Dynamic Storage Mechanism using MD5 Algorithm over Multi-Cloud Environment

Sandhiyachinnadurai[1] Ms. M. Sasikala[2]
[1]Research Scholar [2]Head of the Department
[1,2]Bharathiar University, Coimbatore, Tamil Nadu, India

Abstract— Multi cloud is an important concept for these days for the organization people who do on-line method. It provides information to the user through cloud computing technology. User of the Cloud need to store sizable amount of knowledge within the cloud, by providing storage here we have a tendency to use the dynamic storage mechanism with the assistance of MD5 rule. The MD5 rule may be a wide used hash operates manufacturing a 128-bit hash price. MD5 is employed for science hash operates. For dynamic cloud resource allocation here we have a tendency to use accommodative list programming (ALS) and accommodative min-min programming (AMMS). This pair of ways is used for programming the task, that additionally worked within the offline mode and it works as a static resource allocation repeatedly with predefined frequency. And that we use 3DES cryptography methodology in every file and Elliptic Curve Cryptography (ECC) rule for the cryptography of personal key. And additionally we have a tendency to embrace dynamic file slicing victimization framework interface for determination the key management and key distribution problems.

Key words: Multi Cloud, Dynamic Storage, Cryptography, Key Management & MD5

I. INTRODUCTION

Multi cloud suppliers are wont to have an effect on privacy and knowledge integrity challenges. Multi-cloud model delineated the mix of assorted clouds wherever user knowledge is distributed and dead in those clouds at the same time. It's ascertained that multi–clouds improve performance provided by single cloud setting by dividing security, trust and irresponsibleness among completely different clouds. they need created a survey of assorted techniques on the market for multi cloud security like use of cryptography, secret sharing algorithmic program and redundant array of cloud storage [1]. Multicloud is victimisation over one cloud computing services during a single heterogeneous design. To establishing the multicloud design the varied reasons ought to be right smart like decreasing assurance on any single trafficker, increasing flexibility through selection, and tempering against disasters. It's kind of like over one developer uses the software/applications on a personnel laptop. It's feeling of the very fact that nobody supplier is everything for everybody. It varies from hybrid cloud setting in this it refers to multiple cloud services instead of multiple organization modes like public, private, and heritage [9]. Varied problems also are on the market during a multicloud setting. Security and authority is additional difficult, and additional "moving parts" might produce resiliency problems. Choice of the proper cloud product and services may be a challenge, and shoppers might suffer from the contradiction of selection.

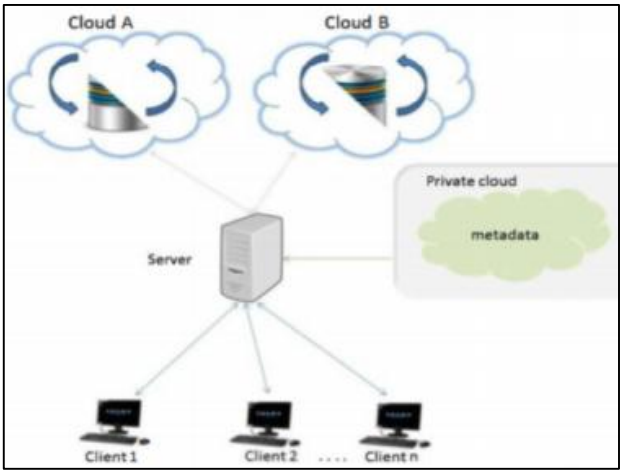

Fig. 1: Multi Cloud Architecture

As is seen, multi-cloud is taking regarding seventy four of enterprises usage that prove the big adaptation of such system in organizations. This huge movement to multi-clouds is reasoned by the power to separate non-public and public knowledge, the dynamic knowledge storage size that's required, and therefore they would like for secondary services that are host on different clouds [2]. A corporation may need each non-public and public data and, during this case, they'll like multi-cloud to create a hybrid cloud that created regarding five hundredth in Fig. 1. during this case, having a multi-cloud system will give a non-public access in one cloud and a public access in another while not admixture the 2 and permitting the IT team to concentrate additional on securing their private knowledge without fear regarding their public ones [3]. The most aim of this analysis is to know the protection threats and determine the acceptable security techniques accustomed mitigate them in Cloud Computing. The most objectives of this analysis are: to know the protection problems and also the techniques utilized in the present world of Cloud Computing. To spot the protection challenges, that is expected within the way forward for Cloud Computing. Multi cloud is a crucial these days for the organization people who do on-line method. It provides knowledge to the user through cloud computing technology. User of the Cloud need to store sizable amount of knowledge within the cloud, by providing storage here we to use the dynamic storage mechanism with the assistance of MD5 algorithmic program. The MD5 algorithmic program may be a wide used hash performs manufacturing a 128-bit hash price. MD5 is employed for science hash performs [4, 5]. For dynamic cloud resource allocation here, we to use reconciling list programming (ALS) and reconciling min-min programming (AMMS). These two strategies are used for programming the task, that conjointly worked within the offline mode and it works as a static resource allocation repeatedly with predefined frequency. And that we use 3DES encoding methodology in every file and Elliptic Curve Cryptography (ECC) algorithmic program for the encoding

of personal key. And also, we to embrace dynamic file slicing victimization framework interface for resolution the key management and key distribution problems.

II. LITERATURE REVIEW

Nisha D. Dable [6], Cloud computing could be a quickest growing technology. It permits business organizations to use or access totally different applications, store info while not access their personal files. Whereas considering the ability, stability and therefore the security of cloud one can't ignore totally different threats to user's knowledge on cloud storage. File access assure in real technique to the file protection because of untrusted cloud servers. In cloud storage system file entrance mechanism is tougher issue. This method in consequence produces redundant copies of comparable files or involves a very reliable cloud server. Attacks from antagonist user are troublesome to prevent in cloud storage. In planned system we to be implementing the thought of multiple cloud storage in conjunction with increased security mistreatment encoding techniques wherever rather storing complete file on single cloud system. The system can split into chunks then encipher it and store on different cloud. the info needed for decrypting and rearranging that file are going to be hold on in information management server for economical retrieval of original file.

Priyanka.R.Raut [7] from trendy centuries use of Cloud computing in numerous mode like cloud storage, cloud servers, cloud hosting are magnified in industries and alternative organization as per needs. Whereas considering the ability, the steadiness and security of cloud one can't ignore totally different threats to user's knowledge on cloud storage. File retrieve is an actual technique to ensure the file safety within the cloud. However file outsourcing and unauthorized cloud servers. The file entrance manufactures an exciting issue in cloud storage systems. In result its right to use mechanism systems aren't any distended associated with cloud storage ideas, as a result of the additionally manufacture totally different born-again copies of the similar files or involve a very reliable cloud server. Multi cloud system within which can transfer and transfer the multiple variety of file .Next we've developed a Multicloud system during this system we've to separate knowledge into totally different cloud for security Triple DES algorithmic program is employed for encoding technique for security.

Ryan K L KO et.al [8] studied the issues and challenges of the sure cloud, wherever the unauthorized user will access the whole knowledge while not troubling the particular user. An unauthorized person could do the 2 things that are accessing data and putt duplicate data as a result of cloud storage provides a geographical info. It's not a sure one to store the info of the users. For this downside Ryan K L KO et al planned a Trust Cloud framework, to realize a sure cloud to the user, to supply a service by creating use of detective controls in cloud atmosphere. Sleuthing method has the answerableness access with the cloud. Here user could be an accountable person for his or her knowledge, thence user should tell the answerableness with the technical and policy based mostly services. By providing the answerableness through user it's going to solve the matter from the untrusted one. Thence this approach provides privacy, security, answerableness and audit ability.

L Ferretti et al [9] studied the matter of information escape of the legitimate user in cloud atmosphere by the cloud provider; they didn't offer higher security to the user for his or her personal knowledge or internal data. Main downside arise due to no encrypted knowledge were found, and additionally it give the protection for the frond-end info solely and not controlled the backend info, that the malicious attackers could gain information access to the outsourced data.

Ankita Ajay Jadhav [10] information sharing among cluster members in the cloud is the characters of low maintenance and little management price. Meanwhile, we have a tendency to tend to tend to produce security guarantees for the sharing knowledge files since they're outsourced. To owing the frequent modification of the membership, sharing knowledge whereas providing privacy protective continues to be a troublesome issue, notably for associate untrusted cloud as results of the collusion attack. Moreover, for existing schemes, the protection of key distribution depends on the secure channel, however, to possess such channel is additionally a sturdy assumption and is difficult for apply. We propose a secure knowledge sharing theme for dynamic members. First, we have a tendency to tend to tend to propose a secure manner for key distribution with none secure communication channels, so the users will firmly acquire their personal keys from cluster manager. Secondly, we have a tendency to do fine-grained access management; any user among the cluster of members can use the supply among the cloud and revoked users feeble to access the cloud yet again once they're revoked. Third, we have a tendency to tend to unit of measurement able to defend the theme from collusion attack that means that revoked users cannot get the initial record though they conspire with the untrusted cloud.

III. PROBLEM DEFINITION

In existing system focus on reducing the malicious insider threats and the proposed procedure ensures the providers resource protection from the malicious files. The SDSMC supports files including video files can be encrypted based on the index based cryptographic technique. In the retrieval of the files a standard procedure is used which increases on demand cost and the conflicts in the merging process. The Storage falls among the services with storage limitation which makes it disadvantageous. They didn't concentrate on dynamic file storage, storage of the file falls in failing state [11].

- Many researchers were proposed effective architecture for the secure data storage using multi cloud storage but they were failed for dynamic storage method.
- And they does not focus on the merging file variance in the recovery process, colluding provider attacks, malicious files, insider attacks, elimination of centralized distribution of data and key management while sharing the data in Multi-Cloud Storage.
- Malicious files are also easily uploaded by the third party authority or role based managers to corrupt the entire scheme.

IV. PROPOSED METHOD

Multi cloud storage provides an important factor in this today environment, where they were lot of data were provided by the company for their transaction. They were getting many data from their business parties for developing their company in a well reputed manner. So they need more storage. So here consideration storage is key challenges in cloud computing environments. File is uploaded by Dynamic and we provide a security through static data Storing by the framework and indexed based slicing and encryption consequently performed on the files before being transferred to the multi-cloud storage server. For this we use the dynamic storage mechanism with the help of MD5 algorithm. The MD5 algorithm is a widely used hash function producing a 128-bit hash value. MD5 is used for cryptographic hash function. For dynamic cloud resource allocation here we use Adaptive list scheduling (ALS) and adaptive min-min scheduling (AMMS). These 2 methods are used for scheduling the task, which also worked in the offline mode and it works as a static resource allocation repeatedly with predefined frequency. And we use 3DES encryption method in each file and Elliptic Curve Cryptography (ECC) algorithm for the encryption of private key [12]. And also we include dynamic file slicing using framework interface for solving the key management and key distribution issues.

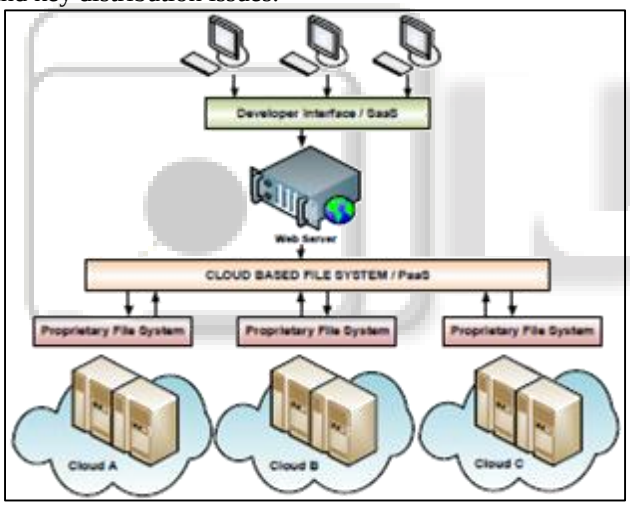

Fig. 2: Proposed Architecture

Proposed work focuses on security and corruption detection of data. For this purpose we developed own system which co-actively work with parallel data processing approach. We also utilized concept of MD5 to tag files with document identity number. Hence if any part of file missing system can recover data using anti-parallel resource algorithm.

A. Data Verifiability in User Level before Upload

In initial stage upload the data, this process expected from its starting condition for N and G these are number of server and cloud storage fixed server respectively. The verification of data is done here from user level before sending or uploading data to destination or cloud server. So in order to maintain the integrity of data as already we told here; before sending data into the cloud server it is verified for its value to the user control [13]. Then, G= {ni,..ni+1,….n(i-m)} and The following equations explain it in clear way as, Elliptic Curve Cryptography

1) n ϵ G, ∀n, here n>1>0 where G is multi cloud identification and n is number of server from user level.
2) n={ia,ia+1,…..ia-n}, where a is data counting for n server.
3) n={{Ri{ ia,ia+1,…..ia-n},Ri+1{ia,ia+1,…ia-n},…Ri-n{ ia,ia+1,…..ia-n}} , where R is the number of different server divided into the cloud.
4) ∀n, n= (R1i,..R2i,…Rn-i), it is up to the ‗R' number of server count
5) ∀i, i=any data in G and while checking for integrity it gets ―n=>R‖ formation. It means that n implies R in all manners.

B. Checking for Same Data in multi cloud

Initially we must always assume for Boolean worth for true and false condition by comparison each user and cloud level knowledge by Adaptive list scheduling (ALS) [14] and adaptive min-min scheduling (AMMS). Then,

1) Verify (Zi={G1i(true)G2i(false)}) Check for condition,
2) if the condition G1i = G2i then it is true in such a way that,
3) n==nu it is set that Z={s(true)} n!=nu otherwise,
4) Z=={s(false)}.

These are the conditions for maintaining the user and cloud level data integrity for all user and server data, since the case has the above condition every user and cloud lever data comparison has different.

C. Putting Server Restore Access Point for Data Recovery in multi cloud

When server failure happens all knowledge is also lost its integrity and since user doesn't have the native copy data there's no additional chance to recover the already lost data from its previous original condition. Thus here we've sculptural one theme ―multi-server knowledge comparison algorithmic rule each for each knowledge transfer for the aim of knowledge. Recover the access for every data in update were done by the users. This prevents entire system collapse from knowledge lose against any such sort of system crash as well as Byzantine, and connected internal and external downside [15]. This prevents entire system collapse from knowledge lose against any such sort of system crash as well as Byzantine, and connected internal and external downside. The on top of theme explains the server crash breaking condition in economical manner by golf stroke one restore access purpose in antecedently updated knowledge from user.

1) Assume server access purpose for already keep knowledge, X and when the server failure
2) Place automatic restore purpose then,
3) Compare for previous worth with current total worth. Currently the previous worth is as, => Σni=0 [(Sd+Td)]d-1=X
4) Current value before crash is as, =>Σni=0[(Sd+Sd1) + (Td+Td1)] =Y
5) Now when we do comparison for both X and Y, the following assumptions are made as, =>X>Y or X<Y then do update otherwise if X==Y then restore to the same condition.

Here this formula is applied for overall data from the server by receiving user and server level data. Here ―S‖ is the cloud level data and ―T‖ is the user level data and ―d‖ is the number of data depending upon the upload condition.

We have implemented MD5 algorithm rule to envision all files are keep because it is or any files are changed because of impact of any mishap. Just in case of information corruption or missing file half, we are able to recover original knowledge from cloud server by mistreatment MD5 hash worth. User's file is spitted and encrypted mistreatment AES algorithmic rule. That file elements are keep on totally different nodes. By mistreatment MD5, we've calculated hash worth and keep on information. Once user desires to transfer his/her file nonetheless hash worth of current file is calculated and verified with previous hash worth. If each hash values are matched then user gets his original file. If hash values aren't same then we able to say that file elements are corrupted or infected. After we understand that file is corrupted then we are able to recover this file.

V. EXPERIMENTAL RESULT

In this paper test execution is that the methodology of execution the system and to look at the expected and actual results. Throughout this stage the take a look of cluster can perform the take a look supported the test strategy and test cases that are automatic. If the expected outcome isn't met, it then it's a defect. Defects are discovered back to the event cluster for modification and retesting is done. take a look at execution focuses on, the take a look at steps for the appliance underneath take a look at, provides the take a look at knowledge and monitors the behaviour of the appliance underneath take a look at to verify whether or not it satisfies the expected outcome or not. We've enforced MD5 algorithmic rule. User's file is spitted and encrypted mistreatment AES algorithmic rule. That file elements are keep on totally different nodes. By mistreatment MD5, we've calculated hash worth and keep on information.

The input file size, encrypted file size, encryption time and decryption time of different files when encrypted for securing data on the cloud using MD5 technique.

A. File Encryption & Upload

When user is registered he/she uploads file on main server and the main server encrypts the file and stored on server.

B. File Decryption & Download

User can download the files from server. The main server decrypts the file using AES algorithm and gives to the user. The AES algorithm is also implemented for decryption of the data. This will provide more security for data and there will not be any direct access of user to auxiliary server's data.

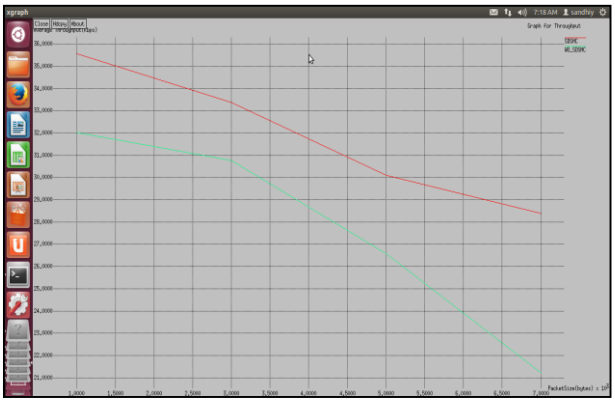

Chart 1: Throughput Graph

Throughput is the maximum rate of production or the maximum rate at which something can be processed. When used in the context of communication networks. By our proposed method it provides a stable solution with more throughput and better performance.

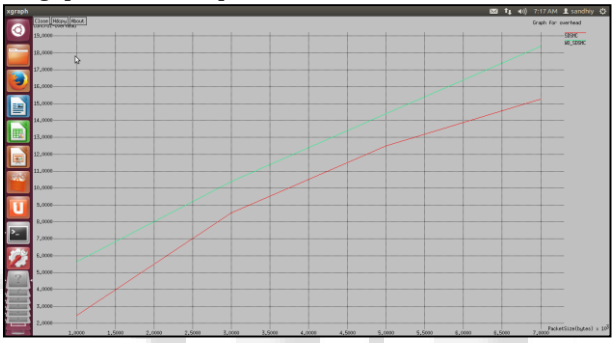

Chart 2: Overhead comparison

In Multi-cloud overhead requires a higher level of expertise in determining what to move to the cloud.

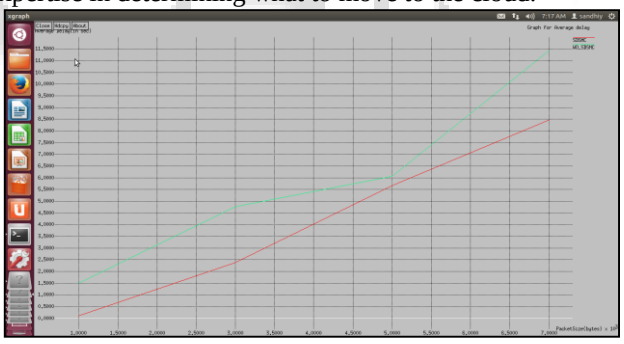

Chart 3: Comparison of Delay

Packet transmission rate is delayed in existing system; hence we reduced in our proposed system.

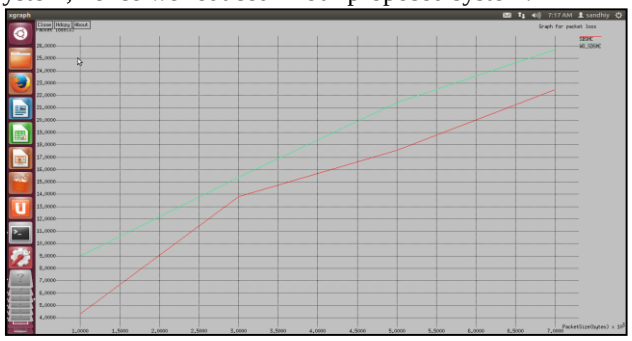

Chart 4: Packet loss comparison

The input file size, encrypted file size, encryption time and decryption time of different files when encrypted for securing data on the cloud using MD5 method.

VI. CONCLUSION

Multi-cloud model explain the mishmash of different clouds where user data is spread and carry out in those clouds concurrently. It is experimental that multi–clouds get better presentation provided by single cloud surroundings by dividing security, trust and dependability among dissimilar clouds. User of the Cloud want to accumulate large number of data in the cloud, by provided that storage here we use the vibrant storage mechanism with the assist of MD5 algorithm. We have implement MD5 algorithm to make sure all files are stored as it is or any files are customized due to impact of any misfortune. In case of data dishonesty or missing file part, we can make progress original data from cloud server by using MD5 hash value. User's file is spitted and encrypted using AES algorithm. That file parts are stored on different nodes. By using MD5, we have designed hash value and accumulate on database. When user needs to download his/her file then over again hash value of current file is considered and established with old hash value. If both hash values are coordinated then user gets his original file.

REFERENCES

[1] J.M. Bohli, N. Gruschka, M. Jensen, L.L. Iacono, and N. Marnau, "Security and Privacy-Enhancing Multi-cloud Architectures" IEEE Transactions on Dependable and Secure Computing,Vol. 10, No. 4, July/August 2013.
[2] Miss. Priyanka.R.Raut and Prof. Vaidehi Baporikar "Design and Implementation of Enhanced Security in Multicloud Storage System Using Distributed File System" International Journal of Science, Engineering and Technology Research (IJSETR), Volume 4, Issue 7, July 2015.
[3] Singhal M., Chandrasekhar S., Tingjian Ge., Sandhu R., Krishnan R., Gail-Joon Ahn., Bertino E(Feb 2013), Collaboration in Multicloud Computing Environments: Framework and Security Issues, IEEE computer society journal, Vol. 46, Issue 2, pp. 76-84
[4] M. A. AlZain, B. Soh and E. Pardede," MCDB: Using Multi-Clouds to Ensure Security in Cloud Computing," in Proceeding of 2011 Ninth IEEE International Conference on Dependable, Autonomic and Secure Computing, IEEE,2011
[5] J.-M. Bohli, M. Jensen, N. Gruschka, J. Schwenk, and =8L.L.L. Iacono, "Security Prospects through Cloud Computing by Adopting Multiple Clouds," Proc. IEEE Fourth Int'l Conf. Cloud Computing (CLOUD), 2011.
[6] Nisha D. Dable, "Enhanced File Security using Encryption and Splitting technique over Multi-cloud Environment "
[7] Priyanka.R.Raut, "Design And Implementation Of Enhanced Security In Multicloud Storage System Using Distributed File System"
[8] Ryan K L Ko, Peter Jagadpramana, Miranda Mowbray, Siani Pearson, Markus Kirchberg , Qianhui Liang , Bu Sung Lee, "TrustCloud: A Framework for Accountability and Trust in Cloud Computing" 2011 IEEE World Congress on Services.
[9] Luca Ferretti, Michele Colajanni, and Mirco Marchetti, "Access control enforcement on query-aware encrypted cloud databases" IEEE 2013.
[10] Ankita Ajay Jadhav, "Anti Collusion Data Sharing Schema for Centralized Group in Cloud".
[11] Saranya.J, "Design for secure data sharing in multi clouds using Luby Transform codes with DES"
[12] Khasim Shaik et al., "Implementation of Encryption Algorithm for Data Security in Cloud Computing",. International Journal of Advanced Research in Computer Science Volume 8, No.3,April 2017.pp.579-583.
[13] S. Vishnupriya, P. Saranya, and A. Rajasri, "Secure multicloud storage with policy based access control and cooperative provable data possession," in Information Communication and Embedded Systems (ICICES), 2014 International Conference on, Feb 2014, pp. 1–6.
[14] J. Li, D. Lin, A. Squicciarini, J. Li, and C. Jia, "Towards privacy-preserving storage and retrieval in multiple clouds," Cloud Computing, IEEE Transactions on, vol. PP, no. 99, pp. 1–1, 2015.
[15] Rajkumar B and Balamurugan K "Service and Data Security for Multi Cloud Environment" International Journal of Innovative Research in Computer and Communication Engineering March 2014

