MJRET
Open Access
Multidisciplinary Journal of Research in Engineering and Technology
Journal homepage: www.mjret.in
ISSN:2348 - 6953

STRONGLY SECURE RAMP SECRET SHARING IN DISTRIBUTED DEDUPLICATION IN SYSTEMS

Kavita Kukade-Ghurde, Prof. Soumitra Das

Department of Computer Engineering, Savitribai Phule Pune University
Dr. D.Y.Patil School of Engineering Charholi, Pune
Pune,India

Abstract: *Information deduplication is the procedure which packs the information by evacuating the copy duplicates of indistinguishable information and it is widely utilized as a part of cloud stockpiling to spare transfer speed and minimize the storage room. To secure the classification of delicate information amid deduplication, the joined encryption system is utilized to encode the information before outsourcing. For better information insurance, this paper talks about the issue of information deduplication approval. Here we propose novel distributed deduplication systems with privileged reliability in which the data pieces are scattered across several cloud servers. There are a few new deduplication executions giving approved deduplication confirmation in a half breed i.e. hybrid cloud approach. Also here we propose a strong secret sharing Ramp secret sharing over Ramp secret sharing scheme that enables more highly reliable and secure level. The strong ramp secret sharing schemes are more desirable because they do not slip out any portion of a secret explicitly even in the situation where some information about the secret leaks from a non-qualified set of shares henceforth, they are more desirable than weak ramp secret sharing schemes.*

Keywords*: deduplicition, distributed storage system, Strong ramp secret sharing,reliability.*

1. INTRODUCTION

Cloud storage service is gaining popularity. To reduce resource consumption in network bandwidth and storage, many cloud storage services employs client-side deduplication**.[1]** That is, when a user tries to upload a file to the server, the server checks whether this particular file is already in the cloud (uploaded by some user previously), and saves the uploading process if it is. In this way, every single file will have only one copy in the cloud (Single Instance Storage). Deduplication has received much attention from both academia and industry because it can greatly improves storage utilization and save storage space, especially for the applications with high deduplication ratio such as archival storage systems.

A secret sharing scheme **[7]** is a technique to encrypt a secret ***S*** into *n* shares each of which has no information of ***S***, but ***S*** can be decrypted by collecting numerous shares. In order to increase the efficiency of secret sharing schemes, ramp secret sharing schemes **[8]** are suggested, which have a trade-off between security and coding efficiency. In this paper, we converse about strong ramp secret sharing schemes with general access structures. We ascertain access secret sharing schemes named as partially decryptable ramp secret sharing schemes, in which each non-qualified set with *k−l* shares can decrypt explicitly (*L − l)/L* parts of a secret **s**. Then, we simplify the relation between partially decrypt able ramp secret sharing schemes and absolute secret sharing schemes with plural secrets. We as well point out that (*k, L, n*)-ramp Secret sharing schemes based on Shamir's polynomial interpolation method**[10]** are not always robust. We propose how to convert partially decryptable ramp secret sharing schemes into strong ramp secret sharing schemes by application a beeline transformation, and we analyze that any access structure that can be recognized as a not strong ramp secret sharing scheme can as well be accomplished as a able access secret sharing scheme.

2. LITERATURE SURVEY

- **M. O. Rabin [3]** Randomly chosen irreducible polynomials p(t) ϵ $Z_2[t]$ are used to "fingerprint" bit-string. This method is applied to create a very simple real time string matching algorithm and technique for securing files against unauthorized variations. The method is proved as highly reliable and efficient for each input.

- **A. Adya , D. Simon ,J. R. Douceur , W. J. Bolosky , and M. Theimer [4]**, In this paper, authors present a mechanism to reclaim space from incidental duplication for controlled file replication to make it available. Authors mechanism includes 1) convergent encryption, which encrypt the file by using hash function then hash value is encrypted using the public key of user, 2) Self Arranging, Lossy, Associative Database(SALAD) it is used for aggregating file content and information location in a decentralized, scalable, fault-tolerant. Huge scale reenactment examinations demonstrate that the duplicate-file merging system is scalable, fault-tolerant , and very effective.

- **M. Bellare, S. Keelveedhi, and T. Ristenpart [5],** In this paper an architecture is proposed by authors which gives secure deduplicated storage struggling brute-force spasms, and identify it in a system called "DupLESS". In DupLESS, clients encrypt message-based keys took from a key-server by an unaware PRF protocol. It allows clients to use an available service to store encrypted data and have the service accomplish deduplication on their behalf, and still provides strong confidentiality guarantees. Using the storage service with plaintext data they show that encryption for deduplicated storage can reach performance and space savings close to these techniques.

- **A. D. Santis and B. Masucci [8]:** Here (t; k; n; S) ramp structure is a protocol to distribute a secret 's' chosen in S amongst a set P of 'n' contributors in a particular way such as: 1) sets of contributors of cardinality are equal to or greater than k can

restructure the secret ‘s’; 2) sets of contributors of cardinality are equal to or less than ‘t’ have no information on s, while 3) sets of contributors of cardinality are less than k and greater than t so they might have some information of ‘s’. In this correspondence author examine numerous ramp schemes, which are protocols to share lots of secrets amongst a set P of contributors, using diverse ramp schemes. Specifically they verify a tight lower bound on the size of the shares held by every participant and on the dealer's randomness in numerous ramp schemes.

- **Jin li,wenjing lou [11],** In this paper author propose by using Dekey,secure deduplication with an efficient and reliable convergent key management scheme. In this paper author introduce disadvantages of a baseline approach. To store convergent keys , Dekey uses Ramp secret sharing scheme.

3. PROPOSED WORK

Since non-forbidden sets with $1 \le l \le L - 1$ in ramp secret sharing schemes are permitted to leak out a portion of a secret, it is significant to analyze how the secret partly outflows . For instance, if a secret is a private data which consists of name, address, phone number, job, income, bank account details, etc., any portion of the secret should not come out explicitly. Conversely, in the situation that the security is measured by the conditional entropy, we cannot know whether or not a part of the secret can be decrypted from a non-forbidden set.

As in the traditional system ramp has some disadvantages so here we propose strongly secure ramp secret share schemes with common access structures. We express strong ramp secret sharing schemes known as partly decryptable ramp secret sharing schemes, in which each non-qualified set with $k-l$ shares can decrypt explicitly $(L - l)/L$ fragments of a secret. After that , we streamline the relation between Partially decryptable ramp secret sharing schemes and flawless secret sharing schemes with plural secrets. The (k, L, n)-ramp secret sharing schemes based on Shamir’s polynomial interpolation method are not always robust this also mention in proposed system.Here we propose how to transform partially descryptable ramp secret sharing schemes into strong ramp secret sharing schemes by using a linear transformation, and we simplify that some access structure which can be understood as a not strong ramp secret sharing scheme can also be understood as a strong ramp secret sharing scheme.

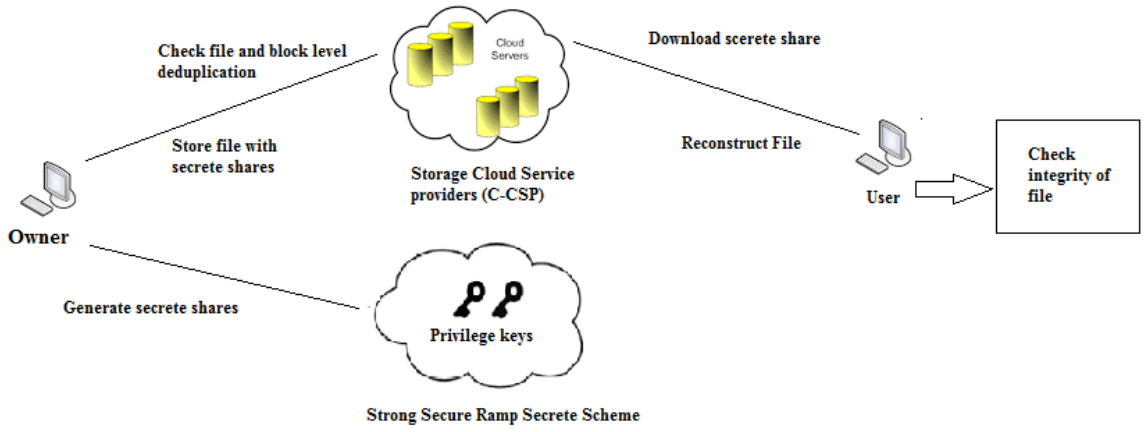

Fig.3.1:- System Architecture Diagram

As shown in architecture diagram in fig 3.1, Storage cloud service provider is assumed to be n with identities represented by id_1, id_2…, id_n, respectively. The Owner who wants to upload file F to storage cloud service provider, owner first interact with storage cloud service provider to check deduplication, for this owner 1st compute TagGen algorithm for file duplicate check. If duplicate is found then owner send TagGen(F, id_j) to the j^{th} server with identity id_j via secure channel. If file metadata matches with existing data on server, the user will be providing a pointer for the shared stored at server id_j.

If duplicate is not found, owner run strong ramp secrete sharing algorithm over fie F to get c_j, where c_j is the j^{th} share of file F. Also owner compute TagGen (F, id_j), for which works as the tag for the j^{th} storage cloud service provider and upload all the parameters to storage cloud service provider with identity id_j via secure channel.

To download file F, user send pointer F to k out of n server. The user first download the secrete shares from $\{c_j\}$ of the file from k out of n storage server. When collecting ample shares the user recreates file *F* by using the algorithm of Recover ($\{c_j\}$). And lastly user check the file integrity using Message authentication check is run by the users, which is used to detect if the downloaded and decrypted data are complete and uncorrupted or not.

4. Expected Result

- Improve the reliability of data.
- Fine-grained block-level data deduplication.
- Highly secure system with strongly ramp secure sharing algorithm.
- Successful reconstruction of file from storage cloud service provider

5. CONCLUSION AND FUTURE WORK

To improve the reliability of data authors proposed the distributed deduplication systems though achieving the privacy of the users outsourced data without an encryption mechanism. In order to support file-level and block-level data deduplication; Authors constructed four new mechanisms which achieve consistency and integrity. Authors implemented deduplication systems by using the Ramp secret sharing scheme. We propose a strong Ramp secret sharing scheme Ramp secret sharing scheme that enables more highly reliable and secure level and also we work on byte level instead of block level deduplication. Byte-level is a form of block-level deduplication that knows the "semantics", of the data. These systems are sometimes called CAS – Content Aware Systems**.** Thus we have studied the concept of Deduplication, Secret Sharing, Distributed System in detail.

ACKNOWLEGEMENT

We would like to thank MJRET for giving such wonderful platform for the PG students to publish their research work. Also would like to thanks to our guide & respected teachers for their constant support and motivation for us. Our sincere thanks to DR. D.Y.PATIL SCHOOL OF ENGINEERING CHARHOLI, PUNE for providing a strong platform to develop our skill and capabilities.

REFERENCES

[1] Amazon, "Case Studies," https://aws.amazon.com/solutions/casestudies /# backup.

[2] J. Gantz and D. Reinsel, "The digital universe in 2020: Big data, bigger digi tal shadows, and biggest growth in the far east," http://www.emc.com/collateral/analyst-reports/idc-the digital-universe-in-2020.pdf, Dec 2012.

[3] M. O. Rabin, "Fingerprinting by random polynomials," Center for Research in Computing Technology, Harvard University, Tech Rep. Tech. Report TR-CSE-03-01, 1981.

[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, 2002, pp. 617–624.

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

[6] "Message-locked encryption and secure deduplication," in EUROCRYPT, 2013, pp. 296–312.

[7] 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.

[8] A. D. Santis and B. Masucci, "Multiple ramp schemes," IEEE Transactions on Information Theory, vol. 45, no. 5, pp. 1720–1728, Jul. 1999.

[9] M. O. Rabin,"Efficient dispersal of information for security, load balancing, and fault tolerance," Journal of the ACM, vol. 36, no. 2, pp. 335–348, Apr. 1989.

[10] A. Shamir, "How to share a secret," Commun. ACM, vol. 22, no. 11, pp. 612–613, 1979.

[11] 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.