A Cryptographic Solution for Cloud Data Storage using DNA Computing

Ruchi Goyal[1], Shreyas Pagare [2]
Department of Computer Science & Engg., RGPV, Bhopal, M.P., India [1]
Department of Computer Science & Engg., RGPV, Bhopal, M.P., India[2]
ruchi.goyal05@gmail.com [1], shreyas.pagare@gmail.com[2]

Abstract: *The data security and network security is a crucial domain of research and development. Everyday a new kind of security loophole is appeared and their solution is required to obtain. On the other hand the computing changes their face and at the same ways the attackers and intruders are also aware about the traditional security techniques. Thus new kind of security is required to find that are not accurately from the traditional backgrounds. In this presented work the cloud storage solutions are investigated in detail and observed for improving the data management the cloud service providers are outsource their data to other data centers. Thus the privacy and confidentiality is a concern for the end client and the service providers. Therefore most of the data centers are utilizes the cryptographic solution for securing the data on storage. But the traditional cryptographic models are computationally cost effective, produce additional storage overheads, and also generate the week cipher for storage. Therefore the proposed work introduces a new DNA computing based cryptographic technique. That scheme first utilizes the MD5 hash generation technique to create a dynamic mapping table for data encoding and decoding. On the other hand for improving the complexity of cipher text the technique implements the genetic algorithm based crossover operation. Finally for more security only a single part of original cipher is transmitted to the receiver end. The proposed working model is developed with the help of JAVA technology. Additionally for providing the effectiveness of the implemented approach the server response time, encryption and decryption time, memory consumption is estimated. All the measured performance factors are found optimum for adopting the cryptographic solution.*

Keywords: *cloud servers, data outsourcing, network transmission, cryptographic cloud, data exchange;*

1. INTRODUCTION

In last some recent years the use of internet is increases due to awareness of technology and their need in daily routine applications i.e. internet banking, email messages and others. Therefore for providing the reliable services various service providers are utilizing the cloud infrastructure and their services to serve their clients better. The cloud infrastructure allows the service provider to promises their clients to provide the scalable storage and computing services. Thus a significant amount of crowed is attracted in this domain of computation and storage. But the client always worried about the data confidentiality and their sensitivity. Therefore a number of research efforts are placed on the cloud security and trust managements.

In this presented work the cloud data center security and their cryptographic solutions are investigated in detail. That observed from various research sources the data on cloud is unsecured during transmission, access, sharing, and storage in third party (outsourcing). Therefore the different cryptographic approaches are applied for securing the data during these events. By the inspiration of these approaches a new cryptographic approach is proposed using DNA computing technique. The proposed DNA computing based cryptography is promises to provide efficient cipher generation in complex manner. That also designed for reducing the amount of cipher size to produce less storage overhead and the time overhead for computing and cryptography. Thus the proposed cryptographic technique is secured and efficient for utilizing with the cloud infrastructure.

The given section provides the basic overview of the proposed work. In the further section the key methodology and the proposed cryptographic solution is presented. Additionally the performed experiments and the performance are also reported in the paper.

2. PROPOSED SYSTEM

Cloud computing is one of the most popular web technology now in these days. In this technology the service providers are offers the computational and storages and other resources as services. Therefore these services are scalable and help for different needs of application development and deployments. In this presented work the cloud computing is studied. During study that is found for scaling the services and for reducing the overhead of data and data management they follow the concept of data outsourcing. In the concept of data outsourcing the cloud service providers are host the client data on third party data centers. on the other hand due to this end client or data owner is worried about the data sensitivity and their privacy concern associated with the data. Therefore the concept of cryptographic cloud is adopted for improving the security and privacy concerns in the data hosting in third party cloud data centers.

In order to secure the data and their privacy concern in cryptographic cloud a number of cryptographic solutions are available classically. But these cryptographic techniques are not much suitable due to their high time and computational complexity. Therefore in this presented work a lightweight cryptographic approach is proposed using the DNA computing technology. Additionally for generating the more complex cipher the dynamic mapping table is proposed for implementation. The proposed cryptographic technique also involves the genetic cross over technique for improving the complexity of cipher.The proposed methodology for secure data hosting and transfer among the two communicating party is given using the figure 1.

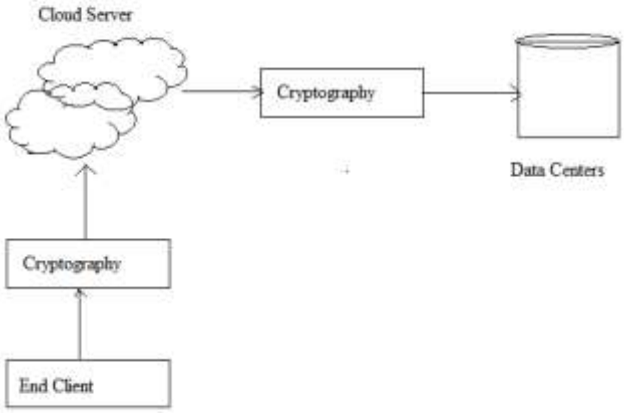

Fig.1 Proposed security aspect

In the given diagram the cloud server is service provider system which interacted with the clients and also sometimes with the different data centers. In order to preserve information of the third party servers the cryptographic solution is required. Additionally to secure the communication between client and server due to the network influenced attacks and unsecured public network that also required a cryptographic solution. Therefore a new cryptographic solution is required which is efficient and generated complex cipher transmission of data.

The proposed secure cryptographic solution is a combination of Morden and traditional cryptographic approach. Therefore it includes the concept of MD5 hash generation technique, DNA cryptography basics, and genetic algorithm based cross over to secure the data in suspected environment. The encryption and decryption process is summarized in this section using two phases' encryption and decryption.

Table 1: Encryption technique

```
Input: Original Text T, elitism e
Output: Cipher Text C
Process
1. D = read_Data_ASCII(T);
2. H = Covert_Binary_Hex(D)
3. $Key_{128}$ = Generate_Hash_MD5(H)
4. $HK_{32}$ = Covert_Binary_Hex($Key_{128}$)
5. $TB = genrateEncodingTable(HK_{32})$
```

```
6.  $[S_1, S_2] = splitData(H, 2)$
7.  compute Cross over point using
        $nc = |\alpha - Ne|/2$
8.  crossover the strings $S_1$ $and$ $S_2$
9.  $ES_1$= Encode_Data($S_1$, TB)
10. $ES_2$= Encode_Data($S_2$, TB)
11. $BS_1$= Convert_Data_Hex_Binary($ES_1$)
12. $BS_2$= Convert_Data_Hex_Binary($ES_2$)
13. $X_{data}$ = XOR($BS_1$,$BS_2$)
14. $C = Combine(X_{data}, BS_2, \alpha, e, TB)$
15. return C
```

The above given table 1 provides the summarized steps of the encryption algorithm for generating cipher text to be send in unsecured network. At the end of receiver how the original data is recovered is given using table 2.

Table 2:Decryption technique

```
Input: Cipher text C
Output: Original text
Process:
1. [$X_{data}$ , $BS_2, \alpha, e, TB$] = Re_Genrate(C)
2. $BS_1$= XOR($BS_2$,$X_{data}$ )
3. $ES_1$= Convert_Data _Binary_Hex($BS_1$)
4. $ES_2$= Convert_Data _Binary_Hex($BS_2$)
5. $S_1$= Decode_Data($ES_1$, TB)
6. $S_2$= Decode_Data($ES_2$, TB)
7. crossover the strings $S_1$ $and$ $S_2$
8. H= $CombineData[S_1, S_2]$
9. D = Covert_Hex_Binary (H)
10. T = write_ASCII_Data(D);
11. return T
```

The given table 2 shows the decryption process of the given encryption technique of data encryption using the three different concepts i.e. MD5 hash generation technique, DNA computing and the genetic algorithm. The proposed technique is promising for improving the cipher complexity and reduction of the computational cost.

3. RESULT ANALYSIS

The given section provides the performance analysis of the proposed cryptographic cloud concept and the different evaluated performance factors are described as:

A. Server response time

The amount of time required to execute the user request for generating the response form the server is termed here as the server response time. The computed server response time for different activities is given using figure 2.

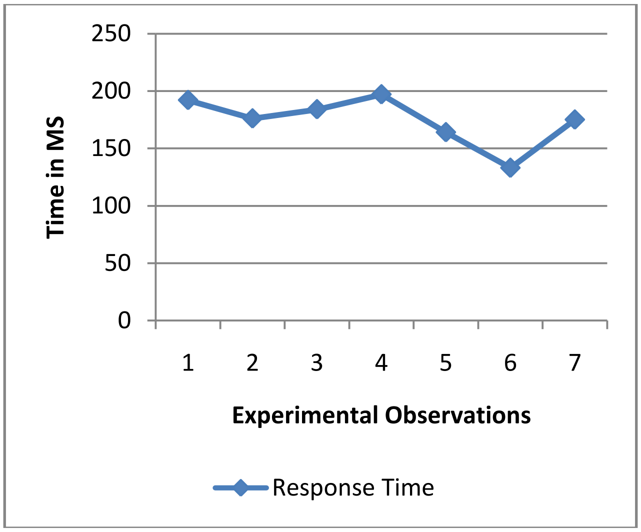

Fig.2 Server response time

In this diagram the X axis contains the different experimental observations with the system and the Y axis shows the amount of time required for finding the response from the server. The different observations are shows the fluctuating time for processing a user request. The noticed fluctuation in the response time is causes by the request load on the cloud server thus as the work load on the server is increases the amount of response time is also increases in the similar manner. Thus the response time is adoptable for use with the different security applications for the cloud.

B. 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 3.

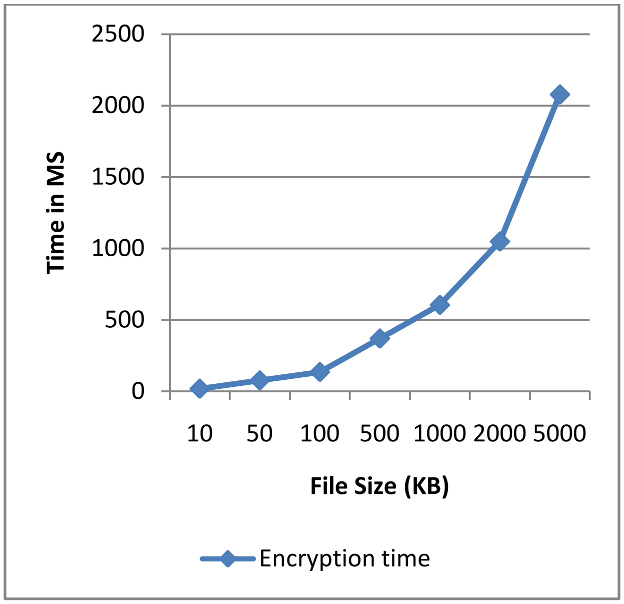

Fig.3 Encryption time

In this diagram the different experimental observations are made with increasing amount of file size in terms of KB which is reported using the X axis of diagram. Additionally the corresponding amount of time for encrypting the file is given using Y axis. According to the obtained results the time for encryption is increases as the amount of data is increases.

C. Decryption time

The amount of time required to decrypt or recover the original data from the encrypted data is known as the decryption time. The decryption time with the same amount of file size is approximated and reported using the figure 4.

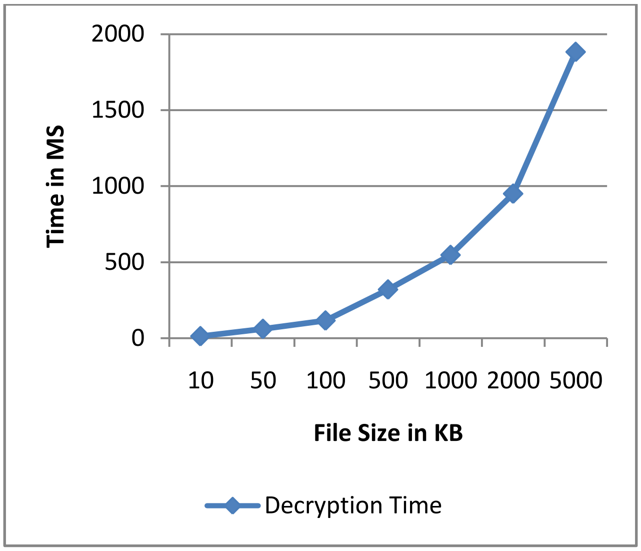

Fig.4 Decryption time

In this diagram the X axis contains the increasing amount of files size in terms of KB (kilobytes) additionally the Y axis contains the amount of time consumed in terms of milliseconds. The obtained results show the encryption time is higher than the decryption time in all the observation. Additionally that demonstrates the similar behaviour as the encryption process. Thus the decryption time of the system is increases as the amount of data increases.

D. Memory consumption

The amount of main memory required executing the file encryption and decryption is known as memory consumption or the space complexity. The memory consumption of the proposed system during encryption and decryption is given using figure 5. In this diagram the encryption process's memory consumption is demonstrated using the blue line and decryption process is given using red line. For demonstrating the performance of the system X axis contains the amount of files in terms of KB (kilobytes) and the Y axis contain the relevant memory size consumed for processing of the input files. According to the obtained results the decryption phase of the system consumes less amount of memory as compared to encryption. But the amount of memory consumption is increases for both the processes as the amount of data to be process is increases.

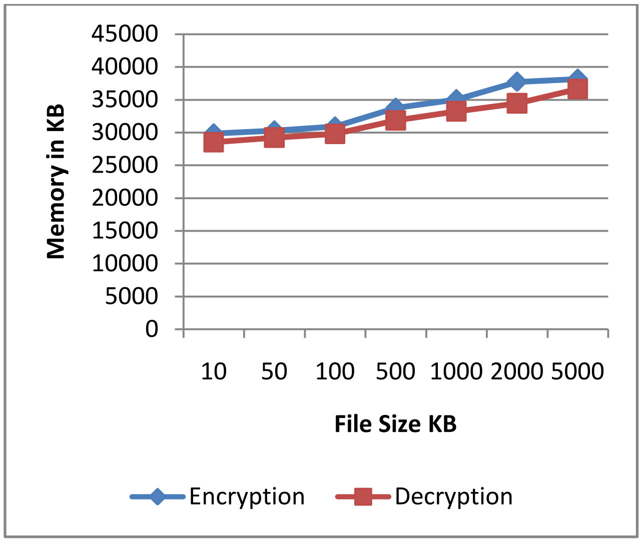

Fig. 5 Memory consumption

E. Space overhead

The amount of additional storage space required when the data is encrypted form their original size is termed as the space overhead. In other words the increment on size of the original text files after encryption of data is termed as the storage overhead. That can be computed using the following formula:

$$space\ overhead = file\ size\ after\ encryption - file\ size\ before\ encryption$$

The performance of the proposed cryptographic system in terms of space overhead is given using figure 6. In this diagram the different amount or size of original text files are reported on X axis and the Y axis reports the space overhead of the encrypted file. In the experimental results that are observed the small amount of file size are increases when the file is transformed into encrypted format but that is also increases in similar ratio as the amount of file is increases. Therefore the proposed technique is adoptable for less space overhead and efficient data processing.

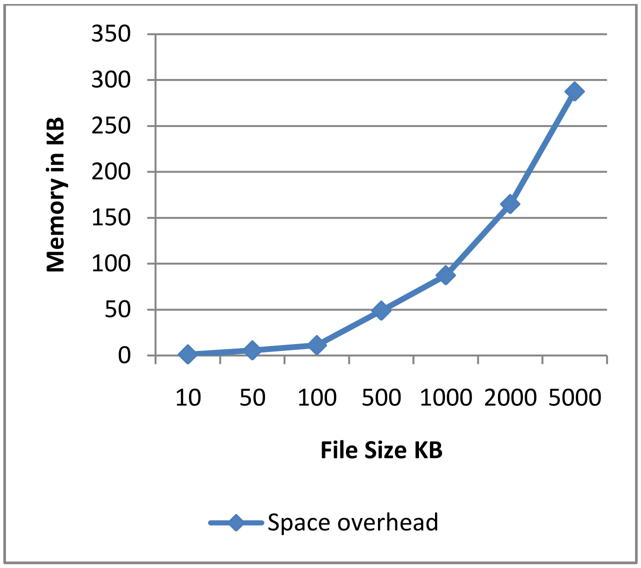

Fig. 6 Space overhead

4. CONCLUSION

The main aim of the proposed study is investigate about the cloud and their security issues when the data is placed in it. Therefore a cryptographic data model is developed using the DNA based computing and their performance is also evaluated on different performance parameters. According to the observations and the experimentations the facts are concluded and the reported in this chapter. Additionally the future extension of the work is also provided in this chapter.

A. Conclusion

The cloud computing is respectively new domain of research and development. A number of new directions are appeared due to introduction of this technology. The technology offers to use the services and different resources remotely on the basis of pay per use. Additionally that technology enables us to work in scalable computing performance and storage resources. Therefore a number of new generation applications are designed for cloud based services. The cloud service providers are utilizes the data out sourcing for providing scalable storage solutions to their clients. Thus the issue of data security and privacy is major area of concern in the cloud environment.

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 solution is required to minimize the computational cost as well storage of cryptographic data. in order to resolve the addressed issue a new DNA computing and genetic computing based cryptographic solution is proposed. That technique provides the hybrid manner of computing and security to make the cipher text more complex and reduces the size of generated cipher text. The proposed technique is different from the existing DNA based encryption technique because according to the data the mapping table is constructed which is not similar to other mapping tables. That is generated according to the data using MD5 hash generation algorithm. In addition of that for encryption the genetic algorithm based crossover technique is also incorporated for finding the appropriate complexity in the cipher text.

The proposed genetic algorithm based DNA cryptography is implemented using the JAVA technology. Additionally after implementation the performance is analysed in terms of server response time, encryption and decryption time complexity, space complexity and space overhead. The performance summaries of the implemented system in terms of the given parameters are reported using table 3.

Table 3: Performance summary

S . No.	Parameters	Remark
1	Server response time	The server response time is not fluctuating much with the amount of data that is equivalent to number of request appeared to the server
2	Encryption time	The time of encryption is increases or decreases according to the amount of data provided for encryption
3	Decryption time	The decryption time is less than the encryption time additionally that is increases and decrease with the amount of data
4	Memory usages	The memory consumption is also fluctuating with the amount of data provided for encryption or decryption
5	Space overhead	Not producing higher space overhead but increases in similar ratio as the amount of data input ratio is increases or decreases

According to the obtained results and performance analysis the proposed cryptographic technique is efficient and consuming less computational resources. Additionally that is also able to provide more complex cipher as compared to traditional cryptographic technique.

B. Future work

The proposed work is indented to find a lightweight cryptographic technique which used with the cloud environment to generate strong cipher with less computational complexity. The required cryptographic technique is implemented and evaluated successfully. During experimentation that is find efficient and effective therefore the following future extension is can be feasible for future work.

1. In place of MD5 the SHA1 can also be used for generating the mapping table
2. That is secure and efficient thus that can also be used with the banking security and access control methodologies.

REFERENCES

[1]. KawserWazedNafi, TonnyShekhaKar, SayedAnisulHoque, Dr. M. M. A Hashem, “A Newer User Authentication, File encryption and Distributed Server Based Cloud Computing security architecture”, (IJACSA) International Journal of Advanced Computer Science and Applications, Vol. 3, No. 10, 2012

[2]. torryharris, “CLOUD COMPUTING – An Overview”, http://www.thbs.com/downloads/Cloud-Computing-Overview.pdf

[3]. Vaishali Jain, Akshita Sharma, “A Taxonomy on Cloud Computing”, International Journal of Emerging Technology and Advanced Engineering, ISSN 2250-2459, ISO 9001:2008 Certified Journal, Volume 4, Issue 3, March 2014

[4]. Balvinder Singh, Priya Nain, “Bottleneck Occurrence in Cloud Computing”, National Conference on Advances in Computer Science and Applications with International Journal of Computer Applications (NCACSA 2012)

[5]. MilenkoRadonic, “Cloud vs. Data Center: What's the difference”, http://www.glbrain.com/index.php?r=tool/view&id=2103&toolType=1

[6]. ChittajalluSaiMeghana, “Security and Services Management Aspects of Cloud Architectures”, http://www.idrbt.ac.in/PDFs/PT%20Reports/2013/Chittajallu%20Sai%20 Meghana_Security%20and%20services%20management%20aspects%20of%20cloud%20architectures_2013.pdf

[7]. V. Abricksen, “A Survey on Cloud Computing and Cloud Security Issues”, International Journal of Engineering Research and Applications (IJERA) ISSN: 2248-9622 International Conference on Humming Bird (01st March 2014)

[8]. SwapnaLia Anil, RoshniThanka, “A Survey on Security of Data outsourcing in Cloud”, International Journal of Scientific and Research Publications, Volume 3, Issue 2, February 2013

[9]. SenyKamara, Kristin Lauter, “Cryptographic Cloud Storage”, Microsoft Research Cryptography Group,

http://research.microsoft.com/en-us/people/klauter/cryptostoragerlcps.-pdf

[10]. KratiMehto, Rahul Moriwal, “A Secured and Searchable Encryption Algorithm for Cloud Storage”, International Journal of Computer Applications (0975 – 8887) Volume 120 – No.5, June 2015

[11]. PradipLamsal, “Understanding Trust and Security”, Department of Computer Science University of Helsinki, Finland, 20th of October 2001

[12]. Zhen Chen, Wenyu Dong, Hang Li, Peng Zhang, Xinming Chen, and Junwei Cao, “Collaborative Network Security in Multi-Tenant Data Center for Cloud Computing”, Tsinghua Science and Technology, Volume 19, Number 1, February 2014

[13]. Jiaqi Zhao, Lizhe Wang, Jie Tao, Jinjun Chen, Weiye Sun, Rajiv Ranjan, Joanna Kołodziej, AchimStreit, DimitriosGeorgakopoulos, “A security framework in G-Hadoop for big data computing across distributed Cloud data centres”, Journal of Computer and System Sciences, © 2014 Elsevier Inc. All rights reserved.

[14]. Victor Chang, MuthuRamachandran, “Towards achieving Data Security with the Cloud Computing Adoption Framework”, IEEE TRANSACTIONS on Services Computing, Volume:9, Issue: 1, Jan.-Feb. 1 2016

[15]. Jianbing Ni, Yong Yu, Yi Mu, and Qi Xia, “On the Security of an Efficient Dynamic Auditing Protocol in Cloud Storage”, IEEE Transactions on Parallel and Distributed Systems, Vol. 25, No. 10, OCTOBER 2014

[16]. Emilianomiluzzo, “I’m Cloud 2.0, and I’m Not Just a Data Center”, 1089-7801/14/$31.00 © 2014 IEEE Published by the IEEE Computer Society

[17]. MeenakshiThapliyal, Dr.HardwariLalMandoria, NehaGarg, “Data Security Analysis in Cloud Environment: A Review”, International Journal of Innovations & Advancement in Computer Science IJIACS Volume 2, Issue 1 January 2014

[18]. Deepak Puthal, B. P. S. Sahoo, Sambit Mishra, and Satyabrata Swain, “Cloud Computing Features, Issues and Challenges: A Big Picture”, 2015 International Conference on Computational Intelligence & Networks (CINE 2015),

[19]. MrinalKantiSarkar, TrijitChatterjee, “Enhancing Data Storage Security in Cloud Computing Through Steganography”, ACEEE Int. J. on Network Security , Vol. 5, No. 1, January 2014

[20]. Mohammad Aazam, Pham Phuoc Hung, Eui-Nam Huh, “Cloud of Things: Integrating Internet of Things with Cloud Computing and the Issues Involved”, Proceedings of International Bhurban Conference on Applied Sciences & Technology Islamabad, Pakistan, January 14 – 18, 2014

[21]. Dan Gonzales, Jeremy Kaplan, Evan Saltzman, Zev Winkelman, Dulani Woods, “Cloud-Trust - a Security Assessment Model for Infrastructure as a Service (IaaS) Clouds”, IEEE TRANSACTIONS ON JOURNAL GONZALES, TCC-2014-03-0102