ISSN:0975-9646

Kanwar Lal Dhakar et al, / (IJCSIT) International Journal of Computer Science and Information Technologies, Vol. 7 (3) , 2016, 1205-1211

Architecture of Secure Cloud Data Center Storage

Kanwar Lal Dhakar[1], Prof. Savita Rathod[*2]

Computer Science& Engineering, Truba College of Engineering & Technology,

Indore (RGTU Bhopal) India

Abstract— Cloud hosts are basically a data center where a significant amount of data appeared and accessed in a fraction of seconds. Among them most of the data is preserved for long terms storage. Due to their efficiency and computational ability of analytics new clients are also attracted with such kind of systems. Due to this the data security in cloud storage or data centers are a critical issue. The security in this server concerned about during data storage, access and transmission in public network. Thus a new security technique is required.

In this work using the available techniques of network and data security a technique is suggested and implemented for achieving all the concerns of data center security. Therefore to store data in data centers a cryptographic technique by enhancing the existing DNA cryptography is proposed for implementation that offers efficient data encryption and decryption with less resource consumption. In addition of that for securing the data during the network transmission the similar cryptographic technique is employed. Furthermore for accessing the data by the end client a secure authentication process using the TPA (third party auditor) is proposed and implemented.

The implementation of the proposed technique J2SE environment is used. After implementation the performance of the entire system is evaluated and compared with the RSA algorithm based secure cryptographic technique. Additionally the performance of system in terms of server response time, memory consumption, time consumption and the space overhead is provided. According to the obtained outcomes the proposed technique find optimum and efficient for securing data in data centers.

Keywords— security, TPA, OTP, cloud data center, network security.

I. INTRODUCTION

The use of internet is increasing rapidly due to technological growth and applications. A number of applications such as internet banking, email messages and others are accessed with the help of internet. These services from the internet are accessible according to the 24X7 manners. Therefore reliability on services distribution is required. A number of service providers for that purpose trust on cloud infrastructure and cloud based services. Using the cloud infrastructure service providers serve their client's better and efficient manner with increasing amounts of clients requests. Therefore need to provide the scalable storage and computing services using the cloud. But most of the applications needs sensitive and private data for the use thus client always worried about the data confidentiality and security.

The presented work is 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 the cryptographic solutions. In literature there are a number of articles are exist that are considering the issues of cloud during transmission, access, sharing, and storage. Therefore a cryptographic approach is required to secure the data during the communication and storage. In order to provide cryptographic solution for cloud data center storage and access a new cryptographic technique using DNA computing is proposed in this work.

The proposed DNA computing based cryptography promises for efficient cipher generation. Additionally promises to provide strength on the cipher for securing data during transmission and storage. That is also promises for reducing the amount of cipher size for less storage overhead. By which the time complexity for cryptography is significantly improved. Thus proposed work introduces the cryptographic technique for improving the security and performance both for data center storage and access.

In literature study about cloud data centers that is found for scaling the storage and other resources outsourcing concepts are developed. According to this the data center owners are exchanging the storage units. 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. Therefore the cryptographic security on cloud is employed for securing the data from outsiders and the data leakage. Thus the security becomes more essential aspect for the cloud computing.

In this presented work a cryptographic algorithm is proposed and implemented order to secure the data in the cloud storage. In addition of that for securing the data during the transmission and data access a new authentication process with the third party auditor is implemented. This technique not only ensures the security of data during the data transmission that also secure data during the data accessing from the end client.

II. PROPOSED WORK

The section discusses about the security system of the cloud storage (data center). Therefore the proposed security aspects of the data security are demonstrated in this section. The proposed security model is responsible for authentication of end client during data access and data storage. Providing security during network transmission and cryptographically hosting and sharing of data. Thus a new scheme is introduced to provide security using the figure 1. According to above given system there are three individual identities are involved namely the client, cloud

storage server and a security server therefore initially these roles are described as.

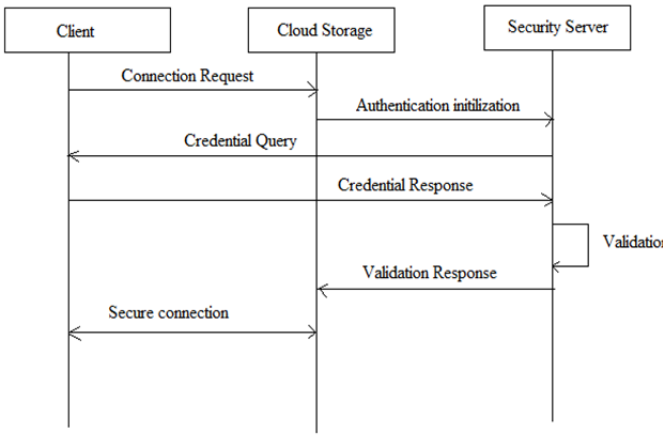


Figure 1 security architecture

- ***Client:*** that is an end client who wishes to store or access the data from the cloud storage server. Therefore the client can be access their cloud storage accounts using any device such as mobile phone, laptop or any PC. These devices are termed here as the client device or client end.
- ***Cloud storage*****:** that is the cloud storage or data center where the data is aggregated from the different client ends. Cloud storage can be a simple repository where the data is preserved accessed on demand basis.
- ***Security server:*** that is third party security auditor which is used to regulate the communication or connection among the client device and the cloud data center. In this presented system the security server or TPA works as the authenticator for the data accessing party.

In order to demonstrate the processes involve in figure 1 the sequence of process is indicated using a sequence diagram. The diagram also includes the arrows heads to demonstrate the steps followed for secure communication and authentication. The following steps are involved:

1. ***Client connection request:*** initially the process is initiated when the client makes a request to the cloud data center for accessing or storing data. To access the defined services by client device a request to the server is made. In this phase the server verifies the registration of end user if the client is registered previously than the server triggers a method to call the authentication or security server. On the other hand if the user is not registered previously server generates error and asks for the registration to user.
2. ***Authentication initialization*****:** in the case when the user is registered then this step is initiated with the help of cloud server host for the authentication of end client. Therefore a message to the secure third party server is convey for authenticating the end client.
3. ***Credential query:*** As the cloud host message received by the third party security host. The secure server asks for the user credentials additionally an additional query is made as the security question randomly to the client. The query is made in through the information submitted by the user during the registration process the security question can be about for date of birth, PAN card number or other relevant information.
4. ***Credential response:*** in the response of the asked query by the security server question the client need to answer the security question. The given answer is submitted to the security server is verified by the server. If the security answers and input credentials are verified successfully the user identity is verified by transmitting the OTP (one time password). If the OTP is submitted correctly the server based authentication is completed.
5. ***Validation response*****:** after completing the verification of user submitted credentials and the one time password the response from the server is generated. If the user provides the correct information the secure server response to the cloud server for authentication steps are completed. Otherwise the secure server couldn't complete the user connection request and produces an error message for the client.
6. ***Secure connection*****:** after successfully validation of user, the system enables communication among the user and cloud server to communicate each other and utilize the different utilities implemented on server using cryptographic techniques. Such as data hosting, access and sharing.

A. Proposed cryptographic technique:

In order to provide the secure and strong cipher generation technique some improvement on traditional DNA based cryptographic solution is suggested. The proposed solution of the cryptography need to enhance for less resource consumption and improved strength of cipher text. Therefore to achieve the required solution for the identified problems, the following solutions for new cryptographic system generation is proposed to incorporate. The method of the encryption is demonstrated using figure 2.

1. ***Input Data*****:** when a user wishes to send, upload, or download the data from the cloud data center then the security is required. In this conditions the user's data is termed here as plain text, original message or text to encrypt. During the process of data request that is user input or the text message that is required to process using the encryption algorithm.

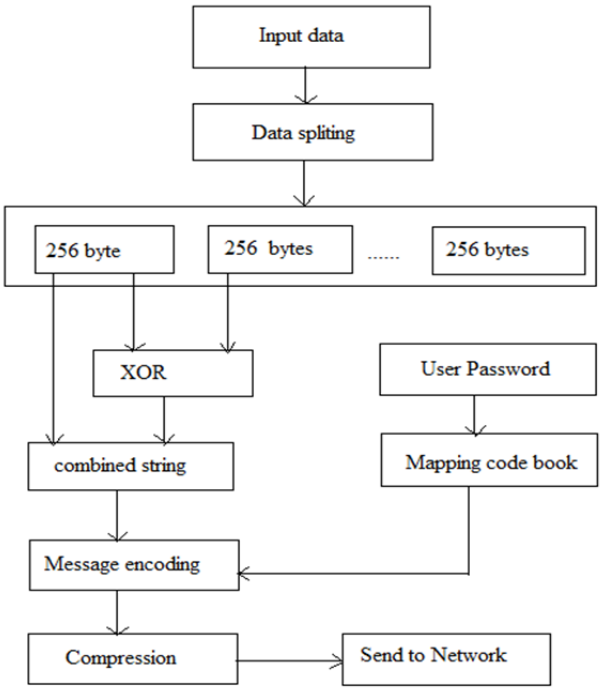


Figure 2 proposed encryption

2. ***Data splitting*:** the user input data is now processed initially in this phase. Therefore the input data is now split in small sizes of the data blocks. The size of these data blocks are 256 bytes. In addition of that if the size of the data block is less than 256 bytes the additional zero bits are appended for completing the length of the 256 bytes. These data blocks are used in next phase for encryption operation.

3. ***XOR operation*:** the previous phase outcomes the fixed size data blocks are paired here first. Each pair of data block contains two blocks of data. In this process the XOR operation is performed first and the outcome of the XOR is combined with any one of the participating block data bytes. For example if there are two blocks of data named as A and B are paired first. For the XOR operation A XOR B = C of the similar length string is generated. Thus the outcome of this process is a combined length of string A and C.

4. ***Password:*** in order to improve the security of the cipher text a user password is required. Using this password the receiver can recover the original data which is transmitted by the sender. This password is used here to generate a dynamic code book. In this code book the characters of password are used with their similar encoding binary sequences.

5. ***The codebook:*** to understand the code book generation process the password is used here. Using this codebook the XOR data is converted or encoded into the similar string as the password provided. For example user enters a password "KANVER" then a dynamic code book is created.

The process of generation of the code book is given in table 1.

K	00
A	01
N	10
V	11
E	000
R	001

Table 1 encoding table

In other hand some time any password string may contain the similar characters or duplicate characters then the process of code book creation is changed by removing the duplicate characters from the input password. For example a user input password is "KANVERLAL". Here characters "L" and "A" repeats 2 times then the given password string is changed in a new string such as "KANVERL" by which the above given table is converted as given table 2.

K	00
A	01
N	10
V	11
E	000
R	001
L	010

Table 2 complex encoding

6. ***Message encoding:*** in this phase the XORed bytes of data are converted in the form of the provided password generated codebook. Therefore the encoding process is taken place. In this process the amount of data is also reduced significantly.

7. ***Compression:*** that is finalization process of cipher text blocks. After encoding of the entire message the generated strings are combined each other and then a ZIP compression algorithm is implemented to reduce the size of cipher more. The final outcome of the encryption process is a compress file. That compress file is used for data exchange between two parties.

8. **Send to network:** the outcomes of the previous step of data processing are used for transmission either during data uploading or for data downloads.

B. Proposed algorithm

The entire process involved in the proposed model for light weight encryption technique for securing the data can be summarized using the simple steps as:

Input: Original Data O_d, User Password U_p Output: Cipher Text C
Process: 1. T_d = readData(O_d) 2. 2. T_d[]= splitData(T_d, 256) 3. T_d^N=XOR_Combine(T_d^i,T_d^{i+1}) 4. MAP = ProcessPassword(U_p) 5. $En_d = encode(T_d^N, MAP)$ 6. C= compressData(En_d) 7. return C

Table 3 cipher generation process

III. RESULTS ANALYSIS

The chapter reports the evaluation of performance of the implemented system. Therefore it includes performance parameters and their descriptions to understand and observations. On the basis of the evaluated behaviour of the system the results are listed in this chapter.

A. Server response time

The amount of time required to execute the user requests for producing the outcomes is termed as server response time. The computed server response time for different activities in the system is given using figure 3.In figure 3 X axis contains the different experimental observations and Y axis shows amount of time required for generating the response from the server. The response time of the server is given here in terms of milliseconds. The different experimental observations show that the fluctuating time for response generation. 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 input file is denoted here as the encryption time. The encryption time of the proposed system and the RSA based cryptographic technique with increasing amount of file size is given using figure 4.

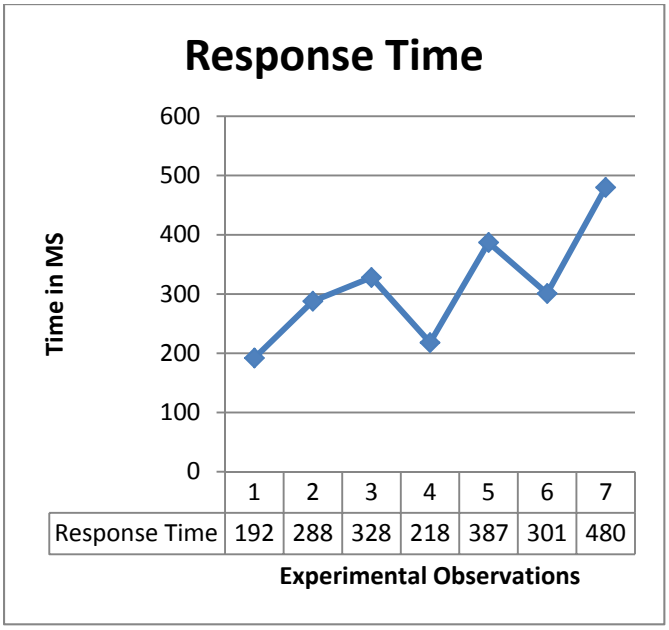


Figure 3 server response time

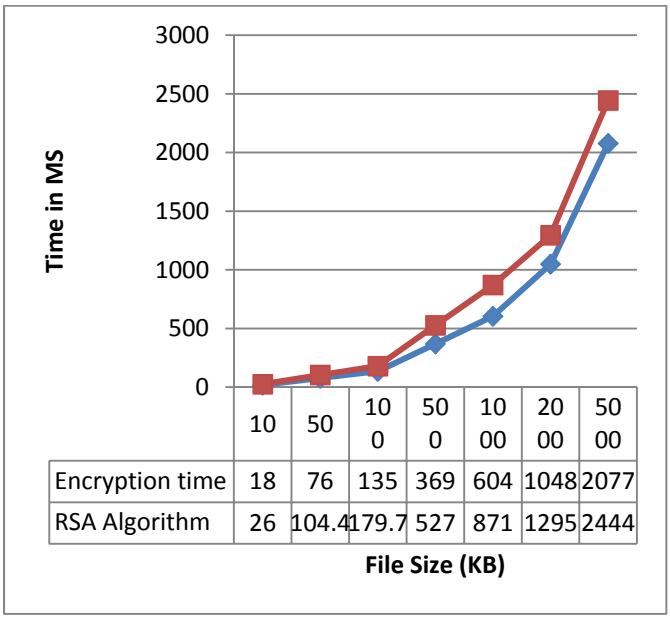
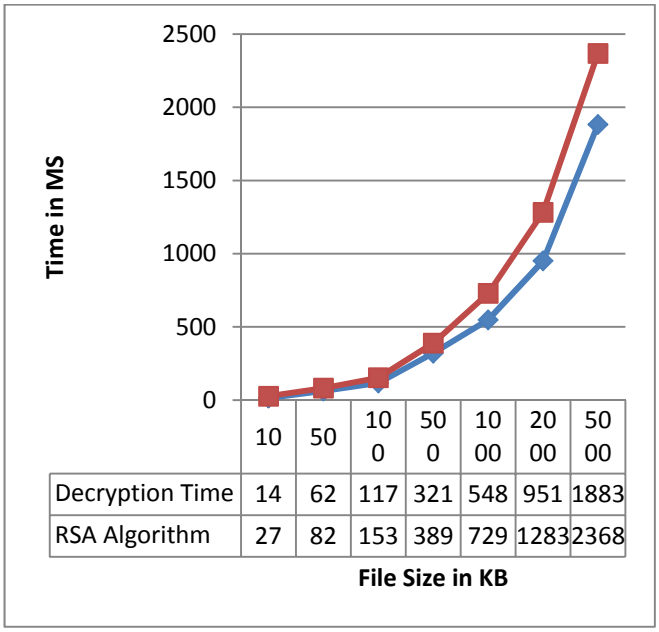


Figure 4 encryption time

In this diagram the different experimental observations are made with increasing amount of file size in terms of KB. The file size used with the system for experimentation is given in X axis. Additionally corresponding amount of time consumed for encrypting file is given in Y axis. The red line in this figure shows the performance of traditional RSA algorithm and the blue line shows the performance of proposed approach. According to the obtained results time consumption for encryption is increases in similar ratio as the amount of data is increases.

C. Decryption time

The amount of time required to decrypt or decipher the encrypted message is known as decryption time. The decryption time with the same amount of file size is reported in figure 5 for both the implemented cryptographic techniques. In this diagram X axis contains increasing amount of files size in terms of KB (kilobytes). And Y axis contains amount of time consumed in terms of milliseconds. The performance of RSA algorithm in this figure is given using red line and the green line is used for providing the performance of proposed algorithm. According to obtained results encryption time is higher than decryption time in all experiments. Additionally demonstrates similar behaviour as encryption process. Furthermore as compared to the traditional technique the proposed technique consumes less amount of time for decryption. Thus the proposed technique is efficient and more adoptable than the traditional approach.

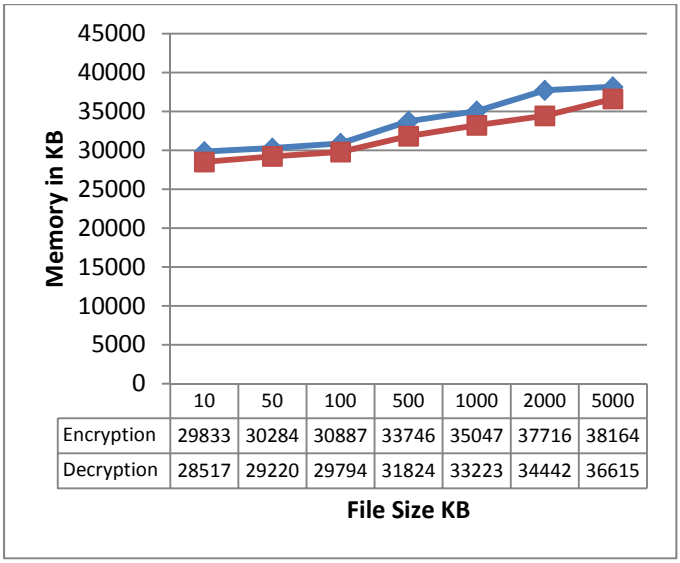


	10	50	100	500	1000	2000	5000
Decryption Time	14	62	117	321	548	951	1883
RSA Algorithm	27	82	153	389	729	1283	2368

Figure 5 decryption time

D. Memory consumption

The amount of main memory required for file encryption or decryption is known as memory consumption or space complexity of the algorithm. The memory consumption of the proposed system and the RSA algorithm during encryption is computed and compared using figure 6. In this diagram the encryption process's memory consumption is demonstrated. The red line shows the performance of proposed technique and blue line is used for traditional algorithm implementation. 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 proposed technique consumes less amount of memory as compared to traditional RSA algorithm. But the amount of memory consumption is increases for both the processes as the amount of data to be process is increases for encryption.



	10	50	100	500	1000	2000	5000
Encryption	29833	30284	30887	33746	35047	37716	38164
Decryption	28517	29220	29794	31824	33223	34442	36615

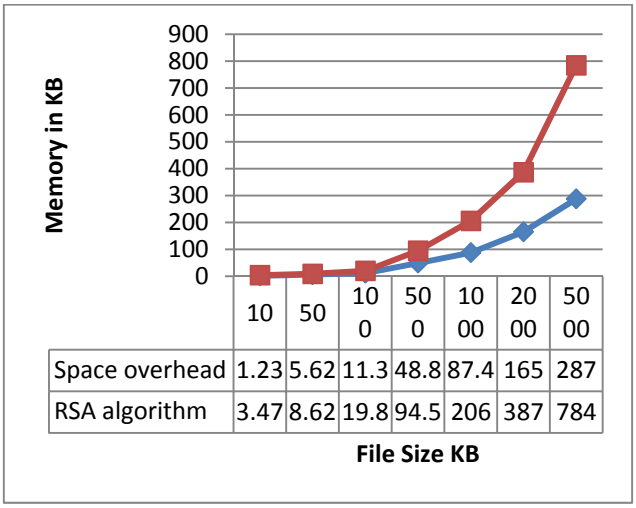
Figure 6 memory consumption

E. *Space overhead*

The amount of additional storage space required when the data is encrypted form their original size of message 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 comparative performance of the proposed and RSA based cryptographic system in terms of KB and demonstrated using figure 7. 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.



	10	50	100	500	1000	2000	5000
Space overhead	1.23	5.62	11.3	48.8	87.4	165	287
RSA algorithm	3.47	8.62	19.8	94.5	206	387	784

Figure 7 space overhead

IV. CONCLUSIONS

In this presented work the cloud based storage security is investigated and for improving the performance of the traditional security based on RSA cryptography a new cryptographic solution is presented with the third party auditor. This section provides the summary of work performed additionally the future extension of the work is also suggested.

A. *Conclusion*

The internet provides ease in our daily life by providing the services at our door steps. Anyone can get the different kinds of service requests and their response using the internet based applications without making any efforts such as banking, e-commerce and others. That's why the traffic on web is increases continuously and to handle this traffic an efficient technique is required. Cloud infrastructure provides the solution for efficient computing and the hosting of data. Due to this a number of individuals and organizations are now adopting the services of the cloud computing. But in cloud the data is moving frequently and availability of data are also changes with the time. Therefore the clients of the cloud are worried about the security of data in data centers.

In this presented work the security of the data center is investigated. In literature a number of articles are suggesting the cryptographic cloud approach for securing the data. but the traditional cryptographic approaches are either less secure or produces the high resource consumption during the encryption and decryption. Thus there is need to have a strong cipher generation technique with less complexity in terms of space and time. In order to provide such kind of solution a new approach using the DNA cryptographic approach is presented to secure the data on cloud additionally this cryptographic approach helps to protect data during the network data exchange. Furthermore for improving the invigilation and authentication process a security auditor is also implemented with the system which provides ease in validation of user request.

The implementation of the proposed working model is provided using the J2SE environment of JAVA technology. After implementation the performance of the implemented system is computed and compared with respect to RSA based cryptographic solution. The comparison of the proposed technique is provided in terms of the following performance parameters listed in below table

S. No.	Parameters	Proposed technique	RSA
1.	Server response	Adoptable	-
2.	Encryption time	Low	High
3.	Decryption time	Low	High
4.	Memory consumption	Low	High
5.	Space overhead	Low	High

Table 4 comparative performance

The key aim of the proposed technique to improve the performance of cryptographic technique in terms of time and space complexity is accomplished successfully. According to the results demonstrated the proposed technique provides security and high performance outcomes. Therefore the technique is adoptable for securing the cloud data center.

B. *Future work*

The proposed work is intended to find a secure solution for the data storage and access in cloud data centers. Therefore different techniques and security schemes are investigated. In addition of that based on the existing approaches a new security model is proposed using the DNA cryptography based technique. In near future the technique is enhanced in the following suggested manner.

1. The attackers and intruders are updating self therefore the cryptographic technique is need to be change after a few months regularly
2. The new advancement on the TPA are developed thus need to change the responsibilities of the TPA over the time.

REFERENCES

[1] Kawser Wazed Nafi, Tonny Shekha Kar, Sayed Anisul Hoque, 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] Torry harris, "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] Milenko Radonic, "Cloud vs. Data Center: What's the difference", http://www.glbrain.com/index.php?r=tool/view&id=2103&toolType=1.

[6] Chittajallu Sai Meghana, "Security and Services Management Aspects of Cloud Architectures", http://www.idrbt.ac.in/PDFs/PT%20Reports/2013/Chittajallu%20Sai%20Meghana_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] M. Geetha Yadav, Dr. N. Chandra Sekhar Reddy, G.Praveen Babu, Ms.I. SuryaPrabha, "Cryptographic Cloud Storage with data sharing and security for Multi access network", IJDCST @Feb-Mar, 2104, Issue- V-2, I-2, SW-16.

[9] 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).

[10] Swapna Lia Anil, Roshni Thanka, "A Survey on Security of Data outsourcing in Cloud", International Journal of Scientific and Research Publications, Volume 3, Issue 2, February 2013.

[11] Krati Mehto, Rahul Moriwal, "A Secured and Searchable Encryption Algorithm for Cloud Storage", International Journal of Computer Applications (0975 – 8887) Volume 120 – No.5, June 2015.

[12] Norman D. Jorstad, Landgrave T. Smith, "Cryptographic Algorithm Metrics", Institute for Defense Analyses Science and Technology Division, January 1997.

[13] C. Chandrasekar, V. Prabhakaran, "A Simple Symmetric Key Cryptographic Algorithm", Vol. 2 Issue 2 ISSN: 2278-7844, 2013 IJAIR. All Rights Reserved.

[14] Sankalp Prakash, Mridula Purohit, "Applied Hybrid Cryptography in Key-pair Generation of RSA implementation", Applied Hybrid Cryptography in Key-pair Generation of RSA implementation IJICCT–JUL 2013;Vol 1,Issue 1;ISSN 2347-7202.

[15] ChaitaliHaldankar, Sonia Kuwelkar, "Implementation Of AES And BLOWFISH Algorithm", International Journal of Research in Engineering and Technology, Volume: 03 Special Issue: 03 | May-2014 | NCRIET-2014.

[16] Norman D. Jorstad, Landgrave T. Smith Jr , "CRYPTOGRAPHIC ALGORITHM METRICS", Directorate for Freedom of Information and Security Review (OASD-PA) Department of Defense, January 1997.

[17] 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.

[18] Victor Chang, Muthu Ramachandran , "Towards achieving Data Security with the Cloud Computing Adoption Framework", IEEE TRANSACTIONS on Services Computing, Volume:9, Issue: 1, Jan.-Feb. 1 2016.

[19] 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.

[20] 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.

[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 Gonales, TCC-2014-03-0102.

[22] Victor Chang, Muthu Ramachandran, "Towards achieving Data Security with the Cloud Computing Adoption Framework", IEEE TRANSACTIONS on Services Computing, Volume:9 Issue:1.

[23] Santosh Kumar Majhi, Sunil Kumar Dhal, "Placement of Security Devices in Cloud Data Centre Network: Analysis and Implementation", International Conference on Information Security & Privacy (ICISP2015), 11-12 December 2015, Nagpur, INDIA, 2016 The Authors. Published by Elsevier.

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

[25] Raja Wasim Ahmad, Abdullah Gani, Siti Hafizah Ab. Hamid, Muhammad Shiraz, Abdullah Yousafzai, Feng Xia, "A survey on virtual machine migration and server consolidation frameworks for cloud data centers", Journal of Network and Computer Applications, & 2015 Elsevier Ltd.

[26] 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 Cloud Computing.