ISSN (Online) 2394-2320

International Journal of Engineering Research in Computer Science and Engineering (IJERCSE)

Vol 5, Issue 3, March 2018

Information Secure Over Unauthorized Attack In Cloud Environment

[1] J. Rajiv Kumar, [2] S. Revathi, [3] N. Sneha, [4] K. Umamaheshwari
[1]Assistant Professor, [2][3][4]UG Student
[1][2][3][4] Department of CSE, VSB Engineering College, Karur

***Abstract* – Cloud computing is a platform to provide different services to the cloud users. User shared the sensitive data over the cloud which gives rise to security issues in cloud computing. So, to protect user's data a secure methodology fragmentation and replication of data is used in this paper. The data is fragmented into pieces and then replicate them over the cloud nodes for maintaining the availability, performance level and backing up the data. T-coloring term is used here which is not giving any idea about locations of the fragments to an attacker. T-coloring method is used to assign the fragments and their replicas to improve the security. Three fish encryption algorithm used to provide high security. Data owner can use their secret key for encrypt the data. Then the files are in ciphertext form. These files are decrypted by the same key that is used for encryption on the receiver end. This system mainly focuses on the data and authentication system with good performance.**

Keywords- T- Coloring Algorithm, Threefish Encryption, DROPS Methodology.

INTRODUCTION

Cloud Computing is a type of internet-based computing which provides resources, virtualization, flexibility, scalability to users. In this methodology, we divide a file into fragments, and replicate the fragmented data over the cloud nodes. Each of the nodes stores only a single fragment of a particular data file that ensures that even in case of a successful attack, no meaningful information is revealed to the attacker. Moreover, the nodes storing the fragments are separated with certain distance by means of graph T-coloring to prohibit an attacker of guessing the locations of the fragments. Data encryption technique is used for data security and implement Three-Fish Cipher algorithm in order to achieve security with minimum number of overheads. Threefish encryption algorithm consists of two factors – fast response and reduced complexity.

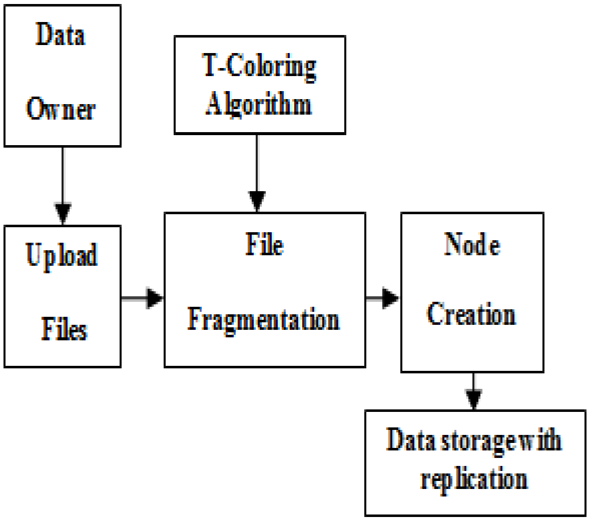
In the existing system, the data are outsourced to a third-party administrative control, gives rise to security concerns. Due to attacks by other users and nodes within the cloud, the data compromise may occur. In traditional cloud storage, the data owner sends copies of files over internet to the data serves, which the records the information to an off-site storage system that is maintained by a third-party. Whenever the data owner wants to retrieve the information, they access the data server through web-based interfaces. The concerns that are facing in existing system are reliability and security. To secure data, most systems use a combination of techniques, including: (i) Encryption is a difficult algorithm is used to encrypt information, (ii) Authentication, which requires creating a user name and password, (iii) Authorization, the data owner lists the people who are authorized to access information stored on the cloud storage system.

In existing system of this security concern, Diffie-Hellman algorithm is used to increase the security aspect. In Diffie-Hellman there is possible to replay attacks. Because if someone is repeatedly trying to access the encrypted file with wrong keys, it might very well be possible that the user is trying permutation and combination to get the correct secret base. Proposed system uses T-coloring and Threefish algorithm to provide more security to the data. Fragmentation in T-coloring algorithm avoids the whole data transferred to the attacker.

T-COLORING FRAGMENTATION:

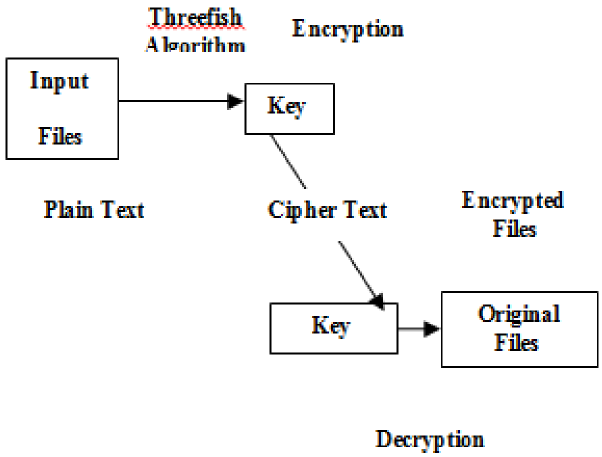
The file fragmented means to be broken up into small pieces. This is exactly what happens to files when they become fragmented. They are broken down into small individual pieces and stored in random locations. This causes less than optimal processing times because it takes longer to read through and find all of the different locations of the file, instead of being able to look in just one location. In a fragmentation schema file f is split into n fragments, all fragments are signed and distributed to n multiples nodes, one fragment per node. The user can reconstruct file f by accessing m fragments arbitrarily chosen.

The fragments allocation provides the security while placing the fragments, the concept of T-coloring is used that was originally used for the node assignment problem. When a fragment is placed on the node, all of the nodes neighborhood nodes at a distance belonging to T are assigned close color. In this process, this loses some of the central nodes that may increase the retrieval time. But it achieves a higher security.



THREEFISH ENCRYPTION:

Threefish is a large, tweakable block cipher. Three fish algorithm consists of three different block sizes: 256 bits, 512 bits, and 1024 bits. The key is the same size as the block, and the tweak value is 128 bits for all block sizes. Threefish consists of just three operations—addition, XOR, and rotations of a fixed amount—all operating on 64-bit words. Threefish-256 and Threefish-512 consist of 72 rounds; Threefish-1024 consists of 80 rounds. Because Threefish only uses simple operations, and because it was designed with performance in mind, Threefish-512 encrypts data at 6.1 clock cycles per byte on 64-bit machines; Threefish-1024 encrypts data at 6.5 clock cycles per byte. Input files are encrypted using threefish algorithm. Data owner can use their secret key for encrypt the data. Then the files are in ciphertext form. These files are decrypted by the same key that is used for encryption on the receiver end. Three fish algorithm give better result in encryption when compared to DES and other encryption algorithms.



PROPOSED SYSTEM:

When data owner wants to send file on cloud server first the user should register, for each registered user a unique secret key is generated. If all credentials are valid then only the user can send file in cloud. After that file is splits, Splitting is used to minimize the total data transfer cost. Fragmentation is a process which cuts every sensitive file into several fragments. For every upload of file a unique secret file key is also generated, so that we can secure our data. The probabilities to find whole fragments are also very low. This proposed system uses a fragmentation technique combined with T-coloring method. Fragmentation is divided into horizontal, vertical and mixed fragmentation.

Data replication methodology is very important in today's popular systems for problems such as data reliability, availability and response time. Data replication means keeping a number of replicas on the same server or on dissimilar servers. In replication data is copied and distributed from one database to another. So, it reduces the workload of the original server. Also the Threefish algorithm is implementing for secure encryption. The threefish block cipher is a tweakable block cipher. Different number of rounds is required for different key sizes of threefish.

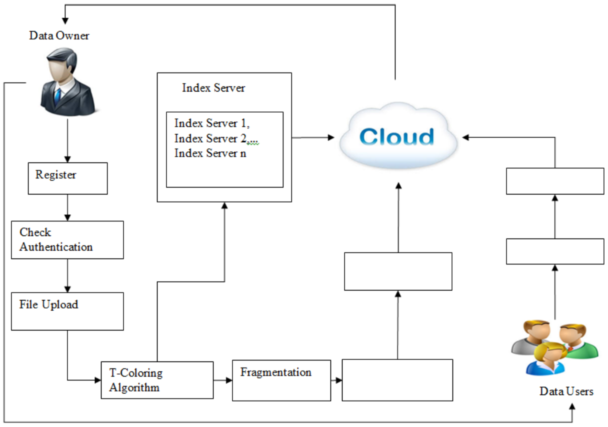
Advantages

• DROPS methodology created to store files in the cloud storage.

• T-Coloring used for node creation in each fragmented files.

• T-Coloring algorithm prohibits an attacker to guess the fragment's location.

• Threefish is a symmetric key algorithm used to encrypt the files.



RELATED WORK:

1. Cloud Security Solution: Fragmentation and Replication

Nowadays the world is known as digital world. As the use of the internet increases day by day, Cloud Computing becomes popular technology among users, customers. The customers are attracted towards the Cloud due to its offers like on-demand network access, reduced space, pay-per-use service, flexibility, scalability etc. Though the remarkable use of cloud computing, there are some hurdles to acceptance. Performance, security, availability, quality of service are the main challenges and issues cloud computing has to face. One of the most barriers is the security because users have to share their information among the cloud nodes. The location of information storage is not known to the user. In this paper, we proposed a new solution which presents the Graphical Authentication System with fragmentation and replication technique. The graphical password authentication provides a security and usability of the proposed system. Here in this system, when user upload any file that the file is fragmented and replicated to provide a better security and performance in terms of access time. When any network is not available to access then, the data will be accessed by using replicas in very short time. T-coloring method is used to assign the fragments and their replicas to improve the security. This system mainly focuses on the data and authentication system with good performance.

2. An Efficient Cloud Security System Using Verifiable Decryption Process

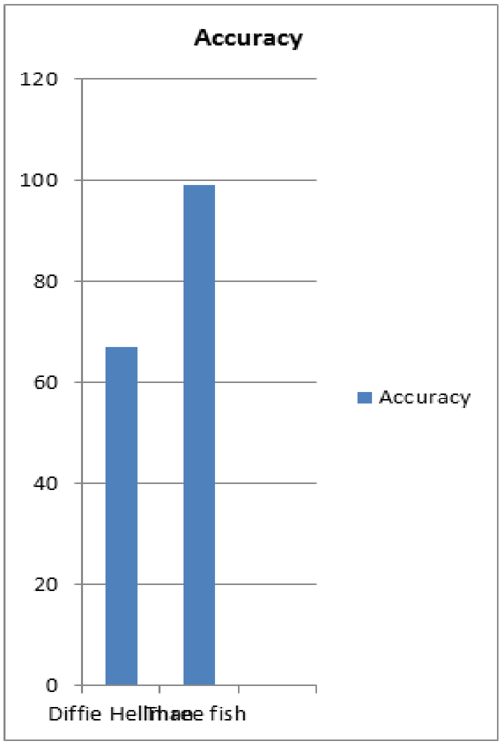
The term cloud computing has the feel of a buzzword any more than the term the web is. Cloud computing is an emerging technology which provides a lot of opportunities for online distribution of resources or services. The most effective benefit of using cloud computing is higher availability of services with lower cost and easy scalability. In cloud computing, usually we transfer the data or submit the data to a third party administrator. It gives rise to security concerns. Even though, there are many security measures applied to protect data, still we are facing some security issues. Therefore, this paper proposes Division and Replication of Data in the cloud for Optimal Performance and Security (DROPS) that provide solution to the existing issues. In this methodology, the files in the cloud storage are encrypted and then divided into number of fragments and replicate the fragmented data over the cloud nodes. To enhance the security, cryptographic technique is used for encryption of data and index server is used to maintain the index terms of the fragments. So that no one can predict either the index terms or the encrypted fragment. Thus the attacker cannot get any meaningful information even in case of successful attack. Finally, it results with higher level of security with slight performance overhead.

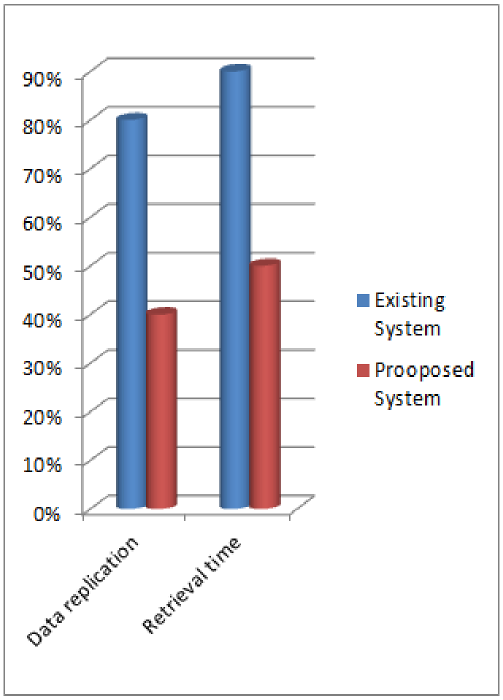
3. Design and Implementation of Three Fish Cipher Algorithm Blocks Using FPGA

In today's world the security has became the major aspect of life. It can be achieved by various techniques such as password, cryptography and biometrics. In this work, to study various encryption algorithms, data encryption standard used for data security and implement Three-Fish Cipher algorithm in order to achieve security with minimum number of overheads then compare the proposed work with test bench and then compile, simulate the test bench with the help of Xilinx ISE software. After the study of various encryption algorithms, the concept of keys has been successfully observed from the observation it has been seen that better secured system can be achieved by increasing the key length. Longer key lengths consume more power and dissipate more heat. Basically it is a tradeoff, between security and overheads. In order to achieve more secured system continuous efforts are required. An efficient encryption algorithm should consist of two factors – fast response and reduced complexity. By keeping the utility of encryption algorithm in secure communication it is desirable to optimize and/or improve the encryption techniques, so security overheads remains under control.

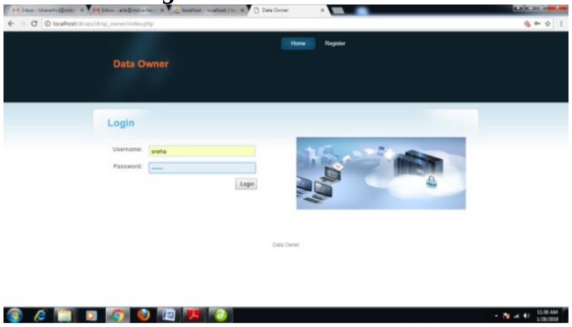
RESULT ANALYSIS:

Comparison Chart





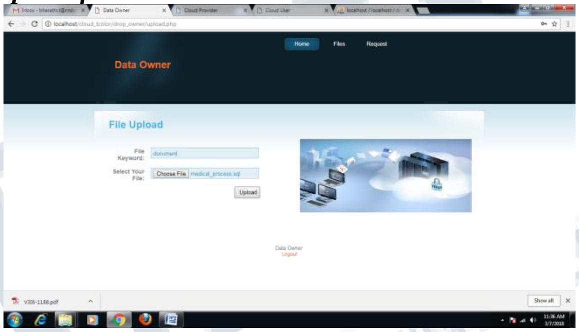
Data Owner Login



Username: sneha

Password: ------

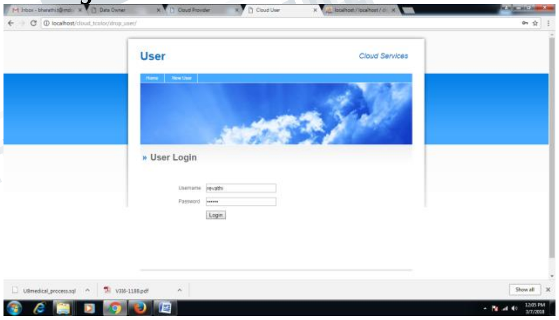
Upload files



File Keyword: document

Select Your File: Choose File medical_process.sql

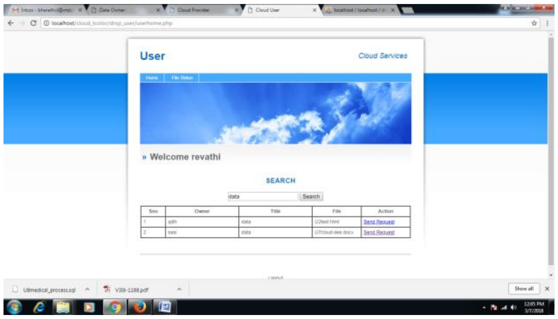
User Login



Username: revathi

Password: ------

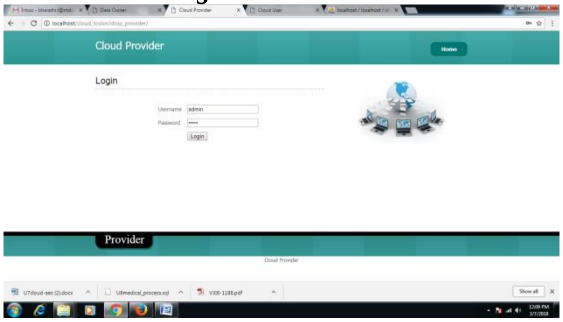
Search Details



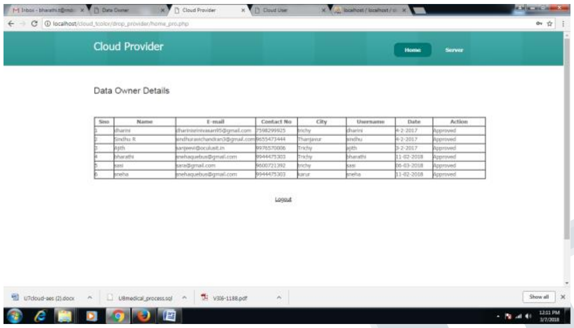
data

Sno	Owner	Title	File	Action
1	ajith	data	U2test.html	Send Request
2	sasi	data	U7cloud-aee.docx	Send Request

Cloud Provider Login



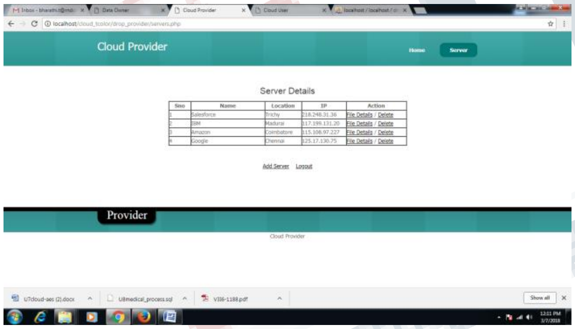
User Details



Data Owner Details

Sno	Name	E-mail	Contact No	City	Username	Date	Action
1	dharini	dharinisrinivasan95@gmail.com	7598299925	trichy	dharini	4-2-2017	Approved
2	Sindhu R	sindhuravichandran3@gmail.com	9655473444	Thanjavur	sindhu	4-2-2017	Approved
3	Ajith	sanjeevi@oculusit.in	9976570006	Trichy	ajith	3-2-2017	Approved
4	bharathi	snehaquebus@gmail.com	9944475303	Trichy	bharathi	11-02-2018	Approved
5	sasi	sara@gmail.com	9600721392	trichy	sasi	06-03-2018	Approved
6	sneha	snehaquebus@gmail.com	9944475303	karur	sneha	11-02-2018	Approved

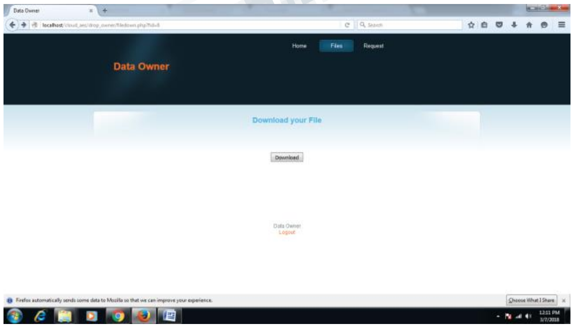
Server Details



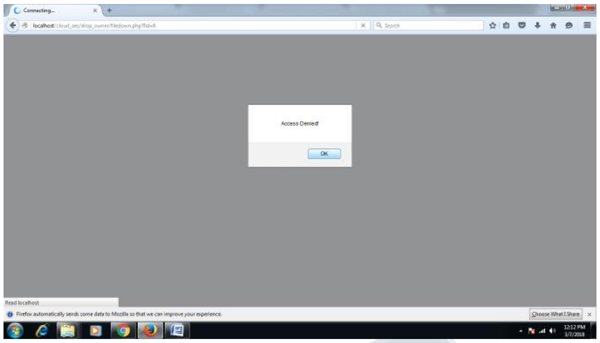
Server Details

Sno	Name	Location	IP	Action
1	Salesforce	Trichy	218.248.31.36	File Details / Delete
2	IBM	Madurai	117.199.131.20	File Details / Delete
3	Amazon	Coimbatore	115.108.97.227	File Details / Delete
4	Google	Chennai	125.17.130.75	File Details / Delete

Unauthorized Access



Access Denied



CONCLUSION:

The cloud storage scheme collectively deals with the security and performance in terms of retrieval time. The user file was fragmented and the fragments are dispersed over multiple nodes. Once the fragment is placed in primary node, remaining nodes are placed over multiple nodes. The cloud manager will store and maintain that primary node for retrieval process. The fragmentation and dispersal ensured that no significant information was obtainable by an adversary in case of a successful attack. Each node in cloud should contain only one fragment. The nodes were separated by means of T-coloring. Using Threefish encryption the key length can be reduced, keeping the same security, in order to optimize the utilization of resources.

FUTURE WORK:

At present work to update and identify the necessary fragments only an automatic update mechanism has to be developed. The time and the resources that are utilized in updating, downloading and again uploading the file will be saved by the above mentioned future work.

REFERENCES:

[1] Mazharali, Kashif Bilal, Samee U. Khan, BharadwajVeeravalli, Keqin Li, Albert Y. Zomaya "DROPS: Division and Replication of Data in Cloud for Optimal Performance and Security" DOI 10.1109/TCC.2015.2400460, IEEE Transactions on Cloud computing.

[2] P. Mell and T. Grance, Draft NIST working definition of cloud computing.

[3] Jun Feng, Yu Chen, Wei-Shinn Ku, Zhou Su "D-DOG: Securing Sensitive Data in Distributed Storage Space by Data Division and Out of- order key stream Generation" IEEE Communications Society subject matter experts for publication in the IEEE ICC 2010 proceeding.

[4] Alessandro Mei, Luigi V. Mancini, and SushilJajodia "Secure Dynamic Fragment and Replica Allocation in Large- Scale Distributed File Systems" IEEE transactions on parallel and distributed systems, vol. 14, no. 9, September 2003.

[5] Parakh A, and Kak S (2009). Online data storage using implicit security, Information Sciences, vol 179(19), 3323–3331.

[6] CongWang, Sherman S.-M. Chow, QianWang, KuiRenandWenjing Lou Privacy-Preserving Public Auditing for Secure Cloud Storage IEEE paper to support US National Science Foundation under grant CNS-0831963, CNS- 0626601, CNS-0716306, and CNS-0831628.

[7] D.H. Patil Rakesh R. Bhavsar and Akshay S. Thorve Data Security over Cloud Emerging Trends in Computer Science and Information Technology 2012 (ETCSIT2012) Proceedings published in International Journal of Computer Applications (IJCA). J. Cryptology, vol. 21,no. 4, pp. 469-491, 2008.

[8] A. Mei, L. V. Mancini, and S. Jajodia, Secure dynamic fragment and replica allocation in large-scale distributed file systems, IEEE Transactions on Parallel and Distributed Systems, Vol. 14, No. 9, 2003, pp. 885-896.

[9] LIU Niansheng, GUO Donghai and HUANG jiaxiang, AES algorithm implemented for PDA secure communication with java, in 2007 IEEE ,DOI:1-4244-1035, vol 5,july 2007.

[10] Deshmukh P M, Gughane A S et al. (2012). Maintaining File Storage Security in Cloud Computing, International Journal of Emerging Technology and Advanced Engineering, vol 2(10),22502459.

[11] Jin Li, Xiaofeng Chen, Xinyi Huang, Shaohua Tang and Yang Xiang ,"Secure Distributed Deduplication Systems with Improved Reliability", IEEE Transactions on Computers Volume, pp.1-12 ,2015

[12] Jin Li, Yan Kit Li, Xiaofeng Chen, Patrick P.C. Lee, and Wenjing Lou ,"A Hybrid Cloud Approach for Secure Authorized Deduplication", IEEE Transactions on Parallel and Distributed systems, vol. 26, pp. 1206-1216, May 2015.

[13] Mazhar Ali,Kashif Bilal, Samee U. Khan,,Bharadwaj Veeravalli,Keqin Li,Albert Y. Zomaya,"DROPS: Division and Replication of Data in Cloud for Optimal Performance and Security",IEEE Transactions on Cloud Computing, pp. 1-15, 2015.

[14] Jian Liu, Kun Huang, Hong Rong, Huimei Wang, and Ming Xian, "Privacy-Preserving Public Auditing for Regenerating-Code-Based Cloud Storage", IEEE Transactions on Information Forensics and Security, Vol. 10, No. 7, 2015.

[15] Backialakshmi.N,Manikandan.M ," Survey based on Secure Authorized Deduplication Hybrid Cloud Approach", IJIRST –International Journal for Innovative Research in Science & Technology, Vo1.1 ,Issue 9, pp. 164-165, 2015.

[16] Ritu Tripathi, Sanjay Agrawal, "Comparative Study of Symmetric and Asymmetric Cryptography Techniques," International Journal of Advance Foundation and Research in Computer (IJAFRC), Volume 1, Issue 6, June 2014. ISSN 2348 – 4853.

[17] Malek Jakob Kakish, "Security Improvements To The DIFFIEHELLMAN Scheme,“ International journal of Engineering and Technology July 2011892, pp.68–73.

[18] Manku, KV Saikumar, and K. Vasanth. "Blowfish encryption algorithm for information security." ARPN Journal of Engineering and Applied Sciences 10.10 (2015): 4717-4719.

[19] NehaKhatri–Valmik, Ms, and V. K. Kshirsagar. "Blowfish Algorithm." IOSR Journal of Computer Engineering 16.2 (1994).

[20] Sehgal, Parth, Nikita Agarwal, Sreejita Dutta, and PM Durai Raj Vincent. "Modification of Diffie-Hellman Algorithm to Provide More Secure Key Exchange." International Journal of Engineering & Technology: 0975-4024.

[21] Forouzan, A. Behrouz. Data communications & networking (sie). Tata McGraw-Hill Education, 2006.

[22] T. K. Hazra and S. Bhattacharyya, "Image encryption by block wise pixel shuffling using Modified Fisher Yates shuffle and pseudorandom permutations," 2016 IEEE 7th Annual Information Technology, Electronics and Mobile Communication Conference (IEMCON), Vancouver, BC, 2016, pp. 1-6. doi: 10.1109/IEMCON.2016.7746312.

[23] T. K. Hazra, R. Ghosh, S. Kumar, S. Dutta and A. K. Chakraborty, "File encryption using Fisher-Yates Shuffle," 2015 International Conference and Workshop on Computing and Communication (IEMCON), Vancouver, BC, 2015, pp. 1-7.doi: 10.1109/IEMCON.2015.7344521

[24] Sreejit Roy Chowdhury, Tapan Kumar Hazra, Ajoy Kumar Chakroborty, " Image Encryption using pseudo random permutations," American Journal of Advanced Computing, 1.1 (2014), doi: http://dx.doi.org/10.15864/ajac.v1i1.2

[25] Li, Chengqing. "Cracking a hierarchical chaotic image encryption algorithm based on permutation." Signal Processing 118 (2016): 203- 210.