Securing Data And Information In The Cloud Using Dna And Morse Coding Techniques

L. Soumya Krishnan and Dr.K.Selvakumar*
Department of Mathematics, Anna University, Chennai, University College of Engineering, Nagercoil, Tamilnadu, India

Abstract: *Cloud computing is a computing strategy that provides services hosted on the Internet to its users/customers. It refers to the computer solutions that are distributed. The cloud allows data to be stored and provides remote access to any work-related data. Enables easy access to cloud computing services at a low cost. Data protection and privacy protection are two major confusions about cloud technology. Various methods have been followed to make data security in the cloud reliable. A two-way DNA encryption algorithm (BDEA) is one such data protection technique. However, the current technology ignores the non-English user of cloud computing and focuses only on the ASCII script. This proposed work focuses on improving BDEA. To increase the security and confidentiality of data in the cloud environment, DNA sequences are used for encryption programs with Morse code. Using Morse code makes it very difficult for an intruder to steal the original data. Theoretical and experimental results show the efficiency of the algorithm, It is also an indication that it can be used in a variety of applications such as security, banking, and medical purposes. The future job is to encrypt color images and videos to upload to the cloud.*

Keywords: **Cloud computing, Data security issues, Bi-Directional DNA Encryption Algorithm, DNA digital code, Morse code**.

I. INTRODUCTION

Communicate with the service provider explaining that cloud computing enables convenient, on-demand network access anywhere. Resources refer to computing applications, network resources, operating systems, software services, virtual servers, and computer infrastructure. In the public cloud, the pay-per-use model is used. In a private cloud, the computing service is distributed to a community. In a hybrid cloud, the computing service is used by both the private cloud service and the public cloud service.

Three well-known and commonly used service models in the cloud paradigm are a software as a service (SaaS), platform as a service (PaaS), and infrastructure as a service (IaaS). In SaaS, software with related data is used by the cloud service provider, Also users can use it through web browsers. In PaaS, a service provider simplifies services for users with a set of software programs that can solve specific tasks. Perhaps, the cloud service provider facilitates services to users with virtual machines and storage to enhance their business efficiency.

In [10], influential articles have been identified to pursue research for the benefit of society in the field of computer science and artificial intelligence, entitled DNA Cryptography Research in Cloud Computing. Both articles are identified as influential. Experimental results are provided using term parallel event and numerical link networks, quoting network analysis tools.

Influential articles [3] and [8]. Both of these articles provide current and future developments in this area of research.

Nithya et al. In [8] have developed a well-intentioned security framework that guarantees the highest level of protection for all types of color images. DNA sequences, Hybrid, secure, and robust HEVC cryptosystem based on confusing maps and Mandelbrod compilations has been proposed by Abdul Aziz Clarify et al. [3]

In [11], articles were selected for review in the field of computer science and artificial intelligence entitled DNA Cryptography Research in Cloud Computing. 85 articles were selected using cluster analysis. Experimental results are provided using term parallel event and numerical link networks, quote network, and cluster analysis tools. In [2, 4,5,6, 7, 9, 12,13, 14,15,16], many DNA encryption methods are applied to encrypt and then store in the cloud and transmit in cloud services, In [1], a Hindi language plaintext is encrypted and uploaded in the cloud and downloaded by the cloud authenticated user and decrypted to get back the Hindi plaintext. The rest of the works are only for English language speaking people.

The system [1] uses an encryption algorithm based on the DNA pattern. This algorithm involves three steps; they are normal encryption of data, generation of arbitrary keys, and Decrypting data. In this encryption process, plain text is converted to ASCII value and then to a binary value, and then complementary and binary coding is applied. In the second step generation of arbitrary keys is used for the next level of encryption.

1.1 The motivation of this research work

The existing security system has failed to provide adequate security for cloud data. In the absence of strong security measures, attackers can use those false configurations to steal cloud data. This forced to use of more techniques like Morse coding and SMS key in addition to DNA encryption to provide security to the cloud data.

1.2 Main Result of this article

The main result of this research work is to provide high-level security to data during storage in the cloud and transmission in the cloud service.

In section 1, the introduction of the topic is given. In section 2, the existing algorithm is provided. In section 3, the proposed algorithm is presented. In section 4, experimental results are provided. Finally, in section 5, the conclusion and future work are discussed.

2. PROPOSED METHOD

To provide high security, DNA-based cryptography is introduced. DNA cryptography is nothing but hiding information in DNA Structure. DNA cryptology is a method to accumulate huge information and provides data integrity and security. Therefore this technique is robust since the encoding technique is difficult to break. The DNA nucleotides are of four types that are A, C, G,

T. By using these four nucleotides DNA based cryptography is implemented. The easiest coding patterns of these four nucleotides are in the following Table.

In information science, binary digital notation is encrypted by two levels, 0 or 1, and is a combination of 0 and 1. But DNA digital code can be encrypted by four types of bases as shown in Table 1. It contains adenine (A) and thymine (D) or cytosine (C) and guanine (G). There can be 4! = 24 formats with a code format like (0123 / ATGC).

Table 1: Coding based on DNA nucleotides

DNA component	Binary coded form
Adenine(A)	00
Cytosine(C)	01
Guanine(G)	10
Thymine(T)	11

Earlier cryptography techniques are based on mathematical equations that may reduce the security of data. DNA-based cryptology is highly secure than other cryptological techniques.

2.1 Key combination

.In this work here, we use ATGC as a key. Each digit contains bits such as A = 00, T = 01, G = 10, and C = 11, and using ATGC, key combinations are generated and numbered, respectively. They are given in Table 1. From Table 2, we can create 64. By adding bit key values and ATGC, we can create a 72-bit key (64 bits key combination and 8 bits ATGC). The ATGC key is sent to the recipient's page. In this work, the core value is changed approximately every time.

Table 2: Key combination

Key combination	**Patterns**	**values**		**Key combinations**	**Patterns**	**values**
AA	0101	5		GA	1010	10
AT	0011	3		GT	0001	4
AG	0001	1		GG	1000	8
AC	0010	2		GC	1100	12
TA	0110	6		CA	1110	14
TT	1111	15		CT	1011	11
TG	0111	7		CG	9999	0
TC	1001	9		CC	1101	13

2.2 Morse coding

Morse coding used in this article is given in the following table

Table 3: DNA Encoding with Morse pattern

DNA Sequence	Morse Pattern
A	.-
C	..
G	-.
T	--

Both the encryption and decryption algorithms are presented in Algorithms 1 and Algorithm 2,

Algorithm 1: The data encryption algorithm

1: Begin
2: Input: D to be stored D, Random DNA R-DNA.
3: Select the D data to be stored securely in the cloud, convert the data to binary and say 'BD'.
4: Digital DNA Converts binary data into DNA sequence based on the DNA coding rule according to Table 1, which generates DNA.
5: Digital Databases Create random DNA strands by selecting DNA sequences from R-DNA.
6: Select R-DNA and schedule it. Select indexed and non-indexed areas approximately or based on index values.
7: Convert the coded R-DNA into short pieces based on the length of the DNA base pair and the DNA-based core value.
8: Remove the non-encoded part, and the generated DNA sequence is used as a cover to attach the DNA.
9: Insert D'DNA in non-encoded areas of R-DNA generated based on coding conditions or randomization according to the selected scheduling rule.
10: The DNA sequence generated by DNA steganography is converted to binary form using the selected binary rule.
11: Re-encrypt the data using Morse coding and provide extra security.
12: Upload the encrypted data in binary format, after which a key will be sent as SMS to the owner's phone.
13: Save data to the cloud.
14: Release: Encrypted data
15: End

Output: Encrypted Data

Algorithm 2: Data decryption algorithm

1: Begin
2: Input: Encrypted data.
3: Extract encrypted data from the cloud in binary format using the main SMS.
4: Apply the selected DNA binary coding rule to the data and obtain the data in the form of a mixed DNA sequence of R-DNA and DNA.
5: Select the encoded and non-encoded parts of the DNA based on the code value status.
6: Recover DNA fragments from a non-encoded area.
7: Separate the D'DNA and R-DNA from the DNA sequence.
8: Use the DNA encoding rule to get binary data by adding fragments of DNA.
9: Convert binary to original data
10: Release: Original Data and Random DNA
11: End

Output: Original plain text

2.3 Application of the encryption algorithm

Step 1: The plaintext is " **My confidential Data**."

Step 2: Convert data to binary format.
0100110101111001010000110110111101101110011001100110100101100100011001010110111001110100011010010110000101101100010001000110000101110100 1100001 (1).

Step 3.: Use DNA binary code on (2) to create (1) in DNA format

Step 4: Random DNA (R-DNA)

ACTGCTGAGAGTTGAGCTCACCCTC AGTCCCTCACAGTTCCACACTGCCT (2)

Step 5: Indexing the R-DNA.

A1C2T3G4C5T6G7A8G9A10G11T12T13G14A15G16C17T18C19A20C21C22C23T24C25 A26G27T28C29C30C31T32

Step 6: Select the index and non-index areas approximately or based on the index positions.
Step 7: Insert D'NA into non-encoded areas of DNA. The index and non-index areas defined in this model are based on the index values:
Coding region:

A1C2T3G4C5

Non-Coding region:

T6G7A8G9A10G11T12T13G14A15G16C17T18C19A20C21C22C23

Coding region from the R-DNA:

T24C25A26G27T28C29C30C31T32

Step 8: Insert the DNA into the respective non-encoded stages. Random DNA acts as a cover medium for the insertion of selected D'DNA and performs DNA steganography.
DNA Replacing:

GATG GTCG GAAT GCTT GCTC GCGC GCCGGCGA GCGG GCTC GTGA GCCG GCAG GCTAGAGA GCAG GTGA GCAG -

Non-coded regional bases with 4 bases (core value) of D'DNA for each site in the non-coded region.
Cover DNA(noncoding region):

T6G7A8G9A10G11T12T13G14A15G16C17T18C19A20C21C22C23 -

DNA Steganography.:

(GATG)6(GTCG)7(GAAT)8(GCTT)9(GCTC)10(GCGC)11(GCCG)12(GCGA)13 (GCAG)18(GCT A)19(GAGA)20(GCAG)21(GTGA)22(GCAG)23

Step 9: Generate the DNA Sequence.

Indexed form:

A1C2T3G4C5(GATG)6(GTCG)7(GAAT)8(GCT T)9(GCTC)10(GCGC)11(GCCG)12

GCGA)13(GCGG)14(GCTC)15(GTGA)16(GCCG)17(GCAG)18(GCT A)19

(GAGA)20(GCAG)21(GTGA)22(GCAG)23T24C25A26G27T28C29C30C31T32

Stego DNA:

ACTGCGATGGTCGGAATGCTTGCTCGCGCGCCGGCGAGCGGGCTCGTGAGCCGGCA GGCTAGAGAGCAGGTGAGCAGTCAGTCCCTCACAGTTCCACACTGCCT

Step 10: Apply Morse coding

.- -.-. - --. -.-. --. .- - --. --. - -.-. --. --. .- .- - --. -.-. - - --. -.-. - -.-. --. -.-. --. -.-. --. -.-. -.-. --. --. -.-. --. .- --. -.-. --. --. --. -.-. - -.-. --. - --. .- -. -.-. -.-. --. --. -.-. .- --. --. -.-. - .- --. .- --. .- --. -.-. .- --. --. - --. .- --. -.-. .- --. - -.-. -.-. -.-. - -.-. .- -.-. .- --. - - -.-. -.-. .- -.-. .- -.-. - --. -.-. -.-. -

Step 11:Data uploading in Cloud

The original data in the file is converted to binary order in the first step. The next step is to convert the binary sequence into a DNA sequence. This mutation uses a secondary mutation in the DNA sequences AGT and C. The tertiary modification is done using the Morse format. The DNA sequence is converted into a data point and line format. The encryption steps above will generate the original data and move it to the cloud environment.

When uploading encrypted data, a four-digit security code is generated and sent as an SMS to the connected phone. We can only download data from the cloud using that key. Data

encryption is carried out using the same method. The DNA sequence is included here to bring this encryption project into one that cannot be broken.

The proposed system converts the original data to binary and then uses DNA encryption algorithm, steganography, and Morse coding techniques to secure the data. While uploading in the cloud, a key will be generated as SMS and sent to the owner's phone. Using the same key only the data can be downloaded and decrypted. The algorithm can be used for military purposes as any country's data is very important, confidential, and be secure. It can be also used for banking applications where it can be used to encrypt the vital data of the customer such as the account number, pin, or password.

3. Experimental Results of the Algorithm

In this section, the proposed algorithm is compared with the already existing algorithm concerning various metrics such as time, efficiency, performance, frequency, speed, and security. The existing algorithm is available in [1] by B., P. Ashishkumar, and P. Barkha.

3.1. Comparison between existing and proposed work

In figures 3 and 4, the horizontal axis refers to various metrics of the system and the vertical axis refers to the percentage of system metrics. From Figures 1 and 2, the proposed system is better than the existing algorithm.

Fig 1: Comparison by a line graph

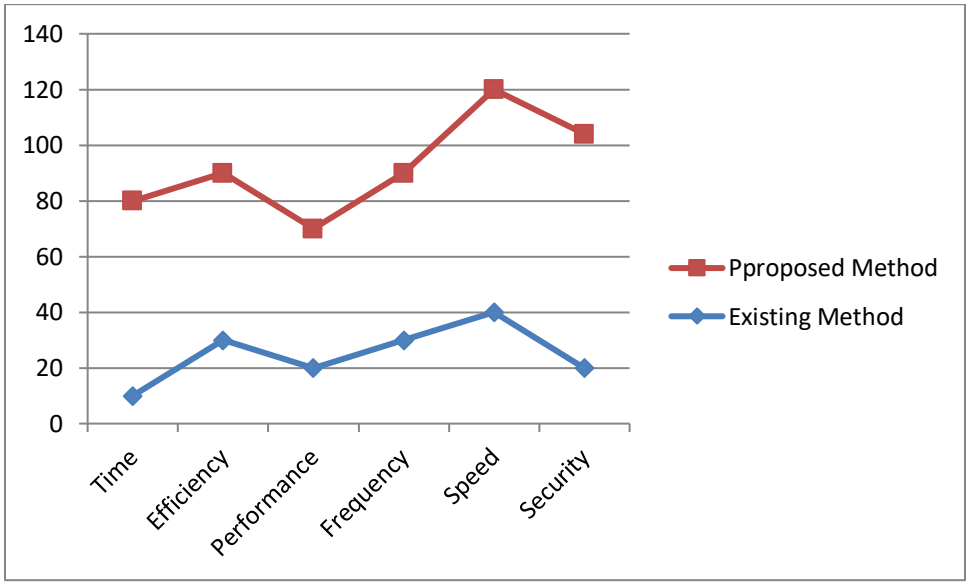
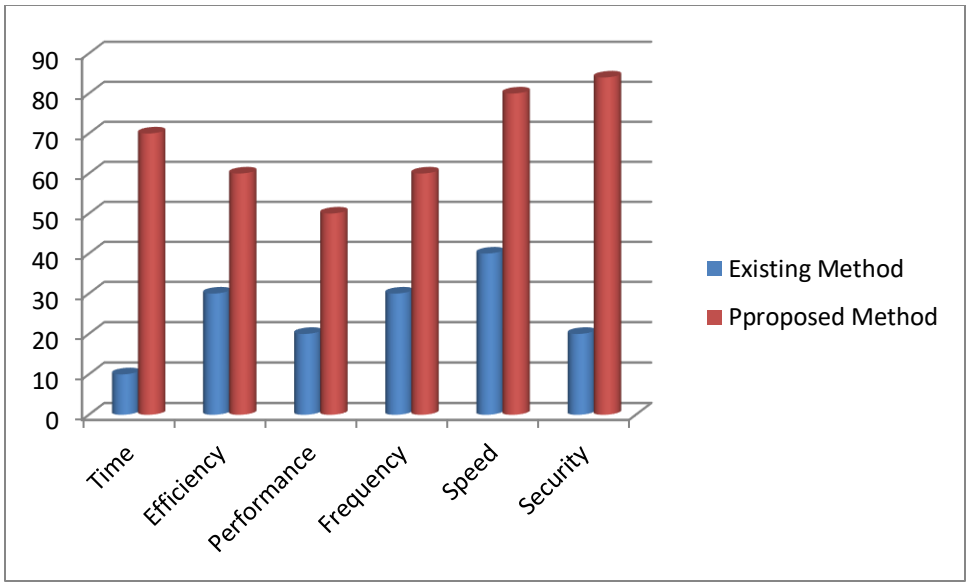


Fig 2: Comparison by column chart



The algorithm presented in this paper has been tried and the results are being presented. The results show the effectiveness of the algorithm and are an indication that it can be used in various applications like defense, banking, and medical purposes

5. CONCLUSION AND FUTURE WORK

Data security is the main challenge for cloud usability. To improve the security of cloud computing a new model has been proposed. DNA encryption and Morse code techniques are used in this work to provide high security to cloud data storage. An SMS key will be sent to the data owner's mobile while uploading data to the cloud and using the same key only data can be retrieved from the cloud. After that, the data can be decrypted using the decryption algorithm and thereby providing HIGH levels of data security. COVID 19 prediction and medical record data set encryption can be done as a future enhancement. Future work will focus on encrypting color images and videos to upload in the cloud.

References

1. B., P. Ashishkumar, and P. Barkha, Implementation of DNA cryptography in cloud computing and using socket programming. *ICCCI -2016*, IEEE Xplore. 1-6. 2016.
2. R. Bhadauria and S. Sanyal, Survey on security issues in cloud computing and associated mitigation techniques, arXiv preprint arXiv:1204.0764, 2012.
3. A. Clarify, S. Sankar, Torki altameem, K. C. Jithin, Mohammed moon, and Walid el-shafai, A Novel Hybrid Cryptosystem for Secure Streaming of High-Efficiency H.265 Compressed Videos in IoT Multimedia Applications, IEEE Access, 8: 128548- 128573, 2020, doi:10.1109/ACCESS.2020.3008644

4. X. Li, C. Zhou, N. Xu, A secure and efficient image encryption algorithm based on DNA coding and spatiotemporal chaos, Int. J. Network Security, 20(1), 110-120, 2018.
5. L. Liu, W. Kong, Z. Cao, J. Wang, Analysis of one certificate less encryption for secure data sharing in public clouds, Int. J. Electronics and Information Eng., 6(2), 110-115, 2017.
6. M. Misbahuddin and C. Sreeja, A secure image-based authentication scheme employing DNA crypto and steganography, in Proceedings of the Third International Symposium on Women in Computing and Informatics, 595–601, 2015.
7. A. Murugan, and R., Thilagavathy, Securing Cloud Data using Dna and Morse Code: A Triple Encryption Scheme. Int. J. Control Theory Appl. 30–38, 2019.
8. C. Nithya, R. Pethuru, K. Thenmozhi1, and R. Amirtharajan, Advanced framework for highly secure and cloud-based storage of color images, IET Image Process, 14(13), 3143-3153, 2020.
9. B. T. Rao and N. Vurukonda, A study on data storage security issues in cloud computing, Procedia Computer Science, 92, 128–135, 2016.
10. L. Soumya Krishnan and K.Selvakumar, Finding Influential Articles on the Topic of DNA Cryptography in Cloud Computing in the Field of Computer Science and Artificial Intelligence, IJIRST, 8: 2(001) 1-3, 2021.
11. L. Soumya Krishnan and K.Selvakumar, DNA Cryptography in Cloud Computing in the Field of Computer Science and Artificial Intelligence, IJIRST, 8: 2(002) 1-8, 2021.
12. C, S. Sreeja, M. Misbahuddin, DNA Cryptography for Secure Data Storage in Cloud, Int. J. Network Security, 20(3), 447-454, 2018. DOI: 10.6633/IJNS.201805.20(3).06.
13. C. S. Sreeja., M. Misbahuddin, and B. S. Bindhumadhava, . DNA-based cryptography to improve the usability of authenticated access of electronic health records. Lect. Notes Inst. Comput. Sci. Soc. Telecommun. Eng. LNICST **218**, 208–219 , 2018.
14. Y. Sun, J. Zhang, Y. Xiong, and G. Zhu, Data security and privacy in cloud computing, Int. J. Distributed Sensor Networks, 2014.
15. Z. Wang, Y. Lu, G. Sun, A policy-based de-duplication mechanism for securing cloud storage, Int. J. Electronics and Information Eng., 2(2). 70-79, 2015.
16. C-H Yang, C-H Yang, L-Y Chuang, T-K Truong, The application of the neural network on Morse code recognition for users with physical impairments, 215(3), 2001.