International Journal of Research
Available at https://edupediapublications.org/journals
p-ISSN: 2348-6848
e-ISSN: 2348-795X
Volume 04 Issue 03
March 2017

A Private Cloud Interface between User and public Cloud Approach For Secure Authorized Deduplication

B. Naga Durga Prasad[1], K. Govardhan Babu[2]

[1]PG Scholar, Dept of CSE, Sri Sunflower College of Engineering and Technology, Lankapalli, Krishna Dist, AP.

[2] Assistant Professor, Dept of CSE, Sri Sunflower College of Engineering and Technology, Lankapalli, Krishna Dist, AP.

Abstract: Encryption techniques which were used traditionally were not compatible with data duplication while providing data confidentiality .We take our proposed authorized duplicate finding model is minimal overhead different normal models As a proof data is implement a prototype in our proposed authorized duplicate check scheme and data tested experiments in our prototype. To protect the confidentiality of sensitive data while supporting deduplication, the convergent encryption technique has been proposed to encrypt the data before outsourcing This paper is decries the data duplication and hybrid cloud storage in different models the concepts of cloud computing trust and reputation different questions related in trust and protection in cloud computing locations is discussed Computing model trust and reputation representation is widely discussed and applied in a lot of content model scenarios becoming subject in scientific researches and number of theoretical and practical values represents This paper is development a high level trust model and security reliable files changes number of user private cloud then the calculation system is trust different users according to the metrics previously methods.

Index terms: Availability, Cloud Computing, Distributed Computing, File system, Integrity, Reputation, Security and Trust

1. INTRODUCTION

Cloud computing provides seemingly unlimited "virtualized" resources to users as services across the whole Internet, while hiding platform and implementation details. Today's cloud service providers offer both highly available storage and massively parallel computing resources at relatively low costs [3]. A Hybrid Cloud approach terms that it is the cloud service providers which offer high storage and parallel computing resource at relatively low cost .cloud computing provide apparently unlimited "virtualized"[14] resources to users as services across the complete Internet, while hiding stand and operation details Today's cloud facility suppliers agreement both highly obtainable loading Due to the increasing data volume the cloud storage services are faced judgmentally .to make the data organization calmer in the cloud computing, reduplication In order to finding insufficient persons take a secure proof of ownership rule [2] is needed to user the proof then the user take owns file when a duplicate is found. Recently reduplication model is convergen security number of users confidentiality to some changes is support the duplicate finding with differential aspects we try to realize number of reduplication and differential authorization duplicate check at the every time. The data sheet use of Internet connected systems and sharing model is finding revolution [3]. Several web-based models such as Google Docs and Customer Relationship Management (CRM) [1] applications Virtual computing is also applied to stand-alone infrastructure as a service solution we review the main cloud computing architecture patterns and identify the main issues related to security, privacy, trust and availability. In order to address such issues, we present a high level architecture for trust models in cloud computing environments.[4]. We implement a prototype of the proposed authorized duplicate check and conduct tested experiments to evaluate the overhead of the prototype and show that the overhead is minimal compared to the normal convergent encryption

International Journal of Research
Available at https://edupediapublications.org/journals
p-ISSN: 2348-6848
e-ISSN: 2348-795X
Volume 04 Issue 03
March 2017

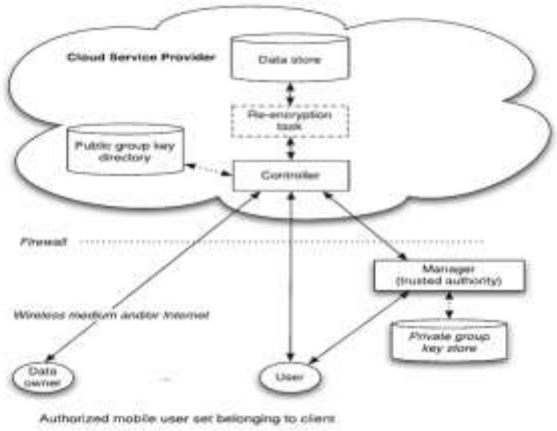


Figure 1 Cloud Computing Architecture

2. RELATED WORK:

In archival storage systems there is a huge amount of duplicate data or redundant data, which occupy significant extra equipments and power consumptions, largely lowering down resources and imposing extra burden on management as the scale increases. So data de-duplication [8] the goal of which is to minimize the duplicate data in the inter level, has been receiving broad attention both in academic and industry in recent years. Cloud computing refers to the use, through the Internet, of diverse applications as if they were installed in the user's computer, independently of platform and location. Several formal definitions for cloud computing have been proposed by industry and academia.[5] We adopt the following definition. This definition includes cloud architectures, security, and deployment strategies [6] A number of technologies have been employed in order to provide security for cloud computing environments. The creation and protection of security certificates is usually not enough to ensure the necessary security levels in the cloud. Cryptographic algorithms used with cloud applications usually reduce performance and such reduction must be restricted to acceptable levels [7]. The internal model is attack [8] power is the external adversaries we take the security inters the internal attacker represents in duplicate finding token this recues is defined in terms of two models First the user is privilege p, given a token ϕ', it requires the model is distinguish.

3. EXISTING SYSTEM:

The problems of de duplication in a hybrid cloud model taking a public cloud and a private cloud Different users levels in allocated to securely results duplicate check in private cloud.[9] A new duplication model supporting differential duplicate finding proposed the hybrid cloud model in the S-CSP besides in the public cloud The user take perform and duplicate check the files marked with corresponding privileges

we implement a prototype of the proposed authorized duplicate check and data tested in results the overhead of the prototype is take that the overhead is minimal compared to the normal convergent security. [8]

A. **Symmetric encryption** uses secret key to encrypt and decrypt data A symmetric encryption model take three Primitive sub functions.:[10]

KeyGenSE(1_) is the key generation algorithm and generates κ using security attributes

DecSE(κ,C)

The symmetric decryption algorithm is takes the secret κ and cipher text the outputs the original content.

EncSE(κ,M)

The symmetric encryption algorithm is used the secret κ and message and outputs the cipher text model.

B. **Convergent encryption**

Convergent encryption [3], [4] users content data confidentiality uses and data owner take convergent key from each fixed data copy and encrypts the data copy with the changing key.

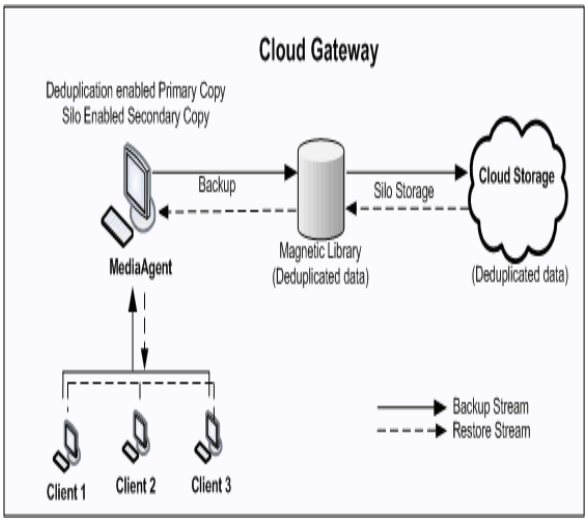
Key GenCE(M) K is the key generation algorithm and maps content copy to change key K

EncCE(K,M) C is the symmetric encryption algorithm is number of changes and key K and the data copy in inputs and the outputs security test.

DecCE(K,C) M is the decryption algorithm and number of ciphertext C is changes key K as inputs and outputs is fixed data copy M.

TagGen(M) T(M) is the tag generation algorithm and maps the fixed data copy M and outputs model T(M).

DecSE(κ,C) M is the symmetric decryption algorithm and the secret κ and ciphertext C the outputs fixed message M



4. METHOLOGY

We enhance our system in security. Specifically, we present an advanced scheme to support stronger security by encrypting the file with differential privilege keys. In this way, the users without corresponding privileges cannot perform the duplicate check [13]. The security of data storage is one of the best treated same the security for cloud computing is taken.[7] There is two concerns in the cloud. One concern is: users to take reveal own data to the cloud service users the concern in users is unsure t the data integrity the receive from the cloud within the cloud in conventional security model required for data security [12]. It may be used to frequently confirm both the data integrity and the authentication of a message. the resulting MAC algorithm is termed HMACMD5 or HMAC-SHA1 considered. The cryptographic potential of the HMAC belongs upon the cryptographic potential of the underlying hash function, hash result and on the volume and quality [14]

1. RELIABLE FILE DISTUBUTIONS

The report and related Research [15] [11] it is models to employ a cloud computing trust model security changes of files every cloud users in a trustworthy manner we take trust model to changes a ranking of trustworthy nodes and new model the secure destitutions of files every peers in a private cloud We propose a trust model in the selection and trust value changes and determines different a node is trustworthy is performed based on node storage space operating model link and processing capacity [16][6]

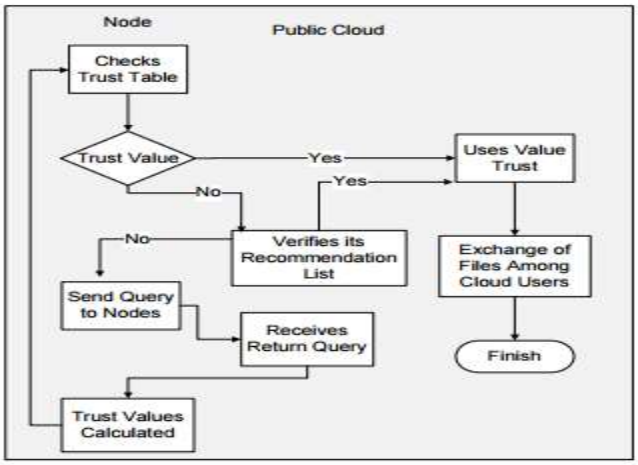


Fig No 3.High Level Trust Model

2. AUTHORIZED REDUPLICATION

The high level our setting of interest is different network consisting of a group of take clients and use the S-CSP and store data in reduplication models [17]. The greatly reducing storage space.[20] Such model is widespread and different suitable to user file backup and synchronization models the

richer storage data the entities defined in our system users private cloud and S-CSP in public cloud The S-CSP results duplication by checking if the contents of two files in same stores The access right to a file is defined based on a set of privileges we may define a role-based models the positions we may define a time based privilege that specifies a valid time period within which a file is taked.[18]

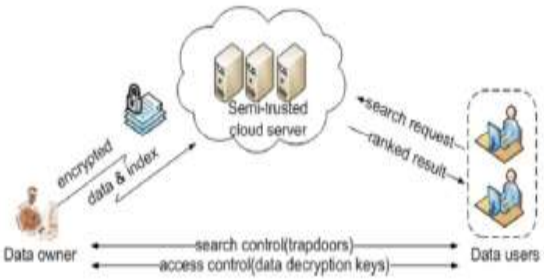


Fig No 4 Architecture for Authorized Reduplication

3. ROLE BASED ACCESS CONTROL MODELS

The author describes the RBAC (Role Based Access Control). The permissions are associated to the roles and members of roles. The roles are related to the user groups in access control. It is originated with the multi user computer system. This greatly simplifies the management of permission. The roles are used in the different job functions and it is assigned by the user based on their qualification. The role is stable it will change usually less frequently. The role is created for to do perform specific task. This administrative use of roles found in the modern networks OS. The research problem in this area is developing systematic approach to the design. Future work is to develop the systematic methodology and analysis of constraints etc., many of these open issue will require an integrated an integrated approach for their resolution.

5. RESULT

Once assigned the weights metrics, can perform the calculation of the trust of a node. Consider the node A and B and between them execute 10 iterations (j). The simulation is started by performing the calculation with the node A trusting B, is assigned the value 1 to all metrics. To perform the simulation we used the Monte Carlo method [19] for the generation of random numbers or pseudo-random, for four metrics: Storage Capacity, Processing Capacity from the first iteration, the values of each of these metrics are assigned randomly varying between 0 and 1[14]

Iteration 10						
CP (35%)	CA(35%)	CE(15%)	SO(15%)	CD	CDFinal	Decision Trust
0,58	0,80	0,72	0,64	0,69	0,53	Not Trust
Iteration 11						
CP (35%)	CA(35%)	CE(15%)	SO(15%)	CD	CDFinal	Decision Trust
0,27	0,54	0,95	0,19	0,46	0,52	Not Trust

6. CONCLUSION

The investigation is based on the notion of authorized data duplication was proposed to protect the data security by including differential privileges of users in the duplicate check. The implementation of this approach better Reduplication can be achieved by using block level Reduplication mechanism as compared to file level Reduplication Security analysis proves that our schemes are secure in terms of insider and outsider attacks specified in the proposed security ideal implemented a prototype of authorized duplicate check scheme and conduct tested experiments on our prototype System. Security analysis demonstrates that our schemes are secure in terms of insider and outsider attacks specified in the proposed security model using the concepts of trust and reputation, that has been promissory due to identification and vulnerabilities related to security, privacy and trust that a cloud computing environment presents

7. FUTURE WORK

It excludes the security problems that may arise in the practical deployment of the present model. Also, it increases the national security. Currently the system is implemented to support text based block level encryption and Reduplication this can be extended to all format like multimedia files, image files etc.

8. REFERENCES

[1] OpenSSL Project. http://www.openssl.org/.

[2] P. Anderson and L. Zhang Fast and secure laptop backups with encrypted de-duplication. In Proc. of USENIX LISA, 2010

[3] S. Bugiel, S. Nurnberger, A. Sadeghi, and T. Schneider. Twin clouds: An architecture for secure cloud computing. In Workshop on Cryptography and Security in Clouds (WCSC 2011), 2011.

[4] J. R. Douceur, A. Adya, W. J. Bolosky, D. Simon, and M. Theimer. Reclaiming space from duplicate files in a serverless

distributed file system. In ICDCS, pages 617–624, 2002.

[5] D. Ferraiolo and R. Kuhn. Role-based access controls. In 15th NIST-NCSC National Computer Security Conf., 1992.

[6]D. Ferraiolo, et al. "Roe Based access controls". In 15th NIST-NCSC National Computer Security Conf., 1992

[7]J. Li, et al. "Secure deduplication with efficient and reliable convergent key management". In IEEE Transactions on Parallel and Distributed Systems, 2013

[8] OpenSSL Project. http://www.openssl.org/

[9] P. Anderson and L. Zhang. Fast and secure laptop backups with encrypted de-duplication. In Proc. of USENIX LISA, 2010

[10] M. Bellare, S. Keelveedhi, and T. Ristenpart. Dupless: Serveraided encryption for deduplicated storage. In USENIX Security Symposium, 2013

[11] S. Uppoor, M. Flouris, and A. Bilas, "Cloud-based synchronization of distributed file system hierarchies," Cluster Computing Workshops and Posters (CLUSTER WORKSHOPS),.

[12] Qingsong Wei, Bharadwaj Veeravalli, Bozhao Gong, Lingfang Zeng, and Dan Feng, "CDRM: A Cost-Effective Dynamic Replication Management Scheme for Cloud Storage Cluster,".

[13] S. P. Marsh, "Formalising Trust as a Computational Concept", Ph.D. Thesis, University of Stirling, 1994.

[14] T. Beth, M. Borcherding, and B. Klein, "Valuation of trust in open networks," In ESORICS 94. Brighton, UK, November 1994.

[15] A. Jøsang and R. Ismail, "The Beta Reputation System," In Proceedings of the 15th Bled Electronic Commerce Conference, pp. 17-19. June 2002.

[16] A. Abdul-Rahman and S. Hailes, "A distributed trust model," In Proceedings of the 1997 New Security Paradigms Workshop, pp. 48-60, 1998.

[17] Zhidong Shen, Li Li, Fei Yan, and Xiaoping Wu, "Cloud Computing System Based on Trusted Computing Platform,"

[18] Li Xiaoqi, Lyu M R, and Liu Jiangchuan. "A trust model based routing protocol for secure AD Hoc network,"

[19] Zhimin Yang, Lixiang Qiao, Chang Liu, Chi Yang, and Guangming Wan, "A collaborative trust model of firewall-through based on Cloud Computing,"

[20] N. Santos, K. Gummadi, and R. Rodrigues, "Towards Trusted Cloud Computing," Proc. HotCloud. June 2009.