Special Issue on Proceedings of International Conference on Newer Trends and Innovation in Nanotechnology, Materials Science, Science and Technology March 2021. International Journal of Aquatic Science, Vol 12, Issue

EFFICIENT DATA ACCESS CONTROL SCHEME USING SPLITTING TECHNIQUE IN CLOUDS

K.ArunPatrick, *Assistant Professor, CSE Department, Nehru Institute of Technology*

T. Palani Raja, *Assistant Professor, CSE Department, Nehru Institute of Technology*

Correspondent e-mail: nitcsehod@nehucolleges.com

***Abstract*—**Data access control is one of the main problem in data transferring over the network. Cloud storage is a model of data storage in which the digital data is stored in logical pools. These cloud storage providers are responsible for keeping the data available and accessible. There are various existing methods are used in cloud storage and they are providing security. Proxy encryption method, Cryptographic methods, third party auditor methods are the some of the existing methods. In these methods uploaded files are not stored in virtualized format. Hence the other users can also view the data. Some hackers may hack the data through back end. This may leak privacy and confidentiality of the files. In this project proposes Splitting Technique will split the uploaded files intosub parts and they are stored in the cloud. Proxy server will create a onetime virtual data storage. Cloud will send a copy of the original data to this virtual storage. One time only data viewer can view the data. Data viewer can not able to edit, update or delete the original data. So, the original data are safe. The files are in randomly occurring in the cloud storage, that arealso in encrypted format. Hence the data hackers cannot able to hack the files. The proposed system shows that it provides more confidentiality and privacy than the existing methods.

Keywords: Cryptography, Proxy encryption, Splitting technique, Virtual storage.

I. INTRODUCTION

Cloud computing is the practice of using a network of remote servers hosted on the Internet to store, manage, and process data, rather than a local server or a personal computer.Cloud computing is one of the main topic in nowadays. There are many peoples and many companies are approach cloud for their uses. Cloud is a virtualized format of storing the data over the internet. Users are approach the cloud for storing their data's most securely and confidentially.

Nowadays there are many issues are faced by the cloud users about their data security. They loss their data privacy over the cloud. Some of the efficient and private documents may have leak by the hackers through the back end. In this project proposes Splitting Technique will split the uploaded files into sub parts and they are stored in the cloud.Proxy server will create a onetime virtual data storage. Cloud will send a copy of the original data to this virtual storage. One time only data viewer can view the data. Data viewer can not able to edit, update or delete the original data. So, the original data are safe. The files are in randomly occurring in the cloud storage, that are alsoin encrypted format. Hence the data hackers cannot able to hack the files.

II. LITERATURE REVIEW

Recent years there are many methods for providing privacy when accessing the data from cloud. They are using many cryptographic methods both encryption and decryption for providing privacy. the existing methods areCryptographic methods, proxy encryption technique. In this paperreview about the various security providing technique in

clouds review about the various security providing technique in clouds.H.-Y. Lin and W.-G. Tzeng, (2012) "A Secure Decentralized Erasure Code for Distributed Network Storage," said that the problem of constructing an erasure code for storage over a network when the data sources are distributed. Specifically,[1] we assume that there are n storage nodes with limited memory and k < n sources generating the data. We want a data collector, who can appear anywhere in the network, to query any k storage nodes and be able to retrieve the data.

Here introduce Decentralized Erasure Codes, which are linear codes with a specific randomized structure inspired by network coding on random bipartite graphs. [2] We show that decentralized erasure codes are optimally sparse, and lead to reduced communication, storage and computation cost over random linear coding.

In this correspondence, we address the problem of distributed networked storage when there aremultiple, distributed sources that generate data that must be stored efficiently in multiple storage nodes, each having limited memory.As a motivating application, one can think of sensor networks where the sensor measurements are inherently distributed and sensor motes have constrained communication, computation, and storage capabilities.[5] In addition, distributed networked storage can be useful for peer-to-peer networks or redundant arrays of independent disks (RAID) systems. The distributed sources are k data nodes, each producing one data packet of interest. We also assume we have n storage nodes that will be used as a distributed network memory. If each storage node can store one data packet, we would like to diffuse the data packets so that by querying any k storage nodes, it is possible to retrieve all the k data packets of interest (with high probability). The key issue, of course, is whether it is possible to achieve this robust distributed storage with minimal computation and communication.

M. Kallahalla, E. Riedel, R. Swaminathan, et.all (2003) "Plautus: Scalable Secure File Sharing on Untrusted Storage studied about Plautus is a cryptographic storage system that enables secure file sharing without placing much trust on the file servers. It makes novel use of cryptographic primitives to protect and share files.

Plautus features highly scalable key management while allowing individual users to retain direct control over who gets access to their files. [7] We explain the mechanisms in Plautus to reduce the number of cryptographic keys exchanged between users by using file groups, distinguish file read and write access, handle user revocation efficiently, and allow an untrusted server to authorize file writes. We have built a prototype of Plautus on Open AFS.

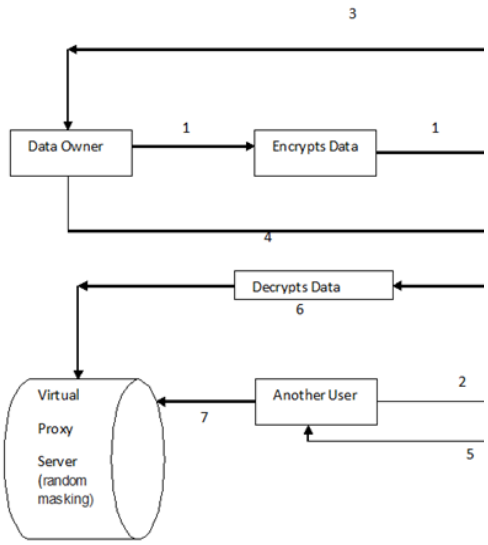
Measurements of this prototype show that Plautus achieves strong security with overhead comparable to systems that encrypt all network traffic. As storage systems and individual storage devices themselves become networked, they must defend both against the usual attacks on messages traversing an untrusted, potentially public, network as well as attacks on the stored data itself. This is a challenge because the primary purpose of networked storage is to enable easy sharing of data, which is often at odds with data security.

To protect stored data, it is not sufficient to use traditional network security techniques that are used for securing messages between pairs of users or between clients and servers. [9]Thinking of a stored data item as simply a message with very long network latency is a misleading analogy

R. Bhagwan, K. Tati, Y.-C. Cheng, et.all, (2010) "Total Recall: System Support for Automated Availability Management, reserched abou**t** availability is a storage system property that is both highly desired and yet

minimally engineered. While many systems provide mechanisms to improve availability – such as redundancy and failure recovery – how to best configure these mechanisms is typically left to the system manager.

III SYSTEM ARCHITECTURE



1. Data owner Store the original data in to the TPA cloud storage server. The data will encrypt and stored in the cloud storage server.

2. Any can view the uploaded data. But the data will be in the encrypted format. Another user can only view the file name of the data. And another user will send request to the cloud server to view the data.

3. Cloud server will forward the request from the user to the data owner.

4. Data owner wants to accept the request from the cloud server.

5. TPA Cloud server will forward a de encrypted key to the user.

6. Simultaneously cloud server will create a virtual server and decrypts the data from the cloud storage server.

7. User can enter the de encrypted key to the proxy server to view the original data. The key will be valid for one time only.

8. After the data view from the proxy server, the virtual data will be deleted automatically.

IV IMPLEMENTATION

Implementation is the stage in the project where the theoretical design is turned into a working system. The most crucial stage is achieving a successful new system & giving the user confidence in that the new system will work efficiently & effectively in the implementation state.

the stage consists of:

- Testing the developed program with simple data.
- Detection's and correction of error.
- Creating whether the system meets user requirements.
- Testing whether the system.
- Making necessary changes as desired by the user.
- Training user personnel.

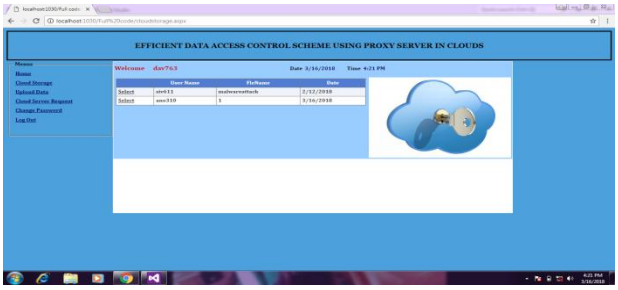
Implementation procedures

The implementation phase is less creative than system design. A system project may be dropped at any time prior to implementation, although it becomes more difficult when it goes to the design phase.

The final report to the implementation phase includes procedural flowcharts, record layouts, report layouts, and a workable plan for implementing the candidate system design into an operational one. Conversion is one aspect of implementation.

- Files are converted in the encrypted format.

- The conversion portion of the implementation plan is finalized and approved.
- Parallel processing between the existing and the new system are logged on a special form.
- Assuming no problems, parallel processing is discontinued. Implementation results are documented for reference.
- Fig: Cloud Storage



V CONCLUSION

Thus, concluding that all the result obtained according to the committed abstract. In this paper, consider a cloud storage system consists of storage servers and key servers. Integrate a newly proposed threshold proxy re-encryption scheme and erasure codes over exponents. The threshold proxy re-encryption scheme supports encoding, forwarding, and partial decryption operations in a distributed way. To decrypt a message of k blocks that are encrypted and encoded ton code word symbols, each key server only must partially decrypt two codeword symbols in our system. By using the threshold proxy re-encryption scheme, present a secure cloud storage system that provides secure data storage and secure data forwarding functionality in a decentralized structure. Moreover, each storage server independently performs encoding and re-encryption and each key server independently perform partial decryption. Storage system and some newly proposed content addressable file systems and storage systems are highly compatible. Storage servers act as storage nodes in a content addressable storage system for storing content addressable blocks. key servers act as access nodes for providing a front-end layer such as a traditional file system interface. Further study on detailed cooperation is required.

In future work Layer 7 virtual proxy servers can be used and Output can be shown, using some medical domain for real time implementation.

VII REFERENCES

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

[2] Ateniese. G, Burns. R, Curtmola. R, Herring. J, Kissner. L, Peterson.Z, and Song. D, (2007)'Provable Data Possession at Untrusted Stores' Proc. 14th ACM Conf. Computer and Comm. Security (CCS), pp. 598-609.

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

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

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

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