International Journal of Innovative Research in Engineering Science and Technology

APRIL 2018 ISSN 2320 –981X

A SECURE ERASURE CODE AND DATA FORWARDING IN CLOUD STORAGE SYSTEM

[1]Kumutha S, [2]Nathiya N,[3]Tamilpriya T, [4]Tharani G

[1]Assistant professor, Dept. of Computer Science and Engineering,
Paavai College of Engineering,
Namakkal – 637018, India,
kumuthaspk@gmail.com

[2]Assistant professor, Dept. of Computer Science and Engineering,
Paavai College of Engineering,
Namakkal – 637018, India,
nathiiraj@gmail.com

[3]UG Student, Dept. of Computer Science and Engineering,
Paavai College of Engineering,
Namakkal – 637018, India,
Tamilpriya7470@gmail.com

[4] UGStudent, Dept. of Computer Science and Engineering,
Paavai College of Engineering,
Namakkal – 637018, India,
tharanigogulan7@gmail.com

Corresponding Author

e.mail: kumuthaspk@gmail.com

Contact: +91 8526637756

Abstract

In order to cater the increasing demands of the user, the scope of the internet is growing exponentially. With the expanding growth, the challenges of storage of data have also increased considerably. The important factor in storing voluminous data is to sustain the integrity of the data. Providing security for the enormous data is a herculean task. It is a task because losing or misplace of a small data in a cloud is actually is massive. In order to address this issue various techniques for providing secure storage in cloud, The whole data is stored in a single place which let the intruder hack the data easily. The asymmetric keys are used which creates a lapse in the security. The data which is stored in so this paper introduces a new technique called "A secure erasure code-based cloud storage system with secured data forwarding". Which would help the user in splitting the data and storing thus the user will retain the data with the symmetric key provided by the end users. The data is split into four servers and these files are inaccessible until we enter the symmetric key. The data stored is digested and this enhances data confidentiality.

Key words:

Cloud Storage,

Decentralized erasure code,

Security Scheme,

Proxy re-encryption,

Servers,

Secure storage system

Introduction

Cloud computing took its basics idea from distributed computing the cloud computing technology was hugely welcome because it allowed sharing of resources to a greater extends it offer facilitated dynamic demand management and went forward and freed company from infrastructure cloud computing provide remote services at various level like software, network, platform, infrastructure other advantages of cloud computing include lesser running cost lower infrastructure investment better scalability and agility and excellent peak demand utilization or management. The cloud storage can be categorized based on their authentication schemes. They are classified in four group namely public cloud, private cloud, community cloud and hybrid cloud. In public cloud the vendor premises hosts the computing infrastructure. The customer has zero visibility on the location of the infrastructure. The organization shares the computing infrastructure. In private cloud the customer has the computing infrastructure with itself and does not share it with other organizations [1]. It is more secure and highly expensive than public clouds. It can be either externally hosted or in premises hosted clouds. Hybrid cloud is one of the type and it is a grouping of public cloud and private cloud. The critical, sensitive, fragile and secure applications are put in the private cloud whereas the less critical data is stored in public cloud. The organization can categorize the data and can store either in private or public cloud. In community cloud, various organizations of the same community will share the cloud services.

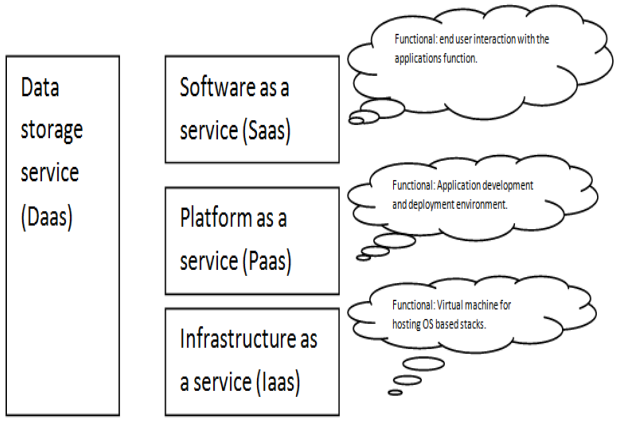

Fig 1.Types of Cloud Services.

The Cloud mainly provides four services, namely, software as a service which is a on demand service which is hosted centrally and can be accessed with the help of web browser over internet and it is free of cost and it is a multi-tenant architecture. (eg: google apps, ms office) platform as a service provides a computing platform over the internet. It works on creating a web application with ease. It also works on the user's demand. It allows various customization techniques over the web application (eg: google app engine) , System infrastructure as a service as they provide infrastructure over the premises. It works on the changing requirements. It provides strong data security. Amazon EC2 is one such example which provides a interface for the user to create and host application online. They are flexible and secure. Google app engine also provides a interface to create a web application. It offers dynamic web serving and provides full backend for common web technologies. TNetwork as a service (bandwidth on demand, bpn) and infrastructure as a service (eg: google compute engine, HP cloud). Data centers are collections of servers which are at different places but act as they are working together. The cloud security was first provided by McAffe. They provided Email protection, end point protection, vulnerability protection and web protection. The cloud security overall can be split into 3 types namely confidentiality, integrity and availability. Some cloud computing system provides backup of data in multiple region.

The cloud documents are intruded by unauthorized third party users. The encapsulated change management and the choice and agility remains the pros of the

cloud computing. There is some cons in cloud security and there is lack of control the user will not be able to retrieve the data once the data is lost in cloud. The data is online and the data is stored as a single entity which the hacker will access if he hacks the single server. The owner of the cloud can access the data at time which again creates a problem to the cloud user. The data security is taken in concern and this area needs to be improvised. In order to enhance the cloud security we provide a new technique "A secure erasure code-based cloud storage system with secured data forwarding" which splits the files and stores the uploaded data in different servers and the message stored is digested and the data that is split cannot be retrieved individually. This technique will ensure that the data confidentiality is enhanced.

This paper is organized as follows. The second section describes about the related works done for the security in cloud computing. The third section describes the existing system, the disadvantages and the proposed technique to enhance the security in cloud computing. Fourth section details the results and the performance evaluation. The fifth section consist of the conclusion and the possible future work for effective security techniques in cloud computing.

Related Work

Distributed file system like Hadoop is required by cloud computing technology to have its benefits. There were many file systems used in the history of computing. They are Network Attached Storage , Network File System [2] and so on. These file systems are decentralized, scalable and distributed in nature. Techniques like replica management, virtual machines, virtualization are widely used along with these file systems. File systems with features like efficiency and scalability are explored in and [3]. For security reasons erasure codes are used and in distributed and complex environments. These techniques are used to convert the given text into a

format that cannot be understood. Each erasure code is like a vector of symbols which can represent storage problems in outsourced data.

The vectors are then used to achieve consistency as the erasure codes are capable of doing so. There is huge communication cost associated with the data outsourcing. Data confidentiality is another problem in such environments. **Lin and Tzeng** [4] proposed this main problem using erasure codes. That schemes support public key encryption, for supporting data forwarding securely. As per the techniques users can provide re-encryption keys to server and then enables server to share data. The storage server re-encrypts the data which has been encrypted already. Tzeng presented a time based proxy re-encryption scheme. This key has more utility when compared with other keys related to security. Another such scheme proposed by **M. Blaze, G. Bleumer** is key – private proxy re-encryption[5] . In the schemes described above, a concept is missing it is known as "pairing". For integrity verification many schemes came into existence where focus was on data store, retrieval and forwarding in secure fashion. Anyway, Lin et al. focused on the cloud storage security with respect to data storage retrieval and forwarding. This paper improves their scheme by implementing a timestamp based mechanism that ensures perfect cooperation among the servers. Thus the problem of communication inconsistencies among the servers is addressed. Key-private proxy re-encryption schemes are proposed by **S. Kleiman et al**. In a key-private intermediary re-encryption conspire, given a re-encryption key, an intermediary server can't decide the character of the beneficiary. Albeit most intermediary re-encryption plans utilize blending activities, there exist intermediary re-encryption plans without pairing.[6]

Dimakis et al. actualized some intermediary re-encryption conspires and connected them to the sharing capacity of secure stockpiling frameworks. In their work, messages are first scrambled by the proprietor and after that put away in a capacity server. At the point when a client needs to share his messages, he sends a re-encryption key to the capacity server. The capacity server re-encodes the scrambled messages for the approved client. In this way, their framework has information classification and backings the information sending function.[7]

The work additionally incorporates encryption, re-encryption, and encoding with the end goal that capacity heartiness is fortified. Sort based intermediary re-encryption plans proposed by M. Kallahalla et al give a superior granularity on the allowed right of a re-encryption key. A client can choose which sort of messages and with whom he needs to partake in this sort of intermediary re-encryption plans. [8].

Existing System

In Existing System we utilize a direct incorporation strategy. In clear incorporation strategy Storing information in an outsider's cloud framework causes genuine worry on information secrecy. With a specific end goal to give solid classification to messages away servers, a client can scramble messages by a cryptographic strategy before applying an eradication code technique to encode and store messages. When he needs to utilize a message, he needs to recover the General encryption plans ensure information secrecy, additionally confine the usefulness of the capacity framework on the grounds that a couple of operations are bolstered over scrambled information. A decentralized engineering for capacity frameworks offers great adaptability, in light of the fact that a capacity server can join or leave without control of a focal specialist.

DISADVANTAGE OF EXISTING SYSTEM

- The client can perform more calculation and correspondence movement between the client and capacity servers is high.
- The client needs to deal with his cryptographic keys generally the security must be broken.
- The information putting away and recovering, it is hard for capacity servers to straightforwardly bolster different capacities.
- The client can't share the information secrecy to the goal.

Proposed system

In our proposed framework the issue of sending information to another client by capacity servers specifically works under the order of the information proprietor. The authoritative application is information sharing. People in general evaluating property is particularly helpful when we anticipate that the assignment will be effective and adaptable. The plans empower a substance supplier to share her information in a secret and particular path, with a settled and little figure content extension, by appropriating to each approved client a solitary and little total key. We consider the framework demonstrate that comprises of appropriated stockpiling servers and key servers. These key servers are very ensured by security systems. The disseminated frameworks require free servers to play out all operations.

In an intermediary re-encryption conspire; an intermediary server can exchange a figure message under an open key to another one under another open key by utilizing the re-encryption key. We propose another edge intermediary re-encryption conspire that are crypto frameworks which permit outsiders (intermediaries) to change a figure content which has been scrambled for one client, with the goal that it might be decoded by another client. By utilizing intermediary re-encryption method the encoded information (figure content) in the cloud is again changed by the client. It gives exceptionally secured data put away in the cloud. Each client will have an open key and private key. Open key of each client is known to everybody except private key is known just the specific client and coordinate it with a safe decentralized code to frame a protected dispersed stockpiling framework. The encryption conspire bolsters encoding operations over scrambled messages and sending operations over scrambled and encoded messages.

Proposed Algorithm

Cipher keys are processed to get the round keys using Rijndael's key schedule and this process is known as key expansion. The occurrence of subsequent process is explained below. Fig 2 Tells about the flowchart of the AES Algorithm.

Step 1- Initial Round

AddRoundKey is carried out in which every single byte of the state is mingled with the round key with bitwise XOR.

Step 2- Intermediate process

i)An unaligned substitution step called as Sub-byte, in which all the bytes are replaced with something else in correspondence to lookups.

ii)Shift Rows are done in which a interdependent step is carried out where all the rows of the state is turn cyclically as a certain number of steps

.iii)MixColumns which is a blending operation where the columns of the state are blended into four bytes in each column is done.

iv)TheAddRoundKey is carried out again in which the sub key is merged with the state and in every round the main key derives the subkey.

Step 3- Final Round

The process sub-byte, Shift Rows, Mix columns are repeated in a cycle.

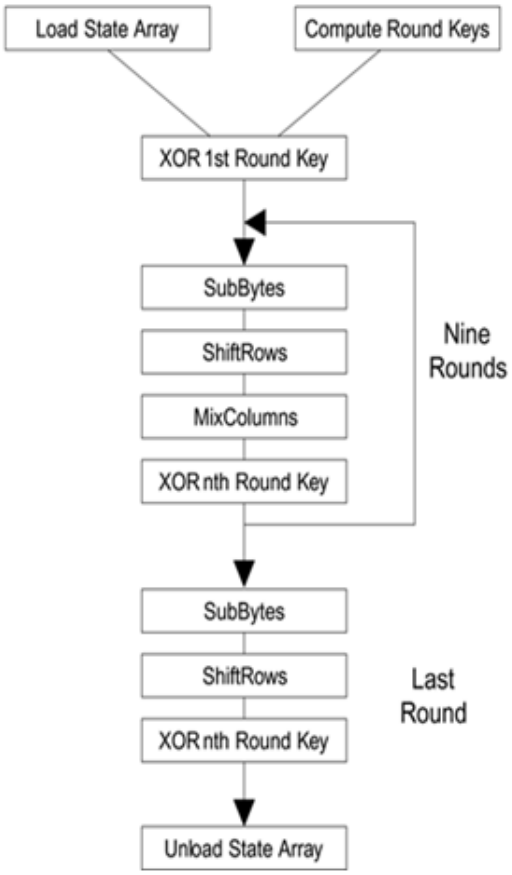

Fig 2 Flowchart describing the AES Algorithm.

Expressed in ***Fig 3***, Storage servers give stockpiling administrations and key servers give key administration administrations. They work autonomously. Our proposed framework comprises of five stages: Registration, Sharing Data, Secure Cloud Storage, Proxy re-encryption, Data recovery. For the enlistment of client with character ID the gathering supervisor arbitrarily chooses a number. At that point the gathering administrator includes into the gathering client list which will be utilized as a part of the traceability stage. After the enlistment, client gets a private key which will be utilized for gathering mark era and record decoding. Information strength is a noteworthy necessity for capacity frameworks. There have been numerous proposition of putting away information over capacity servers. One approach to give information vigor is to imitate a message with the end goal that every capacity server stores a duplicate of the message. A decentralized deletion code is reasonable for use in a disseminated stockpiling

framework. Reports and information are the two essential types of the recovered information from servers. There are a few covers between them, yet questions by and large select a moderately little segment of the server, then again reports indicate bigger measures of information. Inquiries likewise show the information in a standard organization and more often than not show it on the screen; though reports permit arranging of the yield anyway you like and is regularly recovered.

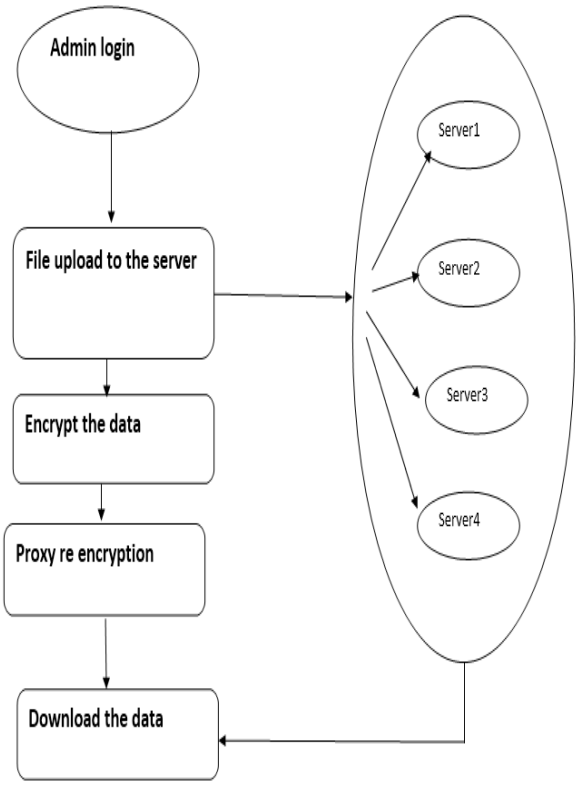

Fig 3 Overview of System Architecture

Conclusion

In In this paper considering a distributed storage framework, which comprises of capacity servers and key servers, A recently coordinated proposed edge intermediary re-encryption plan and deletion codes over examples. The limit intermediary Re-encryption conspire underpins encoding, sending, and incomplete decoding operations distributed. To unscramble a message of k obstructs that are scrambled and encoded to n codeword images, each key server just needs to incompletely decode two codeword images in our framework. By utilizing the limit intermediary re-encryption plot, we display a safe

distributed storage framework that gives secure information stockpiling and secure information sending usefulness in a decentralized structure. In addition, every capacity server freely performs encoding and re-encryption and each key server autonomously performs fractional decoding. Our capacity framework and some recently proposed content addressable record frameworks and capacity are very good. Our capacity servers go about as capacity hubs in a substance addressable capacity framework for putting away substance addressable pieces. Our key servers go about as get to hubs for giving a front-end layer, for example, a customary document framework interface. Additionally ponder on nitty gritty participation is required.

References

[1.] **J. Kubiatowicz, D. Bindel, Y. Chen, P. Eaton, D. Geels,(2000)** An Architecture for Global-Scale Persistent Storage," Proc. *Ninth Int'l Conf. Architectural Support for Programming Languages and Operating Systems (ASPLOS), pp. 190-201*.

[2.] **P. Druschel and A. Rowstron(2001),** "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(2002)**, "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.] **Haeberlen, A. Mislove,Lin and Tzeng and P. Druschel[2005]**, "Glacier: Highly Durable, Decentralized Storage Despite Massive Corr elated Failures," Proc. Second Symp.Networked Systems Design and Implementation (NSDI), pp. 143-158, 2005.

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

[6.] **H.-Y. Lin, Dimakis et al and W.-G.Tzeng[2010],** "A Secure Decentralized Erasure Code for Distributed Network Storage," *IEEE Trans. Parallel and Distributed Systems*, vol. 21, no. 11, pp. 1586-1594.

[7] **S.C. Rhea, P.R. Eaton, D. Geels, H. Weatherspoon, B.Y. Zhao, and J. Kubiatowicz[2003]**, "Pond: The Oceanstore Prototype," *Proc. Second USENIX Conf. File and Storage Technologies (FAST),* pp. 1-14.

[8] **R. Bhagwan, K. Tati, Y.-C. Cheng, S. Savage, and G.M. Voelker[2004],** "Total Recall: System Support for Automated Availability Management," Proc. *First Symp. Networked Systems Design and Implementation (NSDI)*, pp. 337-350.

[9] **A.G. Dimakis, V. Prabhakaran, and K. Ramchandran[2005],** "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.

[15] **M. Mambo and E. Okamoto[1997],** "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.

[16]**Thillaiarasu, N. and ChenthurPandian, S.,** 2017. A novel scheme fo safeguading confidentiality in public clouds fo sevice uses of cloud computing. Cluster Computing, pp.1-10.

[17]**Saravanan, T.** "An Efficient Multi Channel Query Scheduling In Wireless Sensor Networks." International Journal of Computer Science and Network Security (IJCSNS) 14.2 (2014): 71.

[18]**Shyamambika, N. and Thillaiarasu, N.,** 2016, January. A survey on acquiring integrity of shared data with effective user termination in the cloud. In Intelligent Systems and Control (ISCO), 2016 10th International Conference on (pp. 1-5). IEEE.

[19]**Thillaiarasu, N. and ChenthurPandian, S.,** 2016, January. Enforcing security and privacy over multi-cloud framework using assessment techniques. In Intelligent Systems and Control (ISCO), 2016 10th International Conference on (pp. 1-5). IEEE.

[20]**Shyamambika, N. and Thillaiarasu, N.,** 2016. Attaining integrity, secured data sharing and removal of misbehaving client in the public cloud using an external agent and secure encryption technique. Advances in Natural and Applied Sciences, 10(9 SE), pp.421-432.

[21]**Ranjithkumar, S. and Thillaiarasu, N.,** 2015. A Survey of Secure Routing Protocols of Mobile AdHoc Network. SSRG International Journal of Computer Science and Engineering (SSRG-IJCSE)–volume, 2.