Available Online at www.ijcsmc.com

International Journal of Computer Science and Mobile Computing

A Monthly Journal of Computer Science and Information Technology

ISSN 2320–088X

IJCSMC, Vol. 3, Issue. 6, June 2014, pg.109 – 115

RESEARCH ARTICLE

A Cloud Storage System with Information Confidentiality and Forwarding

Dr. M.V.Siva Prasad Phd, M.Tech, **P.Sandeep Reddy** M.Tech, **M.Raghava** B.Tech
raghava.cse432@gmail.com , raghava.workplace@gmail.com
ANURAG ENGINEERING COLLEGE, KODAD, ANDHRA PRADESH

Abstract

Cloud storage suggests that the storage of information on-line within the cloud,wherein a company's knowledge is keep in and accessible from multiple distributed and connected resources that comprise a cloud.Cloud storage will offer the advantages of larger accessibility and reliability; speedy deployment; robust protection for knowledge backup,archival and disaster recovery purposes; and lower overall storage prices as a results of not having to buy, manage and maintain overpriced hardware. However, cloud storage will have the potential for security and compliance issues.Third party's cloud system doesn't offer knowledge confidentiality. Constructing centralized storage system for the cloud system makes hackers scarf knowledge simply. General cryptography schemes shield knowledge confidentiality. within the projected system a secure distributed storage system is developed by desegregation a threshold proxy re-encryption theme with a suburbanised erasure code. The distributed storage system not solely supports secure and strong knowledge storage and retrieval, however conjointly lets a user forward knowledge from one user to a different while not retrieving the info back. the most technical involvement is that the proxy re-encryption theme supports coding operations over encrypted messages still as forwarding operations over encoded and encrypted messages. the strategy totally integrates encrypting, encoding, and forwarding.

1. Introduction

Viewing from the recent years as high-speed networks and the ubiquitous Internet access become available, as many services are provided on the Internet such that users can use them from anywhere at any time. In the concept of cloud computing, it treats the all resources as a unified entity i.e. cloud. The

resource management and the computations are not concerned by the user. In the designing of the cloud system we focus on the confidentiality, functionality and the robustness. A cloud storage system is considered as a large scale distributed storage system that consists of many independent storage servers. many services are provided on the Internet such that users can use them from anywhere at any time .we focus on designing a cloud storage system for robustness,confidentiality,functionality.Data robustness is a major requirement for storage systems.To provide a data robustness 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 a different storage server. A decentralized erasure code is an erasure code that independently computes each codeword symbol for a message Thus, the encoding process for a message can be split into n parallel tasks of generating codeword symbols. A decentralized 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 code- word symbol for the received message symbols and stores it. This finishes the encoding and storing process. The recovery process is the same. The tight integration of encoding, encryption, and forwarding makes the storage system efficiently meet the requirements of data robustness, data confidentiality, and data forwarding. Our system meets the requirements that storage servers independently perform encoding and re-encryption and key servers independently perform partial decryption.

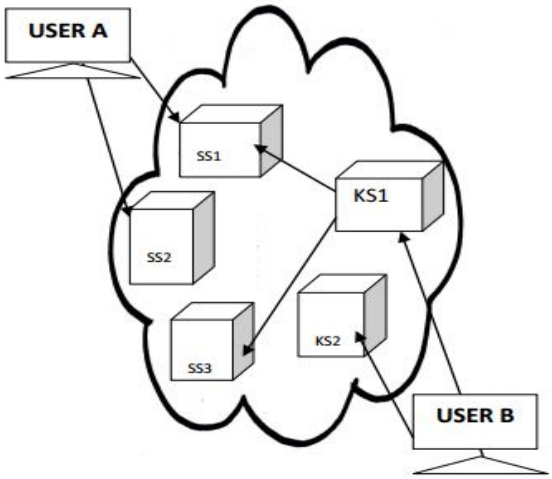

Fig:1 cloud architecture for secure data forwarding

Viewing from the recent years as high-speed networks and therefore the omnipresent web access become obtainable, as several services ar provided on the Internet such users will use them from anyplace at any time. within the idea of cloud computing, it treats the all resources as a unified entity i.e. cloud. The resource management and therefore the computations don't seem to be involved by the user. within the planning of the cloud system we tend to target the confidentiality, practicality and therefore the strength. A cloud storage system is taken into account as an oversized scale distributed storage system that consists of the many freelance storage servers. several services ar provided on the web such users will use them from anyplace at any time .we target planning a cloud storage system for strength, confidentiality, and practicality.Data strength may be a major demand for storage systems.To provide a knowledge strength to cypher a message of k symbols into a codeword of n symbols by erasure committal to writing. To store a message, every of its codeword symbols is keep during a

completely different storage server. A decentralized erasure code is Associate in Nursing erasure code that independently computes every codeword image for a message therefore, the cryptography method for a message are often split into n parallel tasks of generating codeword symbols. A decentralized erasure code is appropriate to be used during a distributed storage system. once the message symbols ar sent to storage servers, every storage server severally computes a code- word image for the received message symbols and stores it. This finishes the cryptography and storing method. The recovery method is that the same. The tight integration of cryptography, encryption, and forwarding makes the storage system with efficiency meet the necessities of information strength, knowledge confidentiality, and knowledge forwarding. Our system meets the necessities that storage servers severally perform cryptography and re-encryption and key servers severally perform partial cryptography.

2. Litreature Survey

Q. Liu et al [1] proposed a time-based re-encryption theme, that permits the cloud servers to mechanically re-encrypt information supported their internal clocks. associate degreeswe is constructed on high of an attribute based mostly encoding (ABE) theme. ABE permits information to be encrypted victimization associate degree access structure comprised of various attributes. A cloud is basically an oversized scale distributed system wherever a information a knowledge an information owner's data is replicated over multiple servers for top handiness. every cloud server can severally re-encrypt information while not receiving any command from the information owner. the tactic extends associate degree ABE theme by incorporating timestamps to perform proxy re-encryption. The higher than resolution doesn't need excellent clock synchronization among all of the cloud servers to take care of correctness. could be a combination of your time based mostly and ABE. Time based mostly user revocation is feasible and it handles dynamic information. information and keys don't seem to be divided and shared.

C.Wang et.al [2] proposed aTime based mostly re-encryption and Attribute based mostly encoding.Information confidentiality and potency. Integrity of knowledge that keep in associate degree untrusted server are often verified while not retrieving it back in . Utilizing the homomorphic token with distributed verification of erasure-coded information projected by achieves the mixing of storage correctness and information error localization.

Lidong Zhou[3] proposed distributed services interacting.The decoding method won't reveal the data since it's cloaked by the glary issue. Verifiable twin coding is employed to verify the correctness of the re-encrypted knowledge. Asynchronous model of computation is used; there's no certain on message delivery delay.Features of this scheme includes ,Asymmetric El- gamal re-encryption. ,Distributed asynchronous service. ,Verifiable dual encryption.

Giuseppe Ateniese[4] proposed a methodology relies on additive maps. The cryptography method are often customised. With an equivalent public key, the sender is given selection of the recipient set. Re-encryption keys are often generated by sender exploitation receiver's public key; no trusty third party or interaction is needed. The algorithmic rule is collusion-resistant.Features of this scheme are , Asymmetric re-encryption ,Non interactive ,Collusion resistant , Unidirectional ,No secret key pre-sharing needed.

Jakobsson et al [5] proposed re-encryption is secure as long as there's no dishonest assemblage of proxy servers the uneven proxy re-encryption theme is associate degree improvement over the previous work that may be a isosceles proxy cryptography.This scheme provides ,Asymmetric re-encryption , Private key is shared as quorum , Verifiable translation certificate.

3. Methodology Used

Proxy Re-encryption Scheme with Multiplicative Homomorphic Property:

In the proxy Re-encryption key the messages area unit 1st encrypted by the owner and so keep in an exceedingly storage server. once a user desires to share his messages, he sends a re-encryption key to the storage server.the storage server re encrypts the encrypted messages for the approved users.thus,thier system has information confidentiality and supports the information forwarding perform.An cryptography theme is increasing homomorphic if it supports a group operation on encrypted plaintexts while not decoding. The increasing homomorphic cryptography theme supports the secret writing operation over encrypted messages. we have a tendency to then convert a proxy re-encryption theme with increasing homomorphic property into a threshold version. A secret secret's shared to key servers with a threshold price t. To decipher for a group of k message symbols, every key server severally queries two storage servers and partly decrypts to encrypted codeword symbols. As long as t key servers area unit obtainable, k codeword symbols area unit obtained from the partly decrypted cipher texts.In order to preserve privacy, the shoppers can write their information after they out- supply it to the cloud. However, the encrypted style of information greatly impedes the employment because of its randomness.Many efforts are in deep trouble the aim of information usage however while not undermining the information privacy. Homomorphism: Given 2 cipher texts c1 and c2 on plaintexts M1 and M2 severally, one will acquire the cipher text on the plaintext M1 +m2 and/or M1 ·m2 by evaluating c1 and c2 while not decrypting cipher texts.Proxy re-encryption keythe proxy will remodel a cipher text of 1 user to a cipher text of the target user.Threshold decryption: By dividing the non-public key into many items of secret shares, all shoppers will work along to decipher the cipher text – the output of the perform.

4. MODULES

Construction of Cloud Data Storage Modul

In Admin Module the admin will login to allow his username and countersign. Then the server setup methodology will be opened. In server setup method the admin initial set the remote servers Ip-address for send that Ip-address to the receiver. Then the server will skip the method to activate or Dis-activate the method. For activating the method the storage server will show the Ip-address. For Dis-activating the method the storage server cannot show the Ip-address. These details will be viewed by clicking the key server. The activated Ip-addresses area unit hold on in accessible storage server. By clicking the accessible storage server button we are able to read the presently accessible Ip-addresses.

4.1 Data Encryption Module

In cloud login module the user will login his own details. If the user cannot have the account for that cloud system 1st the user will register his details for exploitation and getting in the cloud system.The Registration method details square measure Username,email password, ensure arcanum, date of birth, gender and conjointly the placement. when coming into the registration method the small print are often keep in information of the cloud systemThen the user needs to login to allow his corrected username and arcanum the code needs to be send his/her E-mail. Then the user can head to open his account and think about the code that may be generated from the cloud system. In transfer Module the new folder are often produce for storing the files. In folder creation method the cloud system could raise one question for that user. The user ought to answer the question and should keep in mind that account more usage. Then enter the folder name for produce the folder for that user. In file transfer method the user needs to select one file from browsing the system and enter the transfer possibility.

Now, the server from the cloud will provide the encrypted.

4.2 Data Forwarding Module

In forward module first we are able to see the storage details for the uploaded files. once click the storage details possibility we are able to see the file name, question, answer, folder name, forward price (true or false), forward E-mail. If the forward column show the forwarded price is true the user cannot forward to a different person. If the forward column show the forwarded price is fake the user will forward the file into another person. In file forward processes contains the chosen file name,email address of the forwarder and enter the code to the forwarder. Now, another user will check his account properly and think about the code forwarded from the previous user. Then the present user has login to the cloud system and to see the receive details. In receive details the forwarded file is gift then the user can attend the transfer.

4.3 Data Retrieval Module

In transfer module contains the subsequent details. There square measure username and file name. First, the server method are often run which implies the server are often connected with its explicit shopper. Now, the shopper should transfer the file to transfer the file key. In file key downloading method the fields square measure username, filename, question, answer and therefore the code. currently clicking the transfer choice the shopper will read the encrypted key. Then victimisation that key the shopper will read the file and use that file fitly.

5. Test Cases

Test case	Test case name	Test Description	Expected Result	Obtained Result	Result
1	Registration page	Register the owner and user	Owner ans user registration completed	Owner and user registation is success	pass
2	Login page	Owner is entered the user name and password to the login page	Owner is entered valid user name, password	Owner is successful login to login page	pass
3	Login page	Owner is enterded the wrong username and password to login page	Owner is entered not valid user name, password	Owner is not successful login to login page	fail
4	Upload page	Owner is uploades file	File uploaded	File uploadedto cloud server	pass
5	User downloadeing page	User downloading file by using shared key	File downloaded successfully	File downloaded	pass

6. Conclusion

we projected a method for forwarding knowledge firmly in cloud storage system. we tend to divide the information in to blocks and encrypting those blocks and distributing them to every which way chosen storage servers and encryption those cipher blocks for storage. For secure forwarding the information re- secret writing is performed so sent to storage servers. once asked for retrieval key servers perform generation of re-encryption key on demand for partial decipherment. encryption and decipherment operations area unit performed at storage servers and partial decipherment at key servers

REFERENCES

[1] Q. Liu, C. C. Tan, J. Wu, and G. Wang, "Reliable re-encryption in unreliable clouds," IEEE Globecom 2011 proceedings, 2011.

[2] C. Wang, Q. Wang, K. Ren, and W. Lou, "Ensuring data storage security in cloud computing," Proc. 17th Int'l Workshop Quality of Service (IWQoS '09), pp. 1–9, July 2009.

[3] Lidong Zhou ; Schneider, F.B. ; Marsh, M.A.; Redz A. Distributed Blinding for Distributed ElGamal Re-encryption, 25th IEEE International Conference on Distributed Computing Systems, 2005

[4] Giuseppe Ateniese, Kevin Fu, Matthew Green and S. Hohenberger Improved Proxy Re-encryption Schemes with Applications to Secure Distributed Storage, ACM Transactions on Information and System Security, Vol. 9, No. 1, February 2006

[5] M. Jakobsson. On quorum controlled asymmetric proxy re-encryption. In Proceedings of Public Key Cryptography. pp. 112-121

[6] G. Ateniese, R. Burns, R. Curtmola, J. Herring, L. Kissner, Z. Peterson, and D. Song, "Provable data possession at untrusted stores," Proceedings of the 14th ACM conference on Computer and communications security, pp. 598–609, 2007.

[7]D. Chaum. Blind signatures for untraceable payments. In Advances in Cryptology: Proceedings of Crypto'82, pages 199–203, 1983.

[8] T. El Gamal. A public key cryptosystem and a signature scheme based on discrete logarithms, IEEE Transactions on Information Theory, 31:469–472, 1985.

[9] M. Blaze, G. Bleumer, and M. Strauss, "Divertible protocols and atomic proxy cryptography," Advances in Cryptology–EUROCRYPT, 1998.

AUTHORS

Dr. M.V. Siva Prasad was received B.E from Gulbarga University, M.Tech from VTU, Belgaum & awarded Ph.D from Nagarjuna Univeristy, Guntur. Presently Working as a Principal in Anurag Engineering College, Ananthagiri (V), Kodad (M), Nalgonda (Dt.), Andhra Pradesh, India.

P. Sandeep Reddy received Master of Technology (Computer Science & Engineering) from JawaharlalNehru Technological University (JNTUH). My research interests include Information Security, Web Services, Cloud Computing, Data Mining and Mobile Computing. Presently working as Associate Professor in CSE Department in Anurag Engineering College (AEC), Ananthagiri (V), Kodad (M), Nalgonda (Dt.), Andhra Pradesh, India.

M.RAGHAVA Pursuing Master of Technology (Computer Science & Engineering) from Jawaharlal Nehru Technological University (JNTUH). My research interests include Information Security, Web Services, Cloud Computing, Data Mining and Mobile Computing. Presently Pursuing Master of Technology in the department of CSE in Anurag Engineering College (AEC), Ananthagiri (V), Kodad (M), Nalgonda (Dt.), Andhra Pradesh, India.

