ISSN(Online): 2320 - 9801
ISSN (Print) : 2320 - 9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 6, June 2016

Strongly Secure Ramp Secret Sharing Algorithm for Distributed Deduplication System

Kavita Kukade[1], Prof. Soumitra Das[2]

Research Scholar, Department of Computer Engineering, Dr.D.Y.Patil School of Engineering, Pune, India [1]

Head of Department, Department of Computer Engineering, Dr.D.Y.Patil School of Engineering, Pune, India [2]

ABSTRACT: Information deduplication is the technique to compress the information by reducing the copy of duplicates and indistinguishable information. It is widely utilized as a part of cloud storage system structure to spare transfer speed and minimize the storage room. The Delicate and sensitive information is secured before outsourcing by using encryption technique which encodes the information. Here we propose novel distributed deduplication systems in which the data chunks are distributed across several cloud servers. To scatters the data pieces of file amongst numerous cloud servers we present distributed duplication system. Instead of using convergent encryption we proposed strongly secure ramp secret sharing method to achieved data security. We propose a strong secure secret sharing Ramp secret sharing over Ramp secret sharing scheme that enables more highly reliable and secure level. This method are more desirable than weak ramp secret sharing method and it is widely used as even in cases when some information from a secret seep out from a non-qualified set of share, it don't leave any portion of secret openly.

KEYWORDS: Deduplication, secret sharing, Distributed storage system, security.

I. INTRODUCTION

Information deduplication methods are broadly used to backup data and decrease storage overhead by identifying and removing redundancy between the data. Deduplication is used to avoid the storage of multiple data copies with same content. There are various types of deduplication such as block-level, file-level, client-side, server-side deduplication. Client-side deduplication is widely used by Cloud Storage Services ,The server ensure the file is not replicas over the cloud by checking and restricting when a certain file is already in the cloud (uploaded by some user previously), when a user want to upload a file to the server. In this manner, every single file will have only one copy in the cloud (Single Instance Storage). Deduplication is known for resource deployment in network bandwidth and storage space by several cloud academies and industry and for this reason that it can really improves storage consumption and minimize storage space. It diminishes applications like backup storage systems which has high deduplication ratio [1][2]. In Ramp secret sharing technique divide data into number of shares. Data reconstructed after collecting numerous shares. In case the adversities destroy half the parts, he/she cannot hack data, this method enables of secure key management for cryptographic system which can function securely and reliably [3][4][5].In convergent encryption key is derived from data copy itself and this key is used to encrypt data[6][7].In deduplication system we introduce the distributed cloud storage servers. Instead of convergent encryption mechanisms, we used secret sharing method for protect data security, by using the secret sharing technique we first divide file and encoded into pieces and then sends these data pieces to multiple cloud servers [8].

II. RELATED WORK

In [3] paper author show how to data divided into number of parts. Authors specify some threshold value to reconstruct the data. In case the adversities destroy half the parts, he/she cannot able to hack data .This method enables of secure key management for cryptographic system which can function securely and reliably. In [9] authors Worked on confidentiality, access control, fault tolerance. To manage access to files and directories author uses capability access control model, for confidentiality author uses cryptography and for fault tolerance author uses erasure coding. By using

ISSN(Online): 2320 - 9801
ISSN (Print) : 2320 - 9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 6, June 2016

erasure coding and cryptography data in the file system is distributed across multiple servers. Minimize users vulnerability to these servers minimize using both cryptography and erasure coding. In [10] Authors used convergent encryption for encrypting data or file. In convergent encryption key is generated from data copy. In this paper author addressed the problem of key management through distributing these key across the numerous server. In [11] this paper key server is used to stored the keys, client encrypt data or file by using key and that key is obtained from key server through PRF protocol. This technique achieves strong secrecy guarantee, by facilitating the clients to store encrypted data with the existing service and performing deduplication. In [12] authors address the problem of outflow of user's private data by using the proofs of ownership method. By using proof of ownership method any user can prove the ownership of data to the cloud server if user wants to upload file. Authors first construct the hash function this hash function is used to obtain proof of ownership. Proof of ownership run by user with cloud storage server. In this paper authors uses convergent encryption for encrypting file. File is encrypted by using hash value.

III. PROPOSED ALGORITHM

A. *Design goal*

- Distributed deduplication system.
- Secrete sharing.
- To improve the security.
- Divide secret data into number of parts.
- Run the strong secure ramp secret sharing algorithm.
- Set the threshold value for secret message
- Send this part of data to cloud server and other user.
- When user want to download.
- Now we only have the number of shares equal to threshold. But from these shares we can reconstruct the secret using Lagrange interpolation.

B. *Description of the Proposed Algorithm:*

Step 1: Share computation has following three basic steps.

a) Decide secret: first we have to decide that which is our secret message. Then we need to convert it to byte array so that we can treat it as a number.

b) Decide threshold: Further we need to decide the threshold value. Threshold is the minimum number of shares that we need to know to recover the secret.

c) Create polynomial: $s(y) \equiv m + s1y1 + s2y2 + \cdots + sk - 1yk - 1 \ (mod\ p1)$,
Where, p1= a (large) prime number,
m:- secret value
s_1,……,s_{k-1}:- randomly chosen from [0, p1-1],
Select n Random integer y_1, y_2,……,y_n form [0,p1-1]
Deliver (y_i, s(y_i)) to the *i*-th users.

Step2: Secrete reconstruction:
Now we only have the number of shares equal to threshold. But from these shares we can reconstruct the secret using Lagrange interpolation.

IV. PSEUDO CODE

Step 1: Let S be the secret.
Step2: Construct general Access structure Γ *G = {AC*1, *AC2*…… *ACL}.*
Step3: Construct encoder φΓG(S, N),
Where ΓG is access structure,
S is secret and N is random number.
Step4: Then, we choose publicly G× *G* non-singular matrix *M*.

ISSN(Online): 2320 - 9801
ISSN (Print) : 2320 - 9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 6, June 2016

Step5: define a new encoder$\varphi\Gamma G(\boldsymbol{S}', \boldsymbol{N}) \overset{Def}{=} \varphi\Gamma L(\boldsymbol{S}'\boldsymbol{M}, \boldsymbol{N})$.

V. RESULTS

1) Confidential Level:

It shows the encoding / decoding times versus the confidentiality level *r*. To realize this test, the number of S-CSPs $n = 5$ and the reliability level $n - k = 2$ are fixed. From the figure, it can be easily found that the Encoding / decoding time increases with *r*.

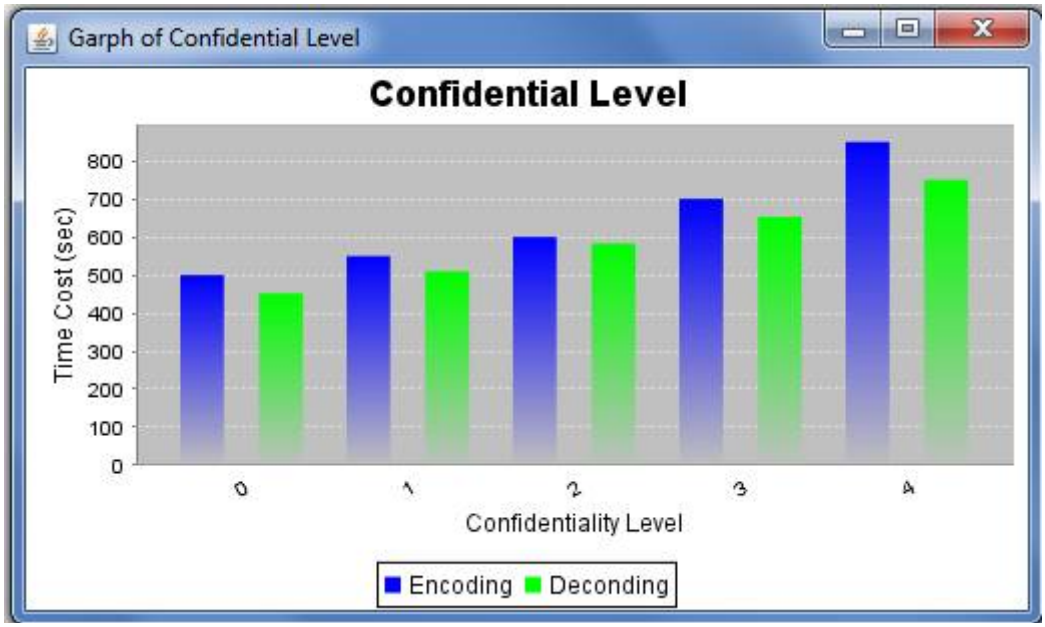

Fig1: Encoding/decoding time versus Confidential Level

The efficiency of the proposed distributed systems are mainly determined by the following three parameters of *n*, *k*, L and *r* in SRSS. The graph of Impact of confidentiality level *r* on the encoding/decoding times where $n = 5$ and $n - L=2$ and L>2 It shows the encoding / decoding times versus the confidentiality level *r*. To realize this test, the number of S-CSPs $n = 5$ and the reliability level $n - k = 2$ are fixed. From the figure, it can be easily found that the Encoding / decoding time increases with *r*.
In this experiment, we choose 1KB as the default data block size, which has been widely adopted for block-level deduplication systems. We choose the hash function SHA-256 with an output size of 32 bytes.

2) Secure Impact of Encoding and Decoding of strong ramp secret sharing:
We can also observe that the encoding time is higher than the decoding time. The reason for this result is that the encoding operation always involves all *n* shares, while the decoding operation only involves a subset of k-$l < n$ shares.

ISSN(Online): 2320 - 9801
ISSN (Print) : 2320 - 9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 6, June 2016

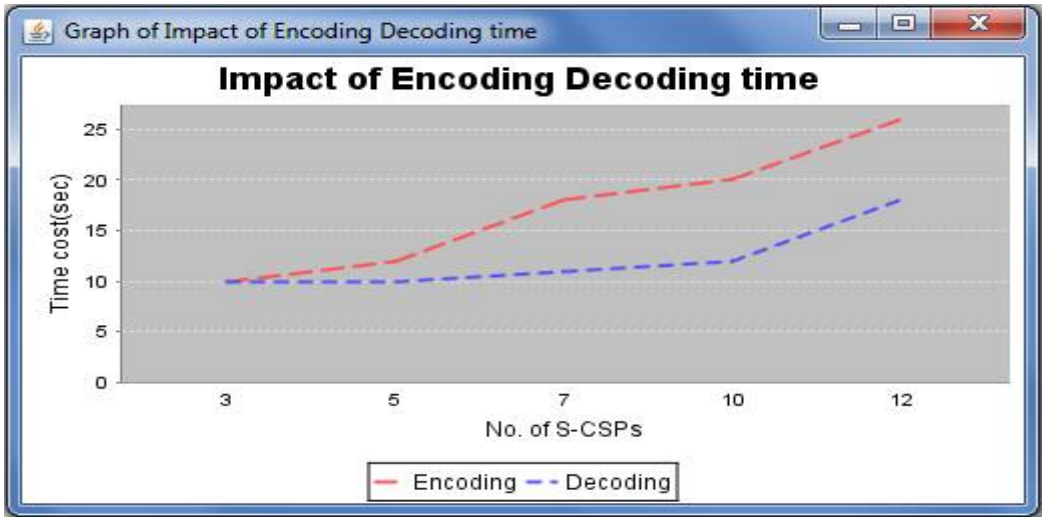

Fig2: Impact of Encoding and Decoding of strong ramp secret sharing

We implement the SRSS for this we choose the erasure code in the (*n*, *k*, *L*)-SRSS whose generator matrix is a *Hilbert matrix* for the data encoding and decoding.
The performance of several basic modules in our constructions is tested in our experiment. First, the average time for generating a secrete output from a 1KB data block. The average time for generating a secrete with the same output length from a file.

3) Security Level:
As existing system user can share k shares out of n, but secret leaks from a non-qualified set of shares, while in proposed system secret cannot leak from non-qualified set of shares.

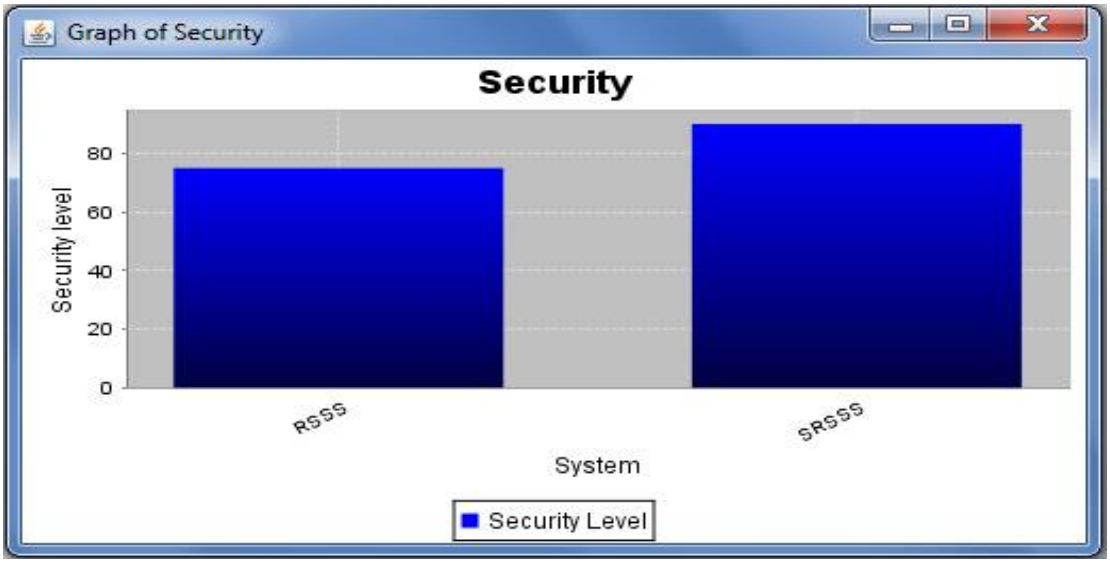

Fig3:-Security comparison between ramp secret sharing and strong secure ramp secret sharing scheme

ISSN(Online): 2320 - 9801
ISSN (Print) : 2320 - 9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 6, June 2016

The above fig shows analysis of RSSS and SRSSS algorithm. We improved the efficiency and security in proposed system. Intermediate sets in ramp SS schemes are allowed to leak out a part of a secret. We analyse how the secret partially leaks out the share. Proposed system not allowed to leak out the information from non-qualified set.

VI. CONCLUSION AND FUTURE WORK

To increase security of data we proposed Strong secure ramp secret sharing algorithm for distributed deduplication system. Instead of using convergent encryption we proposed strongly secure ramp secret sharing method to achieved data security. We also planned how to construct strong ramp secret share schemes through ordinary entrée secret share structures. To calculate a strong Ramp secret share, we can use a transform matrix from partly decryptable Ramp secret share technique.

In future scope we can implement multi-secret sharing scheme which will be generalization of secret sharing in which several secrets are spread according to different entre structures on the same set of participant.

REFERENCES

1. M. W. Storer, K. Greenan, D. D. E. Long, and E. L. Miller, "Secure data deduplication," in Proc. of StorageSS, 2008.
2. J. Stanek, A. Sorniotti, E. Androulaki, and L. Kencl, "A secure data deduplication scheme for cloud storage," in *Technical Report*,2013.
3. A. Shamir, "How to share a secret," *Common. ACM*, vol. 22, no. 11,pp. 612–613, 1979.
4. A. D. Santis and B. Masucci, "Multiple ramp schemes," *IEEE Transactions on Information Theory*, vol. 45, no. 5, pp. 1720–1728,Jul. 1999.
5. G. R. Blakley and C. Meadows, Security of ramp schemes, in Advances in Cryptology: Proceedings of CRYPTO 84, ser. Lecture Notes in Computer Science, G. R. Blakley and D. Chaum, Eds. Springer-Verlag Berlin/Heidelberg, 1985, vol. 196, pp. 242-268.
6. ——, "Message-locked encryption and secure deduplication," in *EUROCRYPT*, 2013, pp. 296–312.
7. W. K. Ng, Y. Wen, and H. Zhu, "Private data deduplication protocols in cloud storage." in *Proceedings of the 27th Annual ACM Symposium on Applied Computing*, S. Ossowski and P. Lecca, Eds. ACM, 2012, pp. 441–446.
8. Jin Li, X. Chen, Xinyi Huang, Shaohua Tang and Yang Xiang Secure Distributed Deduplication Systems with Improved Reliability, IEEE Transactions on Computers Volume: PP Year: 2015.
9. Wilcox-O'Hearn and B. Warner, "Tahoe: the least-authority file system," in *Proc. of ACM, StorageSS*, 2008
10. J. Li, X. Chen, M. Li, J. Li, P. Lee, and W. Lou, "Secure deduplication with efficient and reliable convergent key management," in *IEEE Transactions on Parallel and Distributed Systems*, 2014, pp. vol.25(6), pp. 1615–1625.
11. M. Bellare, S. Keelveedhi, and T. Ristenpart, "Dupless: Serveraided encryption for deduplicated storage," in *USENIX Security Symposium*, 2013.
12. J. Xu, E.-C. Chang, and J. Zhou, "Weak leakage-resilient client-side deduplication of encrypted data in cloud storage," in *ASIACCS* 2013, pp. 195–206.
13. M. Li, C. Qin, P. P. C. Lee, and J. Li, "Convergent dispersal: Toward storage-efficient security in a cloud-of-clouds," in *The 6th USENIX Workshop on Hot Topics in Storage and File Systems*, 2014.

BIOGRAPHY

Kavita B. Kukade is a ME student in the Computer Engineering Department, Dr.D.Y.Patil, School of Engineering from Pune University. She received BE degree from Amravati University, MS, India. Her research interest Cloud Computing.

Prof. Soumitra S. Das received his Bachelor degree in Computer Engineering from North Maharashtra University, Jalgaon, Maharashtra, India and Master degree in Computer Engineering from University of Pune, Pune, Maharashtra, India. Currently, he is PhD researcher at Sathyabama University, Chennai, India. His research interest includes Computer Networks, Wireless Sensor Networks, etc. He is a member of IEEE, CSI, LMISTE, IACSIT and IAENG.