Cryptography In Cloud-Security Using DNA (Genetic) Techniques

Anup R. Nimje*
*(Student of Master Of Engineering, Computer Engineering, College Of Engineering and Technology, Amravati)

ABSTRACT

The security concerns would be still there in cloud systems. Cryptography consists of the encryption-decryption techniques. There are many schemes, algorithms those can be used for security purposes. DNA is now mostly a theoretical concept but if implemented in future would be providing most strong and secure system. In this paper it has been proposed that DNA cryptographic algorithms are adopted for the optimization of data security in cloud security. So that cloud system would be most secure.

Keywords – Cipher text, Decryption, DNA, Encryption, Key, Plaintext, Proteins, Strands.

I. INTRODUCTION

In Cloud computing security mechanisms would be a challenge. The most serious concerns are the possibility of lack of confidentiality, integrity and authentication among the cloud users and service providers. The key intent of this research paper is to represent a new techniques for security schemes and to ensure data confidentiality, integrity and authentication.

In this paper it has been proposed that DNA cryptographic algorithms are adopted for the optimization of data security in cloud computing.

DNA can be used in cryptography for storing and transmitting the information, as well as for computation. Although in its primitive stage, DNA cryptography is shown to be very effective. Theoretical analysis should be performed before its real applications, because it requires high tech lab requirements and computational limitations, as well as the labor intensive extrapolation means so far. These make the efficient use of DNA cryptography difficult in the security world now.

The concept of DNA cryptography is for very powerful and unbreakable encryption technology. That can be used in systems.

II. LITERATURE REVIEW

The research paper that helped in understanding the concepts about DNA cryptography. DNA-Based Cryptography by Ashish Gehani, Thomas LaBean, and John Reif. This paper explains the basic or fundamental approach about DNA cryptography. Using Chip Based Micro array technology.

III. CONCEPT

The chip-based micro-array technology, and can be generally expressed below [1]:

Encryption: Plaintext to cipher text conversion:

1. DNA structure has two strands. Take one or more input DNA strands it can be considered to be the plaintext message.
2. Append to them one or more randomly constructed *"secret key"* strands.
3. Resulting *"tagged plaintext"* DNA strands are *hidden* by mixing them within many other additional "distracter" DNA strands which might also be constructed by random assembly.

Decryption: Recovery of plaintext from cipher text:

1. Given knowledge of the "secret key" strands.
2. Resolution of DNA strands can be decrypted by a number of possible known recombinant DNA separation methods: Plaintext message strands may be separated out by hybridization with the complements of the "secret key" strands might be placed in solid support on magnetic beads or on a prepared surface.

This process is used in 2D image encryption. They also suggested the use of DNA computing on steganography. The method with improved security is also suggested by researchers. [2]

It is easy to see that DNA computing is just classical computing, highly parallelized and mass storage. Thus the idea of this form of DNA computing is at great risk in the field of cryptography. Also, such technology is very hard to use outside laboratories currently, both getting the DNA strands, and extracting the results.

Generally, such a scheme can be formulated as below (M and C are for plaintext and cipher text, respectively) [2]

Encryption key E1 = (the starting and pattern codes of the introns, the places of the introns)

Encryption key E2 = (the codon-amino acids mapping)

Decryption key D1 = E2

Decryption key D2 = E1

C' = E1 (M), C = E2 (C')

M' = D1(C), M = D2 (M')

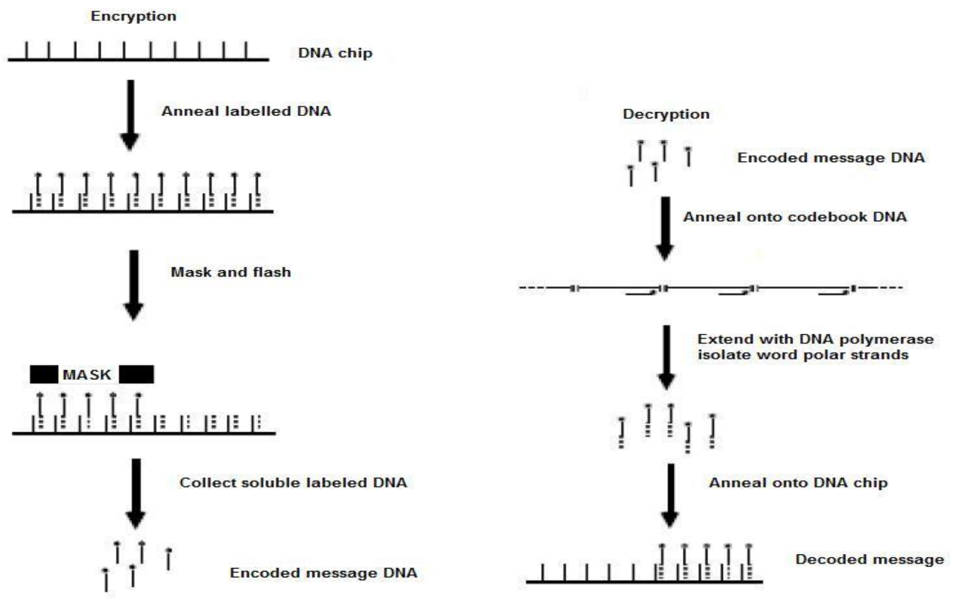

Fig. 1: The process of encryption and decryption for DNA cryptography used in cloud system.

The scheme is principally a symmetric key algorithm, except that the sender initially has only part of the keys, and he generates the rest part of the keys. It is obvious that such a scheme is essentially a 2 step substitution process, though
they are substitutions in a general sense (not letter-by-letter substitution).

The DNA cryptography method that we have proposed is not constraint to the encryption and decryption area, but also such areas like massage authentication. Indeed, the encryption process of the method can be very powerful and more effective if it is used as a hash function for generating message authentication code (MAC). By this means, only the initial key is needed, and the encryption process can be fast. If multiple rounds are used, the security may also be satisfactory.
The problem is that the length of the resulting MAC is hard to control, and one of the solutions to this problem is to do multiple round of the process, together with padding to get the MAC with fix length. If using real DNA data, the steganography can be implemented, especially for image steganography. The use of this method to do message authentication, as well as its other usages, will also be examined in the future.

IV. FUTURE VIEWS

This method based on the central dogma has its nature advantage in software and hardware applications. Since only 4 nucleotides are involved in encipher and decipher process of the plaintext, the program can be turned to be a very efficient program based on primitive codes in C or assembly language. The hardware implementation can be easy based on these simple principles, and it can also be very efficient. With today's advanced hardware technology, the multiple rounds can be easily implemented, and the security can be relatively reasonable. These benefits show that this method is very suitable for software and hardware implementation. The further analysis and experiments on these factors is very interesting topics in the future works. As this technique would be implemented for **confidentiality, integrity and authentication in cloud systems.**

ACKNOWLEDGEMENTS

Author is thankful to all of the professors and colleagues who helped directly or indirectly for working on this paper.

REFERENCES

[1] DNA-Based Cryptography by Ashish Gehani, Thomas LaBean, and John Reif.
[2] A Pseudo DNA Cryptography Method-Kang Ning