ISSN(Online): 2319-8753
ISSN (Print): 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Website: www.ijirset.com

Vol. 6, Issue 7, July 2017

DROPS: Division and Replication of Data in Cloud for Optimal Performance and Security

Harshal Patil[1], Prof.M.D Ingle[2]

P.G. Student, Department of Computer Engineering, Jayawantrao Sawant College of Engineering, Hadapsar, Pune, Savitribai Phule Pune University, Pune, India[1]

PG Co-Ordinator, Department of Computer Engineering, JayawantraoSawant College of Engineering, Hadapsar, Pune, Savitribai Phule Pune University, Pune, India[2]

ABSTRACT: The issues related to security and operation overcomes by the Division and Replication of Data in the Cloud for Optimal Performance and Security (DROPS). In cloud computing, the information is stored on third party space which results in a security concerns. The user and lymph gland within cloud may compromise the data. Therefore, to protect data within the cloud senior high school security measures are required. Divide a data file into fragments, and replicate the fragmented data over the cloud lymph gland is done in DROPS methodological analysis. Only a fragment of a particular data file can be stored by each of the node that ensures that no meaningful information is revealed to the aggressor even in case of a successful attack.

KEYWORDS: Centrality, Cloud Security, Fragmentation, Replication, Performance.

I. INTRODUCTION

Security is a standout amongst the most essential linear perspective among those forbidding the fare Kuki reception of distributed calculation. Distributed calculations projecting adaptability accompanies expanded security business concern. The majority of the taking part substances must be secure for a cloud to be secure. The largest sum of the organization security is equal to the security level of the weakest element in any given framework with numerous unit of measurement. In this way, in a cloud to establish safety, the security of the welfare does not exclusively rely on upon an somebodies efforts. To move selective information in clouds virtualized and shared surroundings that may bring about different security concerns, the offsite information hoarding cloud utility obliges customer. The physical assets to be shared among frequent clients may be per timed by Pooling and flexibility of a cloud. In this paper as a safe information replication return, we by and large approaching the issue of security and execution. We introduce Division and Replication of Data in the Cloud for Optimal Performance and Security system (DROPS). It shares client record into fragments and repeats them at dynamic Dis-tributed calculation. In any case, the surety measures measure concern get expanded by the advantages of minimal effort, insignificant administration (from a client's point of view), and more projecting adaptability accompany. Security is a standout amongst the most pivotal perspective among those forbidding the fare mentum reception of distributed computer science.

The majority of the taking part essence must be secure for a swarm to be secure. The largest amount of the organisation security is equivalent to the security stage of the weakest factor in any given fabric with numerous unit of measurement. In this way, in a cloud, the security of the benefit does not exclusively rely on upon somebodies efforts to establish safety device. To move entropy in clouds virtualized and shared environment that may bring about different security business concern,the offsite information storing cloud utility obliges guest. The physical assets to be shared among numerous guests get permit by Pooling and flexibility of a cloud. In this paper the government issue of security and execution as a safe information reply issue, we by and large approach.

ISSN(Online): 2319-8753
ISSN (Print): 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Website: www.ijirset.com

Vol. 6, Issue 7, July 2017

II. REVIEW OF LITERATURE

Mazhar Ali, Samee U. Khan, DROPS: Division and Replication of Data in Cloud for Optimal Performance and Security IEEE 2015.In this paper, we propose Division and Replication of Data in the Cloud for Optimal Performance and Security (DROPS) that collectively approaches the security and performance issues. In the DROPS methodology, we divide a file into fragments, and replicate the fragmented data over the cloud nodes. Each of the nodes stores only a single fragment of a particular data file that ensures that even in case of a successful attack, no meaningful information is revealed to the attacker[1].

J. J. Wylie, M. Bakkaloglu, V. Pandurangan, M. W. Bigrigg, S. Oguz, K. Tew, C. Williams, G. R. Ganger, and P. K. Khosla, had presented the Cloud computing ontogenesis due to its sum applied science hike the protection yield . So, to achieve the protection as well as performance by using three proficiency , Graphical Word Certification , Fragmentation and Counter , this system provides a better solution. Nowadays, the use of the Graphical Password Assay-mark increases. This is because as compared to alphanumeric method, it is very easy to remember and secure. Fragmentation used to secure data from single distributor point tragedy . In loser situations, Replication can be useful for maintaining availability, reliability and performance. But due to extreme use of bandwidth the extra comeback can also result in high storage cost or drops in systems overall performance. So, here controlled replication is used. The clock time and piece of work on some tone-beginning will get saved in the future work[2]

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. This paper compares and analyzes 10 heuristics to solve the fine-grained data replication problem over the Internet. In fine-grained replication, frequently accessed data objects (as opposed to the entire website contents) are replicated onto a set of selected sites so as to minimize the average access time perceived by the end users.[3].

D.Boru, D.Kliazovich, F.Granelli, P.Bouvry,andA.Y.Zomaya, Divided a file into sherd s, and replicate the fragmented information over the cloud nodes. Each of the nodes entrepot only a single fragment of a particular data file. It ensures that even in case of a successful attack, the attacker fail to get meaningful information [4].

T. Loukopoulos and I. Ahmad To improve the resource limit of Mobile devices, mobile users may utilize cloud-computational and storage Service . The processing and storage capacity of mobile devices, the migration of confidential data on untrusted cloud raises security system and privacy government issue get improved by the utilization of the cloud services improves. [5].

K. Bilal, M. Manzano, S. U. Khan, E. Calle, K. Li, and A. Zomayaanalyzed lustiness of the state-of-the-art DCNs. The papers major contribution are: 1) It presented multilayered graph modeling of various DCNs; 2) It studied the classical hardiness Synonyms/Hypernyms (Ordered by Estimated Frequency) of noun metric considering various failure scenario to perform a comparative analysis; leash) It presented the inadequacy of the classical network hardiness metrics to appropriately evaluate the DCN robustness; and 4) It proposed new subroutine to quantify the DCN robustness. Therefore, for the future DCN robustness research , we believe that this work will lay a firm foundation.[6]

K. Hashizume, D. G. Rosado, E. Fernndez-Medina, and E. B. Fernandez a very wide sketch had been reviewed which signifies scourge with avail and deployment models of swarm ., this study is presented so as to effectively refine the crude security issues under various areas of swarm in order to comprehend these threats. This study also purpose at revealing different security threats which were under the cloud models as well as network concern to stagnate the threats within cloud, facilitating researcher, cloud supplier and end drug user for noteworthy analysis of threats [7].

K. Lai, M. Feldman, I. Stoica, and J. Chuang, Incentives for cooperation in peer-to-peer networks, in Proc. 1st Workshop Economics Peer-to-Peer Syst., 2003, pp. 631660. In this paper we take a game theoretic approach to the problem of cooperation in peer-to-peer networks. Addressing the challenges imposed by P2P systems, including large

ISSN(Online): 2319-8753
ISSN (Print): 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Website: www.ijirset.com

Vol. 6, Issue 7, July 2017

populations, high turnover, asymmetry of interest and zero-cost identities, we propose a family of scalable and robust incentive techniques, based upon the Reciprocative decision function, to support cooperative behavior and improve overall system performance. We find that the adoption of shared history and discriminating server selection techniques can mitigate the challenge of few repeat transactions that arises due to large population size, high turnover and asymmetry of interest[8].

ManishaKalkal, SonaMalhotra, Replication for Improving Availability and Balancing Load in Cloud Data Centres, International Journal of Advanced Research in Computer Science and Software Engineering, Volume 5, Issue 4, 2015. In this paper, to improve the resource limitation of mobile devices, mobile users may utilize cloud-computational and storage services. Although the utilization of the cloud services improves the processing and storage capacity of mobile devices, the migration of confidential information on untrusted cloud raises security and privacy issues. Considering the security of mobile-cloud-computing subscribers information, a mechanism to authenticate legitimate mobile users in the cloud environment is sought. Usually, the mobile users are authenticated in the cloud environment through digital credential methods, such as password. Once the users credential information theft occurs, the adversary can use the hacked information for impersonating the mobile user later on. The alarming situation is that the mobile user is unaware about adversarys malicious activities. In this paper, a light-weight security scheme is proposed for mobile user in cloud environment to protect the mobile users identity with dynamic credentials. The proposed scheme offloads the frequently occurring dynamic credential generation operations on a trusted entity to keep minimum processing burden on the mobile device. To enhance the security and reliability of the scheme, the credential information is updated frequently on the basis of mobile-cloud packets exchange[9].

S. M. Khan and K. W. Hamlen, Hatman: Intra-cloud trust management for Hadoop, in Proc. 5th Int. Conf. Cloud Comput., 2012 Hatman extends Hadoop clouds with reputation-based trust management of slave data nodes based on EigenTrust. To obtain high scalability, all trust management computations are formulated as distributed cloud computations. This leverages the considerable computing power of the cloud to improve the data integrity of cloud computations[10].

S. Pearson and A. Benameur, Privacy, security and trust issues arising from cloud computing, in Proc. 2nd Int. Conf. Cloud Comput., 2010, pp. 693702. Cloud providers need to safeguard the privacy and security of personal data that they hold on behalf of organisations and users. In particular, it is essential for the adoption of public cloud systems that consumers and citizens are reassured that privacy and security is not compromised. Responsible management of personal data is a central part of creating the trust that underpins adoption of cloudbased services without trust, customers will be reluctant to use cloud-based services[11].

E. Bertino, F. Paci, R. Ferrini, and N. Shang, Privacy-preserving digital identity management for cloud computing, IEEE Data Eng. Bull, vol. 32, no. 1, pp. 2127, Mar. 2009. In this paper we have proposed an approach to the verification of digital identity for cloud platforms. Our approach uses efficient cryptographic protocols and matching techniques to address heterogeneous naming. We 6 plan to extend this work in several directions. The first direction is to investigate the delegation of identity attributes from clients to CSPs. Delegation would allow a CSP, called the source CSP, to invoke the services of another CSP, called the receiving CSP, by passing to it the identity attributes of the client. However the receiving CSP must be able to verify such identity attributes in case it does not trust the source CSP[12].

III. PROPOSED SYSTEM ARCHITECTURE

The architecture diagram of the system shown below helps us to understand the system. In this composition, as a secure data replication problem we collectively approach the issue of certificate and performance. We present free fall that fragments user filing cabinet into art object and replicates them at strategic fix within the cloud. The division of a file into fragments is performed based on a given user criteria such that the individual fragment do not contain any meaningful information. Each of the cloud client(we use the term node to represent computing, reposition, physical, and virtual machines) contains a distinct fragment to increase the data security.

ISSN(Online): 2319-8753
ISSN (Print): 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Website: www.ijirset.com

Vol. 6, Issue 7, July 2017

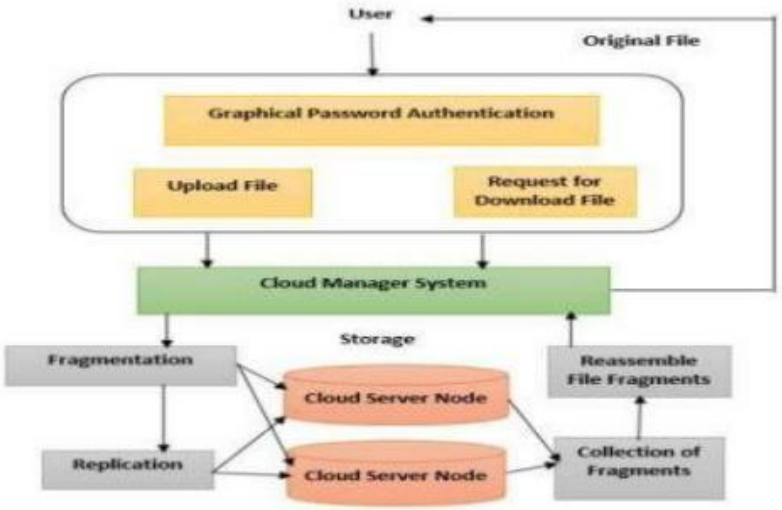

Figure 1: DROPS System Architecture

IV. SET THEORY AND ALGORITHM

SET THEORY :

Below is the set theory which includes the detailed description of the term I,P,R& O ,which describes the steps of file processing in division and replication of data in cloud.

S = I, P, R, O

Where,

I is set of Initial Input to the system.

I = i1, i2, i3

i1 = File given by the user.

i2 = Download request from User.

i3 = Download request from Client.

Procedure or function or processes or methods.

P = p1, p2, p3, p4, p5, p6, p7, p8

p1 = Registration and Authentication.

p2 = Uploading a file on cloud server.

p3 = Fragmentation of file received from user.

ISSN(Online): 2319-8753
ISSN (Print): 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Website: www.ijirset.com

Vol. 6, Issue 7, July 2017

p4 = Replication of that file.

p5 = Download Request from user.

p6 = Download Request from client.

p7 = Collection and reassemble of fragments.

p8 = Downloading the original file.

R is a set of rules or constraints.

R= r1 , r1 = File accessed from Replication when network is busy.

O is a set of outputs.

O = o1

o1 = Downloading the original file.

Fragment Placement Algorithm:

In the DROPS methodology, we propose not to store the entire file at a single node. The DROPS methodology fragments the file and makes use of the cloud for fragment placement. The fragments are placed in such a way that no node in cloud can hold more than one fragment. To deal with security aspects of placing the fragments, we use the concept of T-coloring, here we generates the random non negative number and build the set T starting from zero to generated random number. Initially all the nodes are assigned the open color, once the fragment is placed on the node, all the neighbouring nodes at hop distance belonging to T are assigned the close color, in this way higher security level is achieved by placing the fragments on the node in cloud.

Inputs and Initializations:
O = {O1, O2, ..., ON }
o = {sizeof (O1), sizeof (O2), ...,sizeof (ON)}
col = {open color, closecolor}
cen = {cen1, cen2, ..., cenM }
col ← open color∀ i
cen ← ceni∀ i

Compute:
for each Ok ∈ O **do**
select Si | Si ← indexof(max(ceni))
if colSi = open color and si>= ok then
Si ← Ok
si ← si– ok
colSi ← close color
Si'← distance(Si, T) s at
distance T from Si

ISSN(Online): 2319-8753
ISSN (Print): 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Website: www.ijirset.com

Vol. 6, Issue 7, July 2017

colSi′ ← close color
end if
end for

V. EXPERIMENTAL RESULTS

Cloud computing growth raises the security concern due to its core technology. So, this system provides a better solution to achieve the security as well as performance by using three techniques, Graphical Password Authentication, Division and Replication. The use of the Graphical Password Authentication increases because it is very easy to remember and secure as compared to alphanumeric method. Division used to protect data from single point disaster. Replication can be useful for maintaining availability, reliability and performance in failure situations. Our approach to detect masquerade attacks in cloud environment by improving our CIDS framework. As a first step we divide a file into fragments, and replicate the fragmented data over the cloud nodes. Each of the nodes stores only a single fragment of a particular data file that ensures that even in case of a successful attack, no meaningful information is revealed to the attacker.

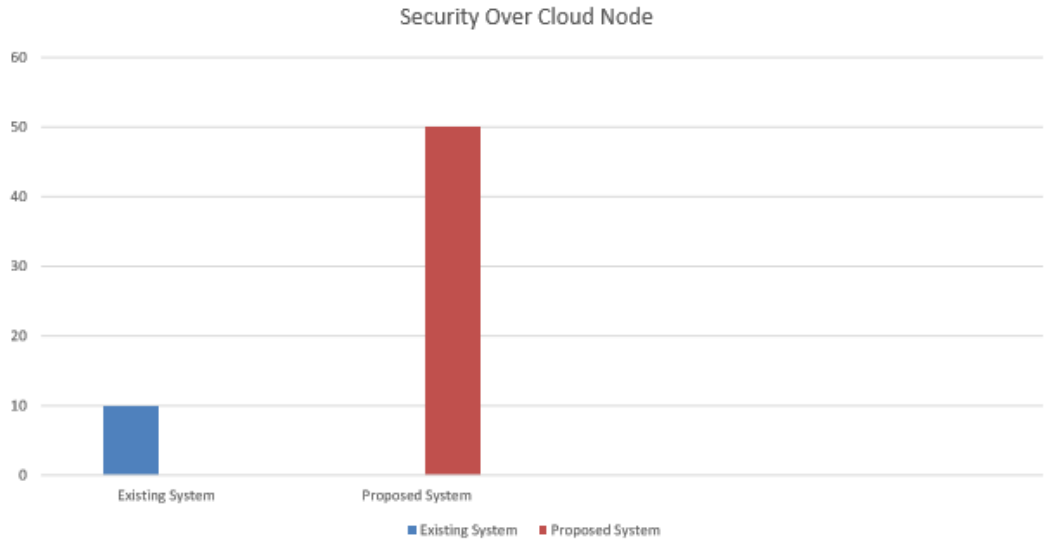

Figure 2:Security Achieved in Cloud Data Storage

Above figure shows the graphical representation of security achieved in cloud data storage, proposed system achieves more security in data storage over the cloud nodes than the existing system .

VI. CONCLUSION

Cloud computing growth raises the certificate displeasure due to its core technology. So, this organization provides a better answer to achieve the security as well as public presentation by using three techniques, Graphical Password Authentication, Fragmentation and Echo. Nowadays, the use of the Graphical Password Authentication increases because it is very easy to remember and secure as compared to alphanumeric method acting. Fragmentation used to protect data from unity point in time disaster. Retort can be useful for maintaining availableness, reliability and public presentation in failure situations. But the extra sound reflection can also result in high computer storage cost or overall performance of the system due to extreme use of bandwidth. So, here controlled replication is used. The future work will saves the time and work on some attacks. Matching Based Overlapping approach reduces the computational load

ISSN(Online): 2319-8753
ISSN (Print): 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Website: www.ijirset.com

Vol. 6, Issue 7, July 2017

of alignment by reducing the form sequence into a smaller set of overlapped subsequence. Furthermore, the detection and the update processes can be parallel with no loss of truth.

REFERENCES

[1] Mazhar Ali, Samee U. Khan, "DROPS: Division and Replication of Data in Cloud for Optimal Performance and Security", IEEE 2015.
[2] J. J. Wylie, M. Bakkaloglu, V. Pandurangan, M. W. Bigrigg, S. Oguz, K. Tew, C. Williams, G. R. Ganger, and P. K. Khosla,"Selecting the right data distribution scheme for a survivable storage system", Carnegie Mellon University, Technical Report CMU-CS-01-120, May 2001.
[3] 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,pp. 113-136,2008.
[4] D. Boru, D. Kliazovich, F. Granelli, P. Bouvry, and A. Y. Zomaya,"Energy-efficient data replication in cloud computing datacenters", In IEEE GlobecomWorkshops,pp. 446-451,2013.
[5] Loukopoulos and I. Ahmad, "Static and adaptive distributed data repli-cation using genetic algorithms", Journal of Parallel and Distributed Computing, Vol. 64, No. 11,pp. 1270-1285,2004.
[6] 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,pp. 1771-1783,2013.
[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,pp. 1-13,2013.
[8] K. Lai, M. Feldman, I. Stoica, and J. Chuang, "Incentives for cooperation in peer-to-peer networks", in Proc. 1st Workshop Economics Peer-to-Peer Syst.,pp. 631660,2003.
[9] ManishaKalkal, SonaMalhotra, "Replication for Improving Availability and Balancing Load in Cloud Data Centres", International Journal of Advanced Research in Computer Science and Software Engineering, Volume 5, Issue 4, 2015.
[10] S. M. Khan and K. W. Hamlen, Hatman,"Intra-cloud trust management for Hadoop", in Proc. 5th Int. Conf. Cloud Comput., 2012
[11] S. Pearson and A. Benameur, Privacy, "security and trust issues arising from cloud computing", in Proc. 2nd Int. Conf. Cloud Comput.,pp. 693702,2010.
[12] E. Bertino, F. Paci, R. Ferrini, and N. Shang, "Privacy-preserving digital identity management for cloud computing", IEEE Data Eng. Bull, vol. 32, no. 1, pp. 2127, Mar. 2009.
[13] F. Skopik, D. Schall, and S. Dustdar, "Start trusting strangers bootstrapping and prediction of trust", in Proc. 10th Int. Conf. Web Inf. Syst. Eng., pp. 275289,2009.
[14] H. Guo, J. Huai, Y. Li, and T. Deng, "KAF: Kalman filter based adaptive maintenance for dependability of composite services", in Proc. 20th Int. Conf. Adv. Inf. Syst. Eng.,pp. 328342,2008.
[15] Y. Wei and M. B. Blake, "Service-oriented computing and cloud computing: Challenges and opportunities", IEEE Internet Comput., vol. 14, no. 6, pp. 7275, Nov./Dec. 2010.
[16] B. Fung, K. Wang, R. Chen, and P. Yu, "Privacy-preserving data publishing: A survey of recent developments", ACM Comput. Surv., vol. 42, no. 4, pp. 153, 2010.