A Review of Encryption Algorithms in Cloud Computing

Derick M. Rakgoale, Topside E. Mathonsi, Tonderai Muchenje, and Vusumuzi Malele

***Abstract*—Cloud computing offers distributed online and on-demand computational services from anywhere in the world. Cloud computing services have grown immensely over the past years especially in the past year due to the Coronavirus pandemic. Cloud computing has changed the working environment and introduced work from work phenomenon which enabled the adoption of technologies to fulfil the new workings including cloud services offerings. The increased Cloud Computing adoption has come with new challenges regarding data privacy and its integrity in the cloud environment. Previously advanced encryption algorithms failed to reduce the memory space required for Cloud Computing performance thus increased the computational cost. This paper reviews the existing encryption algorithms used in Cloud Computing. In the future, Artificial Neural Networks**

(ANN) algorithm design will be presented as a security solution to ensure data integrity, confidentiality, privacy, and availability of user data in Cloud Computing. Moreover, MATLAB will be used to evaluate the proposed solution, and simulation results will be presented.

***Keywords*—Cloud Computing, Confidentiality, Data Integrity, Privacy.**

I. Introduction

Over the recent past years, Cloud computing has grown immensely in the Information Technology industry around the world. Cloud computing is an on-demand resource-sharing platform that provides online services through a subscription license and is central to accessing information services anywhere through the Internet [1, 2]. Cloud services commonly used are Software as a Service (SaaS), which is a way of delivering applications over the Internet as a service. The service provider manages access to the application, including security, availability, and performance [1-5]. The second one is Infrastructure as a Service (IaaS), which is a standardized, highly automated offering in which computing resources owned by a service provider, complemented by storage and networking capabilities, are offered to customers on demand. Resources are scalable and elastic in near real-time and metered by use [1-5].

Finally, the most popular one, Platform as a Service (PaaS) is a cloud computing service that uses virtualization to offer an application-development platform to developers or organizations. This platform includes computing, memory, storage, database, and other app development services [6-10].

Tshwane University of Technology, Private Bag X680, Pretoria 0001, South Africa

The growth of Cloud-based applications has increased in the 21st century, namely WhatsApp, Skype, Microsoft office 365, Google Docs, Business management software such as Customer Relationship Management (CRM), and Enterprise Resource Plan (ERP) which enable access to data from everywhere in the world at any time [1]. However, data security remains a major hurdle to Cloud Computing adoption and has always remained a key issue in the IT industry. This paper attempts to increase the understanding of the importance of securing data in Cloud Computing, especially in the adoption of home computing, which has been triggered by the pandemic of Coronavirus that is spreading in the world at an alarming rate.

Over the past years, researchers have developed security algorithms in order to secure data in Cloud Computing, for example: Thabit et al. [3] proposed a novel cryptographic technique based on logic-mathematical functions, and genetics technique is implemented to increase the secrecy level of data during encryption, first the exploitation of logical operations, such as ("XOR, XNOR, and Shifting") with the division of the original plaintext and key into equal parts, which ensure the key properties of diffusion and confusion keeping ciphertext, layer secrecy and to increase privacy, he used genetics based on "Central Dogma of Molecular Biology" (CDMB) for the cryptographic purpose by stimulating the natural processes of genetic cryptography ("translation from binary to DNA bases"), transcription ("regeneration from DNA to mRNA") and translation ("regeneration from mRNA to protein"), to ensure the secrecy of the second layer.

While Basu et al. [5] proposed the cryptosystem that uses first the text encoded in 16-bit blocks each using the probability-based variable length of Huffman encoding to provide the complexity and difficulty mapping between the plaintext and ciphertext, and also the algorithm is based on the CDMB which simulate the natural processes of genetic coding ("conversion from binary to DNA bases"), transcription ("conversion from DNA to mRNA") and translation ("conversion from mRNA to protein") to allow encryption-decryption processes and outputs from the blocks concatenated to form the new ciphertext in the form of protein.

Furthermore, Biswas et al. [6] proposed a DNA cryptography technique that uses dynamic sequence tables and dynamic DNA encoding to re-assembling the positions of DNA base sequences iteratively combining both the mathematical operations and asymmetric cryptosystem to enhance the level of data secrecy in the cloud environment.

However, existing security algorithms used in Cloud Computing suffer from computational complexity which

increases computational time. Moreover, these algorithms require large memory thus poor QoS in Cloud Computing.

The rest of the paper is structured as follows: In Section 2, we present related work. In Section 3, we present techniques that will be used to design the proposed solution. In Section 4, we present the conclusion and future work.

II. Related Work

Over recent past years, different algorithms have been developed in order to provide data integrity, confidentiality, privacy, and availability in Cloud Computing. In this section, we present these algorithms and the gaps identified.

Tahir et al. [1] proposed a genetic algorithm (GA) based cryptosystem to secure data in the cloud to overcome the data challenges of privacy and integrity. These cryptosystems ensured the privacy and integrity of cloud data by generating keys for encryption and decryption which are integrated with the cryptographic algorithm [1]. The algorithm was evaluated based on the following parameters: throughput, key size, avalanche effect, and execution time to test and validate ten different datasets. The implementation was based on the crossover and mutation technique processes using the genetic algorithm operations with randomness that is nature-inspired, and improved high-security level during the uploading and downloading of the data to and from the cloud or during transmission at the receiver [1].

Firstly, the plaintext is converted into ciphertext by Caesar cipher and then 128-bit chromosomes of the encrypted text are generated. Random point crossover is then performed between 128-bit chromosomes of the ciphertext and a 128-bit key. The mutation is then applied to the child by randomly flipping one bit to obtain the encrypted text [1]. The obtained simulation results showed the robustness of the cryptogram as it performs better compared to the state-of-the-art encryption techniques i.e. Data Encryption System (DES), Advanced Encryption System, Triple Data Encryption System (3DES), Blowfish, and RSA. However, the algorithm presented by Tahir et al [1], did not minimize the space complexity to address the memory requirement challenges. The algorithm was also limited to include other data types e.g. audio, video, and images in the test evaluation performed.

Namasudra et al. [2] developed a new DNA-based encryption algorithm to secure data in Cloud Computing. The algorithm generated a 1024-bit secret-key to improve the password generation technique built on the user's secret attributes. The algorithm allowed the data owners to be online and provide the DNA-based secret key to access a certificate, and then go offline after providing the credentials. the algorithm improved the security of the data in the cloud by using the 1024-bit DNA-based secret key, the data owner's private key, and the user's public key to protect and defend against many cyber-attacks [2]. The obtained simulation and analysis of DNABDS shows effectiveness and efficiency compared to existing techniques, e.g. Blowfish, etc. However, the DNA-based data security algorithm presented by Namasudra et.al [2], did not reduce the space complexity to meet memory requirements and did not provide mathematical evidence for strong security and computational overhead reduction during the authentication processes.

Thabit et al. [3] proposed an algorithm based on genetics techniques and logic-mathematical functions to ensure security, integrity, and authorized access using various methods such as "deoxyribonucleic acid" (DNA) in Cloud Computing. The algorithm used Shannon's theory of diffusion and disorientation with feudal and substitution architecture methods which include logical processes that improve the complexity of cryptography [3].

The algorithm used a novel cryptographic technique based on logic-mathematical functions and genetics techniques to increase the secrecy level of data during encryption, first the exploitation of logical operations, such as ("XOR, XNOR, and Shifting") with the division of the original plaintext and key into equal parts, which ensure the key properties of diffusion and confusion keeping ciphertext, layer secrecy and to increase privacy, he used genetics based on "Central Dogma of Molecular Biology" (CDMB) for the cryptographic purpose by stimulating the natural processes of genetic cryptography ("translation from binary to DNA bases"), transcription ("regeneration from DNA to mRNA") and translation ("regeneration from mRNA to protein"), to ensure the secrecy of the second layer. However, the algorithm presented by Thabit et al. [3] did not decrease the complexity of the memory space required to meet memory requirements as genetics cryptography is still in its early state.

Thabit et al. [4] proposed a "new lightweight cryptographic algorithm" (NLCA) to improve the security of data in the cloud and provide a highly secure encryption-decryption system with low computational cost. The algorithm uses a complex structure and a mixture of Feistel and "Substitution-Permutation" (SP) architecture techniques to provide an effective key scheme to assist in the obfuscation using a matrix and "F-function" extension of a key instead of a single extension key to protect against brute-force attacks. A 16-byte (128-bit) block cipher with a 16-byte (128-bit) key is developed to encrypt the data, using an encryption process that requires multiple encryption rounds in a symmetric key algorithm, where each round always relied on mathematical functions to generate diffusion and confusion [4].

The simulated results obtained showed that the NLCA algorithm improved encryption-decryption processes to achieve a strong security level at a low computational cost. However, the NLCA algorithm presented by Thabit et al. [4] did not use enough hardware components to improve the strength of security and only performed five rounds to maximize the energy efficiency results since 4 bits of data is required for each round required crypto-mathematical operations to work. However, to meet device specifications usually an average of 10 or 20 rounds of configuration is required.

Basu et al. [5] developed a cryptosystem that is inspired by biology called "bio-inspired cryptosystem" and neural

networks which use machine learning and DNA cryptography to improve the capability of the encryption-decryption algorithm to reduce the execution time of large sizes of data. The cryptosystem uses first the text encoded in 16-bit blocks each using the probability-based variable length of Huffman encoding to provide the complexity and difficulty mapping between the plaintext and ciphertext and also the algorithm is based on the CDMB which simulates the natural processes of genetic coding ("conversion from binary to DNA bases"), transcription ("conversion from DNA to mRNA") and translation ("conversion from mRNA to protein") to allow encryption- decryption processes and outputs from the blocks concatenated to form the new ciphertext in the form of the protein [5].

The obtained simulated results are based on a variety of data involving whitespaces and special characters to improve the security of cloud-known cyber-attacks. However, the cryptosystem algorithm presented by Basu et.al, did not incorporate additional security to strengthen authentication measures. The algorithm did not provide high security as DNA cryptography is still in an emerging state.

Biswas et al. [6] designed a DNA cryptography technique using a dynamic sequence table and dynamic DNA encoding to re-assembling the positions of DNA base sequences iteratively combining both the mathematical operations and asymmetric cryptosystem to enhance the level of data secrecy in the cloud environment. First, the technique exploits the dynamic sequence table to hold the characteristics of substitution cipher and ensure first-level secrecy during encryption, and then provide second-level secrecy to increase privacy, lastly to enhance the high-security level using the dynamic DNA encoding that maintains the properties ciphertext used with asymmetric cryptosystem in order to provide third-level secrecy [6]. The obtained simulated results showed that the ciphertext generated is pseudorandom and highly secure. However, the technique for DNA cryptography presented by Biswas et al. [6] did not cover various forms of data and platforms e.g. video, audio, images, and numeric.

Sohal & Sharma [7] implemented a new symmetric key cryptographic algorithm inspired by "BDNA-A" DNA to secure Cloud Computing which uses random dynamic encoding tables to achieve a higher level of security. The BDNA uses a client-side data encryption technique using a symmetric key algorithm to encrypt the data before uploading it in the cloud to prevent unauthorised access to the data [7]. The simulation results showed that their solution performed better than other symmetric key encryption algorithms in relation to ciphertext size, encryption time, and throughput especially DNA, AES, DES, and Blowfish.

Al-Mahdi et al. [8] proposed a DNA cryptography technique using an asymmetric encryption algorithm and cryptosystems is based on data dependency, dynamic encoding table, and dynamic round keys with strong avalanche properties. The algorithm created a dynamic DNA table plaintext, using multilevel security and data dependency by generating 14 dynamic round keys [8]. The obtained results showed that the encryption technique outperforms the RSA algorithm in terms of strong avalanche property, and is not superior in terms of execution time, and was implemented and tested using the Java platform. However, the asymmetric cryptography system used showed that encryption-decryption did not focus and validate computational cost and memory requirements.

Nazeer et al. [9] proposed a cryptography technique based on a genetic algorithm to improve the level of security by modelling simplified genetic processes to ensure the strength of the encryption key to improve the whole algorithm good enough. The algorithm technique first, generated the key through a random number generator and diffuse the data using first the genetic operator and then the logical operator to encrypt the data, in order to improve the unpredictability and encryption key strength using diffused data and the key.

The obtained simulation result using the Java platform has shown that their algorithm improved the key strength and high computational cost because it takes a little longer encryption time than DES and AES. However, the algorithm was more expensive in terms of computation time rather than DES and AES, although the improved the key strength and achieved a higher security level, the computational cost was also higher, including the fact that multimedia encryption i.e. images, video, and audio were not tested.

The review of literature has shown that other researchers have developed and implemented different encryption algorithms for Cloud Computing. However, due to the high computational cost of these algorithms, it is still a very difficult and challenging task to achieve data integrity, confidentiality, privacy, and availability in Cloud Computing. In the next Section, we present an idea of how the proposed solution will be designed in the future.

III. Proposed Solution

This paper proposes the design of a robust encryption algorithm for Cloud Computing using the ANN algorithm. ANN algorithm was chosen because they are non-linear, robust, and adaptive in nature. The adaptive nature of ANN has the competence to adjust the system parameters for the duration of the training phase thereafter the ANN parameters are static and a system is developed to solve the identified problem rapidly. In addition, the non-linear processing unit of ANN provides the system flexibility to accomplish practically any desired input/output map.

In the proposed solution, ANN will be divided into two categories namely supervised learning and unsupervised learning. In supervised learning, the model work over the input and produce the output that is predefined or known while in unsupervised learning, the output will be unknown.

IV. Conclusions and Future Work

Use Cybersecurity attacks have become our daily news in today's IT industry. Encryption algorithm in Cloud Computing plays an important role and puts data privacy and its integrity at

the center of current challenges facing cloud adoption. Previously advanced encryption algorithms failed to reduce the memory space required in Cloud Computing and increased the computational cost. In the future, the design of an ANN algorithm with a high level of security to achieve data integrity, confidentiality, privacy, and availability of user data in Cloud Computing will be presented. Thereafter, MATLAB will be used to evaluate the proposed solution, and simulation results will be presented.

REFERENCES

[1] Tahir, M., Sardaraz, M., Mehmood, Z. and Muhammad, S., “CryptoGA: a cryptosystem based on genetic algorithm for cloud data security”. Cluster Computing, 24(2), pp.739-752, 2021. https://doi.org/10.1007/s10586-020-03157-4

[2] Namasudra, S., Devi, D., Kadry, S., Sundarasekar, R. and Shanthini, A., “Towards DNA based data security in the cloud computing environment”. Computer Communications, 151, pp.539-547, 2020. https://doi.org/10.1016/j.comcom.2019.12.041

[3] Thabit, F., Alhomdy, S. and Jagtap, S., “A new data security algorithm for the cloud computing based on genetics techniques and logical-mathematical functions”. International Journal of Intelligent Networks, 2, pp.18-33, 2021. https://doi.org/10.1016/j.ijin.2021.03.001

[4] Thabit, F., Alhomdy, S., Al-Ahdal, A.H. and Jagtap, S., “A new lightweight cryptographic algorithm for enhancing data security in cloud computing”. Global Transitions Proceedings, 2(1), pp.91-99, 2021. https://doi.org/10.1016/j.gltp.2021.01.013

[5] Basu, S., Karuppiah, M., Nasipuri, M., Halder, A.K. and Radhakrishnan, N., “Bio-inspired cryptosystem with DNA cryptography and neural networks”. Journal of Systems Architecture, 94, pp.24-31, 2019. https://doi.org/10.1016/j.sysarc.2019.02.005

[6] Biswas, M.R., Alam, K.M.R., Tamura, S. and Morimoto, Y., “A technique for DNA cryptography based on dynamic mechanisms”. Journal of Information Security and Applications, 48, pp.102363, 2019. https://doi.org/10.1016/j.jisa.2019.102363

[7] Sohal, M. and Sharma, S., “BDNA-A DNA inspired symmetric key cryptographic technique to secure cloud computing”. Journal of King Saud University-Computer and Information Sciences, pp. 1-9, 2018.

[8] Al-Mahdi, H., Alruily, M., R. Shahin, O., and Alkhaldi, K., “Design and Analysis of DNA Encryption and Decryption Technique based on Asymmetric Cryptography System”. International Journal of Advanced Computer Science and Applications (IJACSA), 10(2), pp. 499-506, 2019. https://doi.org/10.14569/IJACSA.2019.0100264

[9] Nazeer, M.I., Mallah, G.A., Shaikh, N.A., Bhatra, R., Memon, R.A. and Mangrio, M.I., “Implication of genetic algorithm in cryptography to enhance security”. International Journal of Advanced Computer Science and Applications, 9(6), pp.375-379, 2018. https://doi.org/10.14569/IJACSA.2018.090651

[10] Thabit, F., Alhomdy, S.A.H., Alahdal, A. and Jagtap, S.B., “Exploration of Security Challenges in Cloud Computing: Issues, Threats, and Attacks with their Alleviating Techniques”. Journal of Information and Computational Science, 12(10), pp. 35-56, 2020.