DNA Cryptography for Secure Data Storage in Cloud

Sreeja Cherillath Sukumaran[1], Misbahuddin Mohammed[2]
(Corresponding author: Sreeja Cherillath Sukumaran)
Department of Computer Science, Christ University[1]
Hosur Road, Bangalore, Karnataka 560029, India
Computer Networks and Internet Engineering Division, Centre for Development of Advanced Computing (C-DAC)[2]
Electronics City, Bangalore, Karnataka 560100, India
(Email: sreejasukumaran@gmail.com)
(Received Dec. 01, 2016; revised and accepted Mar. 11, 2017)

Abstract

Cloud computing has revolutionized the way the data is stored, processed and made available. It has evolved in various forms of utility computing by sharing resources, infrastructures and data storage facilities and got wide acceptance because of its services and storage capacities. But security issues are a major concern in the cloud which is restricting its use among organizations which deals with sensitive data such as health care, Pharmaceuticals etc. and remain one of the greatest inhibitors for the adoption of Cloud computing if the security issues continue. For data protection, various techniques evolved through years for Ciphers, Cryptography, Steganography and recently DNA based encryption for security is the trend. DNA cryptography was a breakthrough in the field of security which uses bio-molecular concepts and gives us new hope of unbreakable algorithms but the concepts need to be exploited more especially in the cloud computing. This paper discusses cloud computing features, service models, security issues and proposes a DNA based encryption algorithm for securing data in cloud environment which will be cost effective and secure by using bio-computational techniques. The suggested algorithm uses indexing and DNA steganography techniques along with binary coding rules which make algorithm secure as it is an additional layer of biosecurity than conventional cryptographic techniques.

Keywords: Cloud Computing; Confidentiality; Data Security; DNA; DNA Encryption Techniques; Integrity

1 Introduction

Cloud computing received relevant diligence and has a vital role in the growth of information technology as it provides essential infrastructure, platform and software as services [13]. Cloud storage enables to handle a large volume of data which is crucial for business and individuals and a solution for storing exploding data. Cloud computing will become an essential part for everyone as the future is of Big data. The main features of the cloud include scalability, reliability and availability but same time information security, privacy and compliance are major concerns or issues which inhibit the growth and migration to the cloud by organizations especially those who deal with sensitive data. Security is always a major concern in Open System Architectures and considering the threats and vulnerabilities in the cloud various countermeasures has been proposed till now including cryptographic techniques but still there is a need for novel and cost effective techniques to thwart the attacks and biocomputing techniques are a solution to this as it provides novel and secure techniques which enhances the security by a bio-layer which is difficult to break.

2 Literature Review

This section discusses various aspects of Cloud Computing,data security issues and challenges in the Cloud, DNA computing, DNA, DNA Cryptography and a review of literature related to these concepts.

NIST defines [11] Cloud computing is a model for enabling ubiquitous, convenient, on-demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction. The cloud model is composed of five essential characteristics which are on-demand self-service,broad network access,resource pooling,rapid elasticity and measured service, Cloud service models are also known as SPI model. They are Software as a Service (SaaS), Platform as a Service (PaaS) and Infrastructure as a Service (IaaS). Depending upon the customer requirements the Cloud ser-

vices can be deployed as Private cloud,Community cloud, Public cloud and hybrid cloud [8].

2.1 Security Issues in Cloud

Security issues in the cloud is a major concern and a barrier to its adoption by organizations. The virtualized nature of cloud storage makes the traditional mechanisms unsuitable for handling the security issues [5, 14, 18]. SaaS relieves the users from tasks like maintenance and installation of software. It has been used widely all around. Web 2.0, a key technology towards enabling SaaS and its usage is increasing drastically by user community. So, these environments really need a security.

Various security issues exist in cloud some of them are issues in the network level security, application level security but data security is a major concern in the cloud. It may be the security of data during data transfer, securing of data leaving a data- center to another data - center or the data at rest. Data security is most prominent considering the fact apart from business domains, organizations which deal with sensitive information such as health care is also using information technology for providing on time and better treatment for patients [10].

2.2 Data Storage in Cloud

Data security is a major concern in any technology but will become a critical aspect when both customer data and programs are residing at provider premises as in the case of Cloud. This becomes a major challenge in SaaS as the data is often processed in plain text and stored in the cloud and the SaaS users must rely on their providers for proper security [4, 20, 22]. In [17] reviews the data security and privacy issues in cloud computing with special emphasis on data confidentiality, Integrity, and availability. The data storage and confidentiality issues are the major barriers in cloud computing and resolving these issues by enhanced data protection and encryption techniques increases the user's trust which in turn removes the barriers of cloud adoption. Data Integrity and confidentiality are the most critical factors for users storing their confidential data in the cloud. Encryption techniques plays a major role in achieving confidentiality whereas digital signatures play a vital role to achieve data integrity.

Challenges and issues related to data storage remains a major threat for cloud adoption as the client will not have direct control of data stored in the Cloud. Cloud computing has greater security threats and vulnerable to attacks if integrity, confidentiality and privacy of the data is not ensured in the cloud environment. The authors [15] focuses on the security issues related to the confidentiality and privacy of the data stored in the cloud. The research related to data storage and security always emphasizes the need for novel techniques.

2.3 Aspects of Data Security

There are various aspects of data security that need to be taken care while migrating to a cloud environment which includes [3]

- Data-in-transit;
- Data-at-rest;
- Data Lineage;
- Data Remanence;
- Data Provenance.

Data-in-transit is also referred as data in motion and it has highest security risk in the data security aspects. The encryption technique used plays a major role along with a secure transmission protocol secures data to some extent.

Data-at-rest has security issues especially in a shared environment, so encrypting data using secure and strong encryption plays a major role. Data Lineage is critical for cloud computing as it is tracing the path of data which is very difficult in distributed environment.

Data Provenance refer to maintaining the integrity of data which is very important in cloud environment. Data Remanence refers to the data left out especially due to transfer of data or its removal. It causes minimal security but may turn critical for public cloud.

Considering the data security aspects, confidentiality and integrity are the major concerns for data residing in Cloud. For securing the data stored in the cloud the service providers use various Cryptographic techniques such as public key encryption, private key encryption and homomorphic encryption of which homomorphic technique is considered as best for data-at-rest. Security challenges in the cloud (SaaS) is similar to that of any web application technology but traditional security techniques are not enough to resist attacks and which indicates the need for innovative and secure technologies. DNA computing techniques can be exploited and applied for securing data in cloud environment as it provides bio-computational complexity and can be hybridized with conventional encryption techniques.

2.4 DNA Computing

Biocomputing is a trending concept which has application in cryptography to generate secure algorithms using the computational complexity of biomolecular concepts in addition to conventional cryptographic techniques. Biomolecular encryption techniques have given rise to a new branch of cryptography, DNA cryptography as the concepts mainly revolves around DNA and the central dogma of molecular biology. DNA, Deoxyribonucleic acid is a double-stranded helix of nucleotides with each nucleotide containing one of four bases A, G, C, T where A stands for adenine, G for guanine, C for cytosine and T for thymine respectively [2, 9].

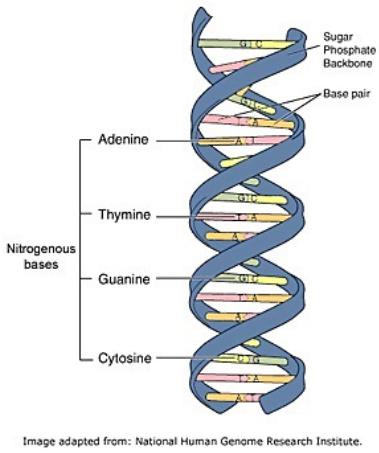

Figure 1: Helical structure of DNA

Figure 1 is the helical structure of DNA, which depicts nitrogenous bases, sugar phosphate backbone and base pair bonding [21]. Figure 2 represents the structure of DNA base pairs and the bonding between adenine and thymine, cytosine and guanine [19]. In eukaryotic genes, the coding regions referred as exons and noncoding regions are introns and the exons are interrupted by introns. Figure3 shows coding and non -coding regions in a segment of eukaryotic DNA [7].

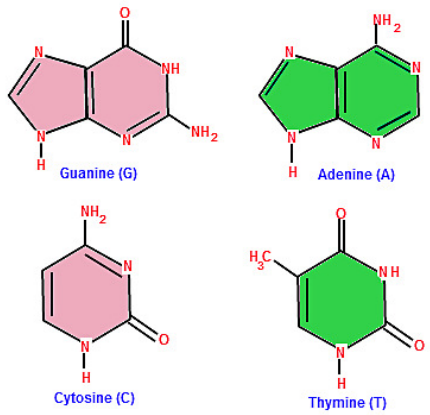

Figure 2: Structure of DNA base pairs

2.4.1 DNA Encryption Techniques for Information Security

Computational properties of DNA became a new branch of science and a research area for cryptographers from 1994 when Dr. Leonard M. Adleman used the computational properties of DNA to solve Hamiltonian path problem [1]. Research on DNA based encryption techniques can be broadly classified into three:

- DNA Cryptography;
- DNA Steganography;

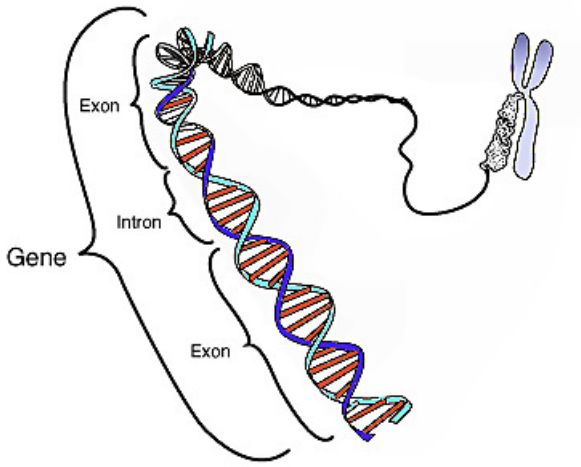

Figure 3: Structure coding region in a segment of eukaryotic DNA

- Pseudo DNA Cryptography.

DNA Cryptography is built on DNA based computations for encryption and various methodologies for both Symmetric and Asymmetric DNA cryptography has been proposed by researchers. The techniques based on biocomputations got wide acceptance due to secure nature of algorithms.

DNA Steganography became popular with a patented technology proposed by Carter Bancroft for hiding messages. The proposed technique involved concealing a DNA-encoded message within a genomic DNA sample followed by further concealment of the DNA sample to a microdot [6]. DNA Steganography is also considered as cryptographic technique even though there is no encryption.Pseudo DNA Cryptography got wide acceptance as it involves simulation by means of computations and arithmetic operations on Pseudo DNA instead of using real DNA with high-tech lab facilities.

DNA digital coding technology denotes the bases A, C, T, G as 00, 01,10,11 and the binary values can be interchanged with bases and this coding forms the basis of algorithms using Digital DNA [16]. DNA computing can be performed in two ways one by the means of biological operations using real DNA and the other technique involves simulation using Digital DNA and Pseudo DNA.

2.5 DNA and Cloud Computing

DNA has an excellent storage capacity of 10^6 TB in 1gm of DNA, which indicates a few grams of DNA may have the capacity to store whole data available in the world [12]. Cloud computing techniques also provide data storage so instead of using DNA for data storage exploiting DNA based encryption for data stored in the cloud will be a combination of trending techniques which ensures data security, Confidentiality, integrity and authentication are considered as most important aspects of in-

formation security whereas context is also an important aspect depending on it, the level required for data security will be different. Cryptographic techniques have a major role in securing data and depending on the context different encryption techniques can be used. The encryption techniques are broadly classified as symmetric key cryptography and asymmetric key cryptography depending on the context it can be used in conjunction with DNA computing.

3 Proposed Methodology

In this section, a methodology is proposed for securing data for cloud storage using DNA based encryption technique. In this method, DNA based coding, encryption technique, DNA Steganography and indexing method are proposed for securing data in the cloud.

The Proposed DNA Cryptography technique is different from that of the DNA cryptography which uses real DNA Sequences or Oligos, as the computations performed are using the digital DNA. A DNA sequence consists of four nucleic acid bases A (adenine), C (cytosine), G (guanine), T (thymine), where A and T are complementary, and G and C are complementary. Table 1 represents one of the gray coding method used for DNA bases.

Table 1: Binary coding based on DNA

Bases	Gray Coding
A	00
G	01
C	10
T	11

Figure4 represents architecture of the proposed DNA based encryption. Figure 5 represents the sequence diagram of the proposed system, where user encrypts the data and stores encrypted data into cloud. Decryption of the data is done after retrieving it from the cloud, which ensures confidentiality of the data as the encryption and decryption is performed at the client side. Figure6 represents architecture of proposed DNA based decryption

Algorithm 1 Data encryption algorithm

1: Begin
2: Input: *Data to be stored D,Random DNA R-DNA.*
3: Select the data D, which has to be stored securely in the cloud, Convert the data into binary, say BD'.
4: Convert the binary data into DNA sequence based on the DNA coding rule as per Table1,which generates a digital DNA→ D'DNA.
5: Create a random DNA strand by selecting DNA sequences from the digital databases→ R-DNA.
6: Select the R-DNA and index it. Select the coding and non- coding regions randomly or based on the index values.
7: Convert indexed R-DNA into short fragments based on the length of D'DNA base pair, and a key value based on D'DNA.
8: Remove the non-coding region and the generated DNA sequence is used as a cover for adding D'DNA.
9: Insert the D'DNA into non-coding regions of the generated R-DNA based on the index positions or random position depending on the indexing rule selected.
10: The resultant DNA sequence generated by DNA Steganography is converted into binary form using the selected binary rule.
11: Upload the encrypted data in the binary form and store it in the cloud.
12: Output: *Encrypted Data*
13: End

Algorithm 2 Data decryption algorithm

1: Begin
2: Input: *Encrypted Data.*
3: Extract the encrypted data from the cloud which is in binary form.
4: Apply the selected DNA binary coding rule to the data and get the data in the form of DNA sequence which is a combination of R-DNA and D'DNA.
5: Based on the index value position,select the coding and non-coding regions of the DNA.
6: Retrieve DNA fragments from the non-coding region.
7: Extract and separate D'DNA and R-DNA from the DNA Sequence.
8: Append the fragments of D'DNA and apply DNA coding rule to get the binary data.
9: Convert the binary to ASCII.
10: Convert ASCII to text.
11: Generates the original data.
12: Output: *Original Data and Random DNA*
13: End

4 Proof of Concept

Step 1. Let us consider the data to be stored in the cloud by the user is → MyConfidential Data.

Step 2. Convert the data to be stored into the Binary form.

MyConfidentialData → 01001101 01111001 01000011 01101111 01101110 01100110 01101001 01100100 01100101 01101110 01110100 01101001 01100001 01101100 01000100 01100001 01110100 01100001 → (1).

Step 3. Apply DNA binary Coding as per Table1 to binary data of Table2 or on (1) generates (2) in DNA form.A,G,C and T values can be altered and used as per user convenience depending on the selected

Table 2: Binary conversion of the data

Data to be stored in the Cloud	ASCII Value	Binary Value
My	77 121	01001101 01111001
Confidential	67 111 110 102 105 100 101 110 116 105 97 108	01000011 01101111 01101110 01100110 01101001 01100100 01100101 01101110 01110100 01101001 01100001 01101100
Data	68 97 116 97	01000100 01100001 01110100 01100001

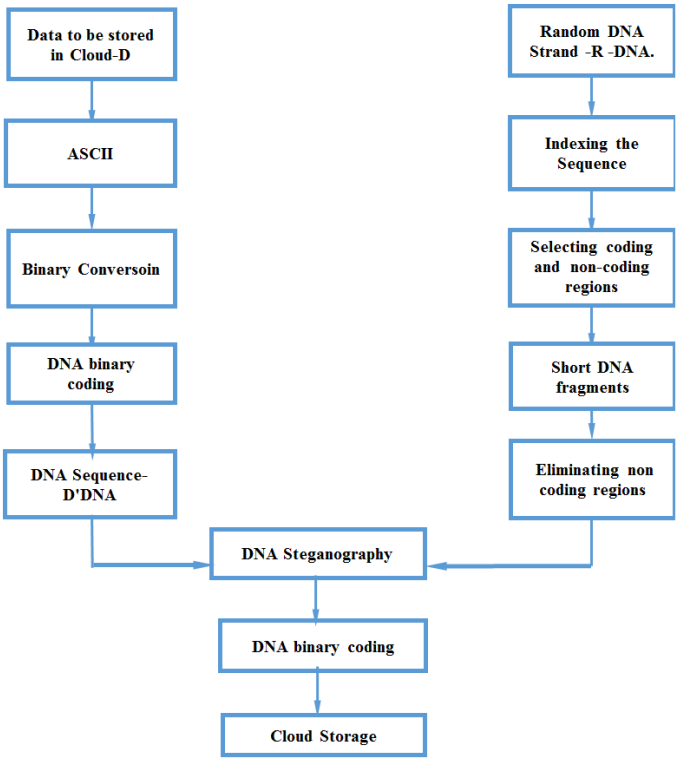

Figure 4: DNA encryption architecture

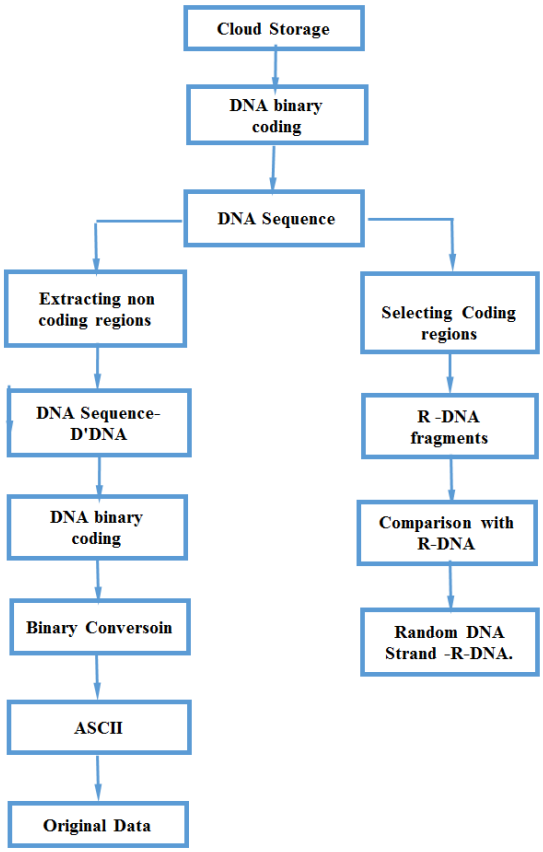

Figure 6: DNA decryption architecture

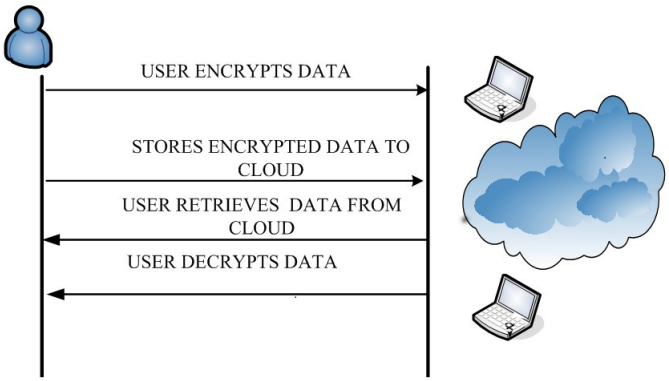

Figure 5: Sequence diagram of the proposed system

binary coding for the bases.

Table 3: Binary coding used in the proof

Bases	Gray Coding
A	00
G	01
C	10
T	11

GATG GTCG GAAT GCTT GCTC GCGC GCCG
GCGA GCGG GCTC GTGA GCCG GCAG GCTA

GAGA GCAG GTGA GCAG (D'DNA) → (2)

Step 4. Select Random DNA→ R-DNA. The random DNA is generated by downloading the sequence available from NCBI. The sequence used in this study is Reference Sequence,NC_006583.3 Canis lupus familiar is breed boxer chromosome 1, CanFam3.1, whole genome shotgun sequence is downloaded and a fragment of the sequence has been selected as R-DNA.A Sample of 32 bases is selected and indexed. Sample R-DNA selected is: ACTGCTGAGAGTTGAGCTCACCCTC AGTCCCTCACAGTTCCACACTGCCT

Step 5. Indexing the R-DNA.

$$A_1C_2T_3G_4C_5T_6G_7A_8G_9A_{10}G_{11}T_{12}$$

$$T_{13}G_{14}A_{15}G_{16}C_{17}T_{18}C_{19}A_{20}C_{21}C_{22}C_{23}$$

$$T_{24}C_{25}A_{26}G_{27}T_{28}C_{29}C_{30}C_{31}T_{32}$$

Step 6. Select the coding and non-coding regions randomly or based on the index positions.

Step 7. This sample is demonstrated using a random selection of coding and non-coding regions. Depending on the security of the data, complexity of the algorithm can be increased by defining index rules.

Step 8. Insert the D'DNA into non-coding regions of R-DNA. In this sample based on index values the coding and non-coding regions defined are:

$$A_1C_2T_3G_4C_5$$

→ Coding region

$$T_6G_7A_8G_9A_{10}G_{11}T_{12}T_{13}G_{14}A_{15}$$
$$G_{16}C_{17}T_{18}C_{19}A_{20}C_{21}C_{22}C_{23}$$

→ Non-Coding region

$$T_{24}C_{25}A_{26}G_{27}T_{28}C_{29}C_{30}C_{31}T_{32}$$

→ Coding region from the R-DNA

Step 9. Insert D'DNA into respective non-coding index positions.Random DNA selected act as cover medium to insert D'DNA and performs DNA steganography.

GATG GTCG GAAT GCTT GCTC GCGC GCCG GCGA GCGG GCTC GTGA GCCG GCAG GCTA GAGA GCAG GTGA GCAG → D'DNA Replacing Non-Coding region bases with 4bases (key value) of D'DNA per each base of non-coding region:

$$T_6G_7A_8G_9A_{10}G_{11}T_{12}T_{13}G_{14}A_{15}$$

$G_{16}C_{17}T_{18}C_{19}A_{20}C_{21}C_{22}C_{23}$ → Cover DNA(non-coding region)

$(GATG)_6(GTCG)_7(GAAT)_8(GCTT)_9(GCTC)_{10}$ $(GCGC)_{11}(GCCG)_{12}(GCGA)_{13}(GCAG)_{18}(GCTA)_{19}$ $(GAGA)_{20}(GCAG)_{21}(GTGA)_{22}(GCAG)_{23}$ → DNA Steganography.

Key value can be increased depending on the required security and length of the original data.

Step 10. Generate the DNA Sequence.

$A_1C_2T_3G_4C_5(GATG)_6(GTCG)_7(GAAT)_8(GCTT)_9$ $(GCTC)_{10}(GCGC)_{11}(GCCG)_{12}(GCGA)_{13}(GCGG)_{14}$ $(GCTC)_{15}(GTGA)_{16}(GCCG)_{17}(GCAG)_{18}(GCTA)_{19}$ $(GAGA)_{20}(GCAG)_{21}(GTGA)_{22}(GCAG)_{23}T_{24}C_{25}A_{26}$ $G_{27}T_{28}C_{29}C_{30}C_{31}T_{32}$ → In indexed form.

ACTGCGATGGTCGGAATGCTTGCTCGCGCG CCGGCGAGCGGGCTCGTGAGCCGGCAGGCT AGAGAGCAGGTGAGCAGTCAGTCCCTCACA GTTCCACACTGCCT → Stego DNA

Step 11. Convert the DNA Sequence into DNA based binary coding depending on the coding rule selected.

ACTGCGATGGTCGGAATGCTTGCTCGCGCG CCGGCGAGCGGGCTCGTGAGCCGGCAGGCT AGAGAGCAGGTGAGCAGTCAGTCCCTCACA GTTCCACACTGCCT → Encrypted Data in DNA form.

00101101100100110101111001010000110110111101 10111001100110011010010110010001100101011011 10011101000110100101100001011011000100010001 10000101110100011000011110000111101010111000 10000111111010001000101101101011 → Encrypted Data in binary form

Step 12. Store the data into cloud in the binary form or in integer form by converting the binary data to integers depending on the convenience of user.

5 Security Analysis

Security analysis of the proposed system is done for integrity and confidentiality which are considered as major threats for data stored in the Cloud environment.

5.1 Confidentiality of the Data

In the proposed algorithm to retrieve the encrypted data user must have the knowledge of selected random sequence, non-coding and coding regions, index value, binary coding rule used for the D'DNA, key value and DNA Sequence coding which increase the complexity of the algorithm.The knowledge of all these parameters are essential for recovering or decrypting the original data which ensures the data confidentiality.

Probability of finding the random DNA sequence $=(\frac{1}{163}) \times 10^8 \times \frac{selectingthefragmentbasesofR-DNA}{Totalnumberofbasesinselected Genome}$

The random sequence is selected from NCBI which has millions of seq, in the same way millions of sequences are available in other data bases that can be exploited

for creating R-DNA which also ensures security as it is difficult to find the sequence selected for the encryption.

$$\begin{aligned} & Complexity \\ = \; & (R-DNA) \times (BinarycodingRule) \times (index) \\ & \times (keyvalue(n)) \times (knowledgeofintrons(K_i)) \\ & \times (knowledgeofexons(K_e)) \\ = \; & (\frac{1}{163}) \times 10^8 \\ & \times \frac{selectingthefragmentbasesofR-DNA}{TotalnumberofbasesinselectedGenome} \\ & \times \frac{1}{24} \times (I_i^n) \times (n) \times (K_i) \times (K_e). \end{aligned}$$

The output of the proposed encryption algorithm can be saved even in the public cloud without any issues as it is difficult to break the system considering the computational complexity and the knowledge factors required.

5.2 Data Integrity Check Using SHA-2

The proposed system can be used as client-side encryption. To ensure the integrity of the data the user can generate a hash of the encrypted data and store it in a local repository. After retrieving data from the cloud each time user can compute the hash of data and can be compared with the hash value value stored in the local hash repository to ensure data integrity.

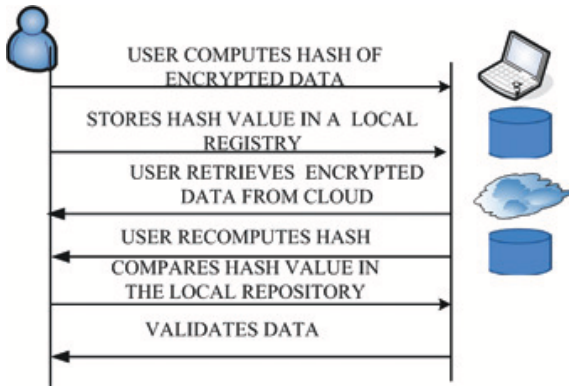

Figure 7: Sequence diagram for data integrity check

The proposed technique is feasible and easy to use and ensures the data integrity using hashing technique. Figure 7 is depicting the sequence diagram of the proposed system for data integrity check. SHA-256 is the suggested one as it is collision resistant. The hash value computed for the encrypted data using proposed methodology is df1140d3a68f05e6bccb16df7fa10f1b404d487994f5d441a9d8621549e0c685.

6 Conclusions and Future Work

Cloud computing is not widely accepted or restricted in few domains because of the security issues related to data storage. In this paper, a DNA based encryption technique is proposed for storing data securely in the cloud especially in the public cloud where data storage is a major concern and for SaaS users where security is a major concern. The technique will provide enhanced security as it adds the computational complexity by using biocomputing techniques in addition to Cryptography and user can check the integrity of the data without relying on the third party.

The proposed DNA Cryptography is a novel encryption technique for secure storage of data in the cloud environment, the method is still primitive, but using DNA cryptography for cloud has great Scope considering the importance of cloud storage in the Industries and day to day life. Everywhere data is bombarding in the form of images, videos and other digital forms. So, a platform for storage is very essential and DNA encryption is a trending concept which is going to dominate the security world in the future.

Table 4: Hash value generated for data integrity check

Encrypted Data	SHA-2
0010110110010	df1140d3a
011010111100	68f05e6bcc
1010000110110	b16df7fa1
11110110111001	0f1b404d48
10011001101001	49e0c6850
01100100011001	
01011011100111	
010001101001011	
000010110110001	
000100011000010	
111010001100001	
1110000111101010	
111000100001111	
110100010001011	
01101011	

References

[1] L. M. Adleman, "Molecular computation of solutions to combinatorial problems," *Nature*, vol. 369, pp. 40, 1994.

[2] E. S. Babu, C. N. Raju, and M. H. K. Prasad, "Inspired pseudo biotic DNA based cryptographic mechanism against adaptive cryptographic attacks," *International Journal of Network Security*, vol. 18, no. 2, pp. 291-303, 2016.

[3] R. Bhadauria and S. Sanyal, "Survey on security issues in cloud computing and associated mitigation techniques," *arXiv preprint arXiv:1204.0764*, 2012.

[4] K. Brindha and N. Jeyanthi, "Securing portable document format file using extended visual cryptography to protect cloud data storage," *International*

Journal of Network Security, vol. 19, no. 5, pp. 684-693, 2017.

[5] Z. Cao, C. Mao, L. Liu, "Analysis of one secure anti-collusion data sharing scheme for dynamic groups in the cloud," *International Journal of Electronics and Information Engineering*, vol. 5, no. 2, pp. 68–72, 2016.

[6] C. T. Clelland, V. Risca, and C. Bancroft, "Hiding messages in dna microdots," *Nature*, vol. 399, no. 6736, pp. 533–534, 1999.

[7] Cold Spring Harbor Laboratory, *Exons and Introns*, Oct. 23, 2016. (http https://www.dnalc.org/view/15549-transcrition-translation-exons-and-introns.html)

[8] M. Hogan, F. Liu, A. Sokol, and J. Tong, "NIST cloud computing standards roadmap," *NIST Special Publication*, vol. 35, 2011.

[9] X. Li, C. Zhou, N. Xu, "A secure and efficient image encryption algorithm based on DNA coding and spatiotemporal chaos," *International Journal of Network Security*, vol. 20, no. 1, pp. 110-120, 2018.

[10] L. Liu, W. Kong, Z. Cao, J. Wang, "Analysis of one certificateless encryption for secure data sharing in public clouds," *International Journal of Electronics and Information Engineering*, vol. 6, no. 2, pp. 110-115, 2017.

[11] P. Mell, T. Grance *et al.*, "The NIST definition of cloud computing," 2011.

[12] 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*, pp. 595–601, 2015.

[13] A. Mosa, H. M. El-Bakry, S. M. Abd El-Razek, S. Q. Hasan, "A proposed E-government framework based on cloud service architecture," *International Journal of Electronics and Information Engineering*, vol. 5, no. 2, pp. 93–104, 2016.

[14] D. Patel, "Accountability in cloud computing by means of chain of trust dipen contractor," *International Journal of Network Security*, vol. 19, no. 2, pp. 251-259, 2017.

[15] B. T. Rao and N. vurukonda, "A study on data storage security issues in cloud computing," *Procedia Computer Science*, vol. 92, pp. 128–135, 2016.

[16] C. Sreeja, M. Misbahuddin, and N. Mohammed Hashim, "Dna for information security: A survey on dna computing and a pseudo dna method based on central dogma of molecular biology," in *International Conference on Computer and Communications Technologies (ICCCT'14)*, pp. 1–6, 2014.

[17] Y. Sun, J. Zhang, Y. Xiong, and G. Zhu, "Data security and privacy in cloud computing," *International Journal of Distributed Sensor Networks*, 2014.

[18] W. L. Tai, Y. F. Chang, "Comments on a secure authentication scheme for IoT and cloud servers," *International Journal of Network Security*, vol. 19, no. 4, pp. 648-651, 2017.

[19] Tutorvista, *Deoxyribonucleic Acid*, Nov. 23, 2016. (http://chemistry.tutorvista.com/biochemistry/deoxyribonucleic-acid.html)

[20] N. Vaanchig, H. Xiong, W. Chen, Z. Qin, "Achieving collaborative cloud data storage by key-escrow-free multi-authority CP-ABE scheme with dual-revocation," *International Journal of Network Security*, vol. 20, no. 1, pp. 95-109, 2018.

[21] Virtual Genetics Education Centre, *DNA, Genes and Chromosomes*, Nov. 22, 2016. (http://www2.le.ac.uk/departments/genetics/vgec/highereducation/topics/dnageneschromosomes)

[22] Z. Wang, Y. Lu, G. Sun, "A policy-based de-duplication mechanism for securing cloud storage," *International Journal of Electronics and Information Engineering*, vol. 2, no. 2, pp. 70–79, 2015.

Biography

Sreeja C.S. did her B.Sc. (Industrial Chemistry) from University of Calicut -Kerala, MCA from Bharathiar University-Tamilnadu and M.Phil in computer science from Christ University-Bangalore. She is currently pursuing her PhD in Christ University-Bangalore under the guidance of Dr. Mohammed Misbahuddin. Her area of interests in research includes Information Security, Biocomputing, DNA Cryptography, Steganography, Authentication Public Key Cryptography and Cloud Security.

Dr. Mohammed Misbahuddin did his B. Tech (CSE) from Gulbarga University, M. Tech (S/w Engg.) from JNTU-Anantapur and PhD (CSE) in Network Security from JNTU Hyderabad. He is currently working as Principal Technical Officer (Scientist D) in Centre for Development of Advanced Computing (C-DAC), E-City, Bangalore, where he is a key member of projects in the areas of PKI and e-Authentication. He is the Co-Investigator of a National Project named e-Pramaan A National e-Authentication Service along with Aadhaar. He has 15 years of experience in Research, Training and Project Management. He has applied 3 patents with IPO in the area of Secure and Usable Authentication. He has been in various Programme committees of IEEE /ACM conferences and is a reviewer for two International Journals. His area of interest is Network Security and Cryptography especially Secure and Usable Authentication, Public Key Cryptography, Risk based Engines, Cloud Security and DNA Cryptography.