Volume No:2, Issue No:3 (August-2016)
ISSN No : 2454-423X (Online)
International Journal of Research in Advanced Computer Science Engineering
A Peer Reviewed Open Access International Journal
www.ijracse.com

A Hybrid Approach to Data Protection in the Cloud

Y.Sushanthi
M.Tech Student,
Dept of Computer Science Engineering,
Prasad College of Engineering.

N.Venkateshwarlu
Assistant Professor,
Prasad College of Engineering.

ABSTRACT:

Data deduplication and compression to eliminate duplicate data necessary for applying one of, data copying, and disk space and speed large scale cloud storage to save money in the collapse of the once was. Sensitive data to protect privacy, the deduplication technology support convergent rescue has to encrypt data before outsourcing. Welcome to protect data security, this document formally unauthorized data deduplication to address the problem, first try. Traditional deduplication system, users consider the following duplicated control rights for differential contrast, data themselves without it. Our hybrid cloud also built several new buildings in the Czech unauthorized copy Deduplication support. Security analysis shows that the proposed model, the security of our systems in terms of definitions as described is secure. As proof of concept of a prototype of our multiple service testing proposal is authorized, and our prototype tests conducted using test rigs. Show us that our system allows control of multiple proposals in normal operation than continue trying.

INTRODUCTION:

Data deduplication system, engage the private cloud as proxy data owner / user to securely copy to check with different privileges. As a practical architecture and has attracted much attention from researchers. The only data owners outsource their data storage by using public cloud, while the operation was successful in the private cloud data. Traditional encryption, in addition to providing data confidentiality, it is not with data deduplication. an identical copy of data from different users will lead to different ciphertexts, so Deduplicationimpossible.In this work, we improve our safety system. In particular, the scheme is set up to support improved security by encrypting your files with different privileges. Thus, unprivileged users can not do the same two checked. Moreover, so the user is not allowed can not decrypt the ciphertext, even in Collusion with S-CSP. safetyanalysis shows that our system safe in terms of the definition set out in the proposed security model. The user is allowed to check only for files marked with the appropriate privileges. advanced scheme is presented to support improved security by encrypting your files with different privileges. Reducing the size of the label to check the integrity of storage.To increase security and protect the confidentiality of data deduplication.

SYSTEM PRELIMINARIES:

1. Cloud Service Provider
2. Data Users Module
3. Private Cloud Module
4. Secure Deduplication System

CLOUD SERVICE PROVIDER:

In this module, the module developed cloud service provider. This is an entity that provides data storage services in the public cloud. S-CSP provides outsourcing services data and data stored on behalf of users. To reduce the cost of storage, S-CSP eliminate redundant data storage through deduplication and retain data only unique data. In this paper, it is assumed that S-CSP is always online and have a lot of storage capacity and computing power.

DATA USERS MODULE:

Users are entities that want to outsource data storage to the S-CSP and to access the data later. In the deduplication storage system support, user charges only unique data, but does not load a copy to save the proliferation of broadband data, which can be purchased by the same user or different users. Deduplication in the ruling system, each user a set of privileges to the system configuration is removed. Each file is protected with encryption keys and the key to realizing the benefits focused differential privileges authorized with Deduplication

Volume No:2, Issue No:3 (August-2016)
ISSN No : 2454-423X (Online)
International Journal of Research in Advanced Computer Science Engineering
A Peer Reviewed Open Access International Journal
www.ijracse.com

PRIVATE CLOUD MODULE

Compared with traditional architecture in data deduplication, cloud computing, it is a new feature introduced to facilitate the safe use of the service in the cloud. In particular, because the computing resources in the data the user / owner is limited and public cloud is not completely reliable in practice, private clouds can provide data users / owners of the runtime environment and infrastructure works the interface between users and the public cloud. Private key benefits managed by the private cloud, which respond to user demand signal files. The interface provides a private cloud, users can send files and questions are kept secure and are calculated respectively.

SECURE DEDUPLICATION SYSTEM:

We take into account the kind of privacy, we need to protect, that is, I) unforgeability copy of the counter-checks: There are two types of opponents, namely, the external opposition and internal opponents. As shown below, external versus internal opponents can be seen as no privileges. If the user has privileges p, it is necessary that the opponent can not make a copy of a valid and output with other p privileges in any of the files F, which does not coincide with p p '. In addition, it also requires that if the opponent does not make a request counter with its own privileges private cloud server, you can not build and copy of valid tokens output by p at any referenced F.

RELATED WORK:

insurancededuplication. With the advent of cloud computing, secure data deduplication has attracted much attention recently of the research community. Yuan Yu and suggested the cloud storage system deduplication to reduce storage size label for the control of data integrity. To increase security and protect the confidentiality of data deduplication, Bellare shows how volatile protect the message message. In their system, a third party is named the primary server is introduced to tag files for check copies. Stanek delivers new encryption scheme that provides security for data and differential data Popular not so popular. The data is highly sensitive not popular, traditional conventional encryption implemented. Another encryption scheme twolayered with more certainty, while supporting the proposed deduplicating data to be unpopular. In this way, a better compromise between efficiency and safety data outside of acceptable sources . Li addressed the issue of key management in a block-level deduplication to distribute these in several key server to encrypt files. convergent encryption. convergent encryption ensures privacy of data deduplication. The formal Bellare primitive terrestrial message encryption, and explore its application in safe outsourcing efficient use of space. Xu also addressed the problem and make secure encryption which focused on encryption efficiently, regardless of issues of key management and deduplicationblocklevel. There are also some implementation of the implementation focused on various versions of unified encryption for secure Deduplication. It is known that some storage vendors in the trade, such as cloud Bitcasa also use encryption concentrated. Halevi is the concept of "proof of ownership" for disposal systems, duplicate data, so that customers can test the efficiency of storage servers in the cloud, that he / she has the file without uploading the file itself.

POW various structures based on tree-Merkle Hash proposed to allow a client deduplication, including fixing leaking borders. Pietro and efficient PowSorniotti proposed another scheme by selecting the file projection in a few randomly selected as test file bitpositions. Please note that all previous regulations do not take data privacy. Recently extended Pow Ng encrypted files, and does not address how to reduce the key management overhead. Double cloud architecture. Recently, Bugiel offers a consistent framework for secure cloud detached outsourcing and arbitrary data to the cloud computing unreliable raw. Zhang also introduced hybrid technology to support cloud computing dataintensive respect for privacy. In our work, we believe that in order to address the problem of unauthorized duplication of data in the public cloud. Security model is the same as our system works in relation to which the private cloud is assumed to be honest, but interesting.

CONCLUSION:

In this paper, the concept Deduplication strong security to protect data by entering a user differential privileges in duplicate record set. We also present some new buildings deduplication support dual power control in a hybrid cloud architecture, where chips duplicate-check the file generated by the personal cloud server with the private key. Safety analysis shows that our system is safe in terms of internal and external attacks, as stated in the proposed security model.

Volume No:2, Issue No:3 (August-2016) ISSN No : 2454-423X (Online)

International Journal of Research in Advanced Computer Science Engineering

A Peer Reviewed Open Access International Journal

www.ijracse.com

As proof of concept, prototype experimental validation of our schedule and behavior of the proposed bank authorized duplication of testing our prototype has been implemented. We have shown that we bear a copy control system authorized.low overhead compared with the encryption and delivery of converged networks.

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

[4] M. Bellare, S. Keelveedhi, and T. Ristenpart.Message-locked encryption and secure deduplication. In EUROCRYPT, pages 296– 312, 2013.

[5] M. Bellare, C. Namprempre, and G. Neven. Security proofs for identity-based identification and signature schemes. J. Cryptology, 22(1):1–61, 2009.

[6] M. Bellare and A. Palacio.Gq and schnorr identification schemes: Proofs of security against impersonation under active and concurrent attacks. In CRYPTO, pages 162–177, 2002.

[7] 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.

[8] 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.

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

[10] GNU Libmicrohttpd. http://www.gnu.org/software/libmicrohttpd/.

[11] S. Halevi, D. Harnik, B. Pinkas, and A. Shulman-Peleg.Proofs of ownership in remote storage systems. In Y. Chen, G. Danezis, and V. Shmatikov, editors, ACM Conference on Computer and Communications Security, pages 491–500. ACM, 2011.

[12] J. Li, X. Chen, M. Li, J. Li, P. Lee, andW. Lou. Secure deduplication with efficient and reliable convergent key management. In IEEE Transactions on Parallel and Distributed Systems, 2013.

[13] libcurl. http://curl.haxx.se/libcurl/.

[14] C. Ng and P. Lee. Revdedup: A reverse deduplication storage system optimized for reads to latest backups. In Proc. of APSYS, Apr 2013.

[15] W. K. Ng, Y. Wen, and H. Zhu. Private data deduplication protocols in cloud storage. In S. Ossowski and P. Lecca, editors, Proceedings of the 27th Annual ACM Symposium on Applied Computing, pages 441–446. ACM, 2012.

[16] R. D. Pietro and A. Sorniotti. Boosting efficiency and security in proof of ownership for deduplication. In H. Y. Youm and Y. Won, editors, ACM Symposium on Information, Computer and Communications Security, pages 81–82. ACM, 2012.

[17] S. Quinlan and S. Dorward.Venti: a new approach to archival storage. In Proc. USENIX FAST, Jan 2002.

[18] A. Rahumed, H. C. H. Chen, Y. Tang, P. P. C. Lee, and J. C. S. Lui. A secure cloud backup system with assured deletion and version control.In 3rd International Workshop on Security in Cloud Computing, 2011.

[19] R. S. Sandhu, E. J. Coyne, H. L. Feinstein, and C. E. Youman. Role-based access control models. IEEE Computer, 29:38–47, Feb 1996.

[20] J. Stanek, A. Sorniotti, E. Androulaki, and L. Kencl. A secure data deduplication scheme for cloud storage. In Technical Report, 2013.