IJARES/July 2014/Volume-2/Issue-7/1226-1231 **ISSN 2347- 9337**

INTERNATIONAL JOURNAL OF ADVANCED RESEARCH IN ENGINEERING AND SCIENCE

TRUSTWORTHY STORAGE FOR SUPPORTING MODERATELY RELIABLE CLOUD SETTING

Uppala Hari Krishna[1], G.Krishna Veni[2]

[1]M.Tech Student, Dept of CSE, RRS College of Engineering & Technology, Muthangi (V), Patancheru (M), Hyderabad, T.S, India

[2]Assistant Professor, Dept of CSE, RRS College of Engineering & Technology, Muthangi (V), Patancheru (M), Hyderabad, T.S, India

ABSTRACT:

Data robustness is a most important obligation for storage systems. There have been numerous proposals of accumulating data above storage servers. We put forward a novel threshold proxy re-encryption system and put together it with a protected decentralized code to form a protected distributed storage system. In proxy re-encryption scheme, server of proxy can get across a cipher text in a public key towards a novel one under an additional public key by re-encryption key. In a proxy re-encryption method, the owner transmits a re-encryption key towards storage servers with the intention of storage servers to carry out re-encryption operation. Decentralized erasure code is erasure code that unconventionally efforts out every codeword symbol for a message thus; encoding procedure for a message is split into parallel responsibilities of generating codeword symbols. Even though most proxy re-encryption system uses pairing operations, there exists proxy re-encryption system devoid of pairing. Proxy re-encryption scheme considerably decrease transparency of data forwarding function in a protected storage system and can considerably reduce communication as well as computation cost of owner.

Keywords: Proxy re-encryption, Storage system, Codeword, Decentralized erasure code, Public key.

1. INTRODUCTION:

A decentralized structural design for storage systems put forward superior scalability, since a storage server can connect or go away devoid of control of a central authority. To make available robustness against server breakdown, an effortless means is to construct replicas of every message and accumulates them in dissimilar servers [4]. One way to make obtainable data robustness is to replicate a message with the intention that each storage server store up a copy of message. Storing information in the system of third party's cloud causes severe concern on data privacy [8]. To make available tough privacy in favour of communication in storage servers, user can encrypt communication by cryptographic means earlier than affecting an erasure code means to programme as well as store messages. Decentralized erasure code autonomously works out every codeword symbol for a message thus, encoding procedure for a message is split into parallel responsibilities of making codeword symbols [13]. Decentralized erasure-code is appropriate for employing in a distributed storage system. Once the message symbols are send towards storage servers, every storage server separately calculate a codeword symbol in support of received message symbols as well as store it [1]. We put forward a novel threshold proxy re-encryption system and put together it with a protected decentralized code to form a protected distributed storage system. Some proxy re-encryption system was proposed and pertain them towards sharing utility of safe storage systems. Many enhancements on scalability, toughness, competence, and protection were proposed [11]. The Network-Attached Storage and the Network File System make available additional storage devices over network so that a user uses the storage devices by the use of network connection. One way to decrease the development rate is to use erasure codes to encode messages. A message is planned as codeword, and every storage server gathers a codeword symbol [3].

2. METHODOLOGY:

Methods of Proxy re-encryption can considerably reduce communication as well as computation cost of owner. In a proxy re-encryption method, the owner transmits a re-encryption key towards storage servers with the intention of storage servers to carry out re-encryption operation [14]. The communication expenditure of holder is

autonomous of extent of forwarded message and computation expenditure of re-encryption is taken care of through storage servers. Proxy re-encryption scheme considerably decrease transparency of data forwarding function in a protected storage system. We make use of a threshold proxy re-encryption system with multiplicative homomorphic property [9. An encryption system is multiplicative homomorphic if it holds up a group operation on encrypted plaintexts devoid of decryption. A multiplicative homomorphic encryption system supports encoding function over encrypted messages. We subsequently converts a proxy re-encryption method by means of multiplicative homomorphic property into a threshold description [7]. Messages are originally encrypted by holder and subsequently stored in storage server. When a user desires to distribute his messages, he transmits a re-encryption key towards storage server which re-encrypts encrypted message in support of authorized user. Their system has data privacy and supports the data forwarding function. In proxy re-encryption scheme, server of proxy can get across a cipher text in a public key towards a novel one under an additional public key by re-encryption key. The server does not be familiar with the plaintext during transformation. Even though most proxy re-encryption system uses pairing operations, there exists proxy re-encryption system devoid of pairing. In a key-private proxy re-encryption system, given a re-encryption key, a proxy server cannot make a decision on individuality of recipient [16]. Proxy re-encryption scheme provides superior confidentiality guarantee against proxy servers. The encryption system supports encoding operations over encrypted messages and self-assured operations over encrypted and encoded messages. The severe incorporation of encoding, encryption, along with forwarding put up storage system efficiently get together the requirements of data robustness, as well as data forwarding [12]. Type-based proxy re-encryption system were proposed which provide an enhanced granularity on approved right of re-encryption key. A client can build a decision which type of communication and with whom he desires to contribute to in this kind of proxy re-encryption system. Another significant functionality concerning cloud storage is purpose of integrity checking [10]. Subsequent to a user store up data into storage system, he no longer possesses

information at hand. The user might want to make sure whether the information is right stored up in storage servers. To store a message of k blocks, every storage server linearly merges the blocks with haphazardly chosen coefficients and stores the codeword symbol and coefficients [5]. To retrieve the message, a user requests k storage servers for the stored codeword symbols and coefficients and work out the linear system. A storage server breakdown is modelled as erasure error of accumulated codeword symbol. Accidental linear codes hold up distributed encoding, that is, each codeword symbol is autonomously computed. By means of threshold proxy re-encryption system, we put forward a safe cloud storage scheme that make available protected data storage and protected data forwarding functionality in a decentralized arrangement [15]. A decentralized structural design for storage systems offers good scalability, since a storage server can join or leave devoid of control of a central influence. To supply robustness against server failures, a straightforward means is to create replicas of every message and amass them in altered servers [6]. Achieving the integration with deliberation of a distributed structure is demanding. Our system assembles the requirements that storage servers separately perform encoding and re-encryption and key servers separately perform incomplete decryption.

3. RESULTS:

The threshold proxy re-encryption system maintains encoding, forwarding, as well as partial decryption procedures in a dispersed means. To decrypt message of k blocks which are prearranged to n codeword symbols, each key server merely has to partly decrypt two symbols of codeword in our system. By means of threshold proxy re-encryption system, we put forward a safe cloud storage system that put together protected data storage and protected data forwarding functionality in a decentralized arrangement. Each storage server separately achieves encoding as well as re-encryption and every key server separately carry out partial decryption.

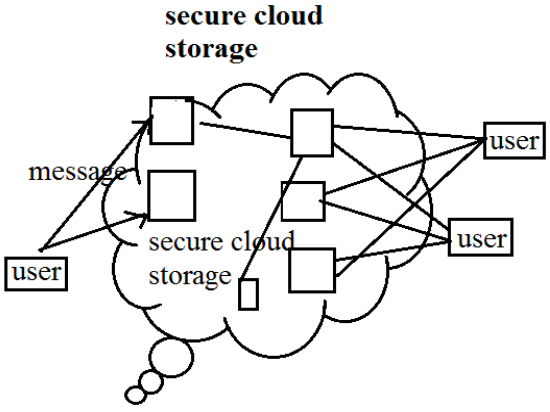

Fig1: An overview of storage model.

4. CONCLUSION:

To make available tough privacy in support of messages in storage servers, a client can encrypt messages through cryptographic means earlier than affecting an erasure code means to programme as well as store messages. The Network-Attached Storage and the Network File System make available extra storage devices above network so that user can right to use the storage devices by the use of network connection. We put forward a novel threshold proxy re-encryption system and put together it with a protected decentralized code to form a protected distributed storage system. By means of threshold proxy re-encryption system, we put forward a safe cloud storage scheme that make available protected data storage and protected data forwarding functionality in a decentralized arrangement. By means of threshold proxy re-encryption system, we present a secure cloud storage system that make available protected data storage and protected data forwarding functionality in a decentralized arrangement. To supply robustness against server failures, a straightforward means is to construct replicas of every message and stock up them in dissimilar servers. The inflexible incorporation of encoding, encryption, as well as forwarding put up the storage system ingeniously meets the requirements of data sturdiness, as well as data forwarding. A multiplicative homomorphic encryption system supports encoding function over encrypted messages. Our system assembles the requirements that storage servers separately perform encoding and re-encryption and key servers separately perform incomplete decryption. Decentralized erasure code autonomously works out every codeword symbol for a message thus; encoding procedure for a message is split into parallel responsibilities of generating codeword symbols.

REFERENCES:

[1] C. Ungureanu, B. Atkin, A. Aranya, S. Gokhale, S. Rago, G.Calkowski, C. Dubnicki, and A. Bohra, "Hydrafs: A High-Throughput File System for the Hydrastor Content-Addressable Storage System," Proc. Eighth USENIX Conf. File and StorageTechnologies (FAST), p. 17, 2010

[2] G. Ateniese, S. Kamara, and J. Katz, "Proofs of Storage fromHomomorphic Identification Protocols," Proc. 15th Int'l Conf.Theory and Application of Cryptology and Information Security(ASIACRYPT), pp. 319-333, 2009

[3] Secure Erasure Code-Based Cloud Storage System with Secure Data Forwarding Hsiao-Ying Lin, Member, IEEE, and Wen-Guey Tzeng,2012

[4] G. Ateniese, K. Fu, M. Green, and S. Hohenberger, "ImprovedProxy Re-Encryption Schemes with Applications to SecureDistributed Storage," ACM Trans. Information and System Security,vol. 9, no. 1, pp. 1-30, 2006

[5] 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.

[6] 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.

[7] G. Ateniese, R. Burns, R. Curtmola, J. Herring, L. Kissner, Z.Peterson, and D. Song, "Provable Data Possession at UntrustedStores," Proc. 14th ACM Conf. Computer and Comm. Security (CCS),pp. 598-609, 2007.

[8] C. Dubnicki, L. Gryz, L. Heldt, M. Kaczmarczyk, W. Kilian, P.St zelczak, J. Szczepkowski, C. Ungureanu, and M. Welnicki, "Hydrastor: A Scalable Secondary Storage," Proc. Seventh Conf. Fileand Storage Technologies (FAST), pp. 197-210, 2009

[9] A.G. Dimakis, V. Prabhakaran, and K. Ramchandran, "Ubiqui- tous Access to Distributed Data in Large-Scale Sensor Net- works through Decentralized Erasure Codes," Proc. Fourth Int'l Symp. Information Processing in Sensor Networks (IPSN), pp. 111- 117, 2005.

[10] 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 Persis- tent Storage," Proc. Ninth Int'l Conf. Architectural Support for Programming Languages and Operating Systems (ASPLOS), pp. 190- 201, 2000.

[11] G. Ateniese, R.D. Pietro, L.V. Mancini, and G. Tsudik, "Scalableand Efficient Provable Data Possession," Proc. Fourth Int'l Conf.Security and Privacy in Comm. Netowrks (SecureComm), pp. 1-10,2008

[12] R. Bhagwan, K. Tati, Y.-C. Cheng, S. Savage, and G.M. Voelker, "Total Recall: System Support for Automated Availability Management," Proc. First Symp. Networked Systems Design and Implementation (NSDI), pp. 337-350, 2004.

[13] A. Haeberlen, A. Mislove, and P. Druschel, "Glacier: Highly Durable, Decentralized Storage Despite Massive Correlated Fail- ures," Proc. Second Symp. Networked Systems Design and Implemen- tation (NSDI), pp. 143-158, 2005.

[14] S.C. Rhea, P.R. Eaton, D. Geels, H. Weatherspoon, B.Y. Zhao, and J. Kubiatowicz, "Pond: The Oceanstore Prototype," Proc. Second USENIX Conf. File and Storage Technologies (FAST), pp. 1-14, 2003.

[15] M. Blaze, G. Bleumer, and M. Strauss, "Divertible Protocols and Atomic Proxy Cryptography," Proc. Int'l Conf. Theory and Applica- tion of Cryptographic Techniques (EUROCRYPT), pp. 127-144, 1998.

[16] 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.