IJDCST @November Issue- V-1, I-7, SW-21
ISSN-2320-7884 (Online)
ISSN-2321-0257 (Print)

Implementation of Secure Cloud Storage Systems with Erasure Code

[1]Suresh Boppana, [2]Nageswara Rao Pambala, [3]Suresh Suravarapu

[1]M. Tech (CNIS) Sri Rama Institute of Technology &Sciences, (Affiliated To JNTU Hyderabad),Kuppenakuntla, Khammam, Andhra Pradesh, India.

[2]Assistant Professor Dept. of Computer Science and Engineering, Sri Rama Institute of Technology &Sciences, (Affiliated To JNTU Hyderabad) Kuppenakuntla, Khammam, Andhra Pradesh, India.

[3]Associate Professor Dept. of Computer Science and Engineering, Sri Rama Institute of Technology &Sciences, (Affiliated To JNTU Hyderabad) Kuppenakuntla, Khammam, Andhra Pradesh, India.

Abstract—Cloud storage may be a model of networked on-line storage wherever information is keep in virtualized pools of storage that are usually hosted by third parties. Organizations cite information confidentiality as their serious concern for cloud computing, with encrypted information keep on third party's cloud system, the practicality of the storage system is proscribed once general cryptography schemes are used for information confidentiality. With this thought, we tend to propose a replacement threshold proxy re-encryption theme to create a secure distributed storage system. This distributed storage system additionally lets a user forward his information within the storage servers to a different user while not retrieving the information back The distributed storage system not solely supports secure and strong data storage and retrieval, however additionally lets a user forward his information within the storage servers to a different user while not retrieving the data back. The most feature contribution is that the proxy re-encryption theme supports encryption operations over encrypted messages in addition as forwarding operations over encoded and encrypted messages.

Index Terms—Shared storage system, encrypting, proxy re-encryption, encrypted information.

I INTRODUCTION

CLOUD computing could be a conception that treats the resources on the web as a unified entity, a cloud. Users simply use services while not worrying regarding however computation is completed and storage is managed. With cloud computing growing in quality, tools and technologies area unit rising to create, access, manage, and maintain the clouds. Cloud computing offers several edges, however it is also prone to threats. Because the uses of cloud computing increase, it's extremely doubtless that a lot of criminals can attempt to realize new ways that to use vulnerabilities within the system. to assist mitigate the threat, cloud computing stakeholders ought to invest heavily in risk assessment to confirm that the system encrypts to shield data; establishes sure foundation to secure the platform and infrastructure; and builds higher assurance into auditing to strengthen compliance. During this paper, we tend to specialize in coming up with a cloud storage system for hardiness, confidentiality, and practicality. There area unit several underlying challenges and risks in cloud computing that increase the threat of information being compromised. Security considerations should be self-addressed so as to determine trust in cloud computing technology. Distributed networked storage systems offer the storage service on the web. We tend to address the privacy issue of the distributed networked storage system. Even though all storage servers within the system area unit compromised.

The major challenge of coming up with these distributed networked storage systems is to supply a stronger privacy guarantee whereas maintaining the distributed structure. to attain this goal, we have a tendency to introduce secure suburbanized erasure code, which mixes a threshold public key cryptography theme and a variant of the suburbanized erasure code. Our secure distributed networked storage system created by the secure suburbanized erasure code is suburbanized and strong [4]. Cloud computing is encircled by several security problems like securing knowledge, and examining the use of cloud by the cloud computing vendors. Initial registration with a cloud computing service may be a pretty easy method. With shared infrastructure resources, organizations ought to worry concerning the service provider's authentication systems that grant access to knowledge. once the registration method every user are going to be given a secret key that is generated by him. The user will store, forward and retrieve

knowledge within the cloud solely once the key generation. Within the existing system, if the user loses his key, he is going to be directly blocked from the system. This could end in interference several users. thus we have a tendency to introduce a system wherever the user are going to be given 2 possibilities. so only the user loses his secret key for 2 times, he are going to be blocked from the system. Attributable to the large quantity of knowledge keep by a cloud, economical process and analysis of knowledge has become a difficult one. One way to provide data robustness is to replicate a message such that each storage server stores a copy of the message. Encoding a message of k symbols into a code word of n symbols by erasure coding is another way to provide data robustness. Each code word symbols is stored in a different storage server to store a message.

One way to produce information strength is to copy a message specified every storage server stores a replica of the message. Cryptography a message of k symbols into a code word of n symbols by erasure cryptography is in our own way to produce information strength. Every code word symbols is kept in a very totally different storage server to store a message.

A suburbanized erasure code is associate degree erasure code that severally computes every code word image for a message. Thus, the cryptography method for a message will be split into n parallel tasks of generating code word symbols [1]. Suburbanized storage systems combination the accessible space of taking part computers to produce an oversized storage facility [2].These systems trust information redundancy to confirm study storage despite of node failures. Once the message symbols square measure 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. Information confidentiality is affected once information is kept in third party's cloud. A user will code messages by a scientific discipline technique before applying associate degree erasure code technique to write and store messages so as to produce sturdy confidentiality for messages in storage servers. Erasure cryptography and reduces the storage price [3]. He must retrieve the code word symbols from storage servers, decipher them, and so decipher them by victimization scientific discipline keys once he desires to use a message. There are three problems in the above straightforward integration of encryption and encoding. First, the user has to do most computation and the communication traffic between the user and storage servers is high. Second, the user has to manage his cryptographic keys. If the user's device of storing the keys is lost or compromised, the security is broken. Finally, besides data storing and retrieving, it is hard for storage servers to directly support other functions. For example, storage servers cannot directly forward a user's messages to another one. The owner of messages has to retrieve, decode, decrypt and then forward them to another user. 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.

There are a unit 3 issues within the higher than simple integration of encoding and secret writing. First, the user must do most computation and therefore the communication traffic between the user and storage servers is high. Second, the user must manage his scientific discipline keys. If the user's device of storing the keys is lost or compromised, the safety is broken. Finally, besides information storing and retrieving, it's arduous for storage servers to directly support alternative functions. For instance, storage servers cannot directly forward a user's messages to a different one. The owner of messages must retrieve, decode, rewrite and so forward them to a different user. Since storing scientific discipline keys in an exceedingly single device is risky, a user distributes his scientific discipline key to key servers that shall perform scientific discipline functions on behalf of the user. These key servers area unit extremely protected by security mechanisms.

To well work the distributed structure of systems, we have a tendency to need that servers severally perform all operations. With this thought, we have a tendency to propose a brand new threshold proxy re-encryption theme and integrate it with a secure decentralized code to make a secure distributed storage system. The encoding theme supports secret writing operations over encrypted messages and forwarding operations over encrypted and encoded messages [1]. The tight integration of secret writing, encryption, and forwarding makes the storage system with efficiency meet the necessities of information hardiness, information confidentiality, and information forwarding. Accomplishing the combination considerately of a distributed structure is difficult. Our system meets the necessities that storage servers severally perform secret writing and re-encryption and key servers severally perform partial cryptography. Moreover, we have a tendency to contemplate the system in an exceedingly additional general setting than previous works. This setting permits additional versatile adjustment between the quantity of storage servers and hardiness.

II. EXISTING SYSTEM

Storing information in an exceedingly third party's cloud system causes serious concern on information confidentiality. so as to produce sturdy

confidentiality for messages in storage servers, a user will write in code messages by a cryptologic methodology before applying An erasure code methodology to cypher and store messages. Once he desires to use a message, he must retrieve the code word symbols from storage servers, rewrite them, and then decipher them by exploitation cryptologic keys.

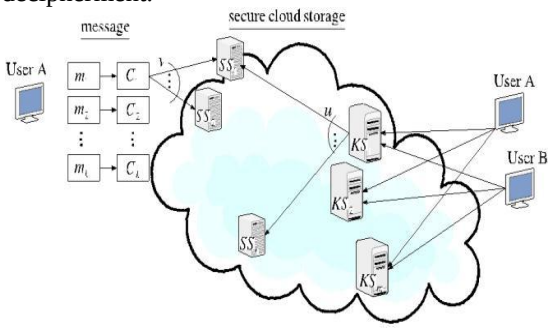
2.1 Limitations of Existing System

There square measure 3 issues within the higher than easy integration of coding and encryption.
1. The user should do most computation and also the communication traffic between the user and storage servers is high.
2. The user should manage his cryptanalytic keys. If the user's device of storing the keys is lost or compromised, the protection is broken.
3. Finally, besides information storing and retrieving, it's arduous for storage servers to directly support alternative functions

III. PROPOSED SYSTEM

In this paper, we have a tendency to address the matter of forwarding knowledge to a different user by storage servers directly beneath the command of the info owner. we have a tendency to think about the system model that consists of distributed storage servers and key servers. Since storing crypto graphical keys during a single device is risky, a user distributes his crypto graphical key to key servers that shall perform crypto graphical functions on behalf of the user. These key servers are extremely protected by security mechanisms.

To well work the distributed structure of systems, we have a tendency to need that servers severally perform all operations. With this thought, we have a tendency to propose a replacement threshold proxy re-encryption theme and integrate it with a secure redistributed code to make a secure distributed storage system. The cryptography theme supports encryption operations over encrypted messages and forwarding operations over encrypted and encoded messages. The tight integration of encryption, encryption, and forwarding makes the storage system expeditiously meet the wants of information hardiness, knowledge confidentiality, and knowledge forwarding. Accomplishing the combination considerately of a distributed structure is difficult. Our system meets the wants that storage servers severally perform encryption and re-encryption and key servers severally perform partial decipherment.



Once the system has been designed, consequent step is to convert the designed one in to actual code, therefore on satisfy the user needs as excepted. If the system is approved to be error free it are often enforced. once the initial style was in serious trouble the system, the department was consulted for acceptance of the look so additional proceedings of the system development are often carried on. once the event of the system, an illustration was given to them regarding operating of the system. The aim of the system illustration was to spot any amiss of the system. Implementation includes correct coaching to end-users. The enforced package ought to be maintained for prolonged running of the package. at first the system was run parallel with manual system. The system has been tested with knowledge and has tried to be error-free and easy. Coaching was given to finish -user regarding the package and its options.

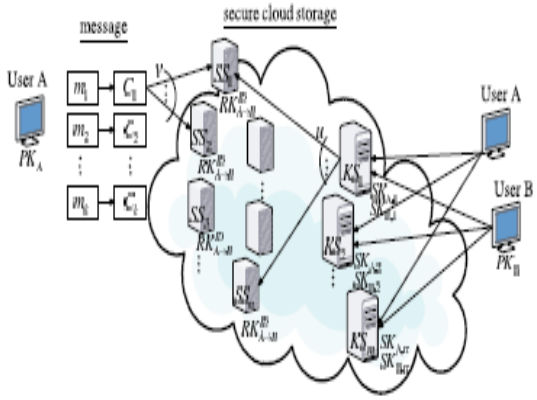
The coding theme supports encryption operations over encrypted messages and forwarding operations over encrypted and encoded messages. The tight integration of encryption, encryption, and forwarding makes the storage system with efficiency meet the necessities of information lustiness, knowledge confidentiality, and knowledge forwarding. The knowledge is been encrypted exploitation cryptologic keys to produce data confidentiality. Authenticating the users coming into the network can even be done to secure the info. The cryptologic keys should be unbroken secret and it should not be lost by the user. they need to be allowed to enter the system solely once registration method or login method.

The following steps are followed in our system:

1. User creates associate account.
2. His data are hold on in storage server and a key are given.
3. The genuine user will transfer files.
4. He may also forward and retrieve files. The user may also forward information to alternative user by sharing the id of the info and id of the user to the storage server. It forwards the info to the opposite user. This reduces the computation done by the user

IV. SYSTEM IMPLEMENTATION

When a user desires to share his messages, he sends a re-encryption key to the storage server. The storage server re-encrypts the messages for the licensed user supporting the information forwarding operates. Our work any integrates re-encryption, and encryption specified storage strength is reinforced.



A. System Setup

The established method generates the system parameters. A user uses KeyGen to get his secret key try to share his secret key to a collection of m key servers with a threshold t. The user regionally stores the third element of his secret key. The server generates secret key and sends to the user.

B. Checking Integrity

When the users request to access the info, he should verify himself with the key sent to him by server. Once the verification user will access his account. The key are going to be sent to the users various mail id.

C. Data Encryption and Storage

After accessing the account, user will able to transfer the info within the style of files. Once the user uploads the file it'll be encrypted by the server and keep in to the info within the illegible format. I.e. the enter the server is keep are going to be keep within the encrypted format solely. The first files are going to be erased because it is encrypted.

D. *Data Forwarding*

User A desires to forward a message to a different user B. He doesn't take the chance of forwarding the information himself. He simply offers information id to data server and also the of the user to whom he desires to send the message to the key server. And also the knowledge is send to the user by the information and key server. This reduces the computation performed by the user.

E. *Data Retrieval*

There are 2 cases for the info retrieval section. the primary case is that a user A retrieves his own message. User A informs all key servers with the identity token once he needs to retrieve the message. Original code word symbols are retrieved by the key server and partial secret writing is performed on them. The ensuing code word is named partly decrypted code word image. These symbols and coefficients are sent to user A by the key server. once user A collects replies from a minimum of t key servers and a minimum of k of them, he executes on the t partly decrypted code word symbols to recover the blocks m1; m2; . . .; mk. The second case is that a user B retrieves a message forwarded to him. User B informs all key servers directly. Here the key servers retrieve re-encrypted code word symbols and perform partial secret writing.

V. DISCUSSIONS AND CONCLUSION

In this paper, we tend to take into account a cloud storage system consists of storage servers and key servers. We tend to integrate a recently planned threshold proxy re-encryption theme. The brink proxy re-encryption theme supports coding, forwarding, and partial cryptography operations during a distributed means. To decipher a message of k blocks that area unit encrypted and encoded to n code word symbols, every key server solely needs to part decipher 2 code word symbols in our system. By victimization the brink proxy re-encryption theme, we tend to gift a secure cloud storage system that gives secure information storage and secure information forwarding practicality during a suburbanized structure. Moreover, every storage server severally performs coding and re-encryption and every key server severally perform partial cryptography. Our storage system and a few recently planned content available file systems and storage system [7], [8], [9] area unit extremely compatible. Our storage servers act as storage nodes during a content available storage system for storing content available blocks. Our key servers act as access nodes for providing a front-end layer like a conventional classification system interface. Additional study on careful cooperation is needed.

VI. FUTURE WORK

Thus by employing a secure cloud system was setup and therefore the users were able to store their information. Future work is to freshly propose a additional secured system within which solely

approved users will access all the info within the cloud. If the users access information while not permission they need to be blocked from the network. A threshold proxy re-encryption theme may be projected that supports coding, forwarding, etc. information forwarding methodology is additional secured victimization cryptologic keys.

REFERENCES

[1] 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.

[2] 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.

[3] 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.

[4] 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.

[5] Z. Wilcox-O'Hearn and B. Warner, "Tahoe: The Least-Authority Filesystem," Proc. Fourth ACM Int'l Workshop Storage Security and Survivability (StorageSS), pp. 21-26, 2008.

[6] 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.

[7] A. Shamir, "How to Share a Secret," ACM Comm., vol. 22, pp. 612- 613, 1979.

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

[9] 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 Storage Technologies (FAST), p. 17, 2010.

[10] W. Dong, F. Douglis, K. Li, H. Patterson, S. Reddy, and P. Shilane, "Tradeoffs in Scalable Data Routing for Deduplication Clusters," Proc. Ninth USENIX Conf. File and Storage Technologies (FAST), p. 2, 2011.

[11] 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.

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

[14] A.G. Dimakis, V. Prabhakaran, and K. Ramchandran, "Decentralized Erasure Codes for Distributed Networked Storage," IEEE Trans. Information Theory, vol. 52, no. 6 pp. 2809-2816, June 2006.

[15] M. Mambo and E. Okamoto, "Proxy Cryptosystems: Delegation of the Power to Decrypt Ciphertexts," IEICE Trans. Fundamentals of Electronics, Comm. and Computer Sciences, vol. E80-A, no. 1, pp. 54- 63, 1997.

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

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

[18] Q. Tang, "Type-Based Proxy Re-Encryption and Its Construction," Proc. Ninth Int'l Conf. Cryptology in India: Progress in Cryptology (INDOCRYPT), pp. 130-144, 2008.

[19] G. Ateniese, K. Benson, and S. Hohenberger, "Key-Private Proxy Re-Encryption," Proc. Topics in Cryptology (CT-RSA), pp. 279-294, 2009.

[20] J. Shao and Z. Cao, "CCA-Secure Proxy Re-Encryption without Pairings," Proc. 12th Int'l Conf. Practice and Theory in Public Key Cryptography (PKC), pp. 357-376, 2009.

AUTHOR

SureshBoppana pursuing M.Tech II-year in Computer Science and Engineering from Sri Rama Institute of Technology and Sciences Engineering College during 2011-2013.

Nageswara Rao Pambala received His M.Tech Degree from JNTUH. He is currently working as an Asst Professor in the Dept of Computer Science Engineering in Sri Rama Institute of Technology &Sciences, (Affiliated to JNTU Hyderabad) Kuppenakuntla, Khammam, Andhra Pradesh, India. His interests are Sofware Engineering, Data Mining.

Suresh Suravarapu received His M.Tech Degree from JNTUK. He is currently working as an Associate Professor in the Dept of Computer Science Engineering in Sri Rama Institute of Technology &Sciences, (Affiliated to JNTU Hyderabad) Kuppenakuntla, Khammam, Andhra Pradesh, India. His interests are Cloud Computing, Data Mining.