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. 2, Issue 12, December 2014

Enhanced Secure Distributed System Implementing Proxy Re-Encryption

Raji.N[1], K.G.S. Venkatesan[*2]

Professor, Department of Computer Science and Engineering, Jerusalem College of Engineering, Chennai, Tamil Nadu, India[1]

Assistant Professor, Department of Computer Science Engineering, Bharath University, Chennai, Tamil Nadu, India[2]

[*]Corresponding Author

ABSTRACT: Cloud Storage System has a collection of storage servers provides long-standing storage services over the internet. Data privacy becomes a major concern in cloud storage system because user stores his data in third party cloud system. Encryption schemes available for data privacy but it limit the number of functions done in storage system. Building a secure storage system that supports multiple functions is tough when the storage system is distributed and has no central authority. A new idea is proposed proxy re-encryption scheme for decentralizes erasure code for defending the distributed system. The distributed storage system not only supports secure and robust data storage and retrieval, but also lets a user forward his data in the storage servers to another user without retrieving the data back. The main technical contribution is that the proxy re-encryption scheme supports encoding operations over encrypted messages as well as forwarding operations over encoded and encrypted messages. Our method fully integrates encrypting, encoding, and forwarding.

KEYWORDS: cloud, Data privacy, proxy re-encryption.

I. INTRODUCTION

Cloud Storage System is storing the data in virtual memory. It has a collection of storage servers provides long-standing storage services over the internet. Data privacy becomes a major concern in cloud storage system because user stores his data in third party cloud system. Encryption schemes available for data privacy but it limit the number of functions done in storage system. Building a secure storage system that supports multiple functions is tough when the storage system is distributed and has no central authority[1]. A new idea is proposed proxy re-encryption scheme for a well fortified data moving and storing using keys in cloud system. Proxy re-encryption allows a proxy to transform a ciphertext computed under Alice's public key into one that can be opened by Bob's secret key.

Storing data in a third party's cloud system causes serious concern on data confidentiality. In order to provide strong confidentiality for messages in storage servers, a user can encrypt messages by a cryptographic method before applying an erasure code method to encode and store messages. When he wants to use a message, he needs to retrieve the codeword symbols from storage servers, decode them, and then decrypt them by using cryptographic keys[2]. There are three problems in the above straightforward integration of encryption and encoding. First, the user has to do most computation and the communication traffic between the user and storage servers is high. Second, the user has to manage his cryptographic keys. If the user's device of storing the keys is lost or compromised, the security is broken. Finally, besides data storing and retrieving, it is hard for storage servers to directly support other functions[3]. For example, storage servers cannot directly forward a user's messages to another one. The owner of messages has to retrieve, decode, decrypt and then forward them to another user.

We consider the system model that consists of distributed storage servers and key servers. Since storing cryptographic keys in a single device is risky, a user distributes his cryptographic key to key servers that shall perform cryptographic functions on behalf of the user. These key servers are highly protected by security mechanisms[4]. To well fit the distributed structure of systems, we require that servers independently perform all operations. With this consideration,

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. 2, Issue 12, December 2014

we propose a new threshold proxy re-encryption scheme and integrate it with a secure decentralized code to form a secure distributed storage system[5]. The encryption scheme supports encoding operations over encrypted messages and forwarding operations over encrypted and encoded messages. The tight integration of encoding, encryption, and forwarding makes the storage system efficiently meet the requirements of data robustness, data confidentiality, and data forwarding. Accomplishing the integration with consideration of a distributed structure is challenging[6]. Our system meets the requirements that storage servers independently perform encoding and re-encryption and key servers independently perform partial decryption. Moreover, we consider the system in a more general setting than previous works. This setting allows more flexible adjustment between the number of storage servers and robustness.
A bob store the data in cloud and storing methodology is encryption. Alice sent a request to Bob, Bob receive the particular request and get data from cloud and sent to the Alice. The hackers are participating between Bob and Alice[7]. They are fetching data. Data robustness is a major requirement for storage systems. There have been many proposals of storing data over storage servers. The encoding process for a message can be split into n parallel responsibilities of generating codeword cipher[20]. It had several demerits.
That are follows:

- Encoding is not involved in existing system.
- Try and get the success in hacking of data by the third party transfers.
- Transmission is based on third party server to server to client.
- Loss of time in intermediate transmission

II. REPLICA MANAGEMENT

Replica management adjusts the number and location of floating replicas in order to service access requests more efficiently[8]. Event handlers monitor client requests and system load, noting when access to a specific replica exceeds its resource allotment. When access requests overwhelm a replica, it forwards a request for assistance to its parent node. The parent, which tracks locally available resources, can create additional floating replicas on nearby nodes to alleviate load. Conversely, replica management eliminates floating replicas that have fallen into disuse[9]. Notification of a replica's termination also propagates to parent nodes, which can adjust that object's dissemination tree. In addition to these short-term decisions, nodes regularly analyze global usage trends, allowing additional optimizations[10]. For example, Data Store can detect periodic migration of clusters from site to site and pre fetch data based on these cycles.

Thus users will find their project files and email folder on a local machine during the work day, and waiting for them on their home machines at night[19].

A.Other Issues

Data store uses introspective mechanisms in many other aspects as well[11]. Specifically, introspection improves the manageability and performance of the routing structure, enables construction of efficient update dissemination trees, ensures the availability and durability of archival fragments, identifies unreliable peer organizations, and performs continuous confidence estimation on its own optimizations in order to reduce harmful changes and feedback cycles.

III. FUTURE WORK

A proposed system is going to implement well fortified data moving between Bob and Alice. The cloud system has been classified into two parts. One is database and another one is key or code and Secret Word(SW) area[12] The Bob stored data in cloud and also create a key& SW for particular data. The key size is high. The request will come from Alice, Bob sent only Key and the SW. Alice get a key from Bob and put key in the cloud system[18]. Alice will get data from cloud directly.A secure cloud storage system implies that an unauthorized user or server cannot get the content of stored messages.A storage server cannot generate re-encryption keys by himself[13]. Each storage server independently performs encoding and re-encryption and each key server independently perform partial decryption.

Decisional bilinear Diffie-Hellman assumption. This assumption is that it is computationally infeasible to distinguish the distributions[14]. Formally, for any probabilistic polynomial time algorithm

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. 2, Issue 12, December 2014

IV.TIME EFFICIENCY

Many of the mechanisms already described have been designed in part for their effect on system performance[15]. Caching encrypted file content on client disks improves not only file availability[17]. This delay permits a dramatic reduction in network file- replication traffic.

A.System Architecture

Fig:1 Architecture Diagram

IV. DISCUSSION AND CONCLUSION

we consider a cloud storage system consists of storage servers and key servers. We integrate a newly proposed threshold proxy re-encryption scheme and erasure codes over exponents. The threshold proxy reencryption scheme supports encoding, forwarding, and partial decryption operations in a distributed way[16]. To decrypt a message of k blocks that are encrypted and encoded to n codeword symbols, each key server only has to partially decrypt two codeword symbols in our system[21].

By using the threshold proxy re-encryption scheme, we present a secure cloud storage system that provides secure data storage and secure data forwarding functionality in a decentralized structure[23]. Our storage system and some newly proposed content addressable file systems and storage system are highly compatible. Our storage servers act as storage nodes in a content addressable storage system for storing content addressable blocks[25]. Our key servers act as access nodes for providing a front-end layer such as a traditional file system interface.

REFERENCES

1. J. Kubiatowicz, D. Bindel, Y. Chen, P. Eaton, D. Geels, R.Gummadi, S. Rhea, H. Weatherspoon, W. Weimer, C. Wells, and B. Zhao, "Oceanstore: An Architecture for Global-Scale Persistent Storage," Proc. Ninth Int'l Conf. Architectural Support for Programming Languages and Operating Systems (ASPLOS), pp. 190-201, 2000.
2. P. Druschel and A. Rowstron, "PAST: A Large-Scale, Persistent Peer-to-Peer Storage Utility," Proc. Eighth Workshop Hot Topics in Operating System (HotOS VIII), pp. 75-80, 2001.
3. Udayakumar R., Khanaa V., Saravanan T., "Chromatic dispersion compensation in optical fiber communication system and its simulation", Indian Journal of Science and Technology, ISSN : 0974-6846, 6(S6) (2013) pp. 4762-4766.
4. A.Adya, W.J. Bolosky, M. Castro, G. Cermak, R. Chaiken, J.R. Douceur, J. Howell, J.R. Lorch, M. Theimer, and R. Wattenhofer, "Farsite: Federated, Available, and Reliable Storage for an Incompletely Trusted Environment," Proc. Fifth Symp. Operating System Design and Implementation (OSDI), pp. 1-14, 2002.
5. A.Haeberlen, A. Mislove, and P. Druschel, "Glacier: Highly Durable, Decentralized Storage Despite Massive Correlated Failures," Proc. Second Symp. Networked Systems Design and Implementation (NSDI), pp. 143-158, 2005.
6. Udayakumar R., Khanaa V., Saravanan T., "Analysis of polarization mode dispersion in fibers and its mitigation using an optical compensation technique", Indian Journal of Science and Technology, ISSN : 0974-6846, 6(S6) (2013) pp. 4767-4771.
7. Z. Wilcox-O'Hearn and B. Warner, "Tahoe: The Least-Authority Filesystem," Proc. Fourth ACM Int'l Workshop Storage Security and Survivability (StorageSS), pp. 21-26, 2008.

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. 2, Issue 12, December 2014

8. H.-Y. Lin and W.-G. Tzeng, "A Secure Decentralized Erasure Code for Distributed Network Storage," IEEE Trans. Parallel and Distributed Systems, vol. 21, no. 11, pp. 1586-1594, Nov. 2010.
9. R. Sandberg, D. Goldberg, S. Kleiman, D. Walsh, and B. Lyon, "Design and Implementation of the Sun Network Filesystem," Proc. USENIX Assoc. Conf., 1985.
10. M. Kallahalla, E. Riedel, R. Swaminathan, Q. Wang, and K. Fu, "Plutus: Scalable Secure File Sharing on Untrusted Storage," Proc. Second USENIX Conf. File and Storage Technologies (FAST), pp. 29-42, 2003.
11. R. Bhagwan, K. Tati, Y.-C. Cheng, S. Savage, and G.M. Voelker, "Total Recall: System Support for Automated AvailabilityManagement," Proc. First Symp. Networked Systems Design andImplementation (NSDI), pp. 337-350, 2004.
12. Udayakumar R., Khanaa V., Kaliyamurthie K.P., "Performance analysis of resilient ftth architecture with protection mechanism", Indian Journal of Science and Technology, ISSN : 0974-6846, 6(S6) (2013) pp. 4737-4741
13. A.G. Dimakis, V. Prabhakaran, and K. Ramchandran, "Ubiquitous Access to Distributed Data in Large-Scale Sensor Networks through Decentralized Erasure Codes," Proc. Fourth Int'l Symp. Information Processing in Sensor Networks (IPSN), pp. 111-117, 2005.
14. M. Mambo and E. Okamoto, "Proxy Cryptosystems: Delegation of the Power to Decrypt Ciphertexts," IEICE Trans. Fundamentals of Electronics, Comm. and Computer Sciences, vol. E80-A, no. 1, pp. 54- 63, 1997.
15. Udayakumar R., Khanaa V., Saravanan T., "Analysis of polarization mode dispersion in fibers and its mitigation using an optical compensation technique", Indian Journal of Science and Technology, ISSN : 0974-6846, 6(S6) (2013) pp. 4767-4771.
16. M. Blaze, G. Bleumer, and M. Strauss, "Divertible Protocols and Atomic Proxy Cryptography," Proc. Int'l Conf. Theory and Application of Cryptographic Techniques (EUROCRYPT), pp. 127-144, 1998.
17. Q. Tang, "Type-Based Proxy Re-Encryption and Its Construction," Proc. Ninth Int'l Conf. Cryptology in India: Progress in Cryptology (INDOCRYPT), pp. 130-144, 2008.
18. G. Ateniese, K. Benson, and S. Hohenberger, "Key-Private Proxy Re-Encryption," Proc. Topics in Cryptology (CT-RSA), pp. 279-294,2009.
19. Udayakumar R., Khanaa V., Saravanan T., "Chromatic dispersion compensation in optical fiber communication system and its simulation", Indian Journal of Science and Technology, ISSN : 0974-6846, 6(S6) (2013) pp. 4762-4766.
20. G. Ateniese, R.D. Pietro, L.V. Mancini, and G. Tsudik, "Scalable and Efficient Provable Data Possession," Proc. Fourth Int'l Conf. Security and Privacy in Comm. Netowrks (SecureComm), pp. 1-10, 2008.
21. H. Shacham and B. Waters, "Compact Proofs of Retrievability," Proc. 14th Int'l Conf. Theory and Application of Cryptology and Information Security (ASIACRYPT), pp. 90-107, 2008.
22. C.Wang, Q. Wang, K. Ren, and W. Lou, "Privacy-Preserving Public Auditing for Data Storage Security in Cloud Computing," Proc. IEEE 29th Int'l Conf. Computer Comm. (INFOCOM), pp. 525- 533, 2010.
23. A.Shamir, "How to Share a Secret," ACM Comm., vol. 22, pp. 612-613, 1979.
24. C.Dubnicki, L. Gryz, L. Heldt, M. Kaczmarczyk, W. Kilian, P.Strzelczak, J. Szczepkowski, C. Ungureanu, and M. Welnicki, "Hydrastor: A Scalable Secondary Storage," Proc. Seventh Conf. File and Storage Technologies (FAST), pp. 197-210, 2009.
25. Hsiao-Ying Lin, Member, IEEE, and Wen-Guey Tzeng, Member, IEEE, "A Secure Erasure Code-Based Cloud Storage System with Secure Data Forwarding".
26. .Dr.K.P.Kaliyamurthie, D.Parameswari, Load Balancing in Structured Peer to Peer Systems, International Journal of Innovative Research in Computer and Communication Engineering, ISSN: 2249-2615,pp 22-26, Volume1 Issue 1 Number2-Aug 2011
27. Dr.R.Udayakumar, Addressing the Contract Issue,Standardisation for QOS, International Journal of Innovative Research in Computer and Communication Engineering, ISSN (Online): 2320 – 9801,pp 536-541, Vol. 1, Issue 3, May 2013
28. Dr.R.Udayakumar, Computational Modeling of the StrengthEvolution During Processing And Service Of9-12% Cr Steels, International Journal of Innovative Research in Computer and Communication Engineering, ISSN(Online): 2320-9801,pp 3295-3302, Vol. 2, Issue 3, March 2014
29. P.GAYATHRI, ASSORTED PERIODIC PATTERNS INTIME SERIES DATABASE USINGMINING, International Journal of Innovative Research in Computer and Communication Engineering, ISSN(Online): 2320-9801, pp 5046- 5051, Vol. 2, Issue 7, July 2014.
30. Gayathri, Massive Querying For Optimizing Cost – CachingService in Cloud Data, International Journal of Innovative Research in Computer and Communication Engineering, ISSN(Online): 2320-9801,pp 2041-2048, Vol. 1, Issue 9, November 2013