Secure Data Sharing With Data Fragmentation In Cloud Computing Using Hierarchical Attribute Based Encryption Algorithm

R.Viji[1], R.Priyadharsini[2],V.Vinitha[3]
[1, 2, 3] Dept of CSE
[1, 2, 3] E.G.SPillayEngg. College.,

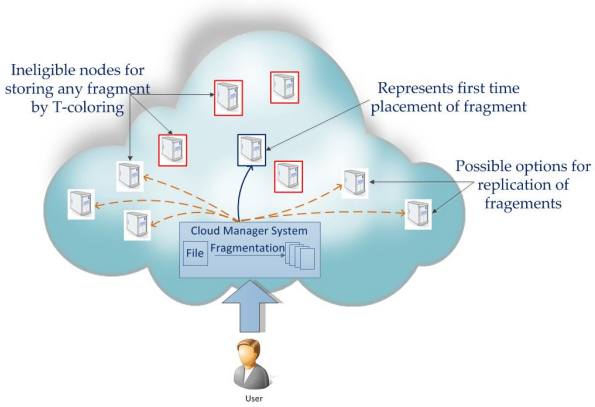
Abstract- *Cloud storage is basically giving all the data to a third party to store it and to retrieve them whenever we wish.This compromises the security of the data.So high security measures are meant to be taken but, it should be simple and easy to use. To upload a file, it is divided into many fragments, and replicate the fragmented data over the cloud nodes. Each of the nodes stores only a single fragment of a particular file so that even in the case of a successful attack, no meaningful information is revealed to the attacker. The cloud manager or simply the CM takes care of all these activities and during the retrieval of a file, the cloud manager collects all the fragments of a file and combines them to form the original file and is given to the user. The main idea is to give added security and protection against all types of attacks, to the data that is being stored in cloud storage with the implementation of hierarchical attribute based encryption algorithm(HABE.)*

Keywords- cloud storage, fragment, cloud manager, hierarchical attribute

I. INTRODUCTION

The distributed computing worldview has transformed the use and the executives of the data innovation framework [7]. Distributed computing is described by on-request self-administrations, omnipresent system gets to, asset pooling, versatility, and estimated administrations [22, 8]. The previously mentioned attributes of distributed computing make it a striking hopeful for organizations, associations, and individual clients for selection [25]. Notwithstanding, the advantages of ease, immaterial administration (from a clients viewpoint), what's more, more noteworthy adaptability accompany expanded security concerns [7]. Security is a standout amongst the most pivotal angles among those restricting the wide-spread selection of cloud figuring [14, 19].Cloud security issues may stem because of the center technologyœs execution (virtual machine (VM) escape, session riding, and so forth.), cloud administration contributions (organized question language infusion, frail validation plans, and so on.), and emerging from cloud qualities (information recuperation defenselessness, Internet convention powerlessness, and so forth.) [5]. For a cloud to be secure, the majority of the taking an interest substances must be secure. In some random framework with numerous units, the most astounding dimension of the systemœs security is equivalent to the security dimension of the weakest substance [12]. Accordingly, in a cloud, the security of the benefits does not exclusively rely upon a person's safety efforts [5]. The neighboring elements may give a chance to an aggressor to sidestep the clients safeguards.

The off-site information stockpiling cloud utility requires clients to move information in cloud's virtualized and shared condition that may result in different security concerns. Pooling and flexibility of a cloud, permits the physical assets to be shared among numerous clients [22]. Also, the mutual assets might be reassigned to different clients at some case of time that may result in information bargain through information recuperation philosophies [22]. Besides, a multi-inhabitant virtualized condition may result in a VM to get away from the limits of virtual machine screen (VMM). The got away VM can meddle with different VMs to approach unapproved information [9]. Correspondingly, cross-inhabitant virtualized arrange access may likewise bargain information protection also, honesty. Ill-advised media purification can likewise spill customers private information [5].



The information redistributed to an open cloud must be verified. Unapproved information access by different clients and forms (regardless of whether incidental or intentional) must be forestalled [14]. As talked about over, any powerless element can put the entire cloud in danger. In such a situation, the security component should significantly increment an aggressor's push to recover a sensible sum of information even after a fruitful interruption in the cloud. Additionally, the plausible measure of misfortune (because of information spillage) should likewise be limited.

A cloud must guarantee throughput, dependability, and security [15]. A key factor deciding the throughput of a cloud that stores information is the information recovery time [21]. In huge scale frameworks, the issues of information unwavering quality, information accessibility, and reaction time are managed with information replication techniques [3]. In any case, putting copies information over various hubs expands the assault surface for that specific information. For example, putting away m copies of a record in a cloud rather than one copy builds the likelihood of a hub holding document to be picked as assault unfortunate casualty, from 1 n to m n , where n is the complete number of hubs. From the above talk, we can find that both security and execution are basic for the cutting edge expansive scale frameworks, for example, mists. Accordingly, in this paper, we on the whole methodology the issue of security and execution as a safe information replication issue. We present Division and Replication of Data in the Cloud for Optimal Performance furthermore, Security (DROPS) that judicially sections client records into pieces and duplicates them at key areas inside the cloud. The division of a record into parts is performed dependent on a given client criteria with the end goal that the individual sections don't contain any significant data. Every one of the cloud hubs (we utilize the term hub to speak to processing, stockpiling, physical, and virtual machines) contains a particular section to expand the information security. A fruitful assault on a solitary hub must not uncover the areas of different sections inside the cloud.To keep an assailant questionable about the areas of the document parts and to additionally improve the security, we select the hubs in a way that they are not nearby and are at sure separation from one another. The hub division is guaranteed by the methods for the T-coloring[6]. To improve information recovery time, the hubs are chosen dependent on the centrality estimates that guarantee an improved access time. To additionally improve the recovery time, we judicially reproduce pieces over the hubs that create the most elevated read/compose demands. The choice of the hubs is performed in two phases.In the principal stage, the hubs are chosen for the underlying situation of the pieces dependent on the centrality measures. In the second stage, the hubs are chosen for replication. The working of the DROPS technique is appeared as an abnormal state work stream in Fig. 1. We actualize ten heuristics based replication systems as near procedures to the DROPS strategy. The executed replication procedures are: (a)A-star based scanning system for information replication issue (DRPA-star), (b) weighted A-star (WA-star),(c) A-star, (d) imperfect A-star1 (SA1), (e) suboptimalA-star2 (SA2), (f) problematic A-star3 (SA3), (g)Local Min-Min, (h) Global Min-Min, (I) Greedy algorithm,and (j) Genetic Replication Algorithm (GRA).The previously mentioned methodologies are fine-grained replication strategies that decide the number and locationsof the copies for improved framework execution. For our examinations, we utilize three Data Center Network (DCN) models, to be specific: (a) Three level, (b) Fat tree, and(c) DCell. We utilize the previously mentioned designs since they comprise the advanced cloud frameworks and the DROPS approach is proposed to work for the distributed computing worldview.

Our real commitments in this paper are as per the following:

We build up a plan for re-appropriated information that considers both the security and performance.The proposed plan pieces and duplicates the information record over cloud hubs.

- The proposed DROPS conspire guarantees that even on account of a fruitful assault, no important data is uncovered to the aggressor.
- We don't depend on customary cryptographic strategies for information security. The non-cryptographic nature of the proposed plan makes it quicker to play out the required tasks (arrangement and recovery) on the information.
- We guarantee a controlled replication of the record fragments,where every one of the sections is reproduced once with the end goal of improved security.

The rest of the paper is sorted out as pursues.

Area 2 gives a review of the related work in the field. In Section 3, we present the primers. The DROPS approach is presented in Section 4. Area 5 clarifies the trial setup and results, furthermore, Section 6 finishes up the paper.

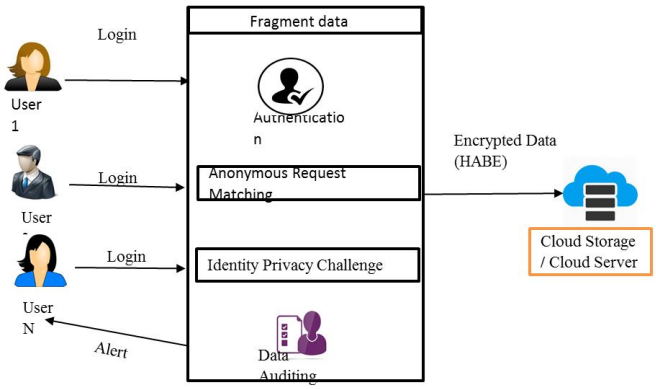
T-COLOURING

Assume we have a chart G = (V;E) and a set Tcontaining non-negative numbers including 0. The T-shading is a mapping capacity f from the vertices of V to the arrangement of non-negative whole numbers, to such an extent that |f(x)- f(y)| T, where (x; y) > E. The mapping capacity f doles out a shading to a vertex. In straightforward words, the separation between the shades of the neighboring vertices must not have a place with T. Detailed by Hale [6], the T-shading issue for channel task relegates channels to the hubs, with the end goal that the channels are isolated by a separation to maintain a strategic distance from obstruction.

II. RELATED WORK

Juels et al. [10] displayed a procedure to guarantee the respectability, freshness, and accessibility of information in a cloud.The information relocation to the cloud is performed by the Iris record framework. An entryway application is planned furthermore, utilized in the association that guarantees the respectability and freshness of the information utilizing a Merkletree. The record squares, MAC codes, and form numbers are put away at different dimensions of the tree. The proposed system in [10] vigorously relies upon the users utilized conspire for information classification. Additionally, the plausible measure of misfortune if there should arise an occurrence of information treating as a consequence of interruption or access by different VMs can't be diminished. Our proposed methodology does not depend on the customary cryptographic methods for information security. Besides, the DROPS strategy does not store the entire document on a solitary hub to dodge bargain of the majority of the information if there should be an occurrence of fruitful assault on the hub. The creators in [11] drew nearer the virtualized and multi-tenure related issues in the distributed storage by using the united stockpiling and local access control. The Dike approval design is proposed that consolidates the local access control and the inhabitant name space confinement. The proposed framework is planned and works for item based document frameworks. Be that as it may, the spillage of basic data in the event of ill-advised cleansing and malevolent VM isn't taken care of.

The DROPS strategy handles the spillage of basic data by dividing information document and utilizing various hubs to store a solitary document. The utilization of a confided in outsider for giving security benefits in the cloud is supported in [22]. The creators utilized the open key foundation (PKI) to improve the dimension of trust in the confirmation, uprightness, what's more, secrecy of information and the correspondence between the included gatherings. The keys are produced furthermore, overseen by the accreditation specialists. At the client level, the utilization of temper confirmation gadgets, for example, keen cards was proposed for the capacity of the keys. Correspondingly, Tang et. al. have used the open key cryptography and confided in outsider for giving information security in cloud situations [20]. Nonetheless, the creators in [20] have not utilized the PKI framework to decrease the overheads. The confided in outsider is in charge of the age and the board of open/private keys. The believed outsider might be a single server or different servers. The symmetric keys are secured by consolidating the



open key cryptography also, the (k, n) limit mystery sharing plans. In any case, such plans don't secure the information records against hardening and misfortune because of issues emerging from virtualization and multi-tenure. A safe and ideal position of information questions in aappropriated framework is exhibited in [21]. An encryption key is separated into n shares and circulated on various destinations inside the system.

The network is divided into clusters. The number of replicas and their placementis determined through heuristics. A primary site is selected in each of the clusters that allocates the replicas within the cluster. The scheme presented in[21]combines the replication problem with security andaccess time improvement. Nevertheless, the scheme focuses only on the security of the encryption key.The data files are not fragmented and are handled as a single file. The DROPS methodology, on the other hand, fragments the file and store the fragments on multiple nodes. Moreover, the

DROPS methodology focuses on the security of the data within the cloud computing domain that is not considered in [21].

Algorithm 1 Algorithm for fragment placement

Inputs and initializations:

```
O = {O1;O2; :::;ON}
o = {sizeof(O1); sizeof(O2); :::::; sizeof(ON)}
col = {open color; close color}
cen = {cen1; cen2; :::; cenM}
col open color¦ i
cenceni¦ i
Compute:
for each Ok > O do
select Si S Si  indexof(max(ceni))
ifcolSi = open color and si>= ok then
Si Ok
sisi − ok
colSi close color
Si' distance(Si; T) P /*returns all nodes at
distance T from Si and stores in temporary set Si'*/
colSi    close color
end if
end
```

Algorithm 2 Algorithm for fragments replication

```
for each Ok in O do
select Si that has max(Rik
+Wik
)
ifcolSi = open color and si>= ok then
Si Ok
sisi − ok
colSi close color
Si' distance(Si; T) P /*returns all nodes at
distance T from Si and stores in temporary set Si'*/
colSi    close color
end if
end for
```

III. RESULTS

We looked at the execution of the DROPS system with the calculations talked about in Section 5.1. The conduct of the calculations was considered by: (a) expanding the quantity of hubs in the framework, (b) expanding the quantity of articles keeping number of hubs steady, (c) changing the hubs stockpiling limit, and (d) fluctuating the read/compose proportion. The previously mentioned parameters are noteworthy as they influence the issue estimate and the execution of calculations [13].

Impact of increment in number of cloud hubs

We contemplated the execution of the position systems also, the DROPS philosophy by expanding the number of hubs. The execution was contemplated for the three talked about cloud designs. The numbers of hubs chose for the reenactments were 100, 500, 1,024, 2,400, and 30,000. The quantity of hubs in the Dcell engineering increments exponentially [2]. For a Dcell design, with two hubs in the Dcell0, the design comprises of 2,400 hubs.The decrease in system exchange time for a record is named as RC. In the figures, the BC represents the betweenness centrality, the CC represents closeness centrality, and the EC represents flightiness centrality. The fascinating perception is that albeit the majority of the calculations demonstrated comparative pattern in execution inside a particular architecture,the exhibition of the calculations was better in the Dcell design when contrasted with three level and fat tree structures.
The DRPA-star gave best arrangements when contrasted with different methods and enlisted reliable execution with the expansion in the quantity of hubs. Also, WA-star, A-star, GRA, greedy,and SA3 indicated practically predictable execution withvarious number of hubs. The execution of LMMand GMM continuously expanded with the expansion in number of hubs since the increment in the number on hubs expanded the quantity of canisters. The SA1 and SA2 additionally demonstrated practically consistent execution in the majority of the three structures.

IV. CONCLUSION

We proposed this procedure, a distributed storage security conspire that by and large arrangements with the security and execution as far as recovery time. The information document was divided and the pieces are scattered over different hubs. The hubs were isolated by methods for T-shading. The discontinuity and dispersal guaranteed that no noteworthy data was reachable by a foe if there should be an occurrence of a fruitful assault. No hub in the cloud, put away in excess of a solitary piece of a similar record. The execution of this procedure was contrasted and full-scale replication systems. The aftereffects of the reproductions uncovered that the concurrent spotlight on the security and execution, brought about expanded security dimension of information joined by a slight exhibition drop.Currently with this procedure, a client needs to download the document, refresh the substance, and transfer it once more. It is key to build up a programmed refresh system that can recognize and refresh the required pieces as it were. The previously mentioned future work will

save.This article has been acknowledged for production in a future issue of this diary, however has not been completely altered. Substance may change preceding last production. Reference data:DOI10.1109/TCC.2015.2400460, IEEE Transactions on Cloud Computing IEEE TRANSACTIONS ON CLOUD COMPUTING 14 the time and assets used in downloading, updating,and transferring the document once more. Additionally, the ramifications of TCP incast over the DROPS philosophy should be contemplated that is significant to conveyed information stockpiling and access.

REFERENCES

[1] K. Bilal, S. U. Khan, L. Zhang, H. Li, K. Hayat, S. A. Madani,N. Min-Allah, L. Wang, D. Chen, M. Iqbal, C. Z. Xu, and A. Y.Zomaya, "Quantitative comparisons of the state of the art data center architectures," Concurrency and Computation: Practice and Experience, Vol. 25, No. 12, 2013, pp. 1771-1783.

[2] K. Bilal, M. Manzano, S. U. Khan, E. Calle, K. Li, and A.Zomaya, "On the characterization of the structural robustness of data center networks," IEEE Transactions on Cloud Computing,Vol. 1, No. 1, 2013, pp. 64-77.

[3] D. Boru, D. Kliazovich, F. Granelli, P. Bouvry, and A. Y. Zomaya,"Energy-efficient data replication in cloud computing datacenters,"In IEEE Globecom Workshops, 2013, pp. 446-451. .

[4] Y. Deswarte, L. Blain, and J-C. Fabre, "Intrusion tolerance in distributed computing systems," In Proceedings of IEEE Computer Society Symposium on Research in Security and Privacy, OaklandCA, pp. 110-121, 1991.

[5] B. Grobauer, T.Walloschek, and E. Stocker, "Understandingcloud computing vulnerabilities," IEEE Security and Privacy, Vol.9, No. 2, 2011, pp. 50-57.

[6] W. K. Hale, "Frequency assignment: Theory and applications,"Proceedings of the IEEE, Vol. 68, No. 12, 1980, pp. 1497-1514.

[7] K. Hashizume, D. G. Rosado, E. Fernndez-Medina, and E. B.Fernandez, "An analysis of security issues for cloud computing,"Journal of Internet Services and Applications, Vol. 4, No. 1,2013, pp. 1-13.

[8] M. Hogan, F. Liu, A.Sokol, and J. Tong, "NIST cloud computing standards roadmap," NIST Special Publication, July 2011.

[9] W. A. Jansen, "Cloud hooks: Security and privacy issues in cloud computing," In 44th Hawaii IEEE International Conference onSystem Sciences (HICSS), 2011, pp. 1-10.

[10] A. Juels and A. Opera, "New approaches to security andavailability for cloud data," Communications of the ACM, Vol.56, No. 2, 2013, pp. 64-73.

[11] G. Kappes, A. Hatzieleftheriou, and S. V. Anastasiadis, "Dike:Virtualization-aware Access Control for Multitenant Filesystems,"University of Ioannina, Greece, Technical Report No.DCS2013-1, 2013.

[12] L. M. Kaufman, "Data security in the world of cloud computing,"IEEE Security and Privacy, Vol. 7, No. 4, 2009, pp. 61-64.

[13] S. U. Khan, and I. Ahmad, "Comparison and analysis of ten static heuristics-based Internet data replication techniques,"Journal of Parallel and Distributed Computing, Vol. 68, No. 2, 2008,pp. 113-136.

[14] A. N. Khan, M. L. M. Kiah, S. U. Khan, and S. A. Madani,"Towards Secure Mobile Cloud Computing: A Survey," FutureGeneration Computer Systems, Vol. 29, No. 5, 2013, pp. 1278-1299.

[15] A. N. Khan, M.L. M. Kiah, S. A. Madani, and M. Ali, "Enhanced dynamic credential generation scheme for protection of user identity in mobile-cloud computing, The Journal of Supercomputing, Vol. 66, No. 3, 2013, pp. 1687-1706

[16] T. Loukopoulos and I. Ahmad, "Static and adaptive distributeddata replication using genetic algorithms," Journal of Parallel and Distributed Computing, Vol. 64, No. 11, 2004, pp.1270-1285.

[17] 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.

[18] L. Qiu, V. N. Padmanabhan, and G. M. Voelker, "On the placement of web server replicas," In Proceedings of INFOCOM 2001, Twentieth Annual Joint Conference of the IEEE Computer and Communications Societies, Vol. 3, pp. 1587-1596, 2001.

[19] D. Sun, G. Chang, L. Sun, and X. Wang, "Surveying and analyzing security, privacy and trust issues in cloud computing
environments," Procedia Engineering, Vol. 15, 2011, pp. 2852

[20] A. Boldyreva, V. Goyal, and V. Kumar, ―Identity-based encryption with efficient revocation,‖ in Proceedings of the 15th ACM conference on Computer and communications security. ACM, 2008, pp. 417–426.

[21] B. Libert and D. Vergnaud, ―Adaptive-id secure revocable identity based encryption,‖ in Topics in Cryptology–CT-RSA 2009. Springer, 2009, pp. 1–15.

[22] ——, ―Towards black-box accountable authority ibe with short ciphertexts and private keys,‖ in Public Key Cryptography–PKC 2009. Springer, 2009, pp. 235–255.

[23] J. Chen, H. W. Lim, S. Ling, H. Wang, and K. Nguyen, ―Revocable identity-based encryption from lattices,‖ in Information Security and Privacy. Springer, 2012, pp. 390–403.

[24] J. H. Seo and K. Emura, ―Revocable identity-based encryption revisited: Security model and construction,‖ in Public-Key Cryptography–PKC 2013. Springer, 2013, pp. 216–234.

[25] ——, ―Efficient delegation of key generation and revocation functionalities in identity-based encryption,‖ in Topics in Cryptology– CT-RSA 2013. Springer, 2013, pp. 343–358.

[26] K. Liang, J. K. Liu, D. S. Wong, and W. Susilo, ―An efficient cloud based revocable identity-based proxy re-encryption scheme for public clouds data sharing,‖ in Computer Security-ESORICS 2014. Springer, 2014, pp. 257–272.

COMPUSOFT, An international journal of advanced computer technology, 7 (2), February-2018 (Volume-VII, Issue-II)

2630

[27] D.-H. Phan, D. Pointcheval, S. F. Shahandashti, and M. Strefler, ―Adaptive cca broadcast encryption with constant-size secret keys and ciphertexts,‖ International journal of information security, vol. 12, no. 4, pp. 251–265, 2013.

[28] R. Anderson, ―Two remarks on public-key cryptology (invited lecture),‖ 1997.

[29] M. Bellare and S. K. Miner, ―A forward-secure digital signature scheme,‖ in Advances in Cryptology–CRYPTO 1999. Springer, 1999, pp. 431–448.

[30] M. Abdalla and L. Reyzin, ―A new forward-secure digital signature scheme,‖ in Advances in Cryptology–ASIACRYPT 2000. Springer, 2000, pp. 116–129.

[31] A. Kozlov and L. Reyzin, ―Forward-secure signatures with fast key update,‖ in Security in communication Networks. Springer, 2003, pp. 241–256.

[32] X. Boyen, H. Shacham, E. Shen, and B. Waters, ―Forward-secure signatures with untrusted update,‖ in Proceedings of the 13th ACM conference on Computer and communications security. ACM, 2006, pp. 191–200.

[33] J. Yu, R. Hao, F. Kong, X. Cheng, J. Fan, and Y. Chen, ―Forward secure identity-based signature: security notions and construction,‖ Information Sciences, vol. 181, no. 3, pp. 648–660, 2011.

[34] R. Canetti, S. Halevi, and J. Katz, ―A forward-secure public-key encryption scheme,‖ in Advances in Cryptology–Eurocrypt 2003. Springer, 2003, pp. 255–271.

[35] D. Yao, N. Fazio, Y. Dodis, and A. Lysyanskaya, ―Id-based encryption for complex hierarchies with applications to forward security and broadcast encryption,‖ in Proceedings of the 11th ACM conference on Computer and communications security. ACM, 2004, pp. 354–363.

[36] J. M. G. Nieto, M. Manulis, and D. Sun, ―Forward-secure hierarchical predicate encryption,‖ in Pairing-Based Cryptography–Pairing 2012. Springer, 2013, pp. 83–101.

[37] A. Sahai, H. Seyalioglu, and B. Waters, ―Dynamic credentials and ciphertext delegation for attribute-based encryption,‖ in Advances in Cryptology–CRYPTO 2012. Springer, 2012, pp. 199–217.

[38] B. Waters, ―Efficient identity-based encryption without random oracles,‖ in Advances in Cryptology–EUROCRYPT 2005. Springer, 2005, pp. 114–127.

[39] B. Lynn. (2014) Pbc library: The pairing-based cryptography library. [Online]. Available: http://crypto.stanford.edu/pbc/