Computer Science and Information Technology 2(4): 203-210, 2014 http://www.hrpub.org
DOI: 10.13189/csit.2014.020404

Dynamic Data Storage Publishing and Forwarding in Cloud Using Fusion Security Algorithms

Asadi Srinivasulu[1,*], Ch.D.V.Subbarao[2], A.Bhudevi[3]

[1]IT Dept, Sree Vidyanikethan Engineering College, Tirupathi-517102, A.P, India
[2]CSE and Head, SVUCE, Tirupathi, S.V.University,Tirupathi, A.P,INDIA-517501
[3]M.Tech, CSE Dept, Sree Vidyanikethan Engineering College, Tirupathi-517102, A.P, India
*Corresponding Author: srinu_asadi@yahoo.com

Abstract A Cloud storage system consists of a collection of storage servers provide long-term Services over the internet. Storing data in other's Cloud system causes serious concern over data confidentiality. Existing systems protect data confidentiality, but also limit the functionality of the system. Constructing a secure storage system that supports multiple functions is challenging when the storage system is distributed. Proposed system consists of proxy re-encryption scheme integrated with a decentralized erasure code such that a secure storage system is constructed. Planned system not only supports secure and robust data, but also let user forward data in the storage system to another user without retrieving it back. Projected system fully integrates encrypting, encoding and forwarding. Proposed system analyzes and suggests suitable parameters for number of copies of messages delivered to storage servers and number of storage servers queried by key server.

Keywords Decentralized Erasure Code, Proxy Re-Encryption, Threshold Cryptography, Secure Storage System

1. Introduction

Cloud Computing is a concept that treats the resources on the Internet as a unified Entity Cloud. It focuses on designing a cloud storage system for robustness, confidentiality and functionality. One way to provide Data robustness is to replicate a message such that each server stores copy of message. It is very robust because the message can be retrieved as long as one storage server survives. As high-speed networks and ubiquitous Internet access become available in recent years, many services are provided on the Internet such that users can use them from anywhere at any time. For example, the email service is probably the most popular one. Cloud computing is a concept that treats the resources on the Internet as a unified entity, a cloud. Users just use services without being concerned about how computation is done and storage is managed. A cloud storage system is considered as a large scale distributed storage system that consists of many independent storage servers. Moving data into the cloud offers great convenience to users since they don't have to care about the complexities of direct hardware management. The pioneer of Cloud Computing vendors, Amazon Simple Storage Service (S3) and Amazon Elastic Compute Cloud (EC2) are both well known examples. While these internet-based online services do provide huge amounts of storage space and customizable computing resources, this computing platform shift, however, is eliminating the responsibility of local machines for data maintenance at the same time. As a result, users are at the mercy of their cloud service providers for the availability and integrity of their data. Recent downtime of Amazon's S3 is such an example. From the perspective of data security, which has always been an important aspect of quality of service, Cloud Computing inevitably poses new challenging security threats for number of reasons.

Secondly, Cloud Computing is not just a third party data warehouse. The data stored in the cloud may be frequently updated by the users, including insertion, deletion, modification, appending, reordering, forwarding etc. To ensure storage correctness under dynamic data update is hence of paramount importance. However this dynamic feature also makes traditional integrity insurance tech inquest futile and entails new solutions. Last but not the least, the deployment of Cloud Computing is powered by data centers running in a simultaneous, cooperated and distributed manner. Individual user's data is redundantly stored in multiple physical locations to further reduce the data integrity threats. Therefore, distributed protocols for storage correctness assurance will be of most importance in achieving a robust and secure cloud data storage system in the real world. However, such important area remains to be fully explored in the literature. Another way to encode a message of k symbols into a codeword of n symbols by erasure coding. To store a message each of its codeword symbols is stored in different storage server. Storing data in a third party's cloud causes serious concern on data

confidentiality. In order to provide strong confidentiality of messages user can encrypt messages by a cryptographic method before applying an erasure code method to encode and store messages. The proposed system addresses the problem of forwarding data to another user by storage servers directly under the command of data owner. It considers the system model that consists of distributed storage servers and key servers.

1.1. Problem Statement

From the perspective of data security, which has always been an important aspect of quality of service, Cloud Computing inevitably poses new challenging security threats for number of reasons. Firstly, data robustness i.e. the availability of data is the major requirement for storage systems. One way to provide data robustness is to replicate a message such that each storage server makes a copy of that message. But by storing the data in every server will increase the storage cost. Secondly, storing data in the third party's cloud causes serious concerns over data confidentiality. As huge amount of data is stored in the cloud servers providing security to that data will be a great challenge. Lastly to forward the data stored in the cloud to another cloud, the user should retrieve the encrypted data, decrypt it and then he should transfer the data statically to the other user. This whole procedure is a time-taking task.

These techniques, while can be useful to ensure the storage correctness without having users possessing data, cannot address all the security threats in cloud data storage, since they are all focusing on single server scenario and most of them do not consider dynamic data operations. As an complementary approach, researchers have also proposed distributed protocols for ensuring storage correctness across multiple servers or peers. Again, none of these distributed schemes is aware of dynamic data operations. As a result, their applicability in cloud data storage and forwarding can be drastically limited. In this project, we propose an effective and flexible distributed scheme with explicit dynamic data support to ensure the correctness of users' data in the cloud. We rely on decentralized erasure correcting code in the file distribution preparation to provide redundancies and guarantee the data dependability. This construction drastically reduces the communication and storage overhead as compared to the traditional replicate-type message storing. Effective encoding and encrypting operations are being utilized to meet the requirements of data confidentiality. A secure proxy re-encryption scheme is provided to meet the requirements of data forwarding. The tight integration of encoding, encryption and forwarding makes the system to work efficiently.

1. Compared to many of its predecessors, which only provide binary results about the storage state across the distributed servers, the challenge-response protocol in our work further provides the localization of data error.
2. Unlike most prior works for ensuring remote data integrity, the new scheme supports secure and efficient dynamic operations on data blocks, including: update, delete, append and forward.
3. Extensive security and performance analysis shows that the proposed scheme is highly efficient and resilient against Byzantine failure, malicious data modification attack, and even server colluding attacks.

2. Related Work

This Survey identifies the key reported IT-related risks that should be considered by security practitioners when evaluating public cloud computing service providers. Over fifty references, produced by technical and legal experts from public and private organizations in the United States and abroad, are evaluated, organized, and synthesized for this study. Of the aforementioned collection, approximately thirty references are used to identify and describe the various IT-related cloud computing risks that organizations need to evaluate and mitigate. This Survey focuses on a presentation of the primary IT-related risks of cloud computing and suggested mitigation strategies.

IT-related risks are classified into three risk categories:

1) Policy and organizational risks
2) Technical risks
3) Legal risks.

Mitigation strategies include:

1) Audit controls
2) Policies and procedures
3) Service level agreements
4) Other forms of governance.

2.1. Problem Area/Significance

Cloud computing is defined as "a model for enabling convenient, on-demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction". Applications of cloud computing broadly span three areas known as "cloud service delivery models":

a) Infrastructure as a Service (IaaS)
b) Platform as a Service (PaaS)
c) Software as a Service (SaaS).

As suggested by Levitt, cloud computing frees organizations from the need to buy and maintain their own hardware and software infrastructure. Erdogmus reports that there are two key business drivers to consider in relation to cloud computing:

a) Economics
b) Simplification of software delivery.

Leavitt suggests that cloud computing offers additional technical benefits including high availability and easy scalability, providing faster, more direct access to IT resources. Recently, the importance of ensuring the remote

data integrity has been highlighted by the following research works. These techniques, while can be useful to ensure the storage correctness without having users possessing data, can not address all the security threats in cloud data storage, since they are all focusing on single server scenario and most of them do not consider dynamic data operations. As an complementary approach, researchers have also proposed distributed protocols for ensuring storage correctness across multiple servers or peers. Again, none of these distributed schemes is aware of dynamic data operations. As a result, their applicability in cloud data storage can be drastically limited. With respect to reliability, Armbrust, Fox, Griffith, Joseph, Katz, Konwinski, et al argue that few non-cloud IT infrastructures are as robust as cloud computing service offerings, but organizations are still concerned about availability in light of recent outages from Amazon and Google. To support block append operation, we need a slight modification to our token pre-computation. Specifically, we require the user to expect the maximum size in blocks, denoted as *lmax*, for each of his data vector. The idea of supporting b lock append, which is similar as adopted in [1], relies on the initial budget for the maximum anticipated data size *lmax* in each encoded data vector as well as the system parameter. As noted by Leavitt, organizations are now evaluating both the risks and rewards of cloud computing.

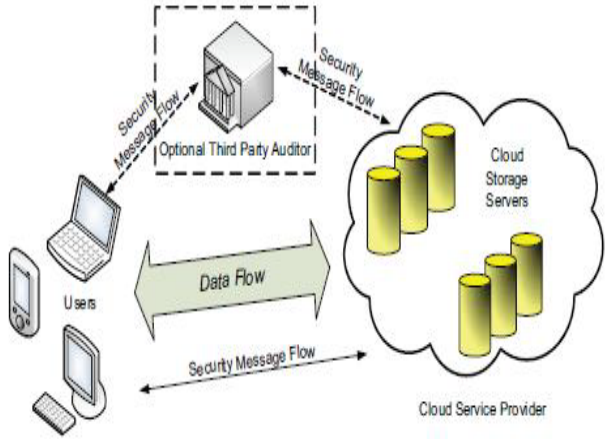

Figure. Architecture of Entire System

2.1.1. Purpose

The purpose of this study is to describe and identify key public cloud computing "IT-related risks" as reported in selected literature. IT-related risk is defined in this study as "the net mission/business impact considering the likelihood that a particular threat source will exploit, or trigger, particular information system vulnerability". The study is designed as a literature review of relevant research between 2007 and 2009. The study addresses the following research question: What are the key IT-related risks that should be considered by security practitioners when evaluating cloud computing service providers".

2.1.2. Audience

The target audience for the study is primarily security practitioners who evaluate, recommend, and lead the implementation of cloud computing services on behalf of their respective organizations. The Cloud Security Alliance acknowledges that cloud computing are an "unstoppable force" and those security practitioners needed to be proactive in leading its secure adoption. Security practitioners face a daunting challenge, as "many of the leading cloud service providers accept no responsibility for the data being stored in their infrastructure". In addition, security practitioners must address the possibility that business users can now bypass IT and engage directly with cloud computing service providers.

2.1.3. Outcome

The intended outcome of this study is an explicated set of cloud computing IT-related risks, along with a review of potential mitigation strategies. The most common and severe IT-related cloud computing risks reported in the selected literature are identified to provide critical areas of focus for security practitioners. IT-related risks are collected and organized into "risk categories," as documented in the Disaster Recovery Journa. A pre-selected set of categories is pulled from a glossary developed jointly by the editorial advisory board of the Disaster Recovery Journal and the DRII Certification Commission and includes: reputation, strategy, financial, investments, operational infrastructure, business, regulatory compliance, outsourcing, people, technology and knowledge. Once identified, the IT-related cloud computing risks are classified into three overarching risk categories (policy and organizational, technical, and legal) that serve as a useful reference to security practitioners as they evaluate cloud computing service providers. Each of these risk categories apply to the three cloud service delivery models associated with cloud computing (IaaS, PaaS, and SaaS), although the specific IT-related risks within each of these three delivery models varies.

3. Existing System

In Existing System use a straightforward integration method. In straightforward integration method 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. General encryption schemes protect data confidentiality, but also limit the functionality of the storage system because a few operations are supported over encrypted data. A decentralized architecture for storage systems offers good scalability, because a storage server can join or leave without control of a central authority.

1. Encoding Techniques
2. Centralized Erasure Code Technique
3. Proxy Re-encryption Schemes

3.1. Disadvatages of Existing System

- The user can perform more computation and communication traffic between the user and storage servers is high.
- The user has to manage his cryptographic keys otherwise the security has to be broken.
- The data storing and retrieving, it is hard for storage servers to directly support other functions.
- High computation cost
- High computation time
- High communication traffic
- Less data confidentiality
- Forwarding data highly time consuming
- Static data storage

4. Proposed System

In our proposed system we address the problem of forwarding data to another user by storage servers directly under the command of the data owner. 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.

The distributed systems require independent servers to perform all operations. We propose a new threshold proxy re-encryption scheme and integrate it with a secure decentralized code to form a secure distributed storage system. The encryption scheme supports encoding operations over encrypted messages and forwarding operations over encrypted and encoded messages.

1. Encoding Techniques using Storage Servers and Key Servers
2. Decentralized Erasure Code Technique
3. Distributed Proxy Re-encryption Schemes
4. Dynamic Data Encryption Techniques
5. Security Algorithms Like RSA, DES and Belief Logic

4.1. Advantages of Proposed System

- Tight integration of encoding, encryption, and forwarding makes the storage system efficiently meet the requirements of data robustness, data confidentiality, and data forwarding.
- The storage servers independently perform encoding and re-encryption process and the key servers independently perform partial decryption process.
- More flexible adjustment between the number of storage servers and robustness.
- To reducing computation cost
- To reducing computation time
- T o reduce communication traffic
- To increase data confidentiality
- Efficient forwarding data
- Efficient dynamic data storage

4.2. Cloud Data Storage Architecture

Representative network architecture for cloud data storage is illustrated in Figure 4.1.

Three different network entities can be identified as follows:

User - Users, who have data to be stored in the cloud and rely on the cloud for data computation, consist of both individual consumers and organizations.

Cloud Service Provider (CSP)- A CSP, who has significant resources and expertise in building and managing distributed cloud storage servers, owns and operates live Cloud Computing systems.

Third Party Auditor (TPA)- An optional TPA, who has expertise and capabilities that users may not have, is trusted to assess and expose risk of cloud storage services on behalf of the users upon request. In cloud data storage, a user stores his data through a CSP into a set of cloud servers, which are running in a simultaneous, cooperated and distributed manner. Data redundancy can be employed with technique of erasure-correcting code to further tolerate faults or server crash as user's data grows in size and importance.

Thereafter, for application purposes, the user interacts with the cloud servers via CSP to access or retrieve his data. In some cases, the user may need to perform block level operations on his data. The most general forms of the most general forms of these operations we are considering are block update, delete, insert and append. As users no longer possess their data locally, it is of critical Importance to assure users that their data are being correctly stored and maintained. That is, users should be equipped with security means so that they can make continuous correctness assurance of their stored data even without the existence of Local copies. In case those users do not necessarily have the time, feasibility or resources to monitor their data, they can delegate the tasks to an optional trusted TPA of their respective choices. In our model, we assume that the point-to-point communication channels between each cloud server and the user is authenticated and reliable, which can be achieved in practice with little overhead. Note that we don't address the issue of data privacy in this paper, as in Cloud Computing, data privacy is orthogonal to the problem we study here.

5. Implementation

Implementation is the stage of the project when the theoretical design is turned out into a working system. Thus it can be considered to be the most critical stage in achieving a successful new system and in giving the user, confidence that the new system will work and be effective. The implementation stage involves careful planning, investigation of the existing system and it's constraints on

implementation, designing of methods to achieve changeover and evaluation of changeover methods.

5.1. Key Generation Algorithm

a. Key Generation (μ)

1.1. Start
1.2. Obtain parameters (g,h,p).
1.3. G1 can be generated by g and h.
1.4. G2 can be generated by prime number p.
1.5. Set μ=(g,h,ẽ,G1,G2,p,f)
1.6. f:Zp*{0,1} Zp*Is a one-way hash function
1.7. User A selects three parameters a_1; a_2; a_3 Z_p^*
1.8. $PK_A=(g^{a_1}, h^{a_1})$,ska=(a_1,a_2,a_3).
1.9. Stop.

5.2. Share Key Generation Algorithm

b) Sharekeygen (SK_A,t,m)

2.1. Start
2.2. Select m key servers
2.3. Share secret key SK_A to key server ks_i
2.4. $SK_{A,i}=(f_{A,1}(i),f_{A,2}(i))$ where $1\leq i \leq m$.
2.5. Stop.

5.3. Encryption Algorithm

c) Encryption (PK_A,T,m_1,m_2,…..m_k)

3.1. Start
3.2. Divide message in to m_1,m_2,…..m_k
3.3. Calculate cipher text c_1,c_2,…..c_k by using

$$C_i = (0, \alpha_i, \beta, \gamma_i) = (0, g^{r_i}, \tau, m_i \tilde{e}(g^{a_1}, \tau^{r_i}))$$

3.4. Stop.

5.4. Key Recovery Algorithm

d)Key Recover($SK_{A,i1}$, $SK_{A,i2}$, $SK_{A,i3}$, $SK_{A,i4}$……, $SK_{A,in}$)

4.1. Start
4.2 .User searches for first component a_1
4.3. if (a1 found)
4.3.1. No need of key recovery.
4.4. if (a1 not found)
4.4.1. Recovered by using

$$a_1 = \sum_{s \in T} \left(f_{A,1}(s) \prod_{s' \in T/\{s\}} \frac{-s'}{s - s'} \right) mod\ p$$

4.5. Stop

5.5. Re Key Generation Algorithm

e) ReKeyGen (PK_A, SKA, ID, PKB)

5.1. Start
5.2. Encrypt the data by using SK_A.
5.3. Select a random number e from Z_p^*.
5.4.Compute rekey for proxy reencryption by using

$$RK_{A\to B}^{ID} = \left((h^{b_2})^{a_1(f(a_3,ID)+e)}, h^{a_1 e}\right)$$

5.5. Stop.

5.6. Proxy Re-Encryption Algorithm

f) Proxy ReEncryption ()

6.1. Start
6.2. Calculate RK, C'.
6.3. ReEncrypted symbol can be computed as

$$C'' = (1, \alpha, h^{b_{2a_1}}(f(a_3, ID)+e), \gamma.\tilde{e}(\alpha, h^{a1e}))$$

$$= (1, g^{r'}, h^{b_{2a_1}}(f(a_3, ID)+e), W\tilde{e}(g,h)^{a1r'((f(a_3, ID)+e)})$$

6.4. Stop

5.7. Main Modules

- Construction of Cloud Data Storage Module
- Data Encryption Module
- Data Forwarding Module
- Data Retrieval Module

6. Modules Description

6.1. Construction of Cloud Data Storage Module

In Admin Module the admin can login to give his username and password. Then the server setup method can be opened. In server setup process the admin first set the remote servers Ip-address for send that Ip-address to the receiver. Then the server can skip the process to activate or Dis-activate the process. For activating the process the storage server can display the Ip-address. For Dis-activating the process the storage server cannot display the Ip-address. These details can be viewed by clicking the key server. The activated Ip-addresses are stored in available storage server. By clicking the available storage server button we can view the currently available Ip-addresses.

6.2. Data Encryption Module

In cloud login module the user can login his own details. If the user cannot have the account for that cloud system first the user can register his details for using and entering into the cloud system. The Registration process details are Username, E-mail, password, confirm password, date of birth, gender and also the location. After entering the registration process the details can be stored in database of the cloud system. Then the user has to login to give his corrected username and password the code has to be send his/her E-mail. Then the user will go to open his account and view the code that can be generated from the cloud system. In Upload Module the new folder can be create for storing the files. In folder creation process the cloud system may ask one question for that user. The user should answer the question and must remember that

answer for further usage. Then enter the folder name for create the folder for that user. In file upload process the user has to choose one file from browsing the system and enter the upload option. Now, the server from the cloud can give the encrypted form of the uploading file.

6.3. Data Forwarding Module

In forward module first we can see the storage details for the uploaded files. When click the storage details option we can see the file name, question, answer, folder name, forward value (true or false), forward E-mail. If the forward column display the forwarded value is true the user cannot forward to another person. If the forward column display the forwarded value is false the user can forward the file into another person. In file forward processes contains the selected file name, E-mail address of the forwarder and enter the code to the forwarder. Now, another user can check his account properly and view the code forwarded from the previous user. Then the current user has login to the cloud system and to check the receive details. In receive details the forwarded file is present then the user will go to the download process.

6.4. Data Retrieval Module

In Download module contains the following details. There are username and file name. First, the server process can be run which means the server can be connected with its particular client. Now, the client has to download the file to download the file key. In file key downloading process the fields are username, filename, question, answer and the code. Now clicking the download option the client can view the encrypted key. Then using that key the client can view the file and use that file appropriately.

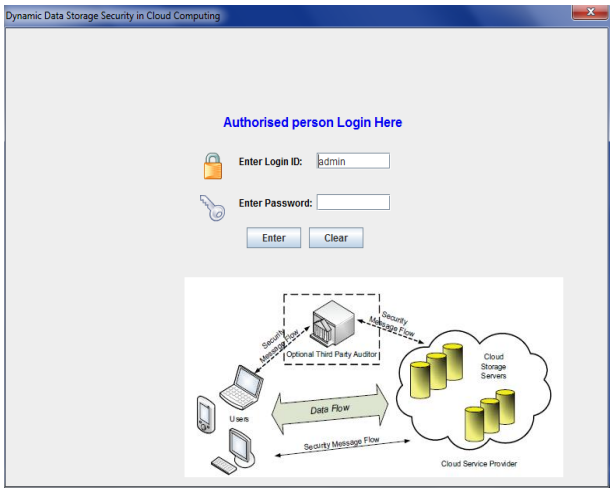

Figure 6.1. Authorised Person Login

Login screen is user interact with the cloud computing system with authentication. This screen is user authentication screen, where user name and password is authenticated, if the authentication process is successfully completed then only user will be allowed to next step. This is the main screen of project.

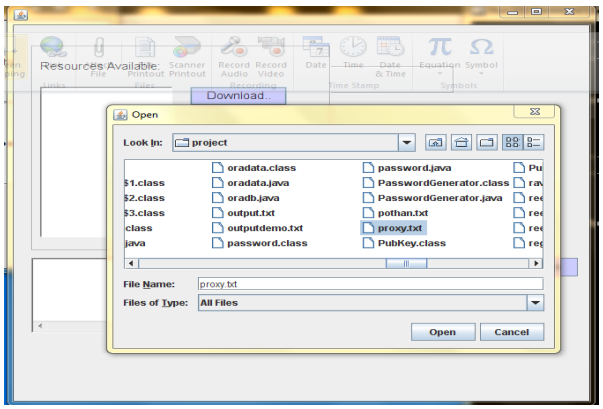

Figure 6.6. Selecting File

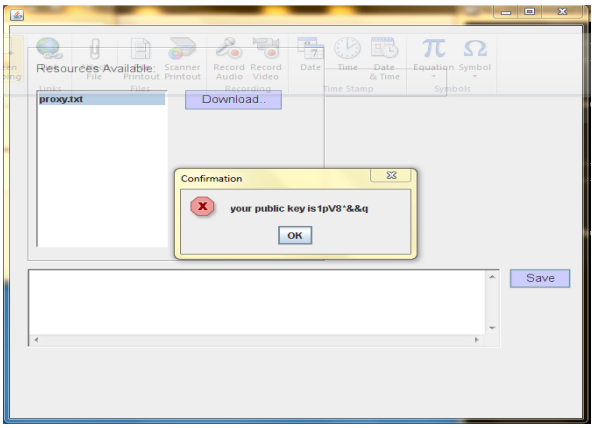

Figure 6.8. Public key Generation

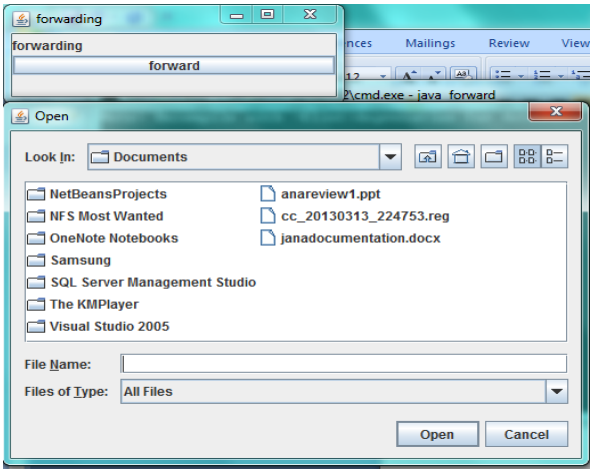

Figure 6.16. Forwarding Screen

Figure 6.18. Public Key

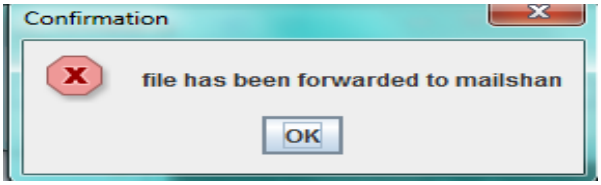

Figure 6.19. Confirmation Message.

7. Conclusions and Future Work

To This project investigates the problem of data security in cloud data storage, which is essentially a distributed storage system. To ensure the correctness of user's data in cloud data storage, we proposed an effective and flexible distributed scheme with explicit dynamic data Storage support and Forwarding, including update, delete, and append. We rely on erasure-correcting code in the file distribution preparation to provide redundancy parity vectors and guarantee the data dependability. By utilizing the proxy re-encryption with distributed verification of erasure coded data and Fusion Security Algorithms, our scheme achieves the integration of Dynamic storage correctness insurance, data error localization, data Forwarding and data Security i.e., whenever data corruption has been detected during the storage correctness verification across the distributed servers, we can almost guarantee the simultaneous identification of the Correct data. Through detailed security and performance analysis, we show that our scheme is highly efficient and resilient to Byzantine failure, malicious data modification attack and Man-in Middle attack.

We believe that data storage security and forwarding in Cloud Computing, an area full of challenges and of paramount importance, is still in its infancy now, and many research problems are yet to be identified. We envision several possible directions for future research on this area. The most promising one we believe is a model in which public verifiability is enforced. Public verifiability, supported allows TPA to audit the cloud data storage without demanding user's time, feasibility or resources. An interesting question in this model is if we can construct a scheme to achieve both public verifiability and storage correctness assurance of dynamic data Storage and Forwarding. Besides, along with our research on dynamic cloud data storage and forwarding, we also plan to investigate the problem of fine-grained data error localization.

REFERENCES

[1] Hsiao-Ying Lin and Wen-Guey Tzeng, "A secure erasure code-based cloud storage system with secure data forwarding",IEEE Transaction on parallel and distributed systems, vol 23,issue no 6,june 2012,pp 1995-1003.

[2] 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.

[3] 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.

[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] Amazon.com, "Amazon Web Services (AWS)," Online at http://aws amazon.com, 2008.

[7] N. Gohring, "Amazon's S3 down for several hours," at http://www.pcworld.com/businesscenter/article/142549/amazons s3 down for several hours.html, 2008.

[8] A. Juels and J. Burton S. Kaliski, "PORs: Proofs of Retrievability for Large Files," Proc. of CCS '07, pp. 584–597, 2007.

[9] H. Shacham and B. Waters, "Compact Proofs of Retrievability," Proc.of Asiacrypt '08, Dec. 2008.

[10] K. D. Bowers, A. Juels, and A. Oprea, "Proofs of Retrievability: Theoryand Implementation," Cryptology ePrint Archive, Report 2008/175,2008, http://eprint.iacr.org/.

[11] G. Ateniese, R. Burns, R. Curtmola, J. Herring, L. Kissner, Z. Peterson, and D. Song, "Provable Data Possession at Untrusted Stores," Proc. of CCS '07, pp. 598–609, 2007.

[12] G. Ateniese, R. D. Pietro, L. V. Mancini, and G. Tsudik, "Scalable and Efficient Provable Data Possession," Proc. of SecureComm '08, pp.1–10, 2008.

[13] T. S. J. Schwarz and E. L. Miller, "Store, Forget, and Check: Using Algebraic Signatures to Check Remotely Administered Storage," Proc. of ICDCS '06, pp. 12–12, 2006.

[14] M. Lillibridge, S. Elnikety, A. Birrell, M. Burrows, and M. Isard, "A Cooperative Internet Backup Scheme," Proc. of the 2003 USENIX Annual Technical Conference (General Track), pp. 29–41, 2003.

[15] K. D. Bowers, A. Juels, and A. Oprea, "HAIL: A High-Availability and Integrity Layer for Cloud Storage," Cryptology ePrint Archive, Report 2008/489, 2008, http://eprint.iacr.org/.

[16] L. Carter and M. Wegman, "Universal Hash Functions," Journal of Computer and System Sciences, vol. 18, no. 2, pp. 143–154, 1979.

[17] J. Hendricks, G. Ganger, and M. Reiter, "Verifying Distributed Erasurecoded Data," Proc. 26th ACM

Symposium on Principles of Distributed Computing, pp. 139–146, 2007.

[18] J. S. Plank and Y. Ding, "Note: Correction to the 1997 Tutorial on Reed-Solomon Coding," University of Tennessee, Tech. Rep. CS-03- 504, 2003.

[19] Q. Wang, K. Ren, W. Lou, and Y. Zhang, "Dependable and Secure Sensor Data Storage with Dynamic Integrity Assurance," Proc. of IEEE INFOCOM, 2009.

[20] R. Curtmola, O. Khan, R. Burns, and G. Ateniese, "MR-PDP: Multiple- Replica Provable Data Possession," Proc. of ICDCS '08, pp. 411–420,2008.

[21] D. L. G. Filho and P. S. L. M. Barreto, "Demonstrating Data Possession and Uncheatable Data Transfer," Cryptology ePrint Archive, Report 2006/150, 2006, http://eprint.iacr.org/.