Design for secure data sharing in multi clouds using Luby Transform codes with DES

[1] Saranya.J, [2] Dr.D.Suganya Devi
[1]Mphil. Scholar, [2] Assistant professor
[1]Department of Computer Science,
[1]Government Arts College, Udumalpet, India

***Abstract*— The cloud data processing is the vision of the processing as value, in which cloud consumer possibly stores its data into the cloud environment over enjoying the first class quality servers and the fast nets, into which applications store and into the services of a divided pool of configurable operational resources. The cloud provides IT services based on Internet and provide a scalable service to easily consume over the Internet on an as-needed basis. A major feature in cloud service is that data processed on clouds are often outsourced, leading to number of issues related to accountability including the handling of personally identifiable information. In this research work, the data storage can provide the security using multilevel encoding and decoding scheme using Luby transform code and DES in multi cloud environment with file access and distribution based integrity security. This work aims to promote the use of multi clouds due to its ability to reduce security risks that affect the cloud computing user. It also suggests that it is better to shift from single to multi clouds for better security.**

***Index Terms*—Cloud Computing, LT Code, Multi cloud security**

I. INTRODUCTION

Cloud computing is a computing model, where a large amount of systems are connected in private or public networks, to provide dynamically mountable infrastructure for applications and different types of data storage. With the commencement of this technology, the computational cost, application hosting, content storage and delivery is reduced significantly.

Cloud computing is the next step in the progression of on-demand information technology services and products. The Cloud is a way of computing in which IT-related capabilities are provided ―as a service, permitting users to access technology-enabled services from the Internet (i.e., the Cloud) without understanding of, knowledge with, or control over the technology infrastructure that supports them. The Cloud Computing helps to share data and other resources between the cloud service users, cloud associates, and cloud vendors.

The research and development of cloud computing brings many solutions to the distributed storage structures of clouds. The Cloud computing service providers offers various services to the consumers of distributed computing with efficient storage capacity. Cloud computing is a different form of distributed computing that offers various services on the basis of pay per use [1].

1.1. MULTICLOUD

Multicloud is using more than one cloud computing services in a single heterogeneous architecture. To establishing the multicloud architecture the various reasons should be considerable like decreasing assurance on any single vendor, increasing flexibility through choice, and tempering against disasters. It is similar to more than one developer uses the software/applications on a personnel computer. It is gratitude of the fact that no one provider can be everything for everyone. It varies from hybrid cloud environment in that it refers to multiple cloud services rather than multiple organization modes such as public, private, and legacy.[28]

Various issues are also available in a multicloud environment. Security and authority is more complicated, and more "moving parts" may create resiliency issues. Selection of the right cloud products and services can also be a challenge, and consumers may suffer from the contradiction of choice.[29]

1.2. REVIEW OF LITRATURE

Mohammed A. AlZainfocuses on the security issues and solutions related to the single cloud and multicloud. In the recent years, it shows that the research into the use of multicloud providers to maintain security has received less attention than the use of single cloud. The aim of the work is to promote the use of multi-clouds by reducing security risks which affects the cloud computing consumer.[2]

Cong Wang, Qian Wang, KuiRenNingCaoandandWenjing Lou proposed a flexible distributed storage integrity auditing mechanism, utilizing the homomorphic token and distributed ensure-coded data to attain secure and reliable cloud storage services. The proposed design supports secure and efficient dynamic operations on outsourced data, including block modification, deletion and append. [3]

In recent years, various issues related to security have been discussed. Possible solutions for these security risks and threats have been studied. Solutions related with application, accessibility, authentication, data verification, tampering, loss and theft, privacy and control, physical access, data confidentiality, trusting computation are discussed by AbhinayB.Angadi, AkshataB.Angadi, KarunaC.Gull.[4]

Security issues in three deployment models i.e. IaaS, PaaS, SaaS are discussed.[5]. In SaaS model, there are traditional security which are related with authentication and authorization, availability, data confidentiality and virtual machine security and cloud specific security issues include information security, network security, resource locality, cloud storage, data segregation, data access, web application security, backup, identify management. To increase the security in cloud computing we need the help of threats and counter measures. [6][7]

In this paper, security in multicloud is provided using the AES encryption algorithm because AES is considered as a secure algorithm. Encryption and decryption time is minimum while using AES algorithm as compared to others. So it is fastest block cipher algorithm amongst all analyzed cipher algorithms such as blowfish, DES, triple DES.[8].

II. CLOUD SECURITY MODEL

The figure 2.1 shows a systematic model looking the cloud data storage service which makes available for share data separating services as well as efficient data recovery and repair service including four different entities: Data owner, data user, cloud server, and third server. The data owner springs the encrypted fragments of the file m to N as a storage server to indicate cloud servers.

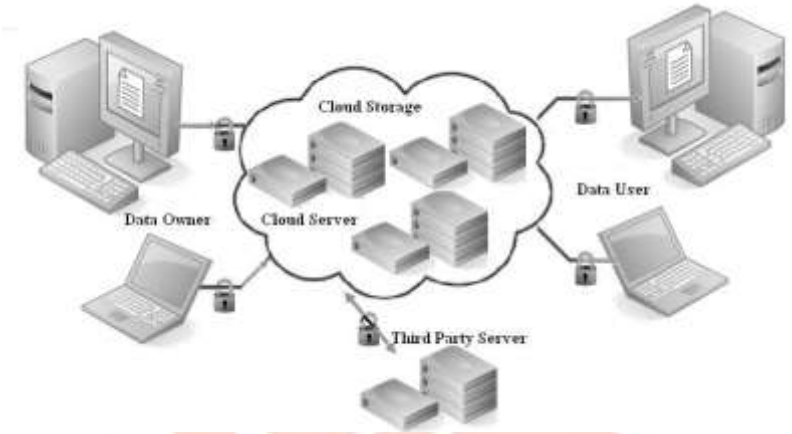

Figure 2.1. Cloud Storage System Model

If the data owner the holds of the data contents confidentially which require file m can be first encrypted before the encoding. Separated data are added by metadata like verification tags to make available integrity control-ability. After the data separating a data user from some k storage server can select to retrieve coded segments, and to regain the file m which can be further deciphered, in case of that the file encrypted is. In the meantime, the third server checks regularly the integrity of data supplied in cloud servers. Fruitless cloud servers can be repaired with the help of other healthy cloud servers. In this available model many threats have, the cloud server is looked as "curious and-vulnerable". Our suggested new model of the system conquered by a lot of screenplay like to make available sure and reliable clouds data storage services should reach our design at the same time achievement guarantees during the data recovery and repair.

III. PROPOSED SECURITY MODEL

In the proposed a design for secure data sharing in a multi cloud storage environment by using multilevel encryption scheme, LT Codes Encryption and DES Encryption standard are used to encrypt the user data before upload to the cloud storage with user access authorization and security keys like file access key, distribution key, private key and public key.

In this proposed scheme, users are classified into two types such as data owner and consumer. Data owner can upload the file after completion of two level encryptions and provide the uploaded file access rights to the data consumer. File access key is sent to the consumer through SMS. Data Consumer can access and download the file after completion of key verification and two level decryptions process. LT Codes and DES encryption standards are used to encrypt and decrypt the file. Registered data owners/ consumers can upload/download the files to/from the multi cloud server environment after their login.

In the encryption process, initially data owner will select the file to upload and generates the access key, private key and public key. Selected file will be splitted and store in the storage node and perform the LT code encryption process. After completion of LT Code encryption, DES encryption process will be performed and two level encrypted file will be uploaded in the multi cloud environment.

Data owner provides the file access rights to the data consumer based on their request. File access rights information and access key are sent to the data consumer's module through SMS. Data Consumer will request the file and provides the file access key. After completion of validation of file access key, data consumer will get the encrypted file, distribution key and public key. In the decryption process, DES decryption process will be performed in the encrypted file and after completion of this decryption process LT Codes decryption process will be performed. After completion of these two level decryption processes, Data consumer can download and view the original data file.

RNG Crypto Service provider is used to generate the file access and distribution keys. File access key is used for data consumer's file access request and distribution key is used to upload and download the encrypted file to/from the multi cloud server.

Each user's MAC Address and IP Address are to be fetched at the time of each login session and maintained by this proposed system for further security. SMS Gateway is used to send the file access details with key to the data consumer by the data owner.

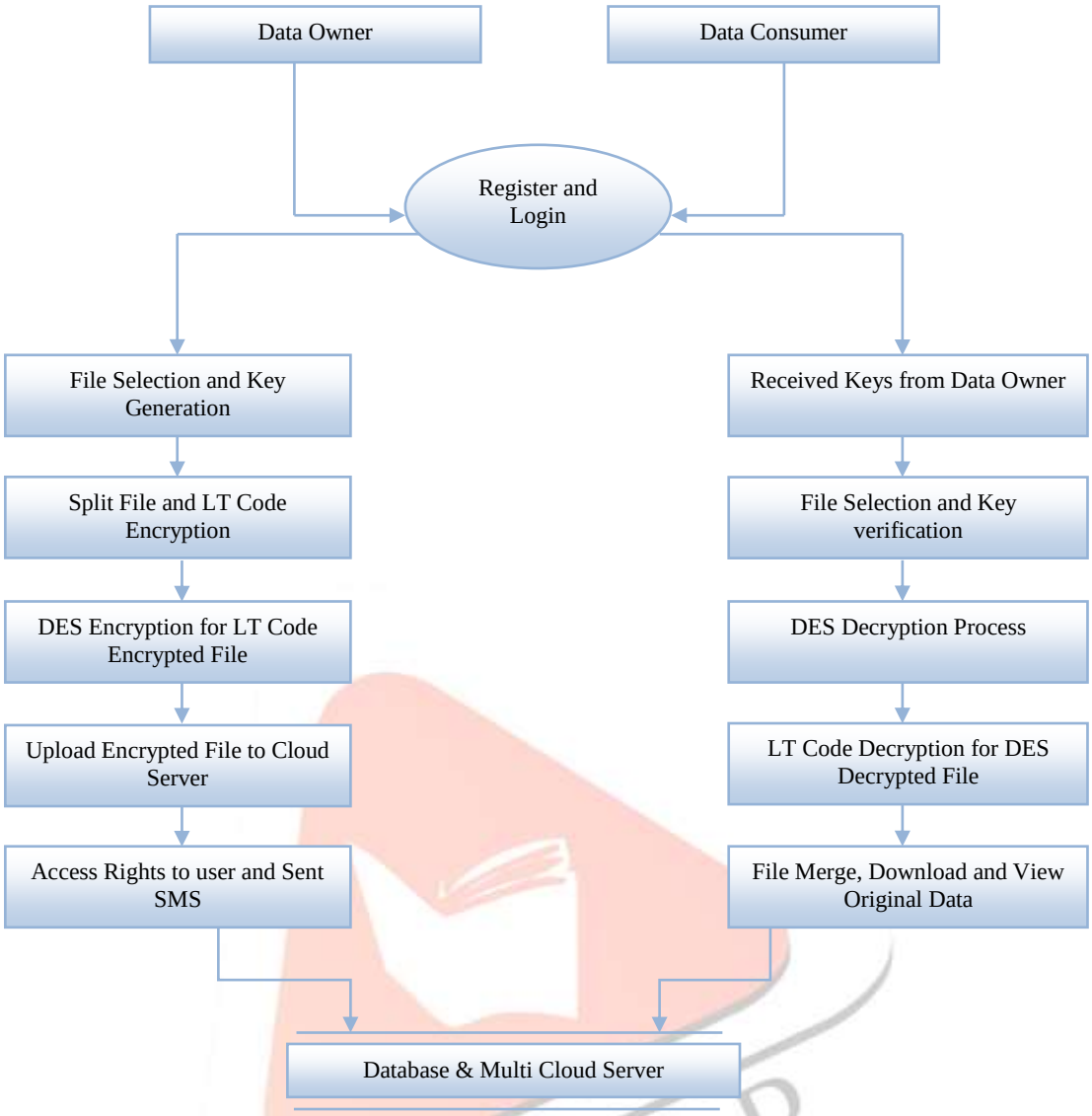

Figure 3.1. The proposed model

The Data Owners of this proposed system performs the following activities

1. Perform the registration process with personal contact and login access details. After completion of successful login process, the registered data owners can login into this system.
2. During the login authentication process, session id is generated based on the data owner's id, MAC address and IP address which are fetched from the client system which one is used to perform the login process by the data owner.
3. After completion of successful login, data owner will get the data owner's page. It allows the owner to edit the existing profile, performing the multilevel encryption and upload process, specify the access rights to the data users for retrieval of uploaded data, view the uploaded files and also view the session details.
4. In the multi level encryption process, data store id is automatically generated based on the user id. Data owner will select the file which is to be encrypted and uploaded to in the cloud server. After selection of file, file properties are extracted by this system such as file type, file name and size of file. File access key, file distribution key, private key and encryption keys are dynamically generated using RNG Crypto service provider. File access key is used to access the file from the cloud server. Distribution key is used to split and distribute the file. Private and encryption keys are used to perform the encryption and decryption process. In the encryption process, selected file is divided into various blocks based on the file size and perform the first level encryption process in the blocks using LT codes. After that the blocks are merged together and perform the second level encryption process using AES encryption process. Multilevel encrypted file is uploaded into the multi cloud storage with access rights and key details.
5. In the Access rights process, data owner can assign the access rights to the data users with key specifications. Data store id and key details are sent to the data users through SMS using SMS gateway with HTTP Request.
6. Data owners can view their uploaded file specification and also session details.

The Data users of this proposed system performs the following activities

1. Perform the registration process with personal contact and login access details. After completion of successful login process, the registered data users can login into this system.
2. During the login authentication process, session id is generated based on the data owner's id, MAC address and IP address which are fetched from the client system which one is used to perform the login process by the data users.
3. After completion of successful login, data users will get the home page. It allows the edit the existing profile, perform the multilevel decryption and download process after completion of file access validation and key verification.
4. In the multi-level decryption process, data users should enter the data store id and access keys to get the encrypted file properties and decrypted keys. Data store id and file access key are received by the data users through SMS. After verification of file access key, user can download the encrypted file from the multi cloud server and perform the multi-level decryption process. In the first level decryption process, DES decryption process will be performed in the encrypted file and after completion of this decryption process LT Codes decryption process will be performed. After completion of these two level decryption processes, Data consumer can download and view the original data file.

IV. IMPLEMENTATION, RESULTS AND DISCUSSIONS

4.1. IMPLEMENTATION

Privacy and security of data and files are the two major concerns for users of cloud system. For privacy reasons, it is desired that intruders cannot outsourced important documents to their owners. A scheme is proposed that employs multi cloud networks with cryptography for achieving unobservable data access.

The implementation of the proposed secured data storage and access model are described below

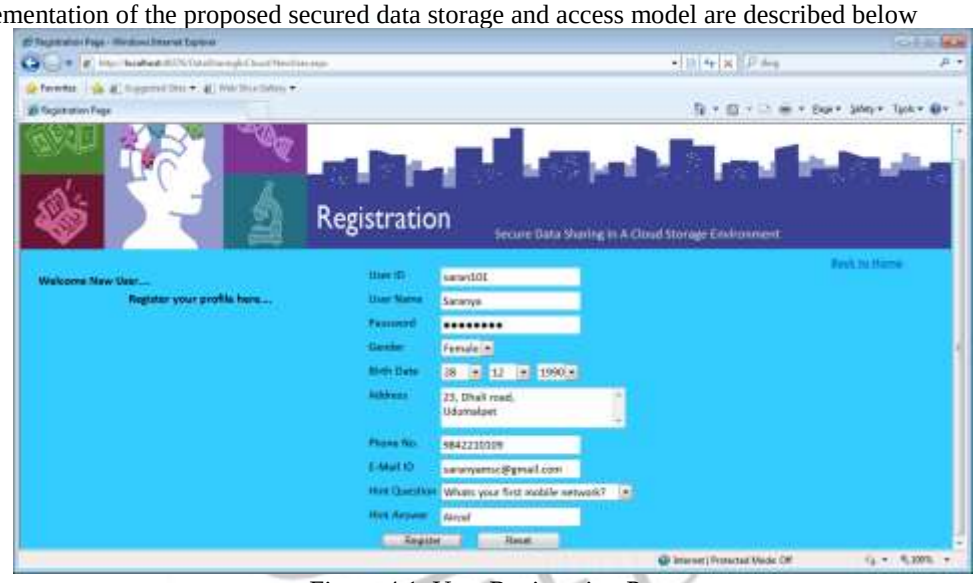

Figure 4.1. User Registration Page

Users of this system are data owner and the data user. The responsibilities of key users are described below.

1. Data Owner is responsible for creating account, select the files to be uploaded, perform the double encryption process, generation of file access and distribution keys, upload the encrypted file in the multi cloud storage, granting file access rights to the data users and send the file access keys to the data users.
2. Data User is responsible for creating account, receiving the file access rights, access the file after validation, perform the decryption process and download the file.

Figure 4.2. Login and Session Establishment

The login process is performed after the completion of successful data owner/user registration process. In the login process, a Unique session id is created for each and every login of the data owner and consumer, then it fetches the MAC and IP address of the system which is used to login into this application. The process ensures that no unauthorized user /access can observe the linkage between a user's home page and its link pages.

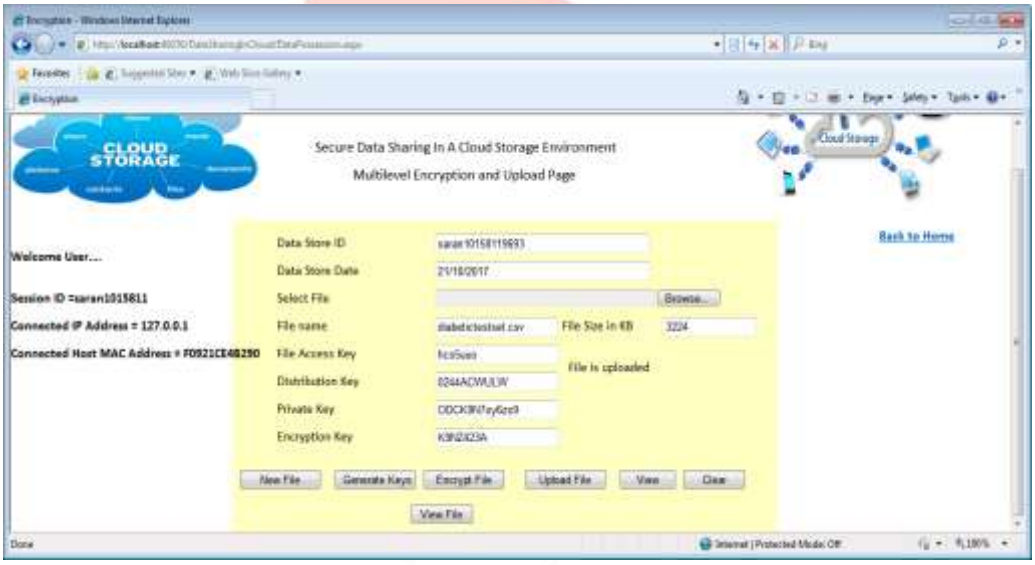

Figure 4.3. Multilevel encryption and Upload Page

This page is accessed by the data owners and performs the data store id creation, file selection, access and distribution key generation, encrypt the file using LT codes and DES, view the encrypted file and upload the encrypted file in the cloud server. Data store id created before the selection of file. Creation of data store id is based on the data owners id and uploaded period. After selection of file, it finds the file size and determines the number of blocks. Selected file is to be splitted based on the block count.

File Access key and Distribution keys are generated for the file using Random Number Generator(RNG) crypto service provider. Generations of keys for encryption and decryption process of data are based on the DES algorithm. In the encryption process, selected file will be splitted into N number of blocks and stored in the storage node and perform the LT code encryption process. After completion of LT Code encryption, DES encryption process will be performed and two level encrypted file will be uploaded in the multi cloud environment. Microsoft Azure tool kit (SDK) is used to upload the files in the cloud environment.

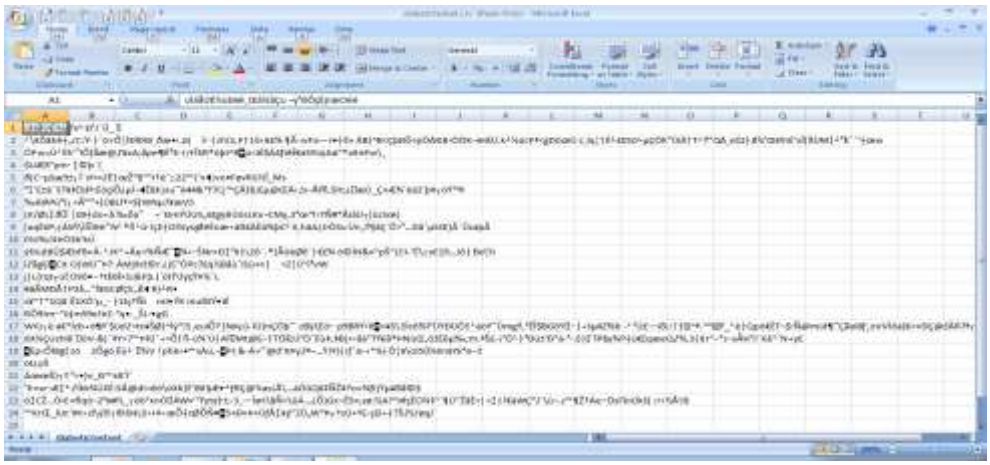

Figure 4.4 Encrypted File

This system allows the data owner to view the multi level encrypted (LT Codes and DES Encryption) file before the uploading of file in the multi cloud storage environment. Multilevel encryption process is performed in the content of the file and it changes the content in to encrypted format and stores in the same file.

Figure 4.5 Uploaded File List with keys

Data owner can view the uploaded file list with uploaded session, name of the file and keys which are used to access, distribute, encrypt and decrypt the file with data store id and uploaded date. Data owner can view their uploaded files only. Files which are uploaded by the others can't be viewed by the data owner.

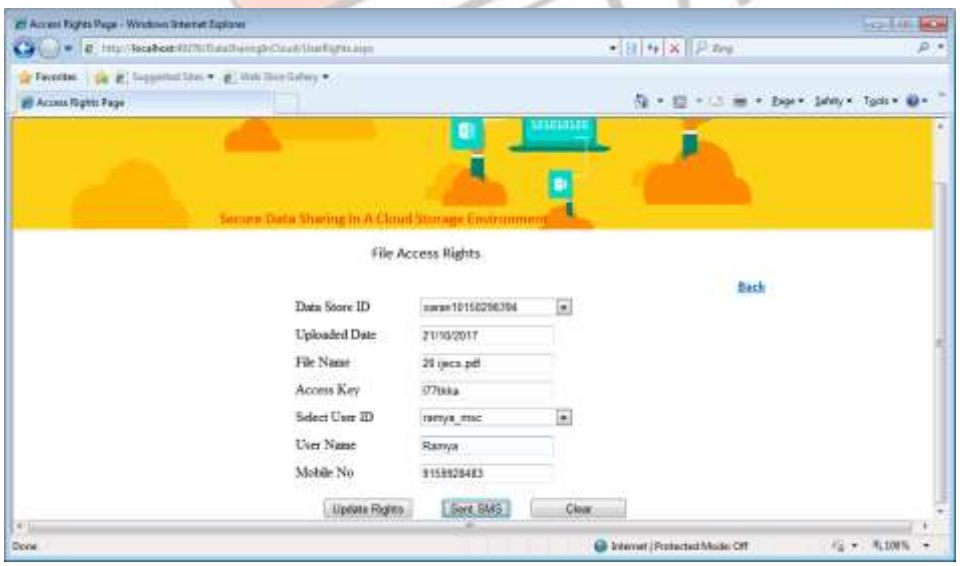

Figure 4.6. File Access Rights updated by the data owner

Data owner will grant the access rights to the data users and sent the information to the data user's mobile number by using SMS gateway and its API. Message consists of data store id, file name and access key. It helps to provide more security to the stored files and prevents unauthorized access of the files. Updated access rights are validated at the time of data user's access of the particular file. After completion of verification, this system allows the users to access the file and also its relevant keys such as distribution key and decryption key.

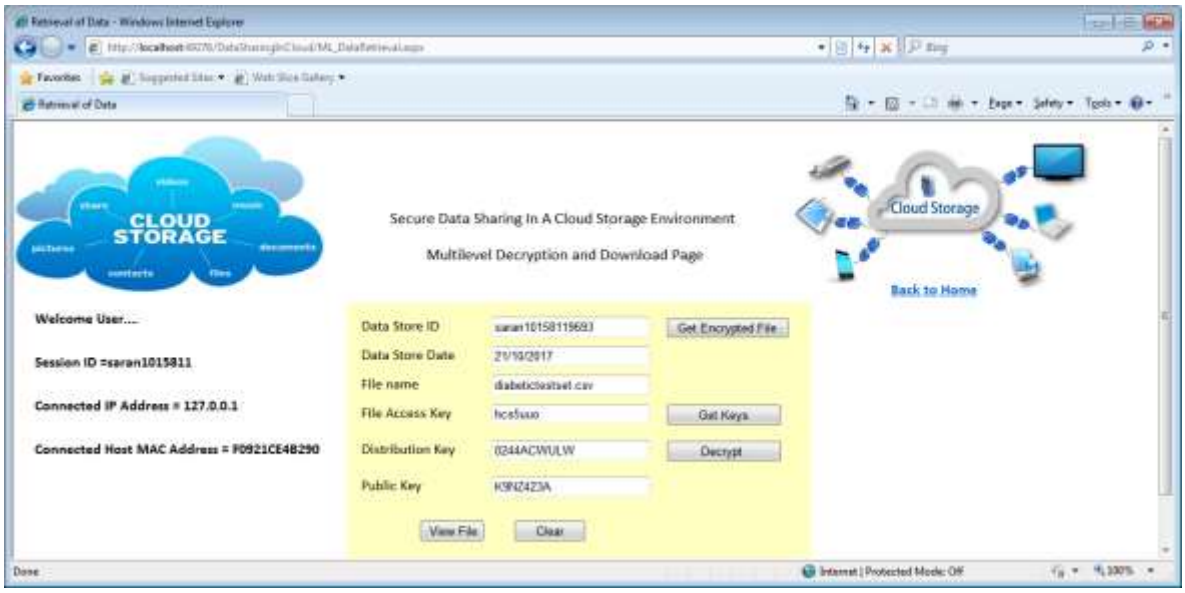

Figure 4.7. Download and Decrypt the File by the data user

This page is accessed by the data user and performs the file access, decrypt, download and view the decrypted file process. Data store id should be entered by the user and gets the decrypted file. File access key helps to get the distribution and public keys. After the completion of file access key verification process, user will get the distribution key and public key. It helps to decrypt the uploaded encrypted file. First it performs the DES decryption process using its public key. After completion of DES decryption process, LT code decryption process will be performed. In the decryption process, downloaded encrypted file will be decrypted using DES decryption process with its public key. After completion of DES decryption process, LT Code decryption process will be performed and two level decrypted file will be viewed by the data user.

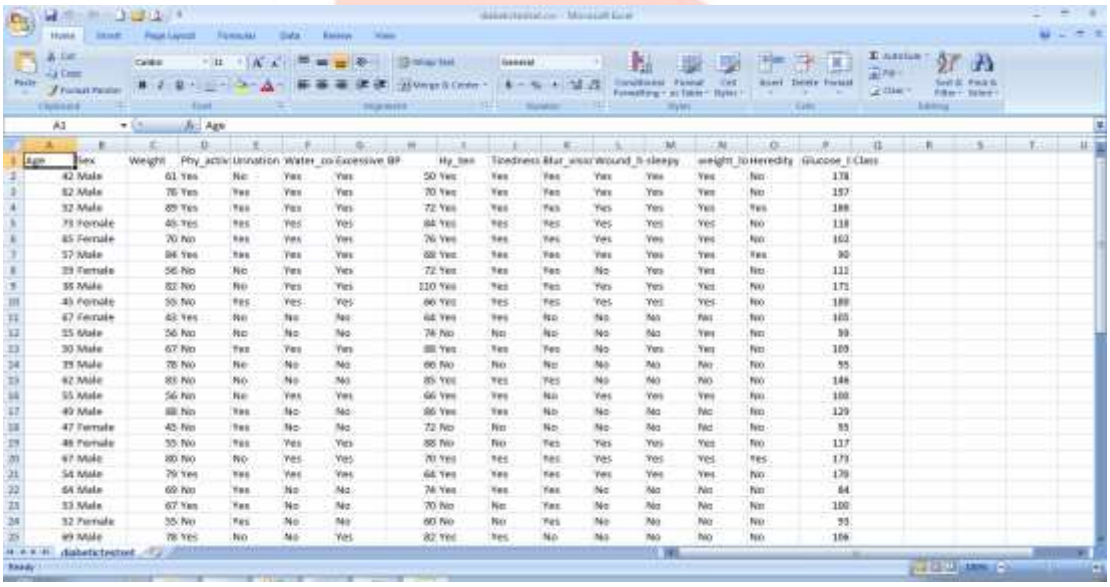

Figure 4.8. Decrypted File View

This system allows the data user to view the multilevel decrypted (LT Codes and DES Encryption) file. Multilevel decryption process performed in the content of the file and it changes the encrypted content into its original data.

4.2. RESULTS AND DISCUSSIONS

Security

To secure data, can be used confidentiality, available multilevel encryption technologies or file access controlling patterns before the encoding process which keep the cloud server from trying to investigate outsourced data. In relation on the data integrity of transforming to itself Luby Coding system uses different cryptographic tags to resist the attack during the data repair and recovery procedure. Multilevel encryption process with LT Code and DES encryption standard Coding system is surely also against the replay-attack which is presented in the net Cong founded cloud data distributed storage system.

Key Management

For additional security, File access key and distribution key are generated by this system. File access key is used to protect the encrypted file from the unauthorized users or intruders of the cloud. Distribution key is used to verify the file at the time of upload and download data in the cloud. RNG crypto service provider is used to generate these keys. In the existing systems, Integrity verification will be performed after the whole files or some blocks of the file are downloaded. In our proposed

system, integrity verification will be performed before file downloading process and keys are verified after completion of downloading process of the encrypted files.

Private verifiability and Privacy preserving

At any time, the data owner can verify the integrity of data stored in the cloud storage using the file id and also data owner id. During the verification process, the cloud service provider cannot obtain any information since the file is in multilevel encrypted form.

Time Complexity

The data owner is not dividing the file into blocks and generating any tags for the blocks at the time of file upload into multi cloud storage. The computation is done by the cloud server only. Data owner finds and calculate the top values only. So the time for verifying the integrity and availability of the files is greatly reduced.

Table 4.1 and figure 4.9 show the comparative analysis of execution time required for various strategies and methods.

Table 4.1. Time Efficiency in Seconds

No of Files	LT Model	Proposed Model
5	1.5	1.0
10	2.4	2.2
20	4.1	3.9

The above table reveals that the proposed security model have less execution time when compares to existing LT model.

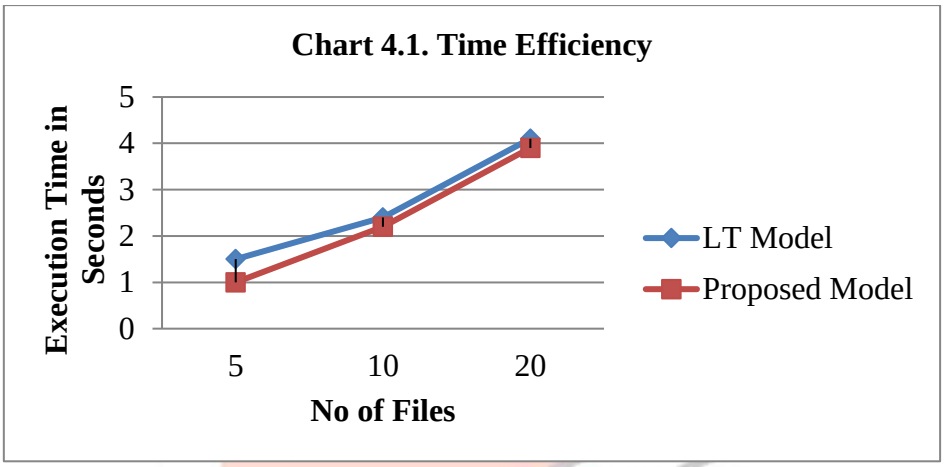

Figure 4.9 Time efficiency chart

Space Efficiency

The size of the original file is also important for the calculation. The size of each source file is 512 KB. The run time complexity of the algorithm is O (log (n)).

Table 4.2. Space Efficiency in KB

No of Files	LT Model	Proposed Model
1	184.5	182.2

The above table reveals that the proposed multilevel encryption based security model have less memory space when compares to existing LT model.

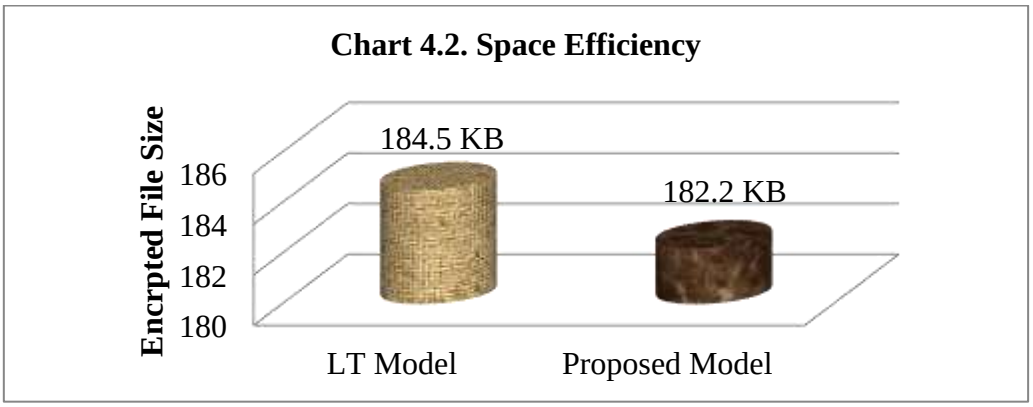

Figure 4.10 Space efficiency chart

CONCLUSION AND FUTURE ENHANCEMENT

It is clear that whereas the use of cloud computing has quickly expanded; cloud computing security is always advised the major issue in the cloud computing natural environment. Data owners do not want to misplace their personal data as an outcome of malicious insiders in the cloud. The purpose of this work is to secure the data storage on multi-clouds to address the security dangers and answers. It has found that much study has been done to ensure the security of the single cloud storage and multi-clouds have gained less attention in the security. This work supports the migration to multi-clouds due to its ability to decline security risks that sway the cloud computing user with multilevel encryption and decryption standard. Although a detailed analysis and comparison of different scheduling strategies is out of the scope of this paper and it is planned for further research, for the sake of completeness, in order to highlight the main benefits of multi-cloud environment capabilities.

Finally optimal data storage retrieval schemes with multi encryption and decryption scheme given requirements on success decidability. Our implementation results suggest a fundamental trade-off between the file-retrieval delay and the target probability of successful file decoding, and that the file-retrieval delay can be significantly reduced by optimally scheduling packet requests in a multi-stage fashion.When compared to existing LT model, the proposed model provides better performance in the execution time efficiency and also memory space efficiency.

FUTURE ENHANCEMENT : Cloud computing gives many advantages like security in data storage with huge storage space, reduce the storage maintenance cost and decreases overheads on cloud, users. This research work primarily concentrates on security and also privacy issues in multi-cloud storage. Further, to enhance the security for the data / data owners, intruders / attackers detection and denial system to be included with this work.

REFERENCES

[1] David S. Linthicum, Cloud Computing and SOA Convergence in Your Enterprise: A Step-by-Step Guide 1st Edition, Addison-Wesley Information Technology Series

[2] Mohammed A. AlZain, Eric Pardede , Ben Soh , James A. Thom “Cloud Computing Security: From Single to Multi-Clouds ”in 45th Hawaii International Conference on System Sciences,2012.

[3] Cong Wang, Qian Wang, KuiRenNingCao and Wenjing Lou, “Towards Secure and Dependable Storage Services in Cloud Computing”,2011.

[4] Abhinay B.Angadi, Akshata B.Angadi, Karuna C.Gull,” Security Issues with Possible Solutions in Cloud Computing-A Survey” in International Journal of Advanced Research in Computer Engineering &Technology (IJARCET) Volume 2, Issue 2, February 2013.

[5] AnujKumarYadav, Ravi Tomar, Deep Kumar and Himanshu Gupta,” Security and Privacy Concerns in Cloud Computing” in International Journal of Advanced Research in Computer Science and Software Engineering,Volume 2, Issue 5, May 2012.

[6] Rashmi, Dr.G.Sahoo, Dr.S.Mehfuz,”Securing Software as a Service Model of CloudComputing: Issues and Solutions” in International Journal on Cloud Computing: Services and Architecture (IJCCSA) ,Vol.3, No.4, August2013.

[7] Keiko Hashizume, David G Rosado, Eduardo Fernández-Medina and Eduardo B Fernandez,” Ananalys is of security issues for cloud computing”, in Journal of Internet Services and Applications 2013.

[8] Sumitra,” Comparative Analysis of AES and DES security Algorithms” in International Journal of Scientific and Research Publications, Volume 3, Issue 1, January 2013.

[9] Jen-Sheng Wang, Che-Hung Liu, Grace TR Lin, How to Manage Information Security in Cloud Computing, 978-1-4577-0653-0/11, IEEE, 2011.C. Cachin, I. Keidar and A. Shraer, Trusting the cloud, ACM SIGACT News, pp. 81–86, 2009.

[10] Odunayo O. Owopetu, Private Cloud Implementation and Security, Bachelor Thesis (UAS) , School of Computing Blekinge Institute of Technology SE - 371 79 Degree Program in Information Technology, Internet Technology, 2013.

[11] Ramgovind S, Eloff MM, Smith E, The Managing of Security in Cloud Computing, 978-1-4244-5495-2/10, IEEE, 2010.

[12] Mohammed A. AlZian, Eric Pardede and Ben Soh, MCDB: Using Multi-Clouds to Warrant Security in Cloud Computing, 976-0-7695-4612-4/11, IEEE, 2011.

[13] Sanjana Sharma, Swati Sengar, SonikaSoni, , Security in Cloud Computing, National Conference on Security Issues in Network Technologies, 2012.

[14] VenkataSravan Kumar, Maddineni Shivashanker Ragi, Security Techniques for Guarding Data in Cloud Computing, Master Thesis Electrical Engineering, School of Computing Blekinge Institute of Technology SE - 371 79 Karlskroa Sweden, November 2011

[15] http://point-at-infinity.org/ssss/ Shamir’s secret sharing scheme.

16] Benjamin Fabian, Tatiana Ermakova, Philipp Junghanns ―Collaborative and secure sharing of healthcare data in multi-clouds‖. Information Systems, Volume 48 Issue C, 2015,pp 132-150

[17] Balasaraswathi, V. R., &Manikandan, S. (2014).‖ Enhanced security for multi-cloud storage using cryptographic data splitting with dynamic approach‖. In Advanced Communication, International Conference onControl and Computing Technologies (ICACCCT), 2014 on (pp. 1190-1194).IEEE.

[18] Mazhar Ali, RevathiDhamotharan, ErajKhan, SameeU.Khan, AthanasiosV.Vasilakos, KeqinLi, Albert.Y.Zomaya ―SeDaSC: Secure Data Sharing in Clouds‖, Systems Journal, IEEE, volume :PP, Issue:99,2015,pp 1-10.

[19] Wang Liang-liang,ChenKe-fei,Mao Xian-ping,Wang Yong-tao ―Efficient and Provably-Secure Certificateless Proxy Re-encryption Scheme for Secure Cloud Data Sharing‖ Journal of Shanghai Jiaotong University Volume 19, issue 4,2014 pp 398-405.

[20] PengXu, XiaqiLiu, ZhenguoSheng, XuanShan,KaiShuang ―SSDS-MC: Slice-based Secure Data Storage in MultiCloud Environment‖ 11th EAI International Conference on Heterogeneous Networking for Quality, Reliability, Security and Robustness (QSHINE) , 2015,pp 304-309.

[21] Shungan Zhou. RuiyingDu, JingChen, HuaDeng, JianShen, Huanguo Zhang ―SSEM: Secure, Scalable and Efficient multi-owner data sharing in clouds‖, China Communications IEEE ,Volume 13,issue 8, 2016,pp 231-243.

[22] Ibrahim Abdullah Althamary, TalalMousaAlkharobi ―Secure File Sharing in Multi-Cloud using Shamir's Secret Sharing Scheme‖,Transactions on Network and communications Vol 4 issue 6, 2016,pp53-67.

[23] Safaa Salam Hatem, Maged H.Wafy,Mahmoud M.EI-Khouly ―Malware Detection in cloud Computing, International Journal of Advanced Science and Computer Science Applications,Vol 5 No 2014.

[24] Dimakis A.G, Godfrey P.B, Wu Y, Wainwright M, and Ramachandran K. Network coding for distributed storage systems. IEEE Transactions on Information Theory 56, 9(Sept. 2010), 4539-4551.

[25] K BadyaNayak, D Krishna, P Ravindra, "Data Integrity and Dynamic Storage Way in Cloud Computing", International Journal of Innovative Technologies vol. 3, issue. 2, pp. 0268-0273, ISSN: 2321-8665, June 2015.

[26] Grobauer, T. Walloschek, E. Stocker, Understanding Cloud Computing Vulnerabilities, Security & Privacy, IEEE, vol. 9, Issue 2, pp. 50-57, March 2011.

[27] King, Rachel. "Pivotal's head of products: We're moving to a multi-cloud world". ZDnet.Retrieved 3 July 2014.

[28] Linthicum, David. "Why you should care about multicloud". Infoworld. Retrieved 3 July 2014.