Empower Data Purity Protection using FMSR Code

R.Suriya[1] Mr.C.Thirumalai Selvan[2] Dr.V.Venkatachalam[3]
[1]M.E. Final Year Student [2]Assistant Professor [3]Professor
[1,2,3]Department of Computer Science and Engineering
[1,2]K.S.R. College of Engineering, Namakkal [3]The Kavery Engineering college, mecheri, Tamil Nadu-637215, India

Abstract— Security of data in cloud storage against data loss is important, so adding algorithm for detection and correction for cloud storage, so in the cloud computing data integrity checking and recovery procedures, is critical. Regenerating codes splitting and verify the data in multiple servers using cryptographic algorithms and MAC verification. To implement the data integrity protection (DIP) scheme for some specific regenerating code to solve the problem of data loss, DIP scheme used some property that enables a client to verify the data in cloud storage system.

***Key words*:** Client Data checking, cryptographic technique, MAC verification.

I. INTRODUCTION

Cloud computing relies on sharing of resources to achieve coherence and economies of scale, similar to a utility over a network. Cloud types are public, private or hybrid. Cloud computing is different from hosting services and assets at ISP data centre. It is all about computing systems are logically at one place or virtual resources forming a Cloud and user community accessing with intranet or Internet. So, it means Cloud could reside in-premises or off-premises at service provider location.

Security concern arise some data loss or failure in data are stored in cloud third party storage system, in this way to secure our data effectively using algorithms. In our exiting papers used two technique, that is proof of data possession (PDP) and proof of irretrievability (POR). Both the technique suitable for only single sever scenario. Suppose that outsource data storage is failure or corrupted means we cannot detect, reconstruct, prevent the data. So go for multiple server scenarios to detect, reconstruct, and prevent the data in cloud storage system. In multiple server concept used two techniques that is HAIL and MR-PDP but what is real fact is mean both for small storage system so security level decreases.

In this paper using Data Integrity Protection (DIP) are using to protect the outsourced data storage system. Our DIP scheme is built on several cryptographic primitives technique for security. Using DIP scheme to reduce the cost of get solution. In the DIP scheme provide functional minimum storage regenerating code (FMSR), codes is used to split the data in storage system. DIP FMSR code capable for smaller storage system, so using MDS property to increase the storage space. MDS property and FMSR technique split the data to store in multiple servers, so repair traffic is reduced by 50 percent to 1.

In the DIP scheme using MAC verification. Existing paper using MD5 for verification of data in cloud system it is the main drawback, because bit size is 128 so not suitable for larger storage system. In our proposed system using SHA1 algorithm, in this is suitable for large file system, this bit size is 160, so storage space increases and also security level increases.

II. RELATED WORK

We briefly summarize the most Further literature review can be found in the supplementary file, We consider the problem to check the integrity of static data, typical in long storage systems suitable for single server scenario by Juels and Kaliski and Ateniese et al., is same as to the POR and PDP scheme. The major problem is limitation is for single server scenario setting. If the attackers is controlled by the server, so detect and reconstruct the data is difficult.

By splitting data across multiple server setting is used to detect, recover the data in the cloud storage system. Efficient DIP scheme are using to verify the replication, erasure code and reconstruct code

Specifically, Chen et al also consider the coded storage system, some key differences with our work. First, design works with the single-server POR scheme by Shacham and Waters. However, such direct adaptation produce the single-server scheme over the large cloud storage system, the amount of data stored increases with a more flexible checking in the scheme.

Second, the storage scheme assumes that storage servers have encoding capabilities for generating encoded data, the servers provides standard read/write functionalities for the availability and compatibility. The multiple server setting mostly worked with HAIL scheme, HAIL operates using regenerating codes to increase the security.

III. PROPOSED SYSTEM

Functional Minimum Storage Regenerating code (FMSR) and Data Integrity Protection (DIP) is used to protect the outsource data using AES algorithm. If not recover by AES means to perform Message Authentication Code (MAC) verification.

MAC verification is effective method to recover the lost content of data in the cloud storage multiple server setting. MAC verification using (Secure Hash Algorithm Version 1) SHA1 algorithm to increase both the byte level and security. It is main advantage of our proposed system.

MAC verification provides hash generation key. Using the key to get the loss data in the cloud in fast manner, it is also advantage of proposed system.

In our proposed system using (Advanced Encryption standard 160 is the bit level) AES 160 technique to increase bit level operation to byte level operation so retrieving the outsource data is easy not difficult to like existing paper. Using of algorithms to improve the performance and security of the outsourced cloud storage data.

In the proposed system is flexibility. There is no limit to store the content of data in cloud storage system. In

the proposed system adjustable because using of cryptographic technique schemes. In our proposed system performs operations such as, upload, check, download, repair operation. Each and every operation is important of our project, because to store the data in cloud follows that operation.

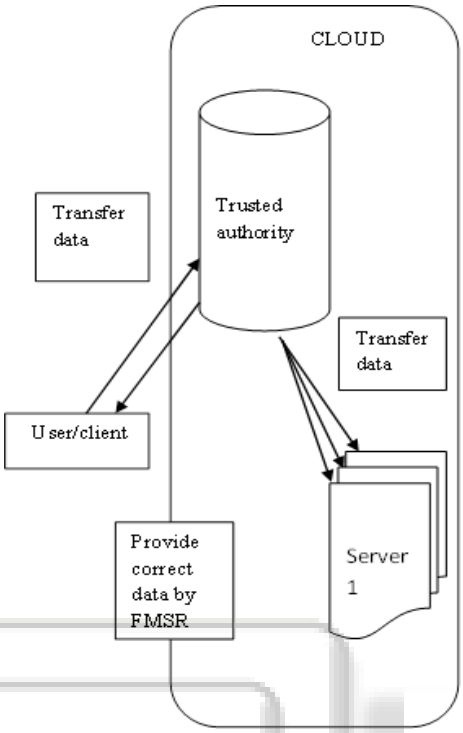

Fig. 1: System Architecture

IV. OPERATIONS

Our goal is to perform four operations such as, Upload, Check, Download, and Repair using with the DIP feature and cryptographic technique and MAC verification.

A. Upload Operation

It is the operation of our project. First to describe how to store the data in cloud multiple server setting. It follows 4 steps to perform the upload operation such as

Step 1: Select the file from client system

Step 2: Encrypt the selected data

Using FMSR to split the data, after that to encrypt the data using the cryptographic security technique, because of security purpose

Step 3: Apply the AECC

Adversarial error-correction code also using for security, it is one type of cryptographic technique. FMSR and DIP is used for protection and if any possible not recover corrupted row means AECC is used for recover the corrupted data, so using AECC in upload operation

Step 4: Upload the data into a cloud server using code.

B. Check Operation

In the Check operation is the next operation of our project, we have to verify the chosen rows of bytes that are stored in the cloud server. In the check operation is performed by 4 steps such as

Step 1: To check the randomly uploaded data

Using the row verification method, so easily prevent the data loss in the cloud server

Step 2: To verify the checked result

Using hash generation technique to detect the lost Content of data in cloud storage

Step 3: Error Identification

Using row verification to easily identify the location of data failure.

Step 4: To perform correction operation to compare the hash generation with both server and client system. So get the optimal solutions using cryptographic technique.

C. Download Operation

The next operation is download operation, To download the data from the server using key. Download operation performed by two steps such as,

Step 1: To check the downloaded data

Using AECC to check the particular downloaded data, that data is correct or not. The downloaded are in decoded form. So we have to encode the data using same decodeded hash key. Otherwise no possible to decode the data, so to prevent from the attackers

Step 2: After download to decode the data

Using cryptographic hash generation technique, to compare the client hash generation with server hash generation code. If any mismatch to reconstruct the data using FMSR and DIP scheme. If not possible to recover the lost data means using AECC with codes to reconstruct the data.

D. Repair Operation

Final operation is repair operation using cryptographic technique to repair the corrupted or failure data. It follows three steps to perform the repair operation

Step 1: To check the random uploaded data

Using the row verification method, so easily prevent the data loss in the cloud server

Step 2: Download and decode the needed particular data from cloud sever.

To compare the both client and server hash generation key. If correct continue the next step. Otherwise to find the correct data using cryptographic security and integrity technique

Step 3: Encrypt, update the data, and upload to cloud storage. Finally, the data is updated to cloud sever, and also copied to all servers

V. SAMPLE REPAIR OPERATION

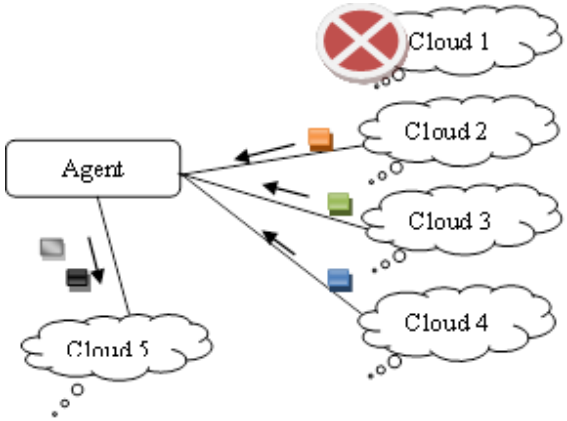

Fig. 2: Repair Operation

Cloud 1 is failed server, so not possible to get data from cloud 1, so using formula to get the data.

Repair traffic = cloud1 + cloud 2 + cloud 3

Using formula to get the new cloud storage that is cloud 5, cloud 5 is similar to the cloud 1 because of integrity protection and MAC verification, in this way to achieve the goal to minimize the traffic.

VI. CONCLUSION

Security of data is important in cloud storage system. Using DIP scheme to verify the integrity in client side is very useful in multi-server setting. FMSR-DIP codes are used to secure and provide the correct the data from the cloud server. Using the cryptographic and DIP scheme improve the performance and security.

ACKNOWLEDGMENT

I extend my sincere thanks to my institution, 'K.S.R. College of Engineering' for giving me the opportunity to write a research paper. A special thanks to my Head of the Department, Dr. A.Rajiv Kannan for encouraging us and to Mr.C.Thirumalai selvan for his support and valuable guidance throughout this project work and makes this project as a successful one.

Finally, I would like to thank authors of the various research papers that I have referred to, for the completion of this work.

REFERENCES

[1] H.C.H. Chen and P.P.C. Lee, "Enabling Data Integrity Protecting Regenerating-Coding-Based Cloud Storage," Proc. IEEE 31stSymp. Reliable Distributed Systems (SRDS '12), 2012.
[2] H. Abu-Libdeh, L. Princehouse, and H. Weatherspoon, "RACS: A Case for Cloud Storage Diversity," Proc. First ACM Symp. Cloud Computing (SoCC '10), 2010.
[3] M. Armbrust, A. Fox, R. Griffith, A.D. Joseph, R. Katz, A.Konwinski, G. Lee, D. Patterson, A. Rabkin, I. Stoica, and M.Zaharia, "A View of Cloud Computing," Comm. ACM, vol. 53,no. 4, pp 50-58, 2010.
[4] G. Ateniese, R. Burns, R. Curtmola, J. Herring, O. Khan, L.Kissner, Z. Peterson, and D. Song, "Remote Data Checking Using Provable Data Possession," ACM Trans. Information and System Security, vol. 14, article 12, May 2011.
[5] K. Bowers, A. Juels, and A. Oprea, "HAIL: A High-Availability and Integrity Layer for Cloud Storage," Proc. 16th ACM Conf.Computer and Comm. Security (CCS '09), 2009.
[6] K. Bowers, A. Juels, and A. Oprea, "Proofs of Retrievability:Theory and Implementation," Proc. ACM Workshop Cloud Computing Security (CCSW '09), 2009.
[7] B. Chen, R. Curtmola, G. Ateniese, and R. Burns, "Remote Data Checking for Network Coding-Based Distributed Storage Systems,"Proc. ACM Workshop Cloud Computing Security (CCSW '10),2010.
[8] L. Chen, "NIST Special Publication 800-108," Recommendation for Key Derivation Using Pseudorandom Functions (Revised), http://csrc.nist.gov/publications/nistpubs/800-108/sp800-108.pdf, Oct.2009.
[9] R. Curtmola, O. Khan, and R. Burns, "Robust Remote DataChecking," Proc. ACM Fourth Int'l Workshop Storage Security and Survivability (Storage SS '08), 2008.
[10] O. Goldreich, Foundations of Cryptography: Basic Tools. Cambridge Univ. Press, 2001.
[11] R. Curtmola, O. Khan, R. Burns, and G. Ateniese, "MR-PDP:Multiple-Replica Provable Data Possession," Proc. IEEE 28th Int'lConf. Distributed Computing Systems (ICDCS '08), 2008.
[12] A. Dimakis, P. Godfrey, Y. Wu, M. Wainwright, and K.Ramchandran, "Network Coding for Distributed Storage Systems," IEEE Trans. Information Theory, vol. 56, no. 9, 4539-4551, Sept. 2010.
[13] D. Ford, F. Labelle, F.I. Popovici, M. Stokel, V.-A. Truong, L.Barroso, C. Grimes, and S. Quinlan, "Availability in Globally Distributed Storage Systems," Proc. Ninth USENIX Symp. Operating Systems Design and Implementation (OSDI '10), Oct. 2010.
[14] O. Goldreich, Foundations of Cryptography: Basic Applications. Cambridge Univ. Press, 2004.
[15] Y. Hu, H. Chen, P. Lee, and Y. Tang, "NCCloud: Applying Network Coding for the Storage Repair in a Cloud-of-Clouds,"Proc. 10th USENIX Conf. File and Storage Technologies (FAST '12),2012

