for Random and Pseudorandom Number Generators for Cryptographic Applications, NIST, Technology Administration, U.S.Department of Commerce.

[11]. Alani, M. M. (2010). Testing Randomness in Ciphertext of Block-Ciphers Using DieHard Tests, 10(4), 53–57.

[12]. Soto, J. (1999). Randomness Testing of the AES Candidate Algorithms.

[13]. Soto, J., & Bassham, L. (2000). Randomness Testing of the Advanced Encryption Standard Finalist Candidates 1.

[14]. Sharifah, M.Y, Ayman, M.H, Izura,U.,Sherzod, T. & Rezal,K.A. (2020). Key Dependent Dynamic S-Boxes Based on 3D Cellular Automata for Block Cipher. Journal of Theoretical and Applied Information Technology. Vol.98. No.23

[15]. Ayman, M.H. (2020). A New KD-3D-CA Block Cipher with Dynamic S-Box Based on 3D Cellular Automata. Universiti Putra Malaysia.

[16]. Daemen, J. & Rijmen, V.(2001). The Design of Rijndael. Springer-Verlag Berlin Heidelberg New York.

[17]. Wei, C.C., Sharifah, Taufik, M., Udzir, N.I. (2018). New DNA Based Dynamical S-Box for Block Cipher. International Journal of Engineering Research and Applications (IJERA), vol. 8, no.7, 2018, pp.64-69

[18]. Georgescu, C., Nita, A., & Toma, A. (2017). A View On NIST Randomness Tests (In) Dependence.

[19]. Shehab, E. (2014). An Image Encryption Technique based on DNA Encoding and Round-reduced AES Block Cipher, 107(20), 1–7.

[20]. Sulak, F., Doğanaksoy, A., Ege, B., & Koçak, O. (2010). Evaluation of Randomness Test Results for Short Sequences, 309–319.

[21]. Ashwak,M. Al-Abiachi, Faudziah, A. & Ku, R. (2011). A Competitive Study of Cryptography Techniques Over Block Cipher. UKSim 13th International Conference on Modelling and Simulation.

[22]. Jamil, N., Mahmod, R., Z, M. R., Udzir, N. I., & Zukarnain, Z. A. (2013). Diffusion Analysis of Message Expansion in STITCH-256, 2013(July), 129–137.

[23]. Mara, U. T. (2017). RANDOMNESS ANALYSIS ON 3D-AES BLOCK. 2017 13th International Conference on Natural Computation, Fuzzy Systems and Knowledge Discovery (ICNC-FSKD), 331–335.

[24]. Bjelland, E. and Haddara, M. (2018) 'Evolution of ERP Systems in the Cloud: A Study on System Updates', Systems, 6(2), p. 22. doi: 10.3390/systems6020022.