IOSR IOSR Journal of Computer Engineering (IOSR-JCE)
e-ISSN: 2278-0661, p- ISSN: 2278-8727Volume 16, Issue 2, Ver. II (Mar-Apr. 2014), PP 53-57
www.iosrjournals.org

Secure Code Based Mostly Information Forwarding System in Cloud Storage

G.Shaik Abdullah
M.E. (CSE), A.V.C College of Engineering, Mayiladuthurai, *Tamilnadu, India.*

Abstract : *Cloud Computing may be a technology that treats the resources on the net as a combined entity, a cloud. This project addresses the matter of forwarding information to a different user by storage servers directly beneath the management of the info owner. With this thought, we tend to propose a completely unique proxy re-encryption theme and integrate it with a secure redistributed code to create a secure distributed wares area structure. The coding set up chains indoctrination operations over encrypted messages and forwarding operations over encrypted and encoded messages. It makes the storage system expeditiously meet the wants of knowledge strength, information confidentiality, and information forwarding. Achieving the mixing considerately of a distributed structure is difficult. Our system meets the wants that storage servers severally perform re- coding and key servers severally perform partial coding. The planned system permits additional versatile adjustment between the quantity of storage servers and strength.*

Keywords: *Cloud computing, Erasure code, Proxy re- coding techniques, Redistributed Storage system.*

I. Introduction

A cloud storage system for strength, confidentiality and practicality. The proxy re-encryption theme supports encryption operations over encrypted messages moreover as forwarding operations over encoded and encrypted messages. to produce information strength is to copy a message specified every Storage server stores a duplicate of the message. it's terribly sturdy as a result of the message may be retrieved as long joined storage server survives. the quantity of failure servers is beneath the tolerance threshold of the erasure code, the message may be recovered from the codeword symbols hold on within the obtainable storage servers by the secret writing method. This provides a exchange between the storage size and also the tolerance threshold of failure servers. A redistributed erasure code is associate degree erasure code that severally computes every codeword image for a message. A redistributed erasure code is appropriate to be used during a distributed storage system. A storage server failure is sculpturesque as associate degree erasure error of the hold on codeword image. we tend to construct a secure cloud storage system that supports the perform of secure information forwarding by employing a threshold proxy re-encryption theme. The coding theme supports redistributed erasure codes over encrypted messages and forwarding operations over encrypted and encoded messages. Our system is extremely distributed wherever storage servers severally cipher and forward messages and key servers severally perform partial coding.

II. Existing System

In our paper describes secure cloud storage with single cloud servers. Constructing a secure storage system that supports multiple functions is difficult once the storage system is distributed and has no central authority. Storing information during a third party's cloud system causes serious concern on information confidentiality. General coding schemes shield information confidentiality, however conjointly limit the practicality of the storage system as a result of few operations are supported over encrypted information. so as to produce robust confidentiality for messages in storage servers, a user will cipher messages by a cryptanalytic technique before applying associate degree erasure code technique to cipher and store messages. once user needs to use a message, user must retrieve the codeword symbols from storage servers, decipher them, and so decipher them by victimization cryptanalytic keys.

A straightforward answer to supporting the info forwarding perform during a distributed storage system is as follows: once the owner A needs to forward a message to user B, user downloads the encrypted message and decrypts it by victimization his secret key and so encrypts the message by victimization B's public key and uploads the new cipher text. Once B needs to retrieve the forwarded message from A, user downloads the cipher text and decrypts it by his secret key. The full information forwarding method desires 3 communication rounds for A's downloading and uploading and B's downloading. The communication price is linear within the length of the forwarded message. The standard cryptanalytic primitives for the aim of knowledge security protection can't be directly adopted because of the users' loss management of knowledge beneath Cloud Computing. The cloud and also the demand of long run continuous assurance of their information safety, the matter of validating correctness of knowledge storage within the cloud becomes even tougher.

III. Planned System

A planned model consists of distributed storage servers, multiple cloud servers and key servers. Since storing cryptanalytic keys during a single device is risky, a user distributes his cryptanalytic key to key servers that shall perform cryptanalytic functions on behalf of the user. These key servers are extremely protected by security mechanism. In planned system Erasure codes are planned in many styles for reducing the storage overhead in every storage server. associate degree erasure code may be a absolutely redistributed encryption method. During this code, the messages are hold on in associate degree encrypted kind. Although the offender compromises all storage servers, offender cannot cypher data concerning the content of the messages. Construct a secure cloud storage system that supports the perform of secure information forwarding by employing a proxy re-encryption theme. A proxy is used within the cloud to remodel encrypted content hold on within the cloud storage to the delivery network or on to the subscribers. During a proxy re-encryption theme, a proxy server will transfer a ciphertext beneath a public key PKA to a brand new one beneath another public key PKB by victimization the re coding key. The server doesn't apprehend the plaintext throughout transformation. In Proxy re-encryption, messages are initial encrypted by the owner and so hold on during a storage server. Once a user needs 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 user. Thus, their system has information confidentiality and supports the info forwarding performs. The user's shopper machine fetches encrypted blocks from the block store. every block includes a deed box encrypted beneath a master public key. The shopper then transmits lockboxes to the access management server for re-encryption beneath the user's public key. If the access management server possesses the mandatory re- coding key, it re-encrypts the deed box and returns the new cipher text. The shopper will then decipher the re-encrypted block with the user's secret key. During this section describe a classification system that uses associate degree untrusted access management server to manage access to encrypted files hold on on distributed, untrusted block stores. Use proxy re-encryption to permit for access management while not granting full coding rights to the access management server. To information, implementation represents the primary experimental implementation and analysis of a system victimization proxy re-encryption.

IV. Planned Formula

In our Paper, Secure Code based mostly information Forwarding System in Cloud Storage describes additional security as a result of victimization RSA. RSA may be a public key cryptanalytic formula.RSA Stands for Rivest, Adi Shamir and author Adleman. This formula was developed at Massachusetts Institute of Technology, printed in 1978.The RSA theme may be a block cipher during which the plaintext and ciphertext are integers between zero and n-1 for a few n. A typical size for n is 1024 bits, or 309 decimal digits. The RSA formula involves 3 steps: key generation, coding and coding.

4.1 Key generation

RSA involves a public key and a non-public key. The general public key may be famed to everybody and is employed for encrypting messages. Messages encrypted with the general public key will solely be decrypted during an affordable quantity of your time victimization the non-public key.

Key Generation	
Select p, q	p, q both prime, $p \neq q$
Calculate $n = p \times q$	
Calculate $\phi(n) = (p-1) \times (q-1)$	
Select integer e	$gcd(\phi(n), e) = 1;\ 1 < e < \phi(n)$
Calculate d	
Public key	$KU = \{e, n\}$
Private key	$KR = \{d, n\}$
Encryption	
Plaintext:	$M < n$
Ciphertext:	$C = M^e \pmod n$
Decryption	
Ciphertext:	C
Plaintext:	$M = C^d \pmod n$

Table 4.1 Key Generation

V. The Planned Framework

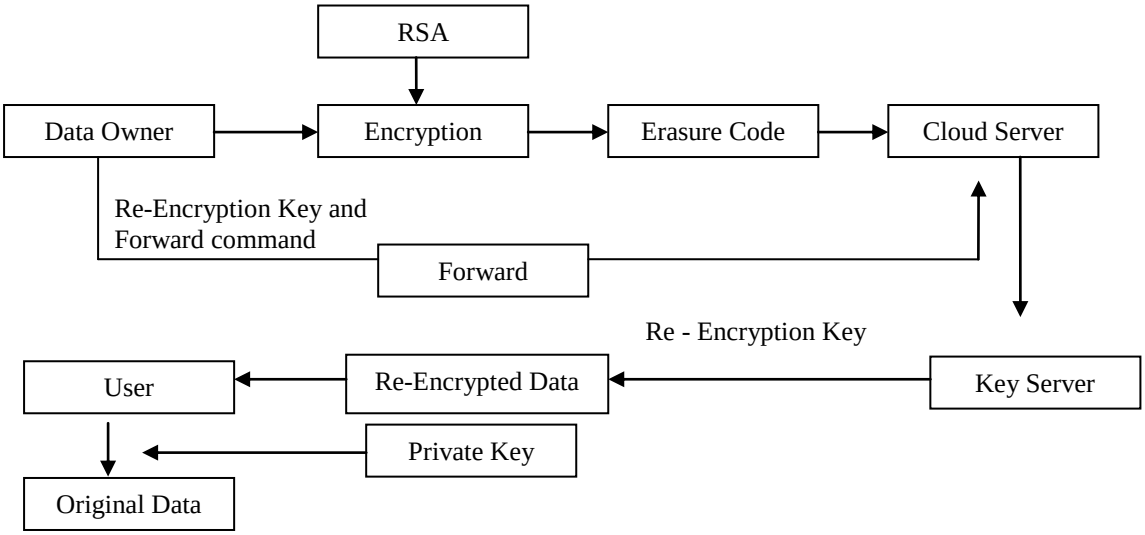

Fig 1: The Planned Framework

VI. Construction Of Cloud Information Storage

In our Admin Module the admin will login to present his username and secret. Then the server setup technique may be opened. In server setup method the admin initial set the remote servers IP-address and Port range. 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. The activated IP-addresses are hold on in obtainable storage server. By clicking the obtainable storage server button we will read the presently obtainable IP-addresses. The admin maintain the Key server, schemes, User Details, transfer Details, and Forward Details.

VII. Cloud Information Concealment

In cloud login module the user will login his own details. If the user will not have the account for that cloud system initial the user can register his details for victimization and getting in the cloud system. once getting into the registration method the main points may be hold on in info of the cloud system. Then the user should login to present his corrected username and secret. Username and secret each are correct. A Home Page, initial show the schemes. The schemes contain Content sort, Duration, price and Size. Then the safety Question, Public Key, non-public Key should be sends his/her E-mail. Then the user can attend open his account and read and consider and think about and look at and examine the Keys which will be generated from the cloud system and conjointly view the safety queries. In transfer Module consists of Folder Name, File Name, Packages, and choose File. Then enter the folder name for produce the folder for that user. In file transfer method the user should select packages, one file from browsing the system and enter the transfer possibility. It clicks transfer, then it'll be show does one need transfer your file, it contains 2 radio buttons. Initial is affirmative and second is not any. You click yes; it'll be asked Enter Your Public Key. Now, the server from the cloud will provide the encrypted type of the uploading file.

VIII. Cloud Information Redirecting

In forward module initial we will see the storage details for the uploaded files. once click the storage details possibility we will see the file name, question, answer, folder name, forward worth (true or false), forward E-mail. If the forward column show the forwarded worth is true the user cannot forward to a different person. If the forward column show the forwarded worth 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 look at the code forwarded from the previous user. Then the present user has login to the cloud system and to envision the receive details. In receive details the forwarded file is gift then the user can attend the transfer method.

IX. Information Informatio Recovery

In the information retrieval section, User sends a retrieval request to key servers. Upon receiving the retrieval request and execution a correct authentication method with user, key server requests storage servers to urge encrypted information and will partial coding on the received encrypted information by victimization the shared secret key. Finally, user decrypts partly decrypted information to get the first message. In transfer module contains the subsequent details. There are username and file name. First, the server method may be run which implies the server may be connected with its specific shopper. Now, the shopper should transfer the file to transfer the file key. In file key downloading method the fields are username, filename, question, answer and also the code. Whenever clicking the transfer possibility the shopper will read the encrypted key. Then victimization that key the shopper will read the file and use that file fittingly.

X. Implementation Results

An implements proxy re-encryption technique and erasure code for information forwarding. It offers low storage and computation price, chance of a no-hit retrieval and Security. A no-hit retrieval is an occasion that a user with success retrieves all k blocks of a message in spite of whether or not the message is closely-held by him or forwarded to him. The randomness comes from the random choice of storage servers within the information storage section, the random coefficients chosen by storage servers, and also the random choice of key servers within the information retrieval section. a knowledge confidentiality of our cloud storage system is secured although storage server, non target users, and up to key servers are compromised by the offender.

XI. Conclusion

In our paper, we tend to propose a good and versatile distributed theme with specific dynamic information support to make sure the correctness of users' information within the cloud. We tend to deem erasure correcting code within the file distribution preparation to produce redundancies and guarantee the info responsibility. we tend to conjointly planned Proxy re-encryption schemes that perform coding operation over the encrypted information. It will considerably decrease communication and computation price of the owner. take into account a cloud storage system consists of storage servers and key servers. Integrate a new planned threshold proxy re-encryption theme and erasure codes over exponents. The brink proxy re-encryption theme supports encryption, forwarding, and partial coding operations during a distributed manner. By victimization the brink proxy re-encryption theme, gift a secure cloud storage system that has secure information storage and secure information forwarding practicality during a redistributed structure. Moreover, every storage server severally performs encryption and re-encryption and every key server severally perform partial coding.

References

[1] Adya, A., Bolosky, W.J., Castro, M., Cermak, G., Chaiken, R.., Douceur, Howell, J.R., Lorch, J.R., Theimer, M., and Wattenhofer, R. (2002). **"Farsite: Federated, available, and reliable storage for an incompletely trusted environment,"** in Proceedings of the 5th Symposium on Operating System Design and Implementation - OSDI, p. 1–14.

[2] Ateniese, G., Benson, K., and Hohenberger, S. (2009) **"Key-private proxy reencryption,"** in Proceedings of Topics in Cryptology - CT-RSA, vol. 5473 of Lecture Notes in Computer Science, p. 279–294.

[3] Ateniese, G., Burns, R., Curtmola, R., Herring, J., Kissner, L., Peterson, Z. and Song, D. (2007) **"Provable data possession at untrusted stores,"** in Proceedings of the 14th ACM Conference on Computer and Communications Security - CCS, p. 598–609.

[4] Ateniese, G., Kamara, S. and Katz, J. (2009) **"Proofs of storage from homomorphic identification protocols,"** in Proceeding of the 15th International Conference on the Theory and Application of Cryptology and Information Security - ASIACRYPT, vol. 5912 of Lecture Notes in Computer Science, p. 319–333.

[5] Ateniese, G., Pietro, R.D., Mancini, L.V. and Tsudik, G. (2008) **"Scalable and efficient provable data possession,"** in Proceedings of the 4th International Conference on Security and Privacy in Communication Netowrks - SecureComm, p. 1–10.

[6] Ateniese, G., Fu, K., Green, M. and Hohenberger, S. (2006) **"Improved proxy re-encryption schemes with applications to secure distributed storage,"** ACM Transactions on Information and System Security, vol. 9, no. 1, p. 1–30.

[7] Bhagwan, R., Tati, K., Cheng, Y.C., Savage, S. and Voelker, G.M. (2004) **"Total recall: System support for automated availability management,"** in Proceedings of the 1st Symposium on Networked Systems Design and Implementation - NSDI, p. 337–350.

[8] Blaze, M., Bleumer, G.and Strauss, M. (1998) **"Divertible protocols and atomic proxy cryptography,"** in Proceedings of the International Conference on the Theory and Application of Cryptographic Techniques - EUROCRYPT, vol. 1403 of Lecture Notes in Computer Science, p. 127–144.

[9] Bowers, K.D., Juels, A. and Oprea, A. (2009) **"Hail: a high-availability and integrity layer for cloud storage,"** in Proceedings of the 16th ACM Conference on Computer and Communications Security - CCS, p. 187– 198.

[10] Brownbridge, D.R., Marshall, L.F., and Randell, B. (1982) **"TheNewcastle connection or unixes of the world unite!,"** Software Practice and Experience, vol. 12, no. 12, p. 1147–1162.

[11] Dimakis, A.G., Prabhakaran, V. and Ramchandran, K. (2006) **"Decentralized erasure codes for distributed networked storage,"** IEEE Transactions on Information Theory, vol. 14, p.2809–2816.

[12] Druschel, P. and Rowstron, A. (2001) **"PAST: A large-scale,persistent peer-topeer storage utility,"** in Proceedings of the 8th Workshop on Hot Topics in Operating System - HotOS VIII, p. 75–80.

[13] Haeberlen, A., Mislove, A. and Druschel, P. (2005) **"Glacier: Highly durable, decentralized storage despite massive correlated failures,"** in Proceedings of the 2nd Symposium on Networked Systems Design and Implementation - NSDI, p. 143–158.

[14] Kallahalla, M., Riedel, E., Swaminathan, R.,Wang, Q. and Fu, K. (2003) **"Plutus: Scalable secure file sharing on untrusted storage,"** in Proceedings of the 2nd USENIX Conference on File and Storage Technologies - FAST, p. 29–42.

[15] Wang, C., Wang, Q., Ren, K. and Lou, W. (2010) **"Privacy-preservingpublic auditing for data storage security in cloud computing,"** in Proceedings of the 29th IEEE International Conference on Computer Communications- INFOCOM, p. 525–533.

Authors Profile

G.Shaik Abdullah received the B.Tech Degree Information Technology and now he is an M.E student in the Department of Computer Science & Engineering, A.V.C College of Engineering – Mayiladuthurai, TN, India.

His research interest includes Cloud Computing and Network Security.