ISSN (Online) 2394-2320

International Journal of Engineering Research in Computer Science and Engineering (IJERCSE)
Vol 4, Issue 8, August 2017

"Implementation of file level and block level deduplication and detecting attacks in cloud environment."

[1] Prof. Samita Mokal., [2] Prof. Nilima Nikam, [3] Prof. Vaishali Londhe
[1]Shivajirao S. Jondhale College Of Engineering, Dombivli ,India
[2][3] Yadavrao Tasgoankar Institute of Engineering and Technology, Bhivpuri Rd, India

***Abstract*— In cloud computing, security and storage space management techniques are most important factors for improving the performance of cloud computing. Secure deduplication is a technique for eliminating duplicate copies of storage data, and provides security to them. To reduce storage space and upload bandwidth in cloud storage deduplication has been a well-known technique.. The basic idea in this paper is that we can eliminate duplicate copies of storage data and limit the damage of stolen data if we decrease the value of that stolen information to the attacker. This paper makes the first attempt to formally address the problem of achieving efficient and reliable key management in secure deduplication. we propose Sekey, User Behavior Profiling and Decoys technology. Sekey new construction in which users do not need to manage any keys on their own but instead securely distribute the convergent key shares across multiple servers for insider attacker. As a proof of concept, we implement Sekey using the Ramp secret sharing scheme and demonstrate that Sekey incurs limited overhead in realistic environments. User profiling and decoys, then, serve two purposes. First one is validating whether data access is authorized when abnormal information access is detected, and second one is that confusing the attacker with bogus information. We posit that the combination of these security features will provide unprecedented levels of security for the deduplication in insider and outsider attacker..**

***Keywords*— Deduplication , proof of ownership, convergent encryption, key management, decoy technology.**

1. INTRODUCTION

Cloud computing is model of the distribution of the information services in which the resources are the retrieved from the web through some of the interfaces and applications, instead forming direct connections to the server.Cloud storage systems provide the management of the ever increasing quantity of data by keeping in mind factors like reduce occupation storage space and the network bandwidth. To make the scalable and consistent management of the data in the cloud computing, deduplication technique plays an important role. Data deduplication also helps to improve the results in efficiency term and searches are quicker. Data deduplication may happen as file level deduplication or as block level data deduplication. Instead of maintaining numerous duplicate copies of file or the data with alike content, deduplication senses and remove the redundant data by keeping original physical copy. Data deduplication is a technique of eliminate duplicate copies of data, and it is used in cloud storage to reduce storage space and bandwidth. An arising challenge is to perform secure deduplication in cloud storage even if convergent encryption is extensively adopted for secure deduplication; a critical issue is that making of convergent encryption practical to manage a huge number of convergent keys efficiently and reliably.

Specifically, each user must associate an encrypted convergent key with each block of its outsourced encrypted data copies, so as to later restore the data copies. Although different users may share the same data copies, they must have their own set of convergent keys so that no other users can access their files. As a result, the number of convergent keys being introduced linearly scales with the number of blocks being stored and the number of users. This key management overhead becomes more prominent if we exploit fine-grained block-level deduplication.

The decoys, then, serve two purposes: First is that validating whether data access is authorized when abnormal information access is detected, and second one is that confusing the attacker with bogus information. Now this is all about of outsider attacker protection while

ISSN (Online) 2394-2320

International Journal of Engineering Research in Computer Science and Engineering (IJERCSE)
Vol 4, Issue 8, August 2017

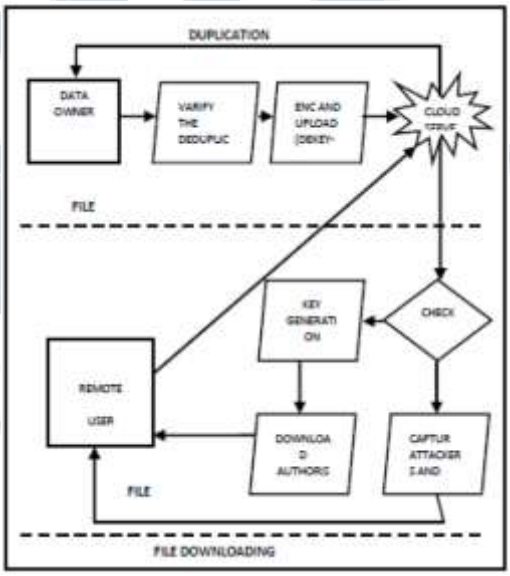
increase insider attacker with secure deduplication we are use convergent encryption [8] provides a viable option to enforce data confidentiality while realizing deduplication. It encrypts/decrypts a data copy with a convergent key, which is derived by computing the cryptographic hash value of the content of the data copy itself [8]. After key generation and data encryption, users retain the keys and send the cipher text to the cloud. Since encryption is deterministic, identical data copies will generate the same convergent key and the same cipher text. This allows the cloud to perform deduplication on the cipher texts. The cipher text scan only is decrypted by the corresponding data owners with their convergent keys. Dekey new construction in which users do not need to manage any keys on their own but instead securely distribute the convergent key shares across multiple servers for insider attacker. As a proof of concept, we implement Sekey using the Ramp secret sharing scheme and demonstrate that Sekey incurs limited overhead in realistic environment.

2.PRAPOSED SCHEME

The basic idea in this paper is that we can eliminate duplicate copies of storage data and limit the damage of stolen data if we decrease the value of that stolen information to the attacker. This paper makes the first attempt to formally address the problem of achieving efficient and reliable key management in secure deduplication. We propose for providing security in insider attacker as well as outsider attacker and monitoring them we use for that Secretekey, user behaviour profiling and Decoy Technology.
We implement Secretekey using the Ramp secret sharing scheme that enables the key management to adapt to different reliability and confidentiality levels. Our Evaluation demonstrates that Secrtekey incurs limited overhead in normal upload/download operations in realistic cloud environments.
We propose Secretkey, an efficient and reliable convergent key management scheme for secure deduplication..
We propose for providing security in insider attacker as well as outsider attacker and monitoring them we use for that secrekey, user behaviour profiling and Decoy Technology.

Diadvantags:
1. It does not provide efficient and reliable convergent key management
2. It is text based encryption and decryption scheme which generates the lot of keys
3. It is inefficient.
4. Each user only needs to keep the master key

Advantages:
1. Distinguishing feature of our proposal is that data integrity, including tag consistency, can be achieved.
2. Our proposed constructions support both file-level and block-level deduplications.
3. Security analysis demonstrates that the proposed deduplication systems are secure in terms of the definitions specified in the proposed security model.
4.Two kinds of collusion attacks are considered in our solutions. These are the collusion attack on the data and the collusion attack against servers.



Data Owner
In this module, the data owner uploads their data in the cloud server. For the security purpose the data owner encrypts the data file and then store in the cloud. The data owner can check the duplication of the file over Corresponding cloud server. The Data owner can have capable of manipulating the encrypted data file and the data owner can check the multiple cloud data as well as the duplication of the specific file

Cloud Server
The cloud service provider manages a cloud to provide data storage service. Data owners encrypt their data files and store them in the cloud for sharing with Remote User.

ISSN (Online) 2394-2320

International Journal of Engineering Research in Computer Science and Engineering (IJERCSE)
Vol 4, Issue 8, August 2017

To access the shared data files, data consumers download encrypted data files of their interest from the cloud and then decrypt them.

Remote User

In this module, remote user logs in by using his user name and password. After he will request for secrete key of required file from cloud servers, and get the secrete key. After getting secrete key he is trying to download file by entering file name and secrete key from cloud server.

Attacker Module

In remote user module, while downloading time if remote user entered any wrong file name or secrete key then cloud servers treats him as attacker and moves his access permission to block/attacker list

3. RESULTS:

3.Results:

Home page.

View all request

View Data owners

View attakers

Cloud server

ISSN (Online) 2394-2320

International Journal of Engineering Research in Computer Science and Engineering (IJERCSE)
Vol 4, Issue 8, August 2017

View all transactions

4. CONCLUSION

We propose Sekey, an efficient and reliable convergent key management scheme for secure deduplication. Sekey applies deduplication among convergent keys and distributes key shares across multiple key servers and provides confidentiality of outsourced data. Sekey implements small encoding/decoding overhead compared to the network transmission overhead in the regular upload/download operations.attacker module makes it more secure

REFERENCES

[1] Jin Li, Xiaofeng Chen, Mingqiang Li, Jingwei Li, Patrick P.C. Lee, and Wenjing louieee ,Secure Deduplication with Efficient and Reliable Convergent Key Management. IEEE transactions on parallel and distributed systems, vol. 25, no. 6, june 2014

[2] M. Bellare, A. Desai, E. Jokipii, and P. Rogaway. A Concrete Security Treatment of Symmetric Encryption: Analysis of the DES Modes of Operation. Proceedings of the 38th Symposium on Foundations of Computer Science, IEEE, 1997.

[3] Abdul Wahid Soomro, Nizamuddin, Arif Iqbal Umar, Noorul Amin."Secured Symmetric Key Cryptographic Algorithm for Small Amount of Data" 3rd International Conference on Computer & Emerging Technologies (ICCET 2013)

[4] M.W. Storer, K. Greenan, D.D.E. Long, and E.L. Miller, „„Secure Data Deduplication,"" in Proc. StorageSS, 2008, pp. 1-10.

[5] W. J. Bolosky, J. R. Douceur, D. Ely, and M. Theimer, "Feasibility of a Serverless istributed File System Deployed on an Existing Set of Desktop PCs", SIGMETRICS 2000, ACM, 2000, pp.34-43.

[6] A. Adya, W. J. Bolosky, M. Castro, R. Chaiken, G. Cermak, J. R. Douceur, J. Howell, J. R. Lorch, M. Theimer, and R. Wattenhofer.FARSITE: Federated, available, and reliable storage for an incompletely trusted environment. In Proceedings of the 5th Symposium on Operating Systems Design and Implementation (OSDI), Boston, MA, Dec.2002. USENIX.

[7] A.D. Santis and B. Masucci, „„Multiple Ramp Schemes,"" IEEE Trans. Inf. Theory, vol. 45, no. 5, pp. 1720-1728, July 1999.

[8] G.R. Blakley and C. Meadows, "Security of Ramp Schemes ", in Proc. Adv. CRYPTO, vol. 196, Lecture Notes in Computer Science,G.R. Blakley and D. Chaum, Eds., 1985, pp. 242-268.

[9] M.O. Rabin, „„Efficient Dispersal of Information for Security, Load Balancing, Fault Tolerance,"" J. 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] NIST"s Policy on Hash Functions, Sept. 2012. [Online]. Available: http:// csrc. nist. gov/ groups/ST /hash/policy.html.

[12] AmazonCase Studies. [Online]. Available: https://aws.amazon. com/solutions/case-studies/#backup.

[13] P. Anderson and L. Zhang, „„Fast and Secure Laptop Backups with Encrypted De-Duplication,"" in Proc. USENIX LISA, 2010, pp. 1-8.

[14] M. Bellare, S. Keelveedhi, and T. Ristenpart, „„Message-Locked Encryption and Secure Deduplication,"" in Proc. IACR Cryptology ePrint Archive, 2012, pp. 296-3122012:631.

[15] G.R. Blakley and C. Meadows, „„Security of Ramp Schemes,"" in Proc. Adv. CRYPTO, vol. 196,

Lecture Notes in Computer Science, G.R. Blakley and D. Chaum, Eds., 1985, pp. 242-268.

[16] 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 Proc. ICDCS, 2002, pp. 617-624.

[17] J. Gantz and D. Reinsel, The Digital Universe in 2020: Big Data, Bigger Digital Shadows, Biggest Growth in the Far East, Dec. 2012. [Online]. Available: http://www.emc.com/collateral/analystreports/ idc-the-digital-universe-in-2020.pdf.

[18] S. Halevi, D. Harnik, B. Pinkas, and A. Shulman-Peleg, „„Proofs of Ownership in Remote Storage Systems,"" in Proc. ACM Conf. Comput. Commun. Security, Y. Chen, G. Danezis, and V. Shmatikov, Eds., 2011, pp. 491-500.

[19] D. Harnik, B. Pinkas, and A. Shulman-Peleg, „„Side Channels in Cloud Services: Deduplication in Cloud Storage,"" IEEE Security Privacy, vol. 8, no. 6, pp. 40-47, Nov./Dec. 2010.

[20] S. Kamara and K. Lauter, „„Cryptographic Cloud Storage,"" in Proc. Financial Cryptography: Workshop Real-Life Cryptograph. Protocols Standardization, 2010, pp. 136-149.