ISSN: 2277-9655
Impact Factor: 4.116
CODEN: IJESS7

IJESRT

INTERNATIONAL JOURNAL OF ENGINEERING SCIENCES & RESEARCH TECHNOLOGY

MULTI LEVEL ENCRYPTION APPROACH TO SECURE CLOUD DATA

Mukesh Kumar Jha*, Veerendra Shrivastava
* M.Tech Research Scholar, IES College of Technology, Bhopal
Asst. Prof. CSE Department, IES College of Technology, Bhopal

DOI: 10.5281/zenodo.168443

ABSTRACT

Now A Days cloud computing become an extensive area of research where data and resource are sharing among the various user through public cloud .However protecting data and resources on cloud is a challenging issue. In the previous HDFS approach when HDFS file system need to secure this is create additional complicity of algorithm. To address this issue and ensuring data security in cloud storage we propose "MESCD" (Multi Level Encryption approach to secure cloud data) has been proposed. In this work file is uploaded and encrypt using N level of different keys further keys are merged into an single key 'K' which is again secure. Decryption processes is reverse of encryption where key (K) is spited into keys 'N' which is applied to decryption algorithm. The proposed algorithm is effective and efficient then previous HDFS approach.

KEYWORDS: Encryption, Decryption, Cloud Storage, Sharing, Aggregate Key.

INTRODUCTION

Cloud storage also **on-demand storage** has emerged as a promising solution for providing ubiquitous, convenient, and on-demand accesses to huge amounts of document shared over the world wide web [1]. Today, millions of users are sharing personal data, such as photos and videos, with their friends through social network applications based on cloud storage on a daily basis. Business users are also being attracted by cloud storage due to its numerous benefits, including lower cost, greater agility, and better resource utilization [6].

However, whereas enjoying the convenience of sharing knowledge via cloud storage, users also are progressively involved concerning accidental knowledge leaks within the cloud. Such knowledge leaks, caused by a malicious human or a misbehaving cloud operator, will typically result in serious breaches of non-public privacy or business secrets (e.g., the recent status incident of celebrity photos being leaked in iCloud). To handle users' issues over potential knowledge leaks in cloud storage, a standard approach is for the info owner to write in code all the info before uploading them to the cloud, such later the encrypted knowledge is also retrieved and decrypted by those that have the secret writing keys. Such cloud storage is commonly known as the crypto logic cloud storage [11]. However, the cryptography of knowledge makes it difficult for users to go looking and so by selection retrieve solely the info containing given keywords. a standard answer is to use a searchable cryptography (SE) theme within which {the knowledge the info the information} owner is needed to write in code potential keywords and transfer them to the cloud at the side of encrypted data, such that, for retrieving knowledge matching a keyword, the user can send the corresponding keyword trapdoor to the cloud for acting search over the encrypted data [13]. We propose "MESCD" (Multi Level Encryption approach to secure cloud data) has been proposed. In this work file is uploaded and encrypt using N level of different keys further keys are merged into an single key 'K' which is again secure. Decryption processes is reverse of encryption where key (K) is spited into keys 'N' which is applied to decryption algorithm

CLOUD STORAGE FRAMEWORK

Cloud storage offers enterprise organizations the potential to dramatically decrease storage costs. Various cloud services provide cloud storage to consumers at no charge, while others charge some type of subscription-based fee [3]. There are also private clouds that are owned and controlled by an organization, providing a secure network for sharing critical software and data. They can create their own cloud archive solution. In addition, hospitals can pool their budgets and resources to create a shared private cloud consortium or group. Private clouds are created

ISSN: 2277-9655
Impact Factor: 4.116
CODEN: IJESS7

using hardware, software and other tools from different vendors, where the actual servers are managed either onsite or offsite. Hybrid clouds, as the name suggests, combine various public and private cloud resources into a service or solution.

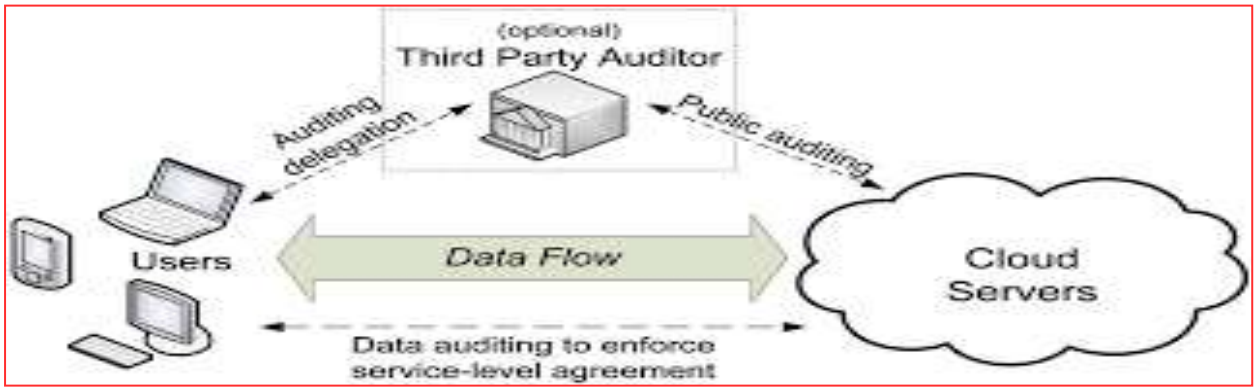

Figure1: Cloud Storage

At the heart of legacy IT, hosting, managed service provider (MSP) and clouds are common building blocks, which include networking, processing and storage technologies. Different types of servers, networks and storage technologies meet various cloud computing and cloud storage requirements (for example, dense rack and blade servers with different numbers of sockets and cores at various GHz speeds, threads, amount of memory and I/O expansion capabilities). Networking options include fast 40GbE and 100GbE for backhaul or trunk circuits, along with the more common 10GbE and 1GbE for virtual private networks (VPN) and bandwidth optimization[4][5]. Data storage options or tiers include ultra-fast SSDs, as well as fast medium- and high-capacity HDDs. Storage management features include data protection — high availability (HA), backup (BC) and disaster recovery (DR) — as well as footprint reduction (DFR) for space optimization, such as compression, de-duplication and thin provisioning, which enables more information to be stored for longer periods at lower costs.

Software tools are also very important in creating services and solutions, and include APIs, middleware, databases, applications, hypervisors for creating virtual machines (VMs) and virtual desktop infrastructures (VDI), along with cloud stack ware, such as Open Stack, and associated management tools. Examples of VMs and VDI hypervisors include Citrix/Xen, KVM, Microsoft Hyper-V, Oracle and VMware ESX/sphere.

CLOUD SERVICE MODEL

Cloud computing is a term that describes a broad range of services. Since the cloud is a collection of services, organizations choose where, when, and how they use cloud computing. In this paper we explain the three different types of service models: [4]

1. Software as a Service (SaaS)
2. Platform as a Service (PaaS)
3. Infrastructure as a service (IaaS)

1. Software as a Service (SaaS) model SaaS is software that is developed over internet. It is a delivery model where the software and the associated data are hosted in a cloud environment by a third party such as Cloud Service Provider (CSP).

2. Platform as a Service (PaaS) model Is a computing platform that allows creation of web applications easily without the complexity of maintaining the software. Is a delivery model where a CSP provides an online software development platform for an organization?

***3. Infrastructure as a Service (IaaS) model*:** This model is used to access essential IT resources. These essential IT resources include services that are linked to resources of computing, data storage and the communications channel.

ISSN: 2277-9655
Impact Factor: 4.116
CODEN: IJESS7

Service Model	Who Uses It	Available Services	Why Use It
SaaS	Members	Applications such as email, word processing and customer relation management tools	Complete business tasks typically performed locally on a computer
PaaS	Developers	Services to facilitate communication and monitoring	To run a cloud application for a particular platform
IaaS	IT Managers	Computing resources, data storage resources, and the communications channel.	Build a customized computing environment

Table 3.1: Cloud computing service models geared for different purpose

CHALLENGES FACING THE CLOUD

Ensuring data storage security in cloud computing with effect of Kerberos

The problem of data security in cloud data storage, which is essentially a distributed storage system. To ensure the correctness of users' data in cloud data storage, and correctness of users who can access to the cloud server, we proposed an effective and flexible distributed scheme with explicit dynamic data support, including Kerberos and authentication service. Kerberos provides a centralize authentication service whose function is to authenticate user to cloud server and cloud server to user. Any user to access the cloud server first should make the profile and password. Then it can use the cloud server with gain the qualify [1].

A Novel Triple Encryption Scheme for Hadoop-based Cloud Data Security

To ensure data security in cloud data storage, a novel triple encryption scheme is proposed. In the triple encryption scheme, HDFS files are encrypted by using the hybrid encryption based on DES and RSA, and the user's RSA private key is encrypted using IDEA. The triple encryption scheme is implemented and integrated in Hadoop-based cloud data storage [2].

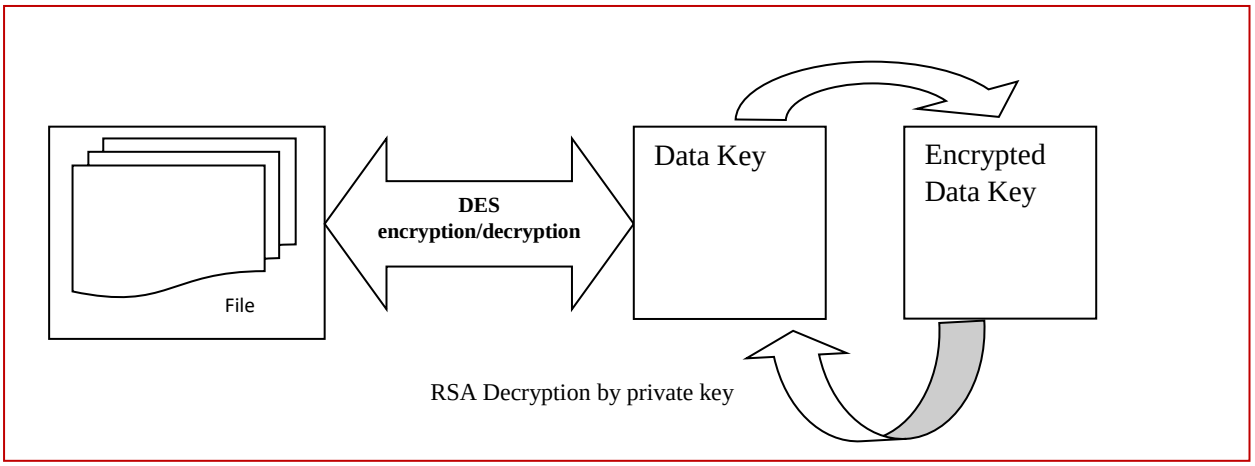

Figure2: RSA Decryption

Key-Aggregate Searchable Encryption (KASE) for Group Data Sharing via Cloud Storage

The practical downside of privacy conserving information sharing system supported public cloud storage which needs an information owner to distribute an oversized range of keys to users to change them to access his/her documents we tend to for the primary time propose the thought of key-aggregate searchable cryptography (KASE) and construct a concrete KASE theme in an exceedingly KASE theme, the owner solely must distribute one key to a user once sharing several documents with the user, and also the user solely must submit one trapdoor once he queries over all documents shared by constant owner [3].

ISSN: 2277-9655
Impact Factor: 4.116
CODEN: IJESS7

Improved Proxy Re-encryption Schemes with Applications to Secure Distributed Storage
We explored proxy re-encryption from both a theoretical and realistic perspective. We outlined the traits and security guarantees of previously recognized schemes, and as compared them to a set of stepped forward re-encryption schemes we gift over bilinear maps. These pairing-primarily based schemes understand crucial new capabilities, consisting of safeguarding the master secret key of the delegator from a colluding proxy and delegate. One of the maximum promising applications for proxy re-encryption is giving proxy capabilities to the key server of a confidential distributed record system; this manner the key server need not be absolutely relied on with all the keys of the device and the name of the game storage for every consumer also can be reduced [5].

Achieving Secure, Scalable, and Fine-grained Data Access Control in Cloud Computing
Finegrainedness, data confidentiality, and scalability simultaneously, which is not provided by current work. In this paper we propose a scheme to achieve this goal by exploiting KPABE and uniquely combining it with techniques of proxy re-encryption and lazy re-encryption. Moreover, our proposed scheme can enable the data owner to delegate most of computation overhead to powerful cloud servers. Confidentiality of user access privilege and user secret key accountability can be achieved. Formal security proofs show that our proposed Scheme is secure under standard cryptographic models [6].

Enabling Data Dynamic and Indirect Mutual Trust for Cloud Computing Storage Systems
Outsourcing data to remote servers has become a growing trend for many organizations to alleviate the burden of local data storage and maintenance. In this work we have studied different aspects of Outsourcing data storage: block-level data dynamic, newness, mutual trust, and access control.

We have proposed a cloud-based storage scheme which supports outsourcing of dynamic data, where the owner is capable of not only archiving and accessing the data stored by the CSP, but also updating and scaling this data on the remote servers The proposed scheme enables the authorized users to ensure that they are receiving the most recent version of the outsourced data [7].

Secure Data Sharing for Dynamic and Large Groups in the Cloud
We have a tendency to tend to style a secure data sharing theme, for dynamic and large groups in associate degree un-trusted cloud. A user is during a position to share data with others at intervals the cluster whereas not revealing identity privacy to the cloud. Additionally, it supports economical user revocation and new user connation. Plenty of specially, economical user revocation is also achieved through a public revocation list whereas not change the personal keys of the remaining users, and new users can directly rewrite files keep at intervals the cloud before their participation. The overall public key remains unchanged if new members square measure any to the cluster. The schemes even conceal the scale of the cluster. The lengths of the ultimate public key and of the signatures are, equally as results of the procedure effort for sign language and verifying, freelance of the number of group members. Moreover, the storage overhead and conjointly the secret writing computation worth are reduced [8].

A Review of Research on An Aggregate Key Sharing Mechanism For Sharing Data Between Different Groups Via Cloud
Due to the characteristic of low maintenance, cloud computing provides financially suitable and efficient solution for sharing group resource among cloud users. Our scheme is also very flexible, and it can be simply extended to support more advanced searching query. Here we conclude that this provides a tremendous building block for the construction of secure services in the cloud storage which are not trusted by user. As we will share only single key the storage space required will become less and more efficient [9].

Achieving Cloud Data Sharing Using Key Aggregate Searchable Encryption
Bearing in mind the matter-of-fact difficulty of privacy preserving information distribution organization based on public cloud storeroom which necessitates an information proprietor to share out a bulky numeral of keys to users to facilitate them to right of entry his or her credentials, we for the foremost time recommend the perception of key aggregate searchable encryption [KASE][10].

Effective Data Sharing in Cloud Using Aggregate Key and Digital Signature
To share data flexibly is a important role in cloud computing. Users prefer to upload their data on cloud and among different users. Outsourcing of data to server may lead to leak the private data of user to everyone. Encryption is a one solution which provides to share selected data with desired candidate. Sharing of decryption keys in secure way plays important role. Key Aggregate Cryptosystems provides delegation of secret keys for different files

ISSN: 2277-9655
Impact Factor: 4.116
CODEN: IJESS7

stored in cloud storage in the form of single aggregate key. The proposed work additionally includes digital signature to provide integrity towards the user's data [11].

A Paper On secure multi-owner group data search by using aggregate key

Considering the pragmatic issue of security saving information sharing framework taking into account open cloud stockpiling which obliges an information proprietor to appropriate a substantial number of keys to clients to empower them to get to his/her records, we surprisingly propose the idea of key-aggregate searchable encryption (KASE) and develop a solid KASE plan[12].

Group Data Searching And Sharing Using Key Aggregate Cryptosystem

In this paper, we reviewed the existing systems papers of sharing the data securely in the cloud. The existing systems based on key encryption may suffer from certain problems such as; these systems are impractical and inefficient as they may require many keys over the cloud data for encryption as well as decryption. Therefore in this paper we are analyzing these problem and aims to overcome them by proposing a novel system called as KASE. In this system, we define general framework for KASE system. Then we describe functional and non-functional requirements of KASE scheme. After describing the KASE scheme we establish its security by detailed analysis [13].

Dynamic Searchable Symmetric Encryption with Minimal Leakage and Efficient Updates on Commodity Hardware

Dynamic Searchable Symmetric Encryption (DSSE) enables a client to perform keyword queries and update operations on the encrypted file collections. DSSE has several important applications such as privacy-preserving data outsourcing for computing clouds. In this paper, we developed a new DSSE scheme that achieves the highest privacy among all compared alternatives with low information leakage, non-interactive and efficient updates, compact client storage, low server storage for large file-keyword pairs with an easy design and implementation [14].

Dynamic Authentication for Client Side Reduplication in Cloud Storage Environment

The growing need for secure cloud storage services and the attractive properties of the convergent cryptography lead us to combine them, thus defining an innovative solution to the data outsourcing security and efficiency issues. The proposed work provides space saving as well as security to the data, but still there are various aspects which need to be address in future. Proposed work addresses only three types of file txt file, doc file and pdf file, we can extend this work for different types of file such as image and sound files and video files in future. We can also apply some searching technique that speed-up the operation by separating the hash key according to the file type [15].

OUR PROPOSED SCHEME

In the Multi Level Encryption Approach to Secure Cloud Data, file is uploaded and encrypted using N level of different keys where N=3 and further keys are merged into single key K and in decryption process again K is split in N different keys and applied all key in decryption process.

Proposed Algorithm

A. For Encryption
   a) User upload N no of file.
   b) For each file 1 to N do
      I. Generate N key for each file.
      II. Apply Encryption Algorithm(3DES)
      III. Upload secure file into cloud.
      IV. Key merger get file ID & Key for each file.
      V. Merge Keys into Super Key K.
      VI. Secure K (AES).
      VII. End for each.
   c) Exit

ISSN: 2277-9655
Impact Factor: 4.116
CODEN: IJESS7

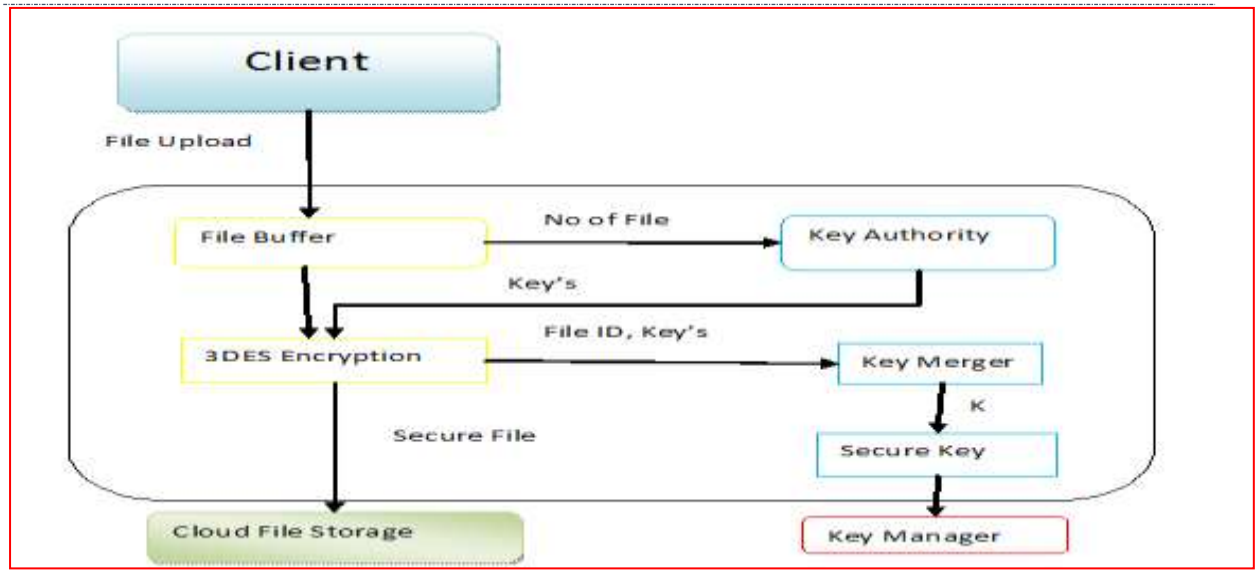

Figure3: MCSCD Encryption

In the above figure first client upload N no file then files goes in file buffer .3DES encryption standard get key's from key authority and by help of this key's file is encrypted and stored in cloud . The N no key's also encrypted from AES .After encryption a single key K is generated for more security purposes.

B. For Decryption
   a) User download N no of file.
      I) Client search which file to be downloaded
      II) Secure file search for download
      III) A file goes to 3DES decryption.
      IV) Key manager send secure key.
      V) Secure Key split into N no Key by Key Splitter.
      VI) BY the help of N no of key 3DES decrypt the file.
   b) Decrypted file goes into file buffer.
   c) File to be downloaded.
   d) Exit

ISSN: 2277-9655
Impact Factor: 4.116
CODEN: IJESS7

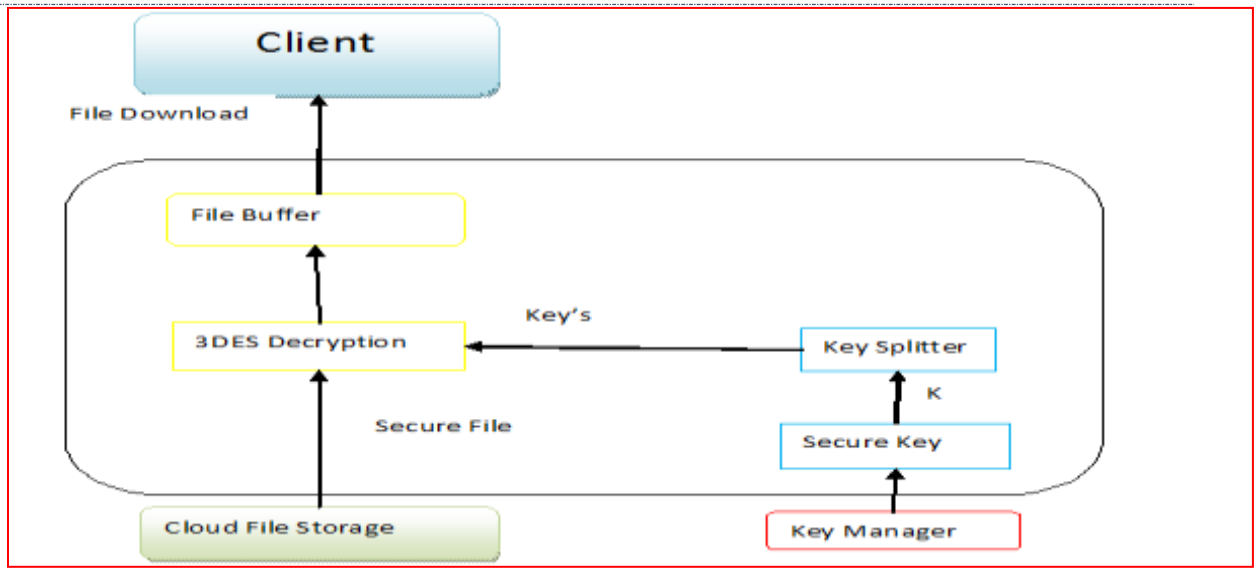

Figure4: MESCD Decryption

The above figure 4 show the decryption process of MESCD approach .In this approach first of all file is searched and key K is split by the help of key splitter and generated N no key .By the help of these key file is decrypted and transferred to client i.e. client get original file.

SIMULATION & RESULT

To measure the performance overhead caused by introducing the Multilevel Encryption Approach to Secure Cloud Data into triple encryption scheme, we have perform some experiments.
In the first Experiment we perform Encryption and measure total encryption time.

S.No.	File Size (MB)	Total upload Time (HDFS Approach)	Total upload Time(MESCD Approach)
1	5	42	22
2	8	58	29
3	20	82	18
4	50	21	17
5	125	32	25

Table 6.1: Total Encryption Time

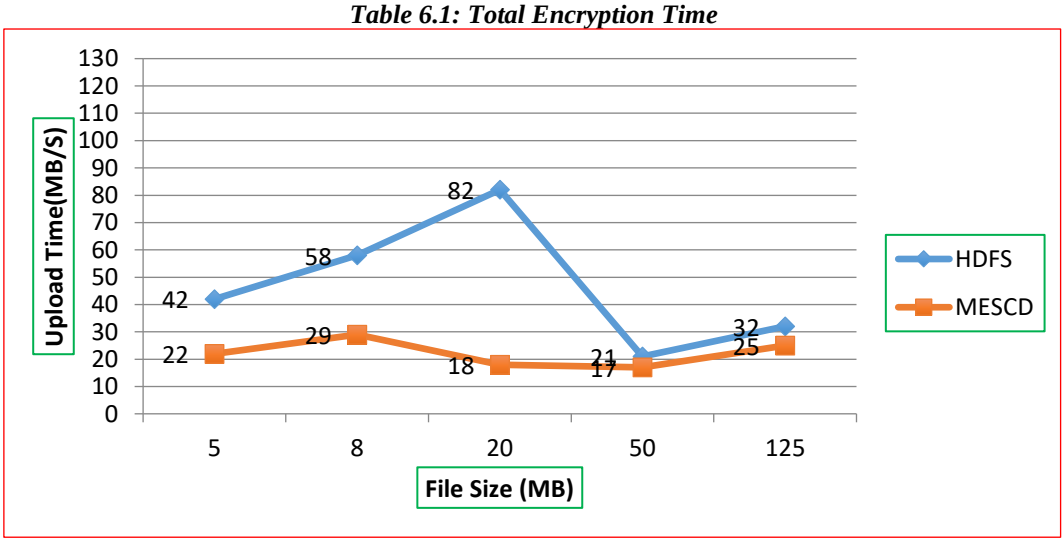

Figure 5: Performance comparison for Encryption

ISSN: 2277-9655
Impact Factor: 4.116
CODEN: IJESS7

In This experiment when user want to upload file of different size then total encryption time consumed by MESCD is less compare to HDFS approach and the comparison is shown in above figure 5.

S.No.	File Size (MB)	Total download Time (HDFS Approach)	Total download Time(MESCD Approach)
1	5	42	22
2	8	58	29
3	20	82	18
4	50	21	17
5	125	32	25

Table 6.2: Total Decryption Time

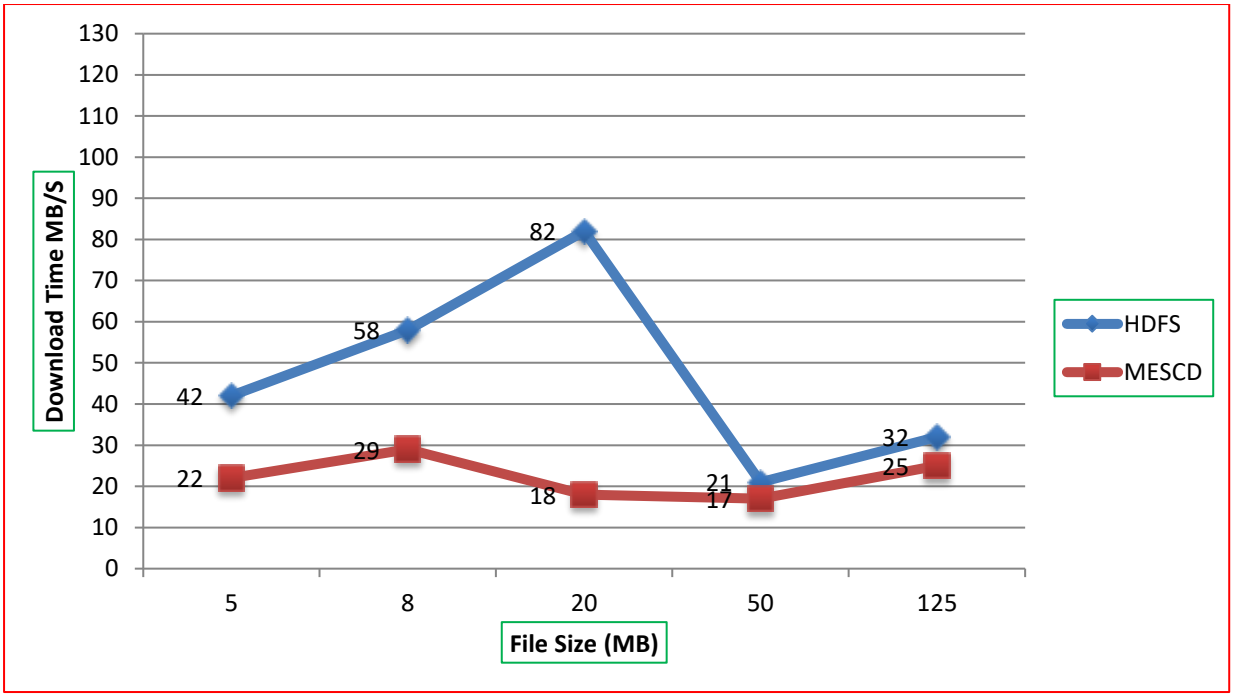

Figure 6: Performance comparison for Decryption

Again Experiment is done on same file size for decryption process and in decryption process our approach i.e. MESCD more efficient compare to previous approach i.e. HDFS and comparison id also shown in above figure 6.

S.No.	File Size (MB)	Total Encryption Key Management Time(ms)	Total Decryption Key Management Time(ms)
1	5	1.173	2.538
2	8	8.998	7.731
3	20	20.362	25.392
4	50	25.481	30.472
5	125	30.731	36.641

Table 6.2: Total Key Management Time

ISSN: 2277-9655
Impact Factor: 4.116
CODEN: IJESS7

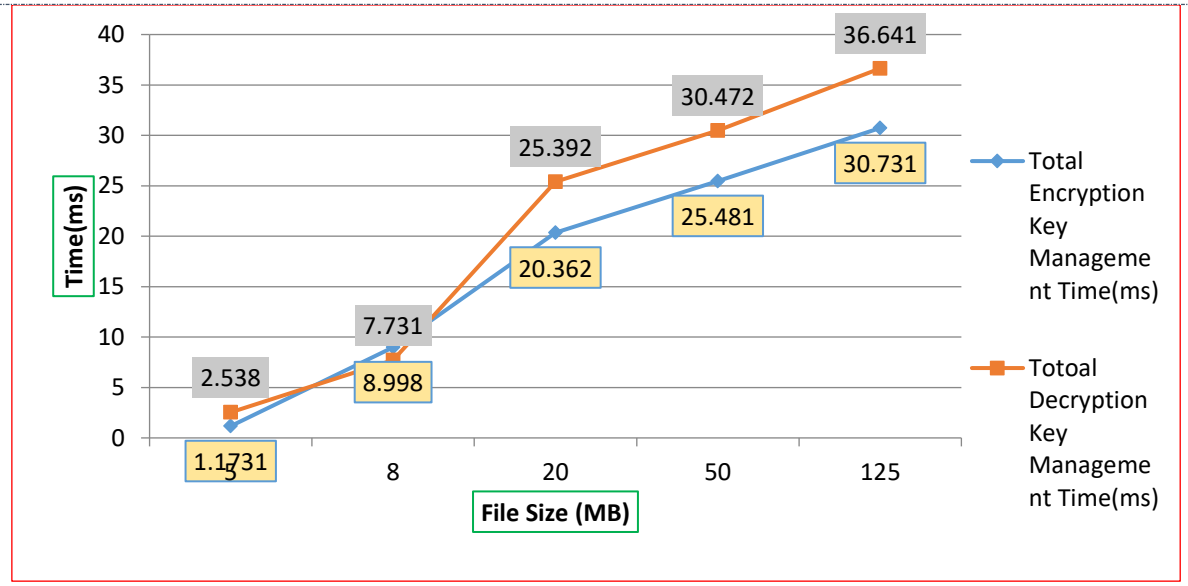

Figure 7: Performance comparison for Key Management Time

The above figure 7 show the comparison between total encryption key management time and total decryption key management time i.e. when any user want to upload or download any file in cloud environment then how much time consumed for key management in encryption as well as decryption

CONCLUSION AND FUTRE WORK

In this paper we focused on the file security protection in the cloud. A novel Multi level Encryption approach to Secure Cloud Data ("MESCD") scheme is proposed. In this approach any file is uploaded and decrypted using using N level of different keys further keys are merged into an single key 'K' which is again secure. Decryption processes is reverse of encryption where key (K) is spited into keys 'N' which is applied to decryption algorithm. We perform many experiment on different file size for encryption and decryption .The Experimental result show that the "MESCD" scheme we proposed is feasible for encryption as well as decryption .As a future work we plan to achieve to generate a unique key if a client want to download or upload any documents shared by multiple owner to reduce no of trapdoors in cloud.

REFERENCES

[1] Mehdi Hojabri " Ensuring data storage security in cloud computing with effect of Kerberos " International Journal of Engineering Research & Technology (IJERT) Vol. 1 Issue 5 , July - 2012 ISSN: 2278- 01 81

[2] Chao YANG, Weiwei LIN*, Mingqi LIU "A Novel Triple Encryption Scheme for Hadoop-based Cloud Data Security" Fourth International Conference on Emerging Intelligent Data and Web Technologies 2013

[3] Baojiang Cui, Zheli Liu_ and Lingyu Wang "Key-Aggregate Searchable Encryption (KASE) for Group Data Sharing via Cloud Storage" IEEE TRANSACTIONS ON COMPUTERS, VOL. 6, NO. 1, JANUARY 2014

[4] Harshitha. K. Raj "A Survey on Cloud Computing" International Journal of Advanced Research in Computer Science and Software Engineering Volume 4, Issue 7, July 2014

[5] GIUSEPPE ATENIESE KEVIN FU MATTHEW GREEN and SUSAN HOHENBERGER "Improved Proxy Re-encryption Schemes with Applications to Secure Distributed Storage" ACM Transactions on Information and System Security, Vol. 9, No. 1, February 2006, Pages 1–30.

[6] Shucheng Yu, Cong Wang, Kui Ren , and Wenjing Lou "Achieving Secure, Scalable, and Fine-grained Data Access Control in Cloud Computing" IEEE INFOCOM 2010

[7] Ayad F. Barsoum and M. Anwar Hasan "Enabling Data Dynamic and Indirect Mutual Trust for Cloud Computing Storage Systems"

[8] M.R. Kalai Selvi1 "Secure Data Sharing for Dynamic and Large Groups in the Cloud "International Journal of Innovative Research in Computer and Communication Engineering Vol.2, Special Issue 1, March 2014

ISSN: 2277-9655
Impact Factor: 4.116
CODEN: IJESS7

[9] Sharayu.J.Lande, Prof. N.B.Kadu "A Review of Research on An Aggregate Key Sharing Mechanism For Sharing Data Between Different Groups Via Cloud" IJEDR | Volume 3, Issue 4 2015
[10] K. Rajasrika1, P.S. Smitha2 "Achieving Cloud Data Sharing Using Key Aggregate Searchable Encryption" International Journal of Innovative Research in Computer and Communication Engineering Vol. 3, Issue 12, December 2015
[11] G. Suganyadevi1 S. PunithaDevi " Effective Data Sharing in Cloud Using Aggregate Key and Digital Signature" International Journal of Innovative Research in Science, Engineering and Technology Vol. 4, Special Issue 6, May 2015
[12] Salman Mujawar "A Paper On secure multi-owner group data search by using aggregate key" Innovation in engineering science and technology (NCIEST-2015)
[13] Wakchaure Sonali Pandharinath. "Group Data Searching And Sharing Using Key Aggregate Cryptosystem" IJARIIE-ISSN(O)-2395-4396 Vol-2 Issue-1 2016
[14] Attila A. Yavuz and Jorge Guajardo "Dynamic Searchable Symmetric Encryption with Minimal Leakage and Efficient Updates on Commodity Hardware"
[15] E. Seetha1, D. Ponniselvi "A Dynamic Authentication for Client Side Deduplication in Cloud Storage Environment" International Journal of Innovative Research in Computer and Communication Engineering Vol. 3, Issue 8, August 2015