A secure cryptographic cloud communication using DNA cryptographic technique

Shruti Goyal[#1], Sourabh Jain[*2]

[#]CSE Department, IES-IPS Academy
M.P, India

[1]sweetshruti2011@gmail.com

Abstract— ***The main aim of the proposed work is to design a secure cloud storage and data distribution platform for the open cloud (public cloud). This platform offers the secure communication among client and server during the data transmission from the client device. In addition of that it also provides the secure technique to share and transfer the file from one user to another. Therefore to secure the entire communication and storage of cloud server a cryptographic cloud is proposed for implementation and design. To provide security using the cryptographic technique a number of traditional and modern cryptographic techniques are studied. In most of the cryptographic techniques either the time and space complexity is much higher or they are much frequently used and utilized from the classical security point of view. Thus in this presented work the DNA based cryptographic algorithm for security is used. The DNA based cryptographic technique is basically developed using the substitution and other basic operator's implementation. Thus this technique is less computational cost effective and efficient. On the other hand the only four symbols are used for transforming entire massage to the cipher. Due to this security is also enhanced in terms of their recovery process. The proposed SaaS (software as a service) demonstrate the security using the upload, download and sharing of files using the proposed platform. The implementation of the proposed security platform for data exchange and sharing is provided using the JAVA technology. Additionally for the deployment the OpenShift cloud (public cloud) is used. The experimental performance in terms of time and space complexity demonstrates the effective and low resource consuming technique for the cloud data security.***

Keywords—***security, cloud computing, cryptography, DNA computing, communication security***

I. INTRODUCTION

Cloud computing is new generation technology; a number of applications are developed now in these days using the cloud platform. Among them social media, banking solutions, ecommerce solutions are played more important role in this era. All of these applications are developed in order to serve continuously without any complexity. Therefore these applications are hosted with the cloud platforms. The main reason behind this, the cloud offers scalable storage and computing solutions. But such kind of applications is requiring some sensitive and private information. Additionally leakage of information and data can make trouble for the organization and also for the end user.

In this context the security is an essential concern in the cloud computing and storage. The proposed work is dedicated to study about the security and privacy issues of the cloud during the data exchange amount client and server. In order to provide security most of the cloud service provides utilizes different security techniques for securing information during data exchange. Among them the cryptographic techniques are widely accepted technique. The main reason for utilizing the cryptographic technique for security is their simplicity and low cost implementation. In this presented work a new cryptographic technique is used namely DNA cryptography for light weight and efficient communication. Additionally the technique is providing enhanced security for file transmission and data security. Thus the existing DNA cryptographic technique is incorporated with the cloud data exchange.

The main aim of the proposed research work is to find a lightweight and efficient solution for securing the communication channel during the data exchange between client and cloud server. Thus the following intermediate objectives are established to achieve.

1. Study of different kinds of cryptographic communication solution: in this phase the different cryptographic solutions are studied and the most efficient and secure technique is obtained for implementing with the cloud data communication. The concluded technique is a DNA based cryptographic technique.
2. Design of a new secure communication technique for cloud platform: in this phase the concluded technique of security is implemented with the SaaS for providing the secure data exchange among different clients and server.
3. Performance assessment for the implemented technique: in this phase the proposed solution is evaluated for finding their performance with the cloud data exchange. Therefore the time and space complexity of the proposed system is computed.

II. PROPOSED WORK

This section provides the understanding about the proposed work involved for securing the cloud based data exchange between more than one parties. Thus the proposed model and the required security algorithm are described in this chapter.

A. System overview

Cloud computing is an answer of new generation computational and storage requirements. Now in these days every application are designed in such manner by which more and more traffic is collected using the applications. In addition of that the reliable and long term services are also deployed using the SaaS (software as a service) concepts. The key reason behind development of SaaS, these applications are never compromises with the performance of applications additionally the cloud platform provides a secure and scalable storage solutions for the applications. Among them the ecommerce, social sites and the banking applications are frequently utilized SaaS platforms. In this applications sometimes private and confidential information are also communicated, such as credit card information, banking credentials or the organizational emails. Leakage on such kind of data can affect the end client. Thus in this presented work the cloud security and channel security is the main to improve.

Therefore various security techniques are studied and found that the cryptographic techniques are providing the security for the communicated data. Thus a new cryptographic technique is required to obtain, so DNA based cryptography is obtained from the modern cryptography stream. The technique is a substitution based technique that transforms the entire text message into the AGTC encoding. This algorithm promises to provide enhance security with less amount of resource consumption. Therefore in order to improve the communication security the DNA cryptographic algorithm is implemented with the cloud service. In this section the basics of the proposed security model for cloud based data storage and secure communication technique is described. In next section the DNA based technique for securing the data during communication is reported.

B. DNA cryptographic algorithm

The selected secure DNA based cryptographic technique works in two major phases both the modules of the encryption is described as.

Round Key Selection

In this phase a key of size 256-bit is selected randomly, this selected key is transform into an 8X8 matrix.

Let, K be the key, K = ' 1111 1111 0101 1010 0001 1001 0000 1000 0101 0001 1010 0001 0000 1010 0011 1100 0101 1010 1100 0011 1010 1111 0001 0000 1111 1110 1111 0001 1010 0101 1100 0011 0000 1010 0001 1111 0001 1010 1011 1001 1010 0101 1000 0101 0000 1000 0001 1100 0001 0011 1111 0011 1010 1010 0000 1111 0000 1111 0101 1000 0001 1010 0001 1000

Transformation of key values into matrix row wise (in tabular form):

1111	1111	0101	1010	0001	1001	0000	1000
0101	0001	1010	0001	0000	1010	0011	1100
0101	1010	1100	0011	1010	1111	0001	0000
1111	1110	1111	0001	1010	0101	1100	0011
0000	1010	0001	1111	0001	1010	1011	1001
1010	0101	1000	0101	0000	1000	0001	1100
0001	0011	1111	0011	1010	1010	0000	1111
0000	1111	0101	1000	0001	1010	0001	1000

Read the key values two columns at a time, that generates four sub-keys. Label the sub-keys with DNA bases A, T, C, and G as follows:

A = '1111 0101 0101 1111 0000 1010 0001 0000 1111 0001 1010 1110 1010 0101 0011 1111'

T = '0101 1010 1100 1111 0001 1000 1111 0101 1010 0001 0011 0001 1111 0101 0011 1000'

C = ' 0001 0000 1010 1010 0001 0000 1010 0001 1001 1010 1111 0101 1010 1000 1010 1010 '

G = '0000 0011 0001 1100 1011 0001 0000 0001 1000 1100 0000 0011 1001 1100 1111 1000'

Let, randomly selected DNA sequence with DNA bases be 'T G C A' then,

Round 1 key: K1= T

Round 2 key: K2= G

Round 3 key: K3= C

Round 4 key: K4= A

Message Encryption

Every 256-bit plaintext block will go through the four round of encryption process. After each round coded blocks will go through a straight D-Box. The D-Box has four input and output terminals. The inputs terminals are labeled with DNA bases (A, T, C, and G). The D-Box will works on the randomly selected DNA sequence of length four. The encryption algorithm is given below:

Step 1: First read the byte values from the input file known as plaintext and transform every byte value into the 8-bit binary representation form.

Step 2: Make 256-bit of plaintext blocks from the binary representation.

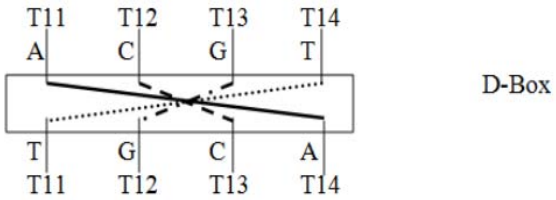
Step 3: Repeat the step 4 and 5 for each block of plaintext.

Step 4: Divide the 256-bit block of plaintext into four 64-bit blocks, which name as P1, P2, P3, P4.

Round 1: Temporary variables: T11, T12, T13, T14

Compute: T14= P4 ⊕ K1, T13= P3 ⊕ T14, T12= P2 ⊕ T13, T11= P1 ⊕ T12

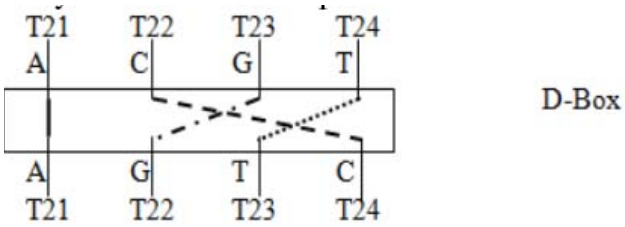
Let, randomly selected DNA sequence be 'T G C A'



Round 2: Temporary variables T21, T22, T23, T24

Compute: T21=T11⊕K2, T22=T12⊕T21, T23=T13⊕T22, T24= T14⊕T23

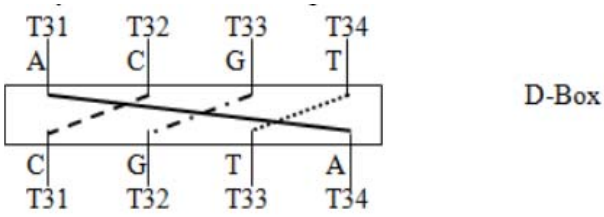
Let, randomly selected DNA sequence be 'A G T C'



Round 3: Temporary variables T31, T32, T33, T34

Compute: T34=T24⊕K3, T33=T23⊕T34, T32=T22⊕T33, T31= T21 ⊕T32

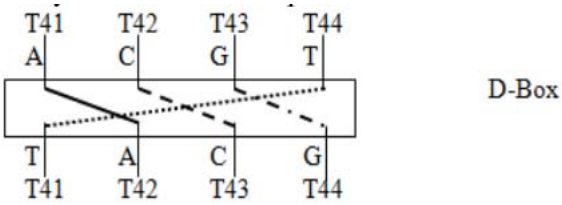
Let, randomly selected DNA sequence be 'C G T A'



Round 4: Temporary variables T41, T42, T43, T44

Compute: T41=T31⊕K4, T42=T32⊕T41, T43=T33⊕T42, T44=T34⊕T43

Let, randomly selected DNA sequence be T A C G



Step 5: Combine all 64-bit cipher blocks to form 256-bit cipher text block.

Step 6: Club together all the 256-bit cipher text blocks.

After that a fixed number of bits are to be added both the end of the coded message and two specific positions within the coded message. After embedding extra coding the final form of the cipher text is mapped to a modified DNA sequence. In order to form modified DNA coding, 16 characters are randomly selected for making the modified DNA coding and transform all the 16 characters into 4X4 matrix form as follows:

	00	01	10	11
00	E	L	G	F
01	R	N	P	A
10	T	Q	C	M
11	D	S	B	H

Taking final form of ciphered as, F n l C T = '1000 1101 0011 0110' to make the final coded form, Take 4-bit at a time, first 2-bit for selecting column while last two for row. Thus '100' is mapped to 'G Therefore, after mapping all the bits, final form becomes, F n l C T = ' G A D Q '

C. Methodology

The proposed methodology of the system design and implementation is discussed using the figure 2.1. In this diagram the entire required components are described.

The proposed security technique is demonstrated with the help of secure file exchange and sharing services through the open cloud (public cloud). Therefore a SaaS (software as a service) is developed and deployed. The system consist of two key roles first the server where the storage is provided for hosting of the user documents. Additionally the clients who are want to connect with the file host and utilize the service to storage their documents on server or distribute them to other users. Between both the systems namely client and server the cryptographic scenario is working that encrypt and decrypt the data during the communication scenarios. In order to support the proposed SaaS three key services are developed and deployed namely upload, download and sharing. During the file upload the user first select the required file to the system (local device or computer) and invoke the cryptographic service. The DNA encryption technique first encrypts the data and process the file. In the next step the encrypted file is uploaded to the server. On the other hand the download is used to localize the server document in the local computer or client device. Therefore during the request of file download, first the list of data is populated and then for the data, request is placed on server. Finally the encrypted data is transmitted from the server to words the client device and client device invoke the DNA decryption service to recover the original file using the encrypted data. In the next phase the sharing of data is also demonstrated using the system. Thus a user who want to share data with other user, select the target user from a list of cloud users and also select the file which is required to

share with a user. The encrypted file is transmitted to the user, and similar operation is performed as during the file download.

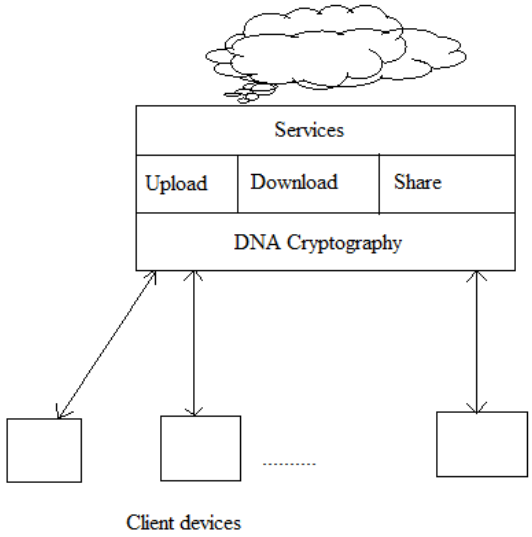


Figure 3.1 proposed system

III. RESULTS ANALYSIS

This chapter provides the understanding about the evaluated performance parameters and the efficiency of the proposed system. Therefore the time and space complexity is computed and reported.

A. Encryption time

The computational algorithms need an amount of time for producing the outcomes. This time requirement is termed as the encryption time for encryption algorithm or the time complexity of encryption. That is computed using the following formula.

$$time\ consumption = end\ time - start\ time$$

S. No.	File size in KB	Time in MS
1	10	27.42
2	50	52.61
3	100	76.92
4	300	102.39
5	500	139.38
6	700	150.23
7	1000	183.28

Table 5.1 encryption time

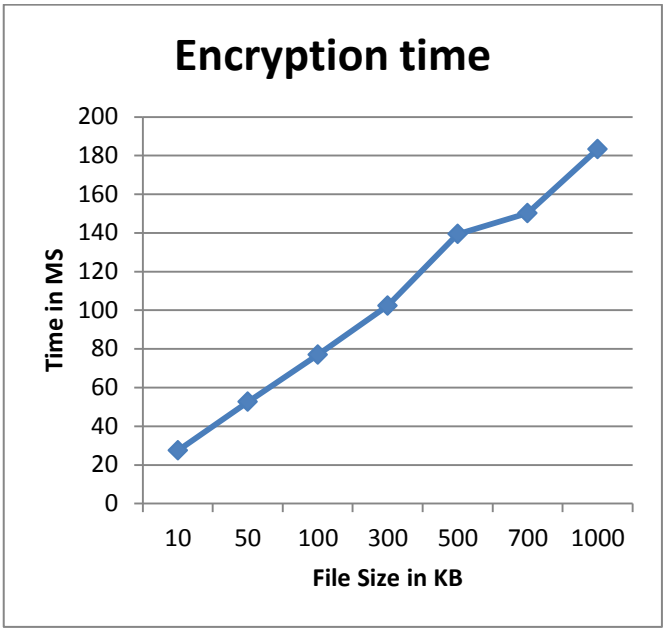


Figure 5.1 encryption time

The time complexity of the proposed DNA based secure technique is given using figure 5.1 and table 5.1. In this diagram the X axis represent the amount of file size (in terms of KB) produced for experimentation and the Y axis shows the amount of time consumed for processing the file data for encryption. According to the obtained results the performance of the system is depends on the amount of data encryption. As the amount of file size is increases the amount of time for encryption is also increases in similar ratio.

B. Decryption time

The decryption time of the system shows the time consumed to recover the original data using the input cipher text. The amount of time consumed is also termed as the time complexity of decryption algorithm. The time consumed for decryption can be computed using the following formula.

$$time\ consumed = end\ time - start\ time$$

S. No.	File size in KB	Time in MS
1	10	22.73
2	50	48.29
3	100	72.49
4	300	98.34
5	500	134.29
6	700	148.32
7	1000	179.38

Table 5.2 decryption time

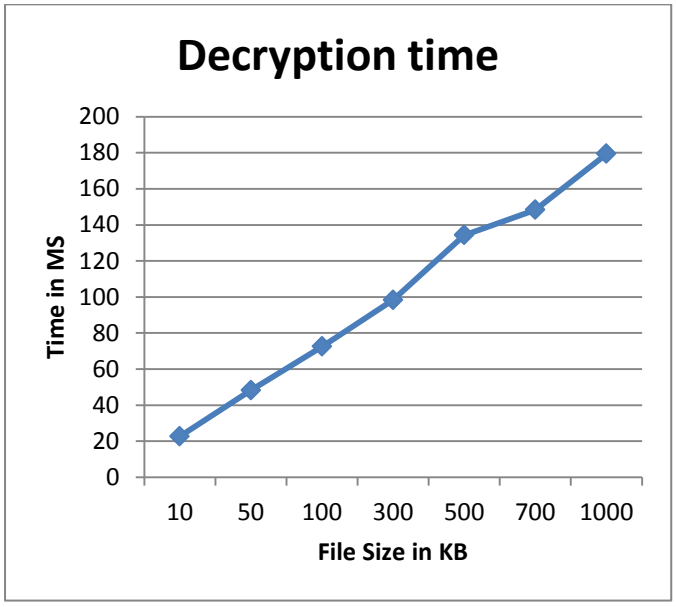


Figure 5.2 decryption time

The amount of time required for decryption of data is given using the figure 5.2 and table 5.2. According to the diagram X axis shows the file size in terms of KB (kilobytes) used for experimentations and Y axis represents the amount of time consumed for decryption of encrypted files in terms of MS (milliseconds). According to the obtained performance the proposed technique consumes less time for decryption as compared to the encryption algorithm. Thus the proposed model is adoptable and efficient for secure communication.

C. Encryption Memory

The algorithms need a significant amount of main memory to store the data for processing. This storage requirement is termed as the memory consumption or the space complexity of the system. Here the encryption based memory consumption is computed. To compute the memory consumption the following formula is used.

$$memory\ consumed = total\ memory - free\ memory$$

S. No.	File size in KB	Memory in KB
1	10	26847
2	50	27372
3	100	27746
4	300	28918
5	500	30917
6	700	32881
7	1000	33275

Table 5.3 encryption memory

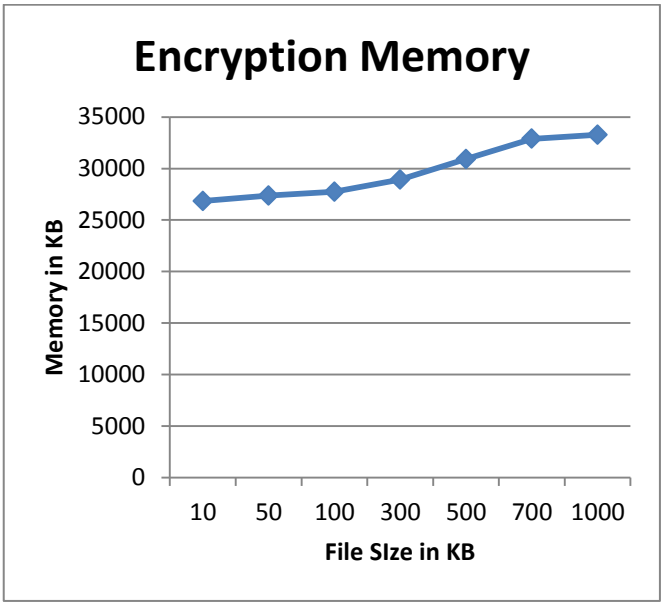


Figure 5.3 encryption memory

The memory consumption of the proposed cloud based secured communication is demonstrated using the figure 5.3 and table 5.3. In this diagram the X axis shows the amount of file size used for experimentation and Y axis shows the memory consumption of the implemented system in terms of KB (kilobytes). According to the obtained results the performance of system is depends on the amount of file for process. Thus as the file size increases the required memory is also increases. According to the system performance the proposed technique is adoptable due to less amount of memory consumption.

D. Decryption memory

The amount of main memory storage is required during the recovery of original data from the input cipher is termed here as the decryption memory consumption. The amount of main memory requirement is computed using the following formula for JAVA based technique.

$$memory\ consumed = total\ memory - free\ memory$$

S. No.	File size in KB	Memory in KB
1	10	26716
2	50	27391
3	100	28173
4	300	29459

5	500	30911
6	700	32138
7	1000	33019

Table 5.4 decryption memory

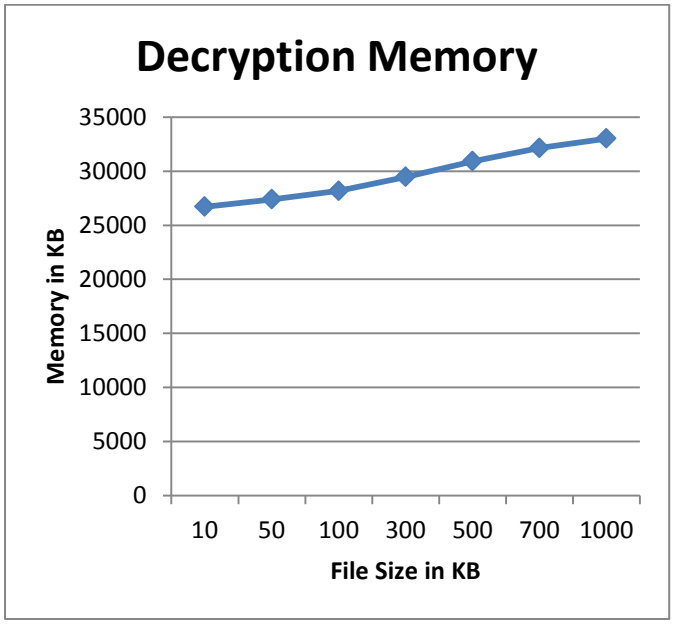


Figure 5.4 decryption memory

The amount of memory consumption during the decryption process is given using figure 5.4 and table 5.4. In this diagram the X axis shows the experimental file size and Y axis shows the amount of consumed memory. Both the terms are computed in terms of KB (kilobytes). According to the results the memory consumption is dependent on the amount of data for decryption. Thus the memory consumption is increases with the amount of data for decryption.

E. Server response

The amount of time required to produce the outcome after making the request from the server is termed as the server response time. The response time not included the encryption or decryption activity during these measurements. The computed response time of the proposed technique for cloud based secure communication is demonstrated using the figure 5.5 and table 5.5. the X axis of this diagram contains the amount of experiments performed using the system and the Y axis shows the amount of time required for generating the response through the server. That can also termed as the communication overhead for the system. According to the computed results the response time is not depends on the amount of file size or other parameters. That is directly depends on the amount of work load on the target server where the data is stored or the application is hosted.

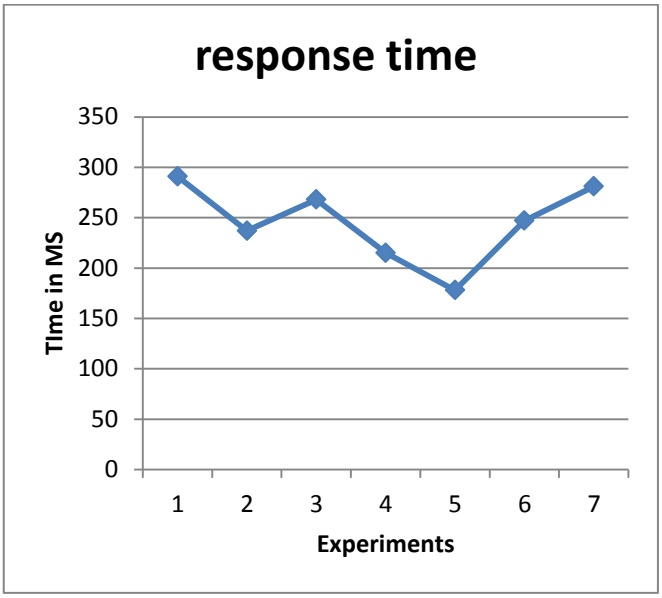


Figure 5.5 response time

Number of experiments	Response time
1	291
2	237
3	268
4	215
5	178
6	247
7	281

Table 5.5 response time

IV. CONCLUSIONS

The proposed work is intended to find solution for the secure communication and data exchange in cloud environment. Therefore a cryptographic cloud model proposed using the available DNA based cryptographic technique. The chapter provides the conclusion as the research summary and their future extension of the work is also suggested.

A. Conclusion

Cloud computing is a new generation technology. That is becomes more and more popular as the new and traditional end clients are increasing for their personal and professional use. The main reason behind this popularity is their efficient and scalable computing and storage solutions. According to the needs of applications the cloud offers storage and computing resources on demand. Thus the applications are also becomes more and more effective and efficient. Due to

this a significant amount of new applications are deployed on cloud servers among some of them are utilizes the personal and confidential information of the end user. Additionally these online cloud service are accessible in public networks, thus security is key concern in such open communication. Due to this a cryptographic security is proposed for implementation.

The proposed work is intended to develop a SaaS (software as a service) for providing the secure communication over the cloud data storage. Therefore to secure the communication an available DNA computing based cryptographic technique is adopted and integrated. The implemented system offers security during communication among client and server. In addition of that it also offers security during storage of data over cloud. In order to demonstrate the security between communicating parties three main services are deployed first is used for preservation of data on cloud host, secondly recovery of data from the secure cryptographic cloud storage and finally the sharing service for providing access to other persons who want to utilize other persons file or data.

The implementation of the proposed technique is performed using the JAVA development environment. After implementation of the system the performance of the system over different parameters are computed. Based on the experimentation the following performance outcomes are obtained as listed using table 6.1.

S. No.	Parameters	Remark
1	Encryption time	The encryption time is efficient and varies in terms of MS (milliseconds). Additionally encryption time is increases as the amount of file is increases
2	Decryption time	The decryption time is increases with the amount of file size but less than the encryption time
3	Encryption memory	The memory is depends on the amount of file size for processing, but not much fluctuating in various different file sizes
4	Decryption memory	The similar behavior is observed for decryption as demonstrated in encryption memory
5	Response time	The response time of the system depends on the work load on server

Table 6.1 performance summary

According to the obtained performance the proposed security model is efficient and secure for small and large file based data exchange. During the different communication scenarios the proposed technique found efficient and less resource consuming.

B. Future work

The main aim of the proposed work for finding secure communication using the DNA cryptography for cloud platform is achieved successfully. In near future the following extension is possible for the proposed concept.

1. In current system the randomly generated key are used for encryption and decryption the same key is required. Thus a mapping for the decryption is required for future decryption. This process is needed to enhance for more securing the system.
2. For future point of view it is required to add a third party auditor for invigilation of the entire communication.

REFERENCES

[1] Atanu Majumder, Tanusree Podder, Meenakshi Sharma, Abhishek Majumdar, Nirmalya Kar, “Secure Data Communication and Cryptography Based on DNA Based Message Encoding”, 2014 IEEE International Conference on Advanced Communication Control and Computing Technologies (ICACCCT)

[2] D. Prabhu, M. Adimoolam, “Bi-serial DNA Encryption Algorithm (BDEA)”, arXiv Cryptography and Security, 2011

[3] Scott D. Kahn, On the Future of Genomic Data, 11 FEBRUARY 2011, VOL 331, SCIENCE, www.sciencemag.org, Illumina, 9885 Towne Centre Drive, San Diego, CA 92121, USA

[4] Suman Chakraborty, Prof. Samir K. Bandyopadhyay, An approach of image staganography by combine application of DNA sequence and arithmetic encoding, International Journal of Management & Information Technology, Vol. 5, No. 3

[5] Michael Armbrust, Armando Fox, Rean Griffith, Anthony D. Joseph, Randy Katz, Andy Konwinski, Gunho Lee, David Patterson, Ariel Rabkin, Ion Stoica, and Matei Zaharia, “Above the Clouds: A Berkeley View of Cloud Computing”, UC Berkeley Reliable Adaptive Distributed Systems Laboratory, http://radlab.cs.berkeley.edu/, February 10, 2009

[6] Jonathan Grudin, “Introduction- A MOVING TARGET: THE EVOLUTION OF HCI”, Human-Computer Interaction Handbook (3rd Edition), Taylor & Francis, 2011

[7] “Getting Started with AWS”, Copyright © 2016 Amazon Web Services, Inc. and/or its affiliates. All rights reserved.

[8] Alexa Huth and James Cebula, “The Basics of Cloud Computing”, © 2011 Carnegie Mellon University, Produced for US-CERT

[9] Nariman Mirzaei, Cloud Computing, Fall 2008,Community Grids Lab, Indiana University Pervasive Technology Institute

[10] Mike Ricciuti, “Stallman: Cloud computing is 'stupidity'”, http://news.cnet.com/8301-1001_3-10054253-92.html

[11] Cloud Storage: Nonprofit Technology Collaboration, Last Updated: 3/05/2013, http://www.baylor.edu/business/mis/nonprofits/doc.php/197132.pdf

[12] Y. Chen, V. Paxson, and R. Katz, "What’s New About Cloud Computing Security?", 2010.

[13] A. Leinwand, "The Hidden Cost of the Cloud: Bandwidth Charges," http://gigaom.com/2009/07/17/the-hidden-cost-of-the-cloud-bandwidthcharges/, 2009.

[14] J. Gray, "Distributed computing economics," ACM Queue, vol. 6, pp. 63-68, 2008.

[15] M. May, "Forecast calls for clouds over biological computing," Nature Medicine, vol. 16, p. 6, 2010.

[16] Rajnish Noonia, ".Net Cryptography (Encryption / Decryption)", http://www.pixytech.com/rajnish/2013/04/net-cryptography-encryption-decryption/

[17] Jyoti Chauhan, Anchal Jain, "Survey On Encryption Algorithm Based On Chaos Theory And DNA Cryptography", International Journal of Advanced Research in Computer and Communication Engineering, Vol. 3, Issue 8, August 2014

[18] Monika, Shuchita Upadhyaya, "Secure communication using DNA cryptography with secure socket layer (SSL) protocol in wireless sensor networks", 4thInternational Conference on Eco-friendly Computing and Communication Systems, Procedia Computer Science 70 (2015) 808 – 813

[19] Sanjana Kalyani, Nidhi Gulati, "Pseudo DNA Cryptography Technique using OTP Key for Secure Data Transfer", International Journal of Engineering Science and Computing, May 2016, Volume 6 Issue No. 5

[20] Sarbjeet Kaur, Sheenam Malhotra, "A Review on Image Encryption Using DNA Based Cryptography Techniques", International Journal of Advance Research in Computer Science and Management Studies, Volume 4, Issue 3, March 2016

[21] Tausif Anwar, Dr. Sanchita Paul and Shailendra Kumar Singh, "Message Transmission Based on DNA Cryptography: Review", International Journal of Bio-Science and Bio-Technology Vol.6, No.5 (2014), pp.215-222

[22] Noorul Hussain UbaidurRahman, Chithralekha Balamurugan, Rajapandian Mariappan, "A Novel DNA Computing based Encryption and Decryption Algorithm", International Conference on Information and Communication Technologies (ICICT 2014), Procedia Computer Science 46 (2015) 463 – 475

[23] L.Jani Anbarasi, G.S.Anandha Mala, Modigari Narendra, "DNA based Multi-Secret Image Sharing", International Conference on Information and Communication Technologies (ICICT 2014), Procedia Computer Science 46 (2015) 1794 – 1801

[24] Bibhash Roy, Atanu Majumder, "An Improved Concept of Cryptography Based on DNA Sequencing", International Journal of Electronics Communication and Computer Engineering Volume 3, Issue 6

[25] Shipra Jain, Vishal Bhatnagar, "A Novel Ammonic Conversion Algorithm for Securing Data in DNA using Parabolic Encryption", Information Resources Management Journal, 28(2), 20-31, April-June 2015

[26] Vijay Prakash, Manuj Darbari, "A New Framework of Distributed System Security Using DNA Cryptography and Trust Based Approach", International Journal of Advancements in Research & Technology, Volume 3, Issue 3, March-2014.