International Journal for Rapid Research in Engineering Technology & Applied Science
Vol VIII Issue VI June. 2022
ISSN Online: (2455-4723)

An Analysis for Security of Cloud Data Storage using Client Server Mutual Authentication

Teena Nagar, Prof. Mohit Jain
M-Tech Scholar, Assistant Professor
Department of Computer Science & Engineering
BM College of Technology, Indore (MP)
tinanagar22@gmail.com

Abstract -**The advancement of technology rises many of new area of computer technology, cloud computing is one of them. It is a new conceptual based service that use by many small and big organization. In a cloud computing data may be stored at varied locations, both physically and geographically.Therefore in order to resolve the issues in cryptographic security a new methodology is required to develop. That provides the data security based on DNA cryptography for cloud data storage.In this paper, we proposed cryptography based mutual authentication system for data security. We implement DNA algorithm using AES encryption and decryption. Our experimental results demonstrate the effectiveness and efficiency of our technique when evaluating user authentication.**

Keywords: *Cloud Computing, DNA, Security, Authentication, Cryptography, Data Centre*

I. INTRODUCTION

Cloud computing is an emerging technology which recently has drawn significant attention from both industry and academia. Cloud computing provides a centralized pool of configurable computing resources and computing outsourcing mechanisms that enable different computing services to different people to their perspective. Cloud storage is a networked model of enterprise storage where data is stored in virtualized storage pools which are generally hosted by third parties. Cloud service hosting companies operate large data centers and people who require data to be hosted, buy or lease storage capacity. The data center operators, provides the resources based on the requirements of the customer and expose them as available storage, which the customers can use to store files or data objects. Actually resource may span across multiple servers and multiple locations. Safety of the files depends upon the hosting companies and on the applications that leverage the cloud storage [1] [2].In this research work we demonstrate the security for cloud data security with client server mutual authentication. Therefore need to develop a secure model which aims to find a secure and efficient manner for data storage and access for the cloud data centers. Therefore the work is intended to explore the security techniques over cloud, more specifically in terms of cryptographic solutions.

1. Cloud Computing

Cloud computing now is everywhere. In many cases, users are using the cloud without knowing they are using it. According to [3], small and medium organizations will move to cloud computing because it will support fast access to their application and reduce the cost of infrastructure. The Cloud computing is not only a technical solution but also a business model that computing power can be sold and rented. Cloud computing is focused on delivering services.

Cloud computing is a computing paradigm, where a big pool of systems are associated in confidential or public networks, to provide dynamically scalable infrastructure for purpose, data and file storage. With the arrival of this technology, the cost of computation, application hosting, content storage and release is reduced considerably. Cloud computing is a practical approach to experience direct cost remuneration and it has the impending to convert a data center from a capital-intensive set up to a variable priced environment. The idea of cloud computing is based on a very primary major of, reusability of IT capabilities'. The difference that cloud computing carry compared to conventional concepts of “grid computing”, “distributed computing”, “utility computing”, or “autonomic computing” is to widen horizon across governmental boundaries. Forrester defines cloud computing as [4].

Cloud computing, often referred to as simply “the cloud,” is the delivery of on-demand computing resources—everything from applications to data centers—over the internet on a pay-for-use basis.

- *Elastic resources* — Scale up or down quickly and easily to meet demand
- Metered service so you only pay for what you use
- *Self service* — All the IT resources you need with self-service access.

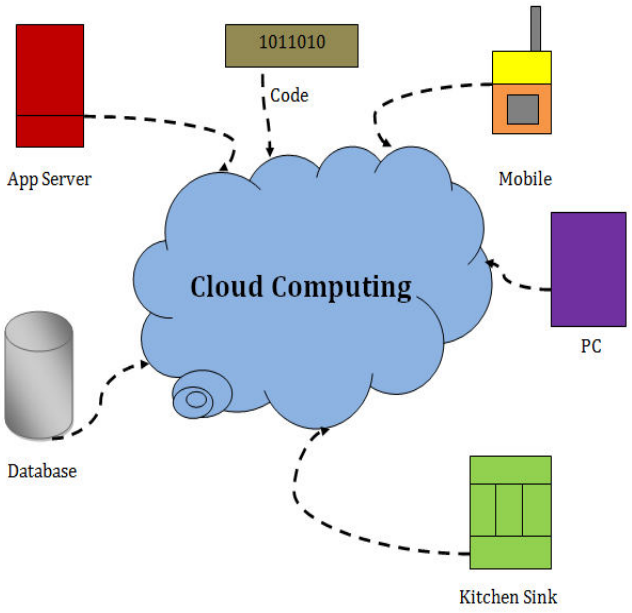

Figure 1: Cloud Computing Scenario

2. Client Server Mutual Authentication

Most web services presently use passwords to authenticate the user. However, regardless of the strength of the passwords, this type of authentication is proving to be no longer sufficient, mainly because it can be easily exposed to attacks such as key logging and phishing. Strong electronic authentication is the identification of users based on two or more factors: something the user knows, such as a password; something the user possesses, such as a chip card, device (mobile); or something that characterizes the user, such as a fingerprint. Such strong authentication mechanisms already exist but, unfortunately, most of them have the drawback of being costly. They often use security tokens that are expensive to deploy and quite impractical for users. Hence, there is a need to create stronger authentication mechanisms while still maintaining a good level of usability [5].

"Mutual Authentication is a security feature in which a client process must prove its identity to a server, and the server must prove its identity to the client, before any application traffic is sent over the client-to-server connection".

3. DNA Computing

DNA computing also known as molecular computing is a new approach to massively parallel computation based on ground breaking. He used DNA to solve a seven-node Hamiltonian path problem, a special case of an NP-Complete problem that attempts to visit every node in a graph exactly once. (This special case is trivial to solve with a conventional computer, or even by hand, but illustrates the potential of DNA computing) [6].

3.1. Advantages of DNA Cryptography

After going through DNA Cryptography various advantages of using DNA along with cryptography came to be known which are described as follows [7]:

- The biggest advantage of cryptography is its secure nature, although, it never needs to be transmitted or exposed to anyone.
- Moreover, encrypting it along the DNA sequence makes it more secure. One gram of DNA contains 10^{21} DNA bases = 10^{8} TB of data. A few grams of DNA can hold all the data stored in world.
- Since DNA is used for encryption, Signature authorization is not needed. DNA replaces the cause of Digital signatures and digital timestamps.
- Can work in a massively parallel fashion: DNA is modified biochemically by a variety of enzymes, which are minute protein machines that read and process DNA according to nature's design. There is a wide variety and number of these "operational" proteins, which manipulate DNA on the molecular level.

II. LITERATURE SURVEY

The given section provides the understanding about the cloud data storage security algorithm that are recently contributing in cloud environment therefore a number of research articles and research papers are included in this section.

In this paper, ***Ahmad-Reza Sadeghi et al. [8]*** focus on applications where the latency of the computation should be minimized, i.e., the time from submitting the query until receiving the outcome of the computation should be as small as possible. To achieve this we show how to combine a trusted hardware token (e.g., a cryptographic coprocessor or provided by the customer) with Secure Function Evaluation (SFE) to compute arbitrary functions on secret (encrypted) data where the computation leaks no information and is verifiable. The token is used in the setup phase only whereas in the time-critical online phase the cloud computes the encrypted function on encrypted data using symmetric encryption primitives only and without any interaction with other entities.

Cloud computing is a recently developed new technology for complex systems with massive-scale services sharing among numerous users. Therefore, authentication of both users and services is a significant issue for the trust and security of the cloud computing. SSL Authentication Protocol (SAP), once applied in cloud computing, will become so complicated that users will undergo a heavily loaded point both in computation and communication. In this paper, ***Hongwei Li et al. [9]***

proposed identity-based hierarchical model for cloud computing (IBHMCC) and its corresponding encryption and signature schemes, presented a new identity-based authentication protocol for cloud computing and services. Through simulation testing, it is shown that the authentication protocol is more lightweight and efficient than SAP, specially the more lightweight user side. Such merit of our model with great scalability is very suited to the massive scale cloud.

With the advent of the World Wide Web and the emergence of e-commerce applications and social networks, organizations across the world generate a large amount of data daily. This data would be more useful to cooperating organizations if they were able to share their data. Two major obstacles to this process of data sharing are providing a common storage space and secure access to the shared data. In this paper ***BhavaniThuraisingham et al. [10]*** address these issues by combining cloud computing technologies such as Hive and Hadoop with XACML policy based security mechanisms that provide fine-grained access to resources. Authors further present a web-based application that uses this combination and allows collaborating organizations to securely store and retrieve large amounts of data.

AmlanJyoti Choudhury et al. [11] proposes a strong user authentication framework for cloud computing, where user legitimacy is strongly verified before enter into the cloud. The proposed framework provides identity management, mutual authentication, session key establishment between the users and the cloud server. A user can change his/her password, whenever demanded. Furthermore, security analysis realizes the feasibility of the proposed framework for cloud computing and achieves efficiency.

SaghebKohpayehAraghi et al. [12] offer an efficient and scalable user authentication scheme for cloud computing environment. It the suggested model, various tools and techniques have been introduced and used by using the concept of agent. Therefore, a client-based user authentication agent has been introduced to confirm identity of the user in client-side. Furthermore, a cloud-based software-as-a-service application has been used to confirm the process of authentication for unregistered devices. Moreover, there are two separate servers for storing authentication and cryptography resources from main servers to decrease the dependency of user authentication and encryption processes from main server. Cryptography agent was also introduced to encrypt resources before storing on cloud servers. In overall, the theoretical analysis of the suggested scheme shows that, designing this user authentication and access control model will enhance the reliability and rate of trust in cloud computing environments as an emerging and powerful technology in various industries.

III. PROPOSED WORK

In this section the basics of the proposed security model for cloud based data storage and secure communication technique is described

1. Methodology

The proposed methodology of the system design and implementation is discussed using the figure 2. In this diagram the entire required components are described.

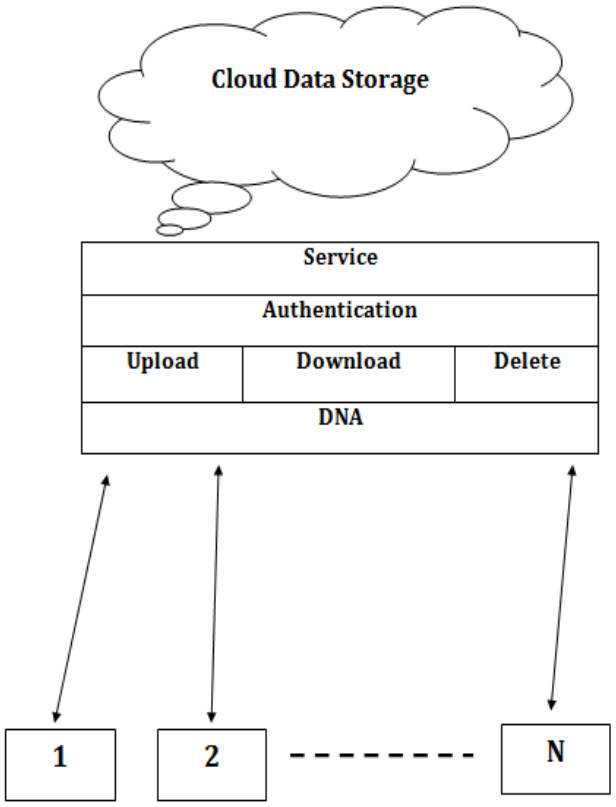

Figure 2: Proposed Systems

The above given diagram show the basic flow of DNA cryptography to secure cloud data. The architecture is designed of three level processes. 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. The entire process of the level demonstrates how the data can be secure in affective using end user authenticity. Whenever we deployed our confidential data over cloud, it is vulnerable by different reason. Therefore there is need to protect the data security by which legitimacy of data still remain. In the first level of the diagram, cloud storage is responsible for store the data in different manner. Many organizations have huge amount of data outsourced on cloud storage platform providing by different hosted companies. In

the second level of the architecture there is four part of this layer. In the first part the services are developed and deployed. Services are the main which is form a basic functioning of the system and demonstrate services.

In second part of level, server authenticate of the register user. While external user register itself by providing email address then server authenticate registered user to send mail including a onetime password for authorization of user. In the third part, three scenario are created namely upload, download and delete the documents. 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 nest scenario, delete option for permanently deletion of document file from the server. The fourth scenario is that DNA algorithm which is process internally, and used AES for document encryption and decryption. Finally last level is client devices which are used to check the correct data availability.

1.1. DNA Encryption and Decryption

In the given figure 3 and 4 for DNA encryption and decryption respectively show that the process of overall DNA cryptography.

Hence, in our implementation we take a document file in byte format as input. Furthermore, we generate binary sequence of the input file. Binary sequence means, the input file can be split in two different parts. Here, we converted file in to string and that string can be converted in to two sub string file i.e. block of the file. A substring should be 256/512/1024 byte format.

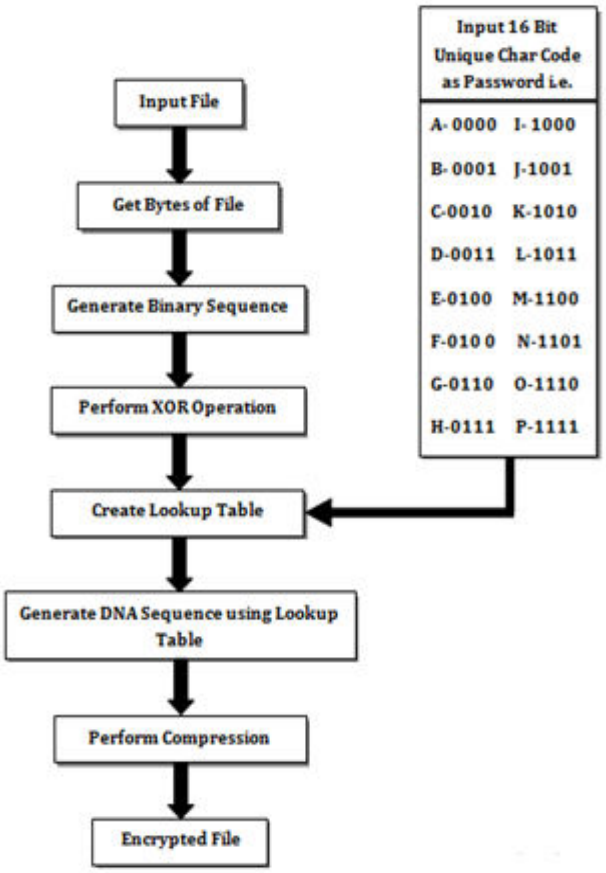

Figure 3: Encryption Process

We use 256-256 substring of file if the file contained 512 byte of the data. On this substring we perform XOR operation. Hence in result of this operation generated substring is 256 byte of data. In DNA cryptography process, we use DNA concept using lookup table for generating string. Thereafter generated XOR operation result pass to DNA lookup table for getting DNA sequencing and on this sequence apply compression technique to compress that output. For compressing file use PCR (Polymerase chain reaction) approach which is a molecular biology technique used to exponentially amplify certain regions of DNA using enzymatic replication and starting with the DNA fragment (primer) to be amplified. After that for encrypting compressed file uses AES for encryption.

Similarly in figure 4 is process of decryption, the main deference is that here we input encrypted file and decompressed using PCR, Again create lookup table get and generate DNA sequence which is pass to XOR calculation. Now on result of XOR operation we retrieved byte array at and write the data file on receiver end. Finally for getting original file use the AES for decryption operation. For the originality of the data file download the file and check this file as is original.

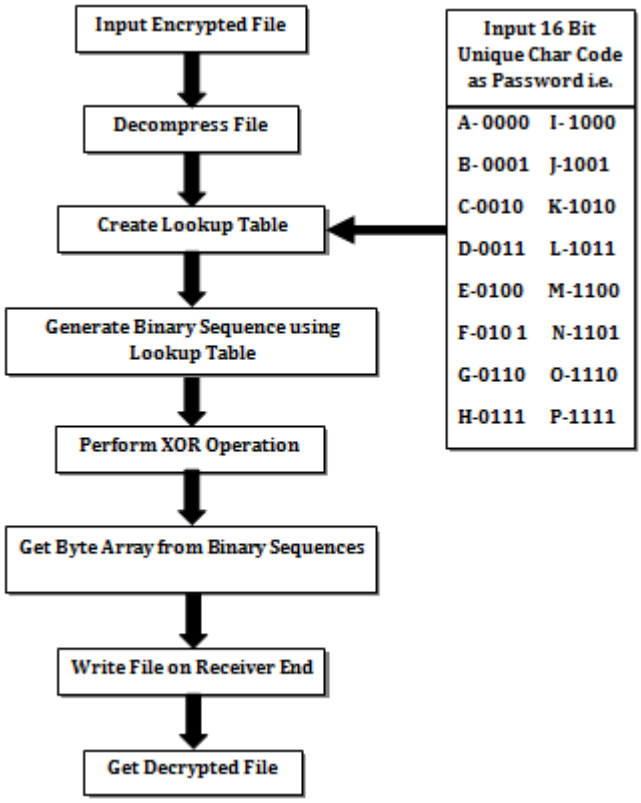

Figure 4: Decryption Process

The overall process depicts the cloud data security which employee client and server end communication. The server end maintained the register user credential and their authenticity for full protection of file. Therefore, this all scenarios concern to the developed methodology and their flow process.

IV. RESULT ANALYSIS

1. *Encryption Time*

The amount of time required to encrypt the given input file is termed here as the encryption time. The encryption time of the proposed system with increasing amount of file size is given using figure 5. This is computed using the following formula:

$$EncryptionTime = EndTime - StartTime$$

The time complexity of the proposed DNA based secure technique is given using figure 5, the Y axis shows the amount of time consumed for processing the data file for encryption process

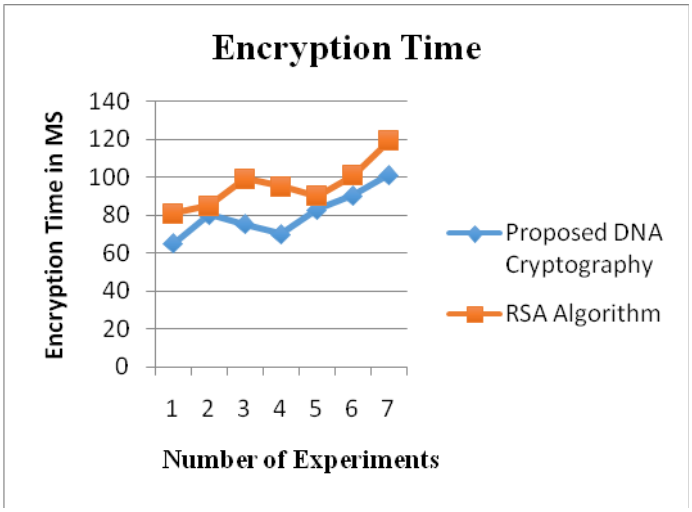

Figure 5: Encryption Time

. In this figure we compared our approach to traditional RSA algorithm. Blue line depicts the proposed DNA approach and orange line show RSA algorithm. 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. By giving both scenarios proposed approach is more adaptable genuine user authentication as compared to traditional RSA.

2. *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.

$$DecryptionTime = EndTime - StartTime$$

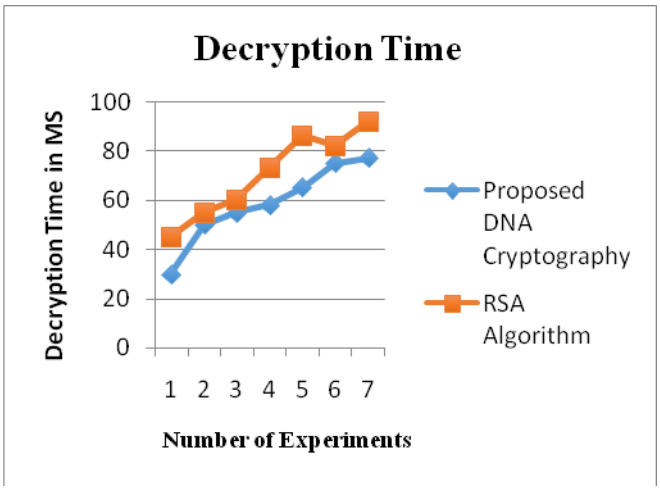

Figure 6: Decryption Time

The amount of time required for decryption of data is given using the figure 6. In figure we compare to implemented approaches i.e. proposed DNA algorithm and Traditional RSA. These two algorithmic demonstrations show that RSA taking more time for decryption process. According to the diagram X axis shows the number of experiments for execution and Y axis represents the amount of time consumed for decryption of encrypted files in terms of MS (milliseconds). According to the generated performance the proposed DNA based technique consumes less time for decryption as compared to the RSA algorithm. Thus the proposed model is flexible and efficient to secure cloud data storage.

3. 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.

$$EncryptionMemory = TotalMemory - FreeMemory$$

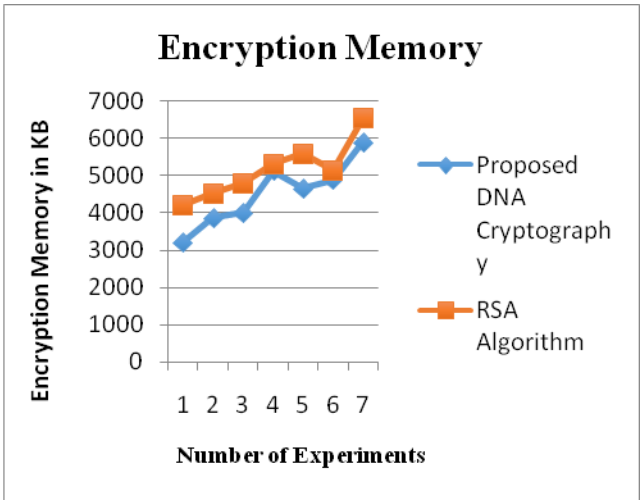

Figure 7: Encryption Memory

The encryption memory consumption of the proposed cloud based secure data storage of client server authentication demonstrated using the figure 7.In this diagram the X axis shows the number of runs and Y axis shows the consumed memory of the implemented system in terms of KB (kilobytes). Thus blue line is for proposed DNA cryptography and orange line is for RSA based algorithm. According to the achieved performance of system is depends on the amount of file for processing. Thus as the file size increases the required memory is also increases. According to the system performance the proposed technique is more secure this is takes less space to process algorithm.

4. 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.

$$DecryptionMemory = TotalMemory - FreeMemory$$

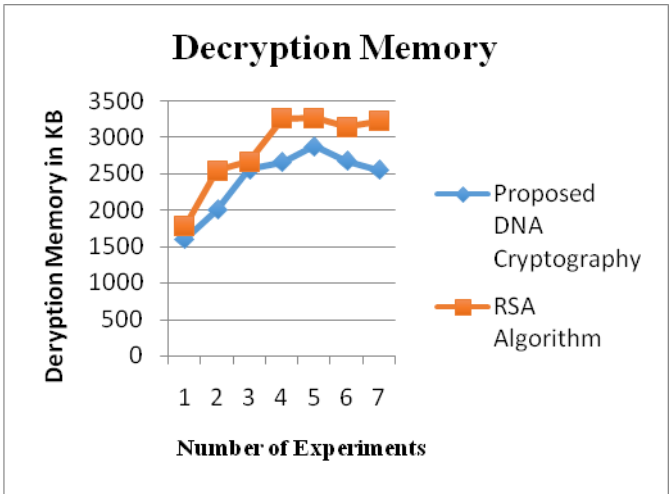

Figure 8: Decryption Memory

The quantity of memory consumption during the decryption process is given using figure 8. In this diagram the X axis shows the experimental scenarios and Y axis shows the amount of consumed memory. Both the terms are computed in terms of KB (kilobytes). According to the generated results the memory consumption is dependent on the amount of data for decryption. Similarly, RSA algorithm takes more space when we execute system. Thus the memory consumption is increases with the amount of data for decryption.

5. Server Response Time

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 secure cloud data storage is demonstrated using the figure 9. X axis of this diagram contains number of experiments performed using the system and the Y axis shows the amount of time required for generating the response through the server. This can also term as the communication overhead for the system.

Security is primary concern for user authentication. Therefore we have developed both algorithm named as Proposed DNA cryptography and traditional RSA algorithm. According both algorithm result we can summarize our conclusion 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.

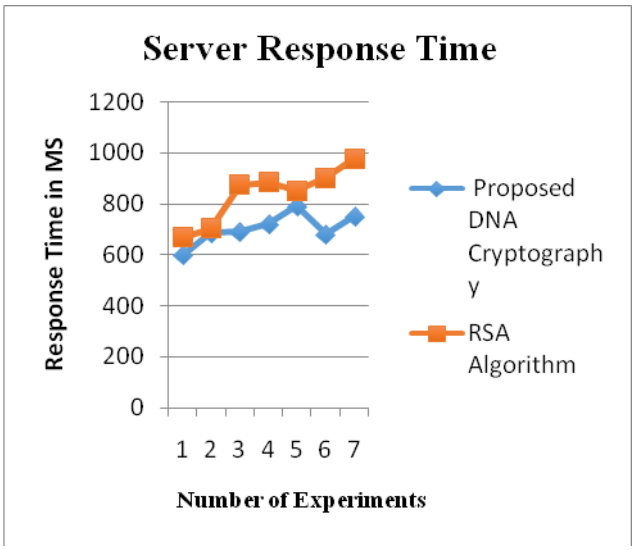

Figure 9: Response Time

V. CONCLUSION

Privacy and security in cloud can be said to be achieved when users have control over information they want to reveal to cloud and who can access their information. Without guarantee of security and privacy users can't make shift to cloud only on the basis of lower cost and faster computing. The cloud computing is respectively new domain of research and development. A number of new directions are appeared due to introduction of this technology. In this presented work the cryptographic cloud and their security issues are investigated. In this context the available cryptographic solutions are not suitable due to higher computational overhead and the storage overheads. Therefore a new kind of cryptographic approach is required to minimize the computational cost as well storage of cryptographic data. Therefore in order to resolve the addressed issue a new DNA computing for client server mutual authentication of data storage is proposed. The proposed security architecture is an enhance hybrid security architecture which is designed through DNA based cryptographic approach and an authentication server implementation. This technique is used for AES for encryption and decryption of data file. On the other hand, a look up table is generated of DNA using MD5 hash generation. The developed system follows an OTP (one time password scheme) for authenticating the users by sending the mail on authenticate user ID. Therefore, the proposed model enhances the security over the cloud data of client mutual authentication.

REFERENCES

[1] Aized Amin Soofi and Fazal-e-Amin, “A Review on Data Security in Cloud Computing”, International Journal of Computer Applications (IJCA), Volume 94 – No 5, May 2014

[2] Sun, Yunchuan, et al., "Data security and privacy in cloud computing", International Journal of Distributed Sensor Networks (2014).

[3] I. Foster, Z. Yong, I. Raicu, and S. Lu, "Cloud Computing and Grid Computing 360-Degree Compared," in Grid Computing Environments Workshop, 2008. GCE '08, 2008, pp. 1-10

[4] Sookhak, Mehdi, et al. "Remote data auditing in cloud computing environments: a survey, taxonomy, and open issues." ACM Computing Surveys (CSUR) 47.4 (2015): 65.

[5] Mrs. Seema P. Nakhate and Prof. R. M. Goudar, “Secure Mutual Authentication Protocol”, International Journal of Computer Networks and Communications Security, Volume 2, Number 4, April 2014, pp. 142–145

[6] Yunpeng, Zhang, et al. "Index-based symmetric DNA encryption algorithm", Image and Signal Processing (CISP), 2011 4th International Congress on, Vol. 5, IEEE, 2011.

[7] Tripathi, Shiv PN, ManasJaiswal, and Vrijendra Singh, "Securing DNA Information through Public Key Cryptography", MIS Review 19.1 (2013): PP. 45-59.

[8] Sadeghi, Ahmad-Reza, Thomas Schneider, and Marcel Winandy, "Token-based cloud computing", International Conference on Trust and Trustworthy Computing, Springer Berlin Heidelberg, 2010.

[9] Li, Hongwei, et al. "Identity-based authentication for cloud computing", IEEE International Conference on Cloud Computing, Springer Berlin Heidelberg, 2009.

[10] Thuraisingham, Bhavani, et al. "Secure data storage and retrieval in the cloud", Collaborative Computing: Networking, Applications and Worksharing (CollaborateCom), 2010 6th International Conference on, IEEE, 2010.

[11] Choudhury, AmlanJyoti, et al. "A strong user authentication framework for cloud computing", Services Computing Conference (APSCC), 2011 IEEE Asia-Pacific, IEEE, 2011.

[12] Moghaddam, FarazFatemi, et al. "A scalable and efficient user authentication scheme for cloud computing environments", Region 10 Symposium, 2014 IEEE, IEEE, 2014.