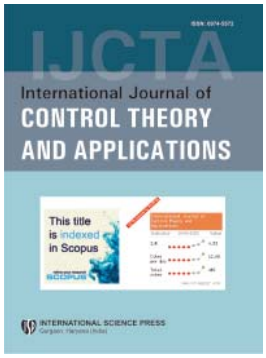

International Journal of Control Theory and Applications

ISSN : 0974–5572

Volume 10 • Number 23 • 2017

Securing Cloud Data using Dna and Morse Code: A Triple Encryption Scheme

A. Murugan[a] and R. Thilagavathy[b]

[a]*Associate Professor, PG and Research Department of Computer Science, Dr. Ambedkar Government Arts College (Autonomous), Affiliated to University of Madras,Chennai, India.*

E-mail: amurugan1972@gmail.com

[b]*Research Scholar, PG and Research Department of Computer Science, Dr. Ambedkar Government Arts College (Autonomous), Affiliated to University of Madras,Chennai, India.*

E-mail: thilagmca@gmail.com

Abstract: Cloud computing offers utility -oriented IT services to users. Cloud computing provides us cheaper, faster, flexible, efficient environment. Due to various advancements many companies are migrating to cloud environment. At the same time, cloud computing faces more challenges, threats and risks related to data security. DNA cryptography is used to encrypt message for secure communication on cloud computing environment. Protecting sensitive data is challenging task in cloud environment. For increased security, the recommended approach is to combine two or more methods – processes, DNA cryptography and Morse pattern. DNA cryptography with Morse pattern is difficult to fabricate, which makes the attacker much harder to steal the original data. Mentioned DNA based Triple encryption algorithm is more secure algorithm and the correctness of proposed system is checked by using various online encryption tools.

Keywords: *Cloud computing, Security, DNA sequence, Morse pattern.*

1. INTRODUCTION

Cloud computing is an internet based service model aims to deliver secure, reliable, fault-tolerant and scalable infrastructure with minimum cost. Cloud provides application, infrastructure, platform and security as services [1]. Cloud computing is divided in to three forms - public, private and hybrid. According to the National Institute of Standards and Technology (NIST), "Cloud computing is an on-demand network access model for the shared pool of configurable computing resources"[2]. Cloud computing provides computing environment [3] with thousands of servers.

The main advantage of cloud computing is to provide secured storage and services. Data security is a critical aspect in the modern and business world. Through cloud computing the sensitive information like financial transactions, medical and personal records are being transmitted between cloud service provider and cloud user. This data is stored at service provider's data centre. The security of the sensitive information poses a great threat by an attacker [4] [5]. Cryptographic techniques help the user to protect the sensitive information.

2. LITERATURE RVIEW

2.1. Cryptography

In Information security, the cryptography is an aspect of building security scheme for secure communications. Cryptography is a technique used in computer science for securing data which is based on the mathematical theory [6]. The cryptography algorithms are practically difficult to decode. In digital rights management and copyright infringement of digital media, the cryptography plays key role [7]. Cryptography can be broadly classified in to two,

1. Symmetric key cryptography(SKC)
2. Asymmetric key Cryptography(AKC)

The same key is used in symmetric key cryptography for the encryption and decryption processes. Asymmetric key cryptography uses the different keys for these processes. In cryptography, key is a parameter that changes the output of the cryptographic algorithm. Cryptography enables to the secure transfer of sensitive data from cloud user to cloud provider and vice-versa. The unbreakable encryption algorithms can be built with the help of DNA computing [8]. Compared to traditional methods the new encryption algorithms were built more efficiently. So the new security algorithms are highly impossible to break [9].

2.2. DNA Based Cryptography

Deoxyribo Nucleic Acid is a hereditary molecule in living organisms. The DNA carries the genetic instructions used in the growth, development, functioning and reproduction of all organisms. DNA and RNA are composed with nucleotides, which in turn composed of four nucleobases cytosine(C), guanine (G), adenine (A), or thymine (T) and deoxyribose and phosphate group[10][11]. According to base pair rule the hydrogen bonds and nucleobases form double stranded DNA to store biological information. This information is used as a key for the encryption algorithm.

DNA sequence	*Binary Sequence*
A	00
T	01
C	10
G	11

Figure 1: DNA sequence table

A	T	G	A	C
T	A	T	C	G

Figure 2: Base Pair

The DNA sequence is represented by the binary numbers 0's and 1's. The binary values for ATCG sequence is shown in the Figure 1. According to base pair rule the nucleobases would pair A-T, T-A, G-C, C-G .The Base pair is shown in the above Figure 2.

2.3. Morse Pattern

International Morse code is a method of transmission of text information between sender and receiver. It is invented by Samuel F.B. Morse in the telegraphy field [12]. This code encodes the original text to non-English natural language called "dots" and "dashes".

3. METHODOLOGY

3.1. DNA Based Triple Encryption Scheme

This model proposes to encrypt original data at three levels. The original data in the file is converted in to binary sequence in first level. The next level is to convert the binary sequence in to DNA sequence. This conversion uses DNA sequences A G T and C for the second level conversion. The third level conversion is done using Morse pattern. The DNA sequence data is converted into dot and dash format. The above three encryption steps are made with the original data and it is moved to cloud environment. This DNA based Triple Encryption Scheme is shown in the Figure 3.

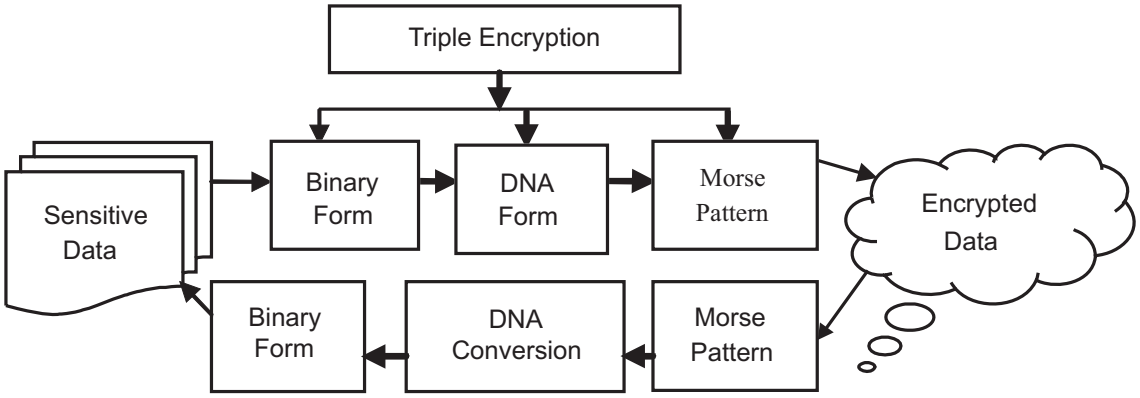

Figure 3: DNA Based Triple Encryption Scheme

The decryption of data is carried out by using the same method. The DNA sequence is added here to bring this encryption scheme unbreakable one. The following figure shows the DNA sequence and its corresponding Morse pattern which is used for the encryption scheme refer Figure 4. In order to make data more secured, a two bit string Morse pattern is used along with DNA sequence.

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

Figure 4: DNA Encoding with Morse pattern

3.2. Conversion of Binary Form

The encryption scheme is started with the conversion of sensitive data in the form of binary (0's and 1's). Here the content of text file is converted and the original form of sensitive data is changed by using Algorithm1. Let str be input data. By using step3 it is converted in to array. Step4 is used to get data up to maximum length. In step5 the conversion is done and data is stored in tmpstr. In further steps the binary data is returned and all the steps are repeated until all the data is converted.

Algorithm1: Conversion of text to binary sequence

Input: Text file

Output: Binary sequence

1. begin
2. Generate str and bit; str ← data, bit ← bits;
3. messchar = = str.tocharArray();
4. for each i ranging from 0 to max_ len_ of _messchar of str do;
5. tmpstr ← integer.tobinary string _of_ messchar;
6. tmpint ← tmpstr.length();
7. end
8. if (tmpint ! = = bits) then
9. tmpint ← bits – tmpint;
10. if (tmpint = = bits) then
11. Result ← result + tmpstr ;
12. end if
13. else
14. if (tmpint > 0) then
15. for each *j* ranging from 0 to tmpint do;
16. result ← result + 0;
17. end for
18. result ← result + tmpstr;
19. end if
20. else
21. result ← result + tmpstr;
22. end if
23. return binary;
24. End

3.2. Conversion of DNA Sequence

The DNA sequence data is discovered from the binary data by using Algorithm 2. Let str1be the input data. Step3 is used to get data up to maximum length. Step4 and step5 are used to get two characters of binary data and by using steps (1-11) it is converted in to the DNA sequence. In step16 the converted data is returned and all the step3 and step7 will repeat until all the data are converted.

Algorithm2: Conversion of binary sequence to DNA sequence

Input: Binary data

Output: DNA sequence

1. begin
2. str1 ← binary;
3. for each *i* ranging from 1 to max len of binary do;
4. char *p* ← binary.charAt(*i*);

5. char $q \leftarrow$ binary.charAt(i + 1);
6. string st $\leftarrow p + q$;
7. if (st = 00) then str1 = A;
8. if (st = 01) then str1 = C;
9. if (st = 10) then str1 = G;
10. if (st = 11) then str1 = T;
11. end
12. end for
13. DNA $\leftarrow$ DNA + str1;
14. end for
15. return DNA;
16. Extended for any number of sequences;
17. End

3.3. Conversion of Morse Pattern

The third encryption step is converting DNA sequence data to Morse pattern data. Let str2 be input data. Step3 is used to get data up to maximum length. In step4 and step5, the first character of the str2 is stored and manipulated using steps6-9. In the step13 the Morse pattern data is returned.

Algorithm 3: Encrypting data using Morse pattern

Input: DNA data

Output: Morse pattern

1. begin
2. str2 $\leftarrow$ DNA;
3. for each m ranging from 1 to max len of DNA do;
4. char $p1 \leftarrow$ str2.charAt(m);
5. char $q1 \leftarrow$ str2.charAt(m + 1);
6. string $st1 \leftarrow p1 + q1$;
7. if ($st1$ = A) then str2 $\leftarrow$ . .-;
8. if ($st1$ = C) then str2 $\leftarrow$ ..;
9. if ($st1$ = G) then str2 $\leftarrow$ -.;
10. if ($st1$ = T) then str2 $\leftarrow$ --;
11. end if
12. end for
13. mos $\leftarrow$ mos + str;
14. return mos;
15. Extended for any number of DNA strands;
16. End

Matching binary sequence and DNA sequence is a tedious job. The probability of finding two bit binary message is ½ ^{30}. The intruder must be aware of the possible combination of DNA sequence in order to find the DNA sequence and Morse pattern [13]. The triple encryption process is carried out in the above data security algorithm.

4. RESULT AND DISCUSSION

The proposed model is based on DNA molecules. The molecules will be working in parallel. So the implementation is done with java because parallel processing is supported by java language. Java is platform independent and can be used with any operating system. According to new requirements in future the simulators can also be attached with the model easily. The model has run in NetBeans IDE environment.

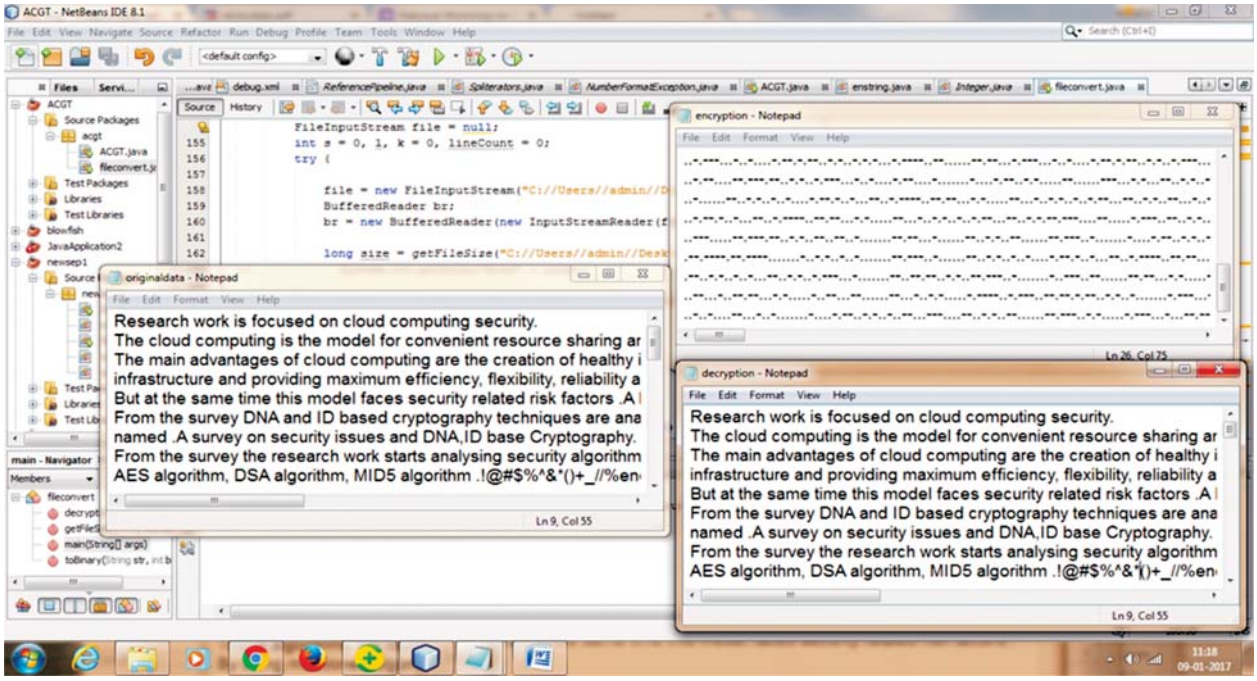

Figure 5: Implementation of Triple Encryption Algorithm

The original data was stored as a text file. The data was encrypted using DNA Based Triple encryption model. The correctness of the above algorithm is verified by using some of online tools. The tools are listed in the below table1.

Table 1
Encryption Tools

S.No	*Tool Name*	*Usage of Tool*
1.	Web Tool Hub	Base64 Encoder Decoder
2.	Seo Chat	HTML Entities Encode Decode
3.	Text Fixer	HTML Character Text Decoder
4.	www.String.Functions.com	Character Encode Decoder
5.	Code Beautify	Encrypt Decrypt String
6.	Tools 4 noobs	Decrypt Tool
7.	Intercrypto	Advance Encryption

The originaldata.txt file is used to store original data or sensitive data. The encryption.txt file is used to store encrypted data. The encrypted data is converted into original data and stored in the file decryption.txt refer Figure 5.

The originaldata.txt file is compared with the decryption.txt file using online **DiffNow tool**. By using online tool [13] the original data is compared with decrypted data and proved that there are no differences between the file. The proposed model has been implemented with 300 line of text file with different symbols.

4.1. Chosen/Known-Plain Text Attack

The chosen-plain text and know-plain text would attack the encryption algorithm .The security algorithm for sensitive data should provide high level of security. These two attacks are chosen by the attacker to hack plain or original text and observe the corresponding encrypted texts. The main goal of this attack is reducing the security of encryption algorithm and gains the sensitive data.

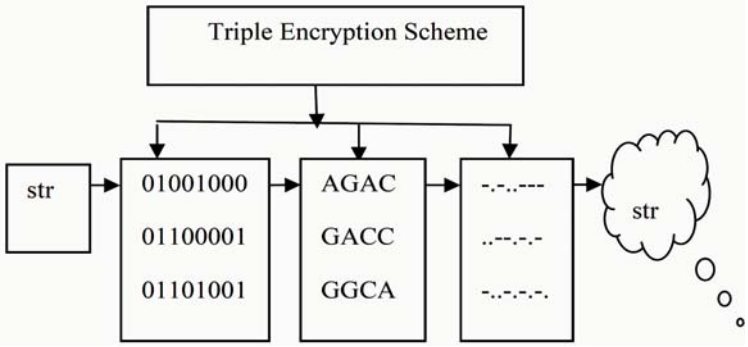

Figure 6: Failed attack on Sensitive data

From the above conversion it is clear that the tracking of original data is highly impossible by the attacker. After encryption the original data is stored in the cloud environment refer Figure 6. Because of DNA based Triple Encryption the system is tightly secured and stored safely.

4.2. Brute Force Attack

Brute force attack in cryptography is an attacking technique that tries all possible key combinations until the exact key is found. The encryption scheme is triple encryption process so finding original data is not possible. Accessing DNA code without knowing the original key will make biological pollution which would lead to a collapsed data. So without key the attacker cannot access the original data.

4.3. Differential Attack

The differential attack is a form of cryptanalysis primarily applicable to block ciphers. This attack introduces a small but unknown change to the plain text of original data. This would result in differences both in original input and encrypted output. So there will not be a meaningful relationship between original text and encrypted text.

A different sequence used in DNA sequence and Morse code will be an impossible process because the DNA based Triple encryption is difficult to identify the secret key behind the algorithm.

5. CONCLUSION

One of the major issue in cloud computing is data security. With today's advanced software technology, the security algorithms are easily breakup by the attacker. The DNA based Triple Encryption and Decryption algorithm is used in the proposed model. So it is highly impossible to hack the original data. These benefits show that this model is suitable for cloud computing security. In future, it is possible to solve more security problems using compression algorithm with DNA based Triple Encryption model.

REFERENCES

[1] Thilagavathy R, and Murugan A, "Cloud Computing: A Survey on Security Issues and DNA, ID-base Cryptography," Indian Journal of Science and Technology (INDJST), Vol. 9(28), pp.1-6, July.2016.

[2] Che Jianhua, Yamin Duan, Tao Zhang, and Jie Fan, "Study on the security models and strategies of cloud computing,"In Procedia Engineering, Vol.(23), pp.586-593,Jan.2011.

[3] A.legrand,L.marchal and h.casanova, "Scheduling distributed applications:the simgrid simulation framework,"IEEE,pp.138-145,May.2003.

[4] Prantosh Kumar Paul and Mrinal K Ghose, "Cloud computing: possibilities, challenges and opportunities with special reference to its emerging need in the academic and working area of Information Science," In Procedia Engineering, Vol. (23), pp.2222-2227, Jan.2012.

[5] Rachna Arora, and Anshu Parashar, "Maintaining Data Confidentiality and Security over Cloud: An Overview,"International Journal of Engineering Research and Applications (IJERA), Vol. (4), pp.1922-1926, July.2013.

[6] Padmaja N, and Priyanka Koduru, "Providing data security in cloud computing using public key cryptography," International Journal of Engineering Sciences Research.2013, 4.

[7] Kandukuri, Balachandra Reddy, and Atanu Rakshit, "Cloud security issues," In Services Computing, 2009. SCC'09. IEEE International Conference on IEEE, pp. 517-520, Sep. 2009.

[8] Wang Lizhe, Jie Tao, Marcel Kunze, Alvaro Canales Castellanos, David Kramer, and Wolfgang Karl, "Scientific Cloud Computing: Early Definition and Experience," In HPCC, Vol. 8, pp. 825-830. Sep.2008.

[9] Jacob, Grasha, and A. Murugan, "An Encryption Scheme with DNA Technology and JPEG Zigzag Coding for Secure Transmission of Images," arXiv preprint arXiv: 1305.1270 (2013).May 2013.

[10] Borda, Monica, and Olga Tornea, "DNA secret writing Techniques," In IEEE conferences, pp. 451-456, Jun.2010.

[11] Sadeg, Souhila, Mohamed Gougache, Nabil Mansouri, and Habiba Drias, "An encryption algorithm inspired from DNA," In Machine and Web Intelligence (ICMWI), International Conference , pp. 344-349, Oct.2010.

[12] https://en.wikipedia.org/wiki/Morse_code.

[13] https://www.diffnow.com/.