International Journal For Recent Developments in Science & Technology
2581-4575
Crossref
A Peer Reviewed Research Journal

Securing Resources in Decentralized Cloud Storage

[1]Mr. M. Parameshwar ,[2]T. Priyanka ,[3]P. Mohan & [4]S. Roja

[1]Assistant Professor, Department of Information Technology, CMR College of Engineering & Technology

[2, 3, 4] B-Tech, Department of Information Technology, CMR College of Engineering &

Abstract:

Storing everything in the local system might need a lot of memory and it costs more to buy and maintain the memory. In order to store the data in the cloud, there is a threat of data thefts and insecure data management. So the storage of the data in a secured manner is needed. There are many ways to store the data in the cloud, and there are even more ways to lose the data stored in the cloud. The storage systems lost the control, and then data thefts might happen. As the data is stored outside our premises, there is chance of loss of data. A reliable system or the process is needed which provides security to data as well as the safe deletion mechanisms. Decentralized Cloud Storage services represent a promising opportunity for a different cloud market, meeting the supply and demand for IT resources of an extensive community of users. The dynamic and independent nature of the resulting infrastructure introduces security concerns that can represent a slowing factor towards the realization of such an opportunity, otherwise clearly appealing and promising for the expected economic benefits. In this project, we present an approach enabling resource owners to effectively protect and securely delete their resources while relying on decentralized cloud services for their storage. Our solution combines All-Or-Nothing-Transform for strong resource protection, and carefully designed strategies for slicing resources and for their decentralized allocation in the storage network. We address availability and security guarantees, jointly considering them in our model and enabling resource owners to control their setting. Here in this project, we are going to upload the files in the cloud and the data users who need those files, can login and search for that file. If the file exists, the request was sent to the data owner who uploaded the file. So by this, the data owner controls that who can view those files. So here we are providing the data privacy. Without the concern of the data owner, the data user cannot access the files.

INTRODUCTION:

Problem statement Storing everything in the local system might need a lot of memory and it costs more to buy and maintain the memory. In order to store the data in the cloud, there is a threat of data thefts and insecure data management. So the storage of the data in a secured manner

International Journal For Recent Developments in Science & Technology
2581-4575
Crossref
A Peer Reviewed Research Journal

is needed. There are many ways to store the data in the cloud, and there are even more ways to lose the data stored in the cloud. The storage systems lost the control, and then data thefts might happen. As the data is stored outside our premises, there is chance of loss of data. A reliable system or the process is needed which provides security to data as well as the safe deletion mechanisms

OBJECTIVES:

- Manage the data in the cloud rather than managing in the local system
- Provide the security to the data by encrypting the data
- To keep the private key unknown to everyone
- Retrieve the data if it was lost unexpectedly
- Store the data in such a way that no one can hack that data

IMPLEMENTATION:

of Stored data in Local System Binary System The term binary means two. So, this system consists of two bits: 0 and 1. The smallest unit of data in a computer is known as a bit (binary digit). As the binary number system has two digits, as a result, a bit can either take the value 0 or 1. We had mentioned earlier that the data is stored in the form of energy in memory cells. The cell carrying data (energy) takes the value 1 and the cell which does not carry any data (energy) takes the value 0. All the data that occupies space in the memory takes the form of bits. 4 bits make up one nibble and 8 bits give us one byte. Going further, we have many names for different sizes of data. The image below gives us the names of different sizes of data.

Bit (0 or 1)
Nibble (4 bits)
Byte (8 bits)
Kilobyte (1024 bytes)
Megabyte (1024 kilobytes)
Gigabyte (1024 megabytes)
Terabyte (1024 gigabytes)
Petabyte (1024 terabytes)
Exabyte (1024 petabytes)
Zettabyte (1024 exabytes)
Yottabyte (1024 zettabytes)

Fig:-1 Units of measure

So, when we enter any number, the computer first converts it into a binary number. This binary number is then stored in the memory of the computer. We shall now learn how to convert a number into a binary number. Securing Resources in Decentralized Cloud Storage CMRCET B. Tech (IT) Page 6 MSB AND LSB MSB stands for Most Significant Bit and LSB stands for Least Significant Bit. As their names suggest, MSB is the bit that carries the most significance in the whole number whereas LSB is the bit that carries the least significance. MSB is also known as the signed bit. It tells us whether a given number is positive or negative based on its

International Journal For Recent Developments in Science & Technology
2581-4575
Crossref
A Peer Reviewed Research Journal

value. If MSB is 0, it means the given number is positive, if it‟s 1, then the number is negative.

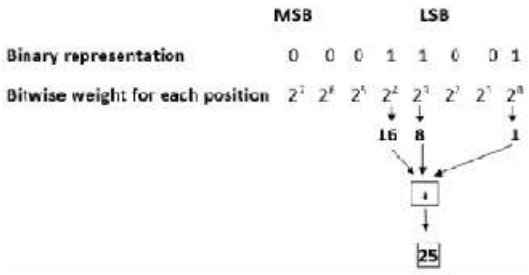


Fig 2 Binary Representation

PROPOSED SYSTEM :

Securing Resources in Decentralized Cloud Storage Objective of Proposed Model

- Data is more secure and kept private.
- File loss is minimised considerably.
- Download speeds are faster.
- Files are easier to transfer.
- Decentralised storage data is cost-efficient.

The proposed solution also enables the resource owners to securely delete their resources when needed, even when some of the nodes in the DCS misbehave. Second, we investigate different strategies for slicing and distributing resources across the decentralized network, and analyse their characteristics in terms of availability and security guarantees. Third, we provide a modelling of the problem enabling owners to control the granularity of slicing and the diversification of allocation to ensure the aimed availability and security guarantees. We demonstrate the effectiveness of the proposed model by conducting several experiments on an implementation based on an available DCS system. Our solution provides an effective approach for protecting data in decentralized cloud storage and ensures both availability and protection responding to currently open problems of emerging DCS scenarios, including secure deletion. In fact, common secret sharing solutions, while considering apparently similar requirements are not applicable in scenarios where the whole resource content (and not simply the encryption key) needs protection, because of their storage and network costs (e.g., each share in Shamir‟s method has the same size as the whole data that has to be protected). Input Design is the process of converting a user-oriented description of the input into a computer-based system. This design is important to avoid errors in the data input process and show the correct direction to the management for getting correct information from the computerized system. It is achieved by creating user-friendly screens for the data entry to handle large volume of data. The goal of designing input is to make data entry easier and to be free from errors. The data entry screen is designed in such a way that

International Journal For Recent Developments in Science & Technology
2581-4575
Crossref
A Peer Reviewed Research Journal

all the data manipulates can be performed. It also provides record viewing facilities. When the data is entered it will check for its validity. Data can be entered with the help of screens. Appropriate messages are provided as when needed so that the user will not be in maize of instant. Thus the objective of input design is to create an input layout that is easy to follow

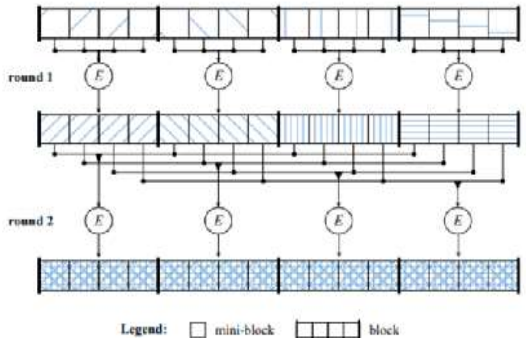
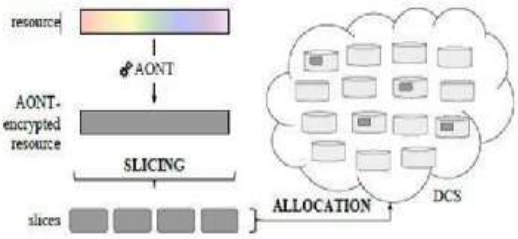


Fig 3All Or Nothing Transform

DesigningSystem

Architectur



RESULTS:

Comparison of Existing Solutions In the literature survey, we took three different data storage systems. The first storage system is the common usage system where we store our data in our physical memory. But, that memory is limited. If the disk or memory was crashed, then there will be no other way to retrieve the lost data. And, if anyone cracks the system password, they will have the access to all the files. So, there is no protection for the files. In the second storage system, we have used many disks to store the data. But, maintenance of those disks becomes somewhat difficult. But, it is better than the previous method, as in this RAID, the data is stored and replicated so that we can retrieve the data in case of data lost from one disk. In the third storage system, every client request is sent to the main server. It is the centralized one. So, this may take a lot of time to process many client requests at a time. As a result, the server will fail to process the user's query appropriately. As a result, it takes longer to process data. There's a good chance it'll cause traffic gridlock.

Fig 5 Accept or Reject request

The data owner can see the requests for the file which was requested by the user and the data owner has an option whether to accept or reject the request

International Journal For Recent Developments in Science & Technology
2581-4575
Crossref
A Peer Reviewed Research Journal

Fig 6 Request status

After the data owner accepts the request, the data user can able to download the file

CONCLUSION :

The existing solutions have some limitations. To overcome those limitations, a method should be implemented which can minimize the risk of threats and data thefts. The encrypted key or the private key might be exposed. This leads to many problems. So, one layer of protection is not sufficient. There should be another method which protects the data. And, being the centralized storage may lead to steal data if the host is not be trusted. The host can able to sell the data to the third party. So, developing a storage system which is decentralized may solve this issue. Our solution combines All-Or-Nothing-Transform for strong resource protection, and carefully designed strategies for slicing resources and for their decentralized allocation in the storage network. We address availability and security guarantees, jointly considering them in our model and enabling resource owners to control their setting.

FUTURE ENHANCEMENTS

1. High-Speed Internet Since decentralized cloud storage relies on storage, the availability of high speed and quality internet bandwidth is the key as it paves way for inexpensive technology where storage is accessed at a click.

2. Peer-to-peer sharing technology Peer-to-peer networks help in storing and sharing data in a distributed file system. It allows the users to receive and host content. This system helps in maintaining many copies of the data with high access speed.

3. Cryptocurrency and Blockchain Blockchain and cryptocurrency help people to transfer value between themselves in a democratized way without any central authority. This enabled the creation of payment and settlement mechanisms that are decentralized too. Decentralized cloud storage is experiencing rapid growth and helping all streams to adopt and experience simpler ways of storing data.

REFERENCES :

[1]. S. Wilkinson, T. Boshevski, J. Brandoff, J. Prestwich, G. Hall, P. Gerbes, P. Hutchins, C. Pollard, and V. Buterin, "Storj: a peer-to-peer cloud storage

network (v2.0)," https://storj.io/storjv2.pdf, Storj Labs Inc., Tech. Rep., 2016

[2]. N. Lambert and B. Bollen, "The SAFE network - a new, decentralised internet," http://docs.maidsafe.net/Whitepapers/pdf/ TheSafeNetwork.pdf, MaidSafe, Tech. Rep., 2014. [3]. J. K. Resch and J. S. Plank, "AONT-RS: blending security and performance in dispersed storage systems," in Proc of FAST, San Jose, CA, USA, February 2011.

[4]. K. D. Bowers, A. Juels, and A. Oprea, "HAIL: A high-availability and integrity layer for cloud storage," in Proc. of ACM CCS, Chicago, IL, USA, November 2009.

[5]. D. A. Patterson, G. Gibson, and R. H. Katz, "A case for redundant arrays of inexpensive disks (RAID)," ACM SIGMOD Records, vol. 17, no. 3, pp. 109–116, Jun. 1988.

[6].S. Wilkinson, T. Boshevski, J. Brandoff, J. Prestwich, G. Hall, P. Gerbes, P. Hutchins, C. Pollard, and V. Buterin, "Storj: a peer-to-peer cloud storage network (v2.0)," https://storj.io/storjv2.pdf, Storj Labs Inc., Tech. Rep., 2016.

[7].D. Irvine, "Maidsafe distributed file system," MaidSafe, Tech. Rep., 2010.

[8].G. Paul, F. Hutchison, and J. Irvine, "Security of the maidsafe vault network," in Wireless World Research Forum Meeting 32, Marrakesh, Morocco, May 2014.

[9].J. Benet, "IPFS-content addressed, versioned, P2P file system," Protocol Labs, Tech. Rep., 2014.

[10]. D. Vorick and L. Champine, "Sia: Simple decentralized storage," https: //sia.tech/sia.pdf, Nebulous Inc., Tech. Rep., 2014.

[11] Latha, Challa Madhavi, and K. L. S. Soujanya. "Key Structure Based Approach towards Scalable Access Control in Cloud Computing."

[12] Yadav, N. S., Rao, M., Parameswari, D. V., Soujanya, K. L. S., & Latha, C. M. (2021). Accessing Cloud Services Using Token based Framework for IoT Devices. Webology, 18(2).

[13] Jaaz, Z.A., Ansari, M.D., Josephng, P.S., Gheni, H.M., 2022, Optimization technique based on cluster head selection algorithm for 5G-enabled IoMT smart healthcare framework for industry, Paladyn, 10.1515/pjbr-2022-0101

[14] Khan, M., Alam, M., Basheer, S., Ansari, M.D., Kumar, N., 2022, A Map Reduce Clustering Approach for Sentiment Analysis Using Big Data, Cognitive Science and Technology, 10.1007/978-981-19-2350-0_22

[15] Goud, B.S., Kalyan, C.N.S., Rao, G.S., Reddy, B.N., Kumar, Y.A., Reddy, C.R., 2022, Combined LFC and AVR Regulation of Multi Area Interconnected Power System Using Energy Storage Devices, 2022 IEEE 2nd International Conference on Sustainable Energy and Future Electric Transportation, SeFeT 2022, 10.1109/SeFeT55524.2022.9909102