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. 3, Issue 8, August 2015

Protected Data Storage and Forwarding in the Storage Systems Based on Alternate – Re-encryption Scheme

S. SriGowthem, Dr. K P Kaliyamurthie, Sundararajan.M, Arulselvi S

Assistant Professor, Department of Computer Science and Engineering, Bharath University, Chennai, Tamil Nadu, India

Professor & Head of Department of Computer Science and Engineering, Bharath University, Chennai Chennai, Tamil Nadu, India

Director, Research Center for Computing and Communication, Bharath University, Chennai, Tamil Nadu, India

Co-Director, Research Center for Computing and Communication, Bharath University, Tamil Nadu, India

ABSTRACT: A storage system consists of a collection of storage servers for the user data to be stored in the third party storage system having thousands of storage servers, but it causes serious concern over data confidentiality.Encryption schemes protect data confidentiality, but storage servers cannot directly forward a user's data to another user. In this paper, a threshold alternate re- encryption scheme is proposed for addressing the problem of forwarding data to another, by storage servers directly under the command of data owner. This method fully integrates encrypting, encoding and forwarding. The distributed storage system not only supports protected 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 parameters regarding the number of copies of a message dispatched to storage servers and number of storage servers is analysed.

KEYWORDS: protected storage system, Distributed Erasure code, Alternate Re-encryption**.**

I. INTRODUCTION

Cloud storage is an industry term for managed data storage through hosted network (typically Internet-based) service. Several types of cloud storage systems have been developed supporting both personal and business uses. The most basic form of cloud storage allows users to upload individual files or folders from their personal computers to a central Internet server. This allows users to make backup copies of files in case their originals are lost. Users can also download their files from the cloud to other devices, and sometimes also enable remote access to the files for other people to share. Cloud networks that serve many customers tend to be expensive to build due to the scalability requirements for reliably handling large amounts of data. The decreasing cost-per-gigabyte of physical digital media storage has helped offset these costs somewhat. Data transfer rates and server hosting costs from an Internet data center provider can also be substantial.

Vendors charge fees for at least their more advanced service offerings. Service plans may be divided into tiers according to usage, with penalty fees charged if you exceed the specified quotas. Cloud storage systems should make working with remote data almost as easy as data on your local hard drives. Even a free cloud storage service can be costly if it suffers from frequent downtimes, loses or corrupts data, or has had past security incidents.

The data is often of great value and its irrecoverable loss or damage could be a total disaster for its owner. This requires protected methods of preserving important data in order to prevent unrecoverable data loss, whilst constantly keeping up with increasing demands for storage space. It is necessary to regularly make extra copies of the information,

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. 3, Issue 8, August 2015

so as to be able to restore it to an earlier version if need be. These copies further escalate the demand for storage space.

So, there must be a protected cloud storage system to protect the user data and it should have a mechanism of forwarding one user data to another user. Confidentiality is the major requirement for the data stored in the storage system. So the data stored are encrypted and then stored. But the forwarding becomes the problem because the storage server cannot directly forward the data because it is encrypted and it is of no use.[14]

II. RELATED WORKS

We briefly review cloud storage systems, alternate re-encryption schemes and distributed erasure code.

2.1 Cloud Storage Systems

Basically, a cloud storage system can be considered to be a network of distributed data centers [1],[3],[4],[5] which typically uses cloud computing technologies like virtualization, and offers some kind of interface for storing data. To increase the availability of the data, it may be redundantly stored at different locations. In general, all of this is not visible to the user.
Advanced cloud storage services mostly employ basic cloud storage services for the actual storage of data, and provide interfaces such as client or web applications which greatly simplify the use of the service for the customer. Many services may also provide an easy to use API to allow integration of the service's capabilities into third-party software.

2.2 Alternate Re-encryption Schemes

Alternate re-encryption [2],[7],[8],[9] allows a alternate to transform a ciphertext computed under Alice's public key into one that can be opened by Bob's secret key. There are many useful applications of this primitive. For instance, Alice might wish to temporarily forward encrypted email to her colleague Bob, without giving him/her secret key. In this case, Alice the delegator could designate a alternate to re-encrypt her incoming mail into a format that Bob the delegate can decrypt using his own secret key. Alice could simply provide her secret key to the alternate, but this requires an unrealistic level of trust in the alternate.Alternate re-encryption has many exciting applications such as protected file systems, Outsourced Filtering of Encrypted Spam.

2.3 Distributed erasure code

Distributed erasure codes [6] are random linear codes over a finite field Fq with a specific randomized structure on their generator matrix. Each data packet Di is seen as a vector of elements of a finite field Fi .We denote the set of data nodes by V1 with |V1| = k and storage nodes by V2, |V2|
= n. We will now give a description of a randomized construction of a bipartite graph that corresponds to the creation of a distributed

erasure code. Every data node i ∈ V1 is assigned a random set of storage nodes N(i). This set is created as follows: a storage node is selected uniformly and independently from V2 and added in N(i) and this procedure is repeated d(k) times. Therefore N(i) distributed erasure code is suitable for use in a distributed storage system. After the message symbols are sent to storage servers, each storage server independently computes a codeword symbol for the received message symbols and stores it. This finishes the encoding and storing process. The recovery process is the same. The proposed system addresses the problem of forwarding data to another user by storage servers directly under the command of the data owner.[10]
A message is encoded as a codeword, which is a vector of symbols, and each storage server stores a codeword symbol. A storage server failure is modeled as an erasure error of the stored codeword symbol. Random linear codes (RLC) support distributed encoding, that is, each codeword symbol is independently computed.

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. 3, Issue 8, August 2015

will be smaller than d(k) if the same storage node is selected twice. In fact, the size of the set N(i) is exactly the number of coupons a coupon collector would have after purchasing d(k) coupons from a set of n coupons. It is not hard to see that when d(k)

≪ n, N(i) will be approximately equal to d(k) with high probability.

III. SCENARIO

The scenario of the storage system is to be considered. The proposed system focus on designing a storage system for robustness, confidentiality and functionality. A distributed erasure code is an erasure code that independently computes each codeword symbol for a message.

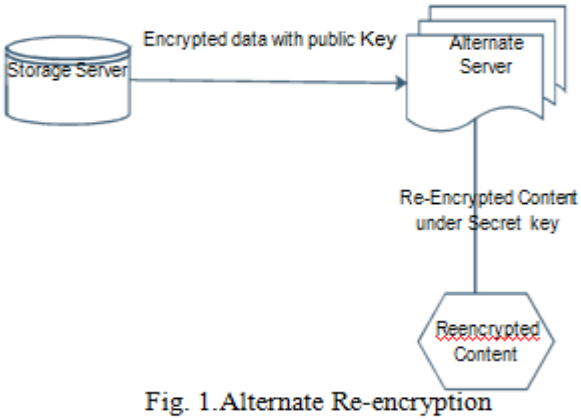

Fig. 1.Alternate Re-encryption

In Proposed System the data confidentiality for both data storage and data forwarding is considered. In this threat model, an attacker wants to break data confidentiality of a target user. The attacker analyzes stored messages in storage servers, the secret keys of nontarget users, and the shared keys stored in key servers. Note that the storage servers store all re-encryption keys provided by users. The attacker may try to generate a new re-encryption key from stored re-encryption keys.[11] As shown in Fig. 1 the alternate re-encryption is done. The alternate server should be a trustworthy one.The system consists of two servers namely key servers and storage servers. As shown in Fig. 2 data confidentiality is present.

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. 3, Issue 8, August 2015

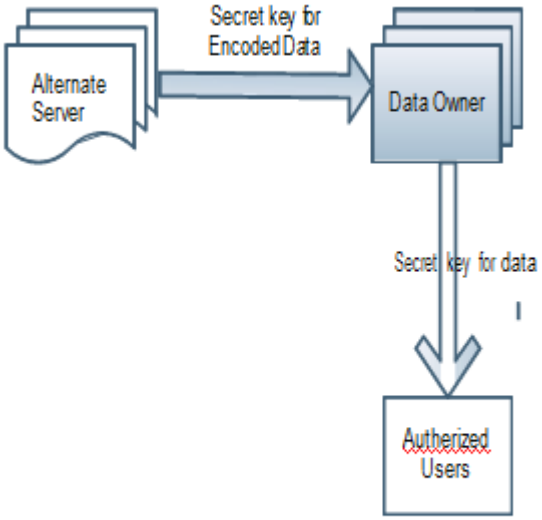

Fig. 2.Data Confidentiality

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. 3, Issue 8, August 2015

A cloud storage system modelled in the above is protected if no probabilistic polynomial time attacker wins the game with a non negligible advantage. A protected cloud storage system implies that an unauthorized user or server cannot get the content of stored messages, and a storage server cannot generate re-encryption keys by himself. If a storage server can generate a re- encryption key from the target user to another user B, the attacker can win the security game by re- encrypting the ciphertext to B and decrypting the reencrypted ciphertext using the secret key SKB. Therefore, this model addresses the security of data storage and data forwarding.[12]

Alternate re-encryption schemes can significantly decrease communication and computation cost of the owner. In a alternate re- encryption scheme, the owner sends a re-encryption key to storage servers such that storage servers perform the re-encryption operation for him. Thus, the communication cost of the owner is independent of the length of forwarded message and the computation cost of re-encryption is taken care of by storage servers. Alternate re-encryption schemes significantly reduce the overhead of the data forwarding function in a protected storage system.[13]

IV. PROTECTED STORAGE SYSTEM

We use a key private alternate re-encryption scheme with multiplicative homomorphic property. An encryption scheme is multiplicative homomorphic if it supports a group operation on encrypted plaintexts without decryption.

$$D(SK, E(PK, m_1) \odot E(PK, m_2)) = m_1 \cdot m_2$$

4.1 The Construction

Scheme π = (Setup, KeyGen, ReKeyGen, Enc, ReEnc, Dec) is described as follows:

Setup (Setup): Run BSetup $(1^k) \rightarrow$ (q, g, G, GT, e), where <g>= G. Choose a random generator H belongs to G. Compute Z = e(g,h), and set the public parameters PP = (g, h,Z). In the following, we assume that all parties have PP.

Key Generation (KeyGen): Choose random values a1,a2 belongs to Zq and set the public key as pk $=(Z^{a1}, g^{a2})$ with secret key sk = (a1,a2).

Re-Encryption Key Generation (ReKeyGen): A user A with secret key (a1,a2) can delegate to a user B with public key (Z^{b1}, g^{b2}) as:

Select random values r,w belongs to Zq. Compute Re-Encryption key.

$$rk_{A \rightarrow B} = ((g^{b_2})^{a_1+r}, h^r, e(g^{b_2}, h)^w, e(g, h)^w)$$

Encryption (Enc): To encrypt a message m belongs to GT under public key pkA = (Z^{a1}, g^{a2}), do:

1. Select random value k belongs to Zq.

2. Compute the ciphertext $(g^k, h^k, m .Z^{a1k})$.

Re-Encryption (ReEnc): Given a re-encryption key rkA→B = (R1,R2,R3,R4) = $(g^{b2(a1+r)}, h^r, Z^{b2w}; Z^w)$, it is possible to convert a second-level ciphertext C_A for A into a first-level ciphertext for B as follows:

1. Verify that the ciphertext is well-formed, by checking that it uses consistent randomness in its first two parts as: e(α,h) = e(g,β). If this does not hold, output ⊥ and abort.

2. Otherwise, there exists some k belongs to Zq and m belongs to GT such that $\alpha = g^k$, $\beta = h^k$ and μ =

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. 3, Issue 8, August 2015

$m.Z^{a1k}$, and thus, (α,β,μ) is a valid encryption of this m under $pk_A = (Z^{a1}, g^{a2})$.

3. Compute $t1=e(R1,\beta)=e(g^{b2(a1+r)},h^{k}) = Z^{b2k(a1+r)}$.

4. Compute $t2= m.Z^{k(a1+r)}$

5. Select a random w′ belongs to Zq.

6. Re-randomize t1 by setting $t1' = t1.R3^{w'}$

7. Re-randomize t2 by setting $t2' = t2.R4^{w'}$

8. Publish C_B

$C_B = (t1', t2') = (Z^{b2y}, m.Z^{y})$

Decryption (Dec): Given secret key (a1,a2), to decrypt a first-level ciphertext (α,β), compute $m = \beta/\alpha^{1/a2}$; and to decrypt a second-level ciphertext (α,β,μ), output ⊥ if $e(\alpha,h)\neq e(g,\beta)$,otherwise output $m = \mu/e(\alpha, h)^{a1}$
Fortunately, this scheme is practical and multi-purpose. Public keys can be used either for re-encryption purposes or for regular Elgamal encryptions.

V. CONCLUSION

In this paper, we consider a cloud storage system with protected data forwarding using key private alternate re-encryption.

REFERENCES

[1] Adya.J, Bolosky W.J, Castro.M, Cermak.G, Chaiken.R, Douceur J.R, Howell.J, Lorch J.R, Theimer.M, and Wattenhofer.M,(2002) "Farsite: Federated, Available, and Reliable Storage for an Incompletely Trusted Environment," Proc. Fifth Symp.perating System Design and Implementation (OSDI), pp. 1-14.
[2] Jebaraj S., Iniyan S., Kota H., 'Forecasting of commercial energy consumption in India using artificial neural network", International Journal of Global Energy Issues, ISSN : 0954-7118, 27(3) (2007) pp.276-301.
[3] Ateniese.G,Benson.K, and Hohenberger.S, (2009)"Key-Private Alternate Re-Encryption," Proc. Topics in Cryptology (CT-RSA), pp. 279-294.
[4] Sharmila S., Jeyanthi Rebecca L., "GC-MS Analysis of esters of fatty acid present in biodiesel produced from Cladophora vagabunda", Journal of Chemical and Pharmaceutical Research, ISSN : 0975 – 7384, 4(11) (2012) pp.4883-4887.
[5] Bowers.K.D, Juels.A., and Oprea.A, (2009) "HAIL: A High-Availability and Integrity Layer for Cloud Storage," Proc. 16th ACM Conf. Computer and Comm. Security (CCS), pp. 187-198.
[6] Kaliyamurthie K.P., Udayakumar R., Parameswari D., Mugunthan S.N., 'Highly secured online voting system over network", Indian Journal of Science and Technology, ISSN : 0974-6846, 6(S6) (2013) pp.4831-4836.
[7] Druschel.P and Rowstron.A,(2001) "PAST: A Large-Scale, Persistent Peer- to-Peer Storage Utility," Proc. Eighth Workshop Hot Topics in Operating System (HotOS VIII), pp. 75-80.
[8] Kiran Kumar T.V.U., Karthik B., 'Improving network life time using static cluster routing for wireless sensor networks", Indian Journal of Science and Technology, ISSN : 0974-6846, 6(S5) (2013) pp.4642-4647.
[9] Haeberlen.A, Mislove.A, and Druschel.P, (2005) "Glacier: Highly Durable, Distributed Storage Despite Massive Correlated Failures,"Proc. Second Symp. Networked Systems Design and Implementation (NSDI), pp. 143-158
[10] Jeyanthi Rebecca L., Susithra G., Sharmila S., Das M.P., 'Isolation and screening of chitinase producing Serratia marcescens from soil", Journal of Chemical and Pharmaceutical Research, ISSN : 0975 – 7384, 5(2) (2013) pp.192-195.
[11] Lin .H.Y and Tzeng.W.G, (2010) "A Protected Distributed Erasure Code for Distributed Network Storage," IEEE Trans. Parallel and Distributed Systems, vol. 21, no. 11, pp. 1586-1594.
[12] Shamir.A(1979), "How to Share a Secret," ACM Comm., vol. 22, pp. 612-613.
[13] Shao J. and Cao.Z, ,(2009) "CCA- Protected Alternate Re-Encryption without Pairings," Proc. 12th Int'l Conf. Practice and Theory in Public Key Cryptography (PKC), pp. 357-376.
[14] Tang.Q(2008), "Type-Based Alternate Re- Encryption and Its Construction,"Proc. Ninth Int'l Conf. Cryptology in India: Progress in Cryptology (INDOCRYPT), pp. 130-144.
[33] Bharthvajan R, Human Resource - Strategy and Outsource, International Journal of Innovative Research in Science, Engineering and Technology, ISSN: 2319-8753,pp 15273-15276, Vol. 3, Issue 8, August 2014

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. 3, Issue 8, August 2015

[34] Bharthvajan R, Human Resource Management and Supply Chain Management Intersection, International Journal of Innovative Research in Science, Engineering and Technology, ISSN: 2319-8753,pp 10163-10167, Vol. 3, Issue 3, March 2014
[35] Bharthvajan R, Women Entrepreneurs & Problems Of Women Entrepreneurs, International Journal of Innovative Research in Science, Engineering and Technology, ISSN: 2319-8753,pp 16105-16110, Vol. 3, Issue 9, September 2014
[36] Bharthvajan R, Organizational Culture and Climate, International Journal of Innovative Research in Science, Engineering and Technology, ISSN: 2319-8753,pp 8870-8874, Vol. 3, Issue 1, January 2014
[37] C.Rathika Thaya Kumari , Dr.A.Mukunthan, M.Nageshwari, Electric and Magnetic Properties of Semiconductors and Metals in One, Two and Three Dimensions, International Journal of Innovative Research in Science, Engineering and Technology, ISSN: 2319-8753,pp 271-279, Vol. 2, Issue 1, January 2013
[38] C.Tamil Selvi & Dr. A. Mukunthan, Different Varieties of Plantain (Banana) and Their Estimation by Chemical Tests, International Journal of Innovative Research in Science, Engineering and Technology, ISSN: 2319-8753,pp 1099-1105, Vol. 2, Issue 4, April 2013