IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
Impact Factor: 7.301
Volume 3, Issue 1, September 2023

Cloud Data Storage with Data Dynamics and Safe Network Coding

E Ramkrishna[1] and Dr. Narender Kumar[2]
Research Scholar, Department of Computer Science and Engineering[1]
Supervisor, Department of Computer Science and Engineering[2]
NIILM University, Kaithal, Haryana, India

Abstract: *Cloud computing has made it possible for those who don't have a lot of storage space to communicate their data to computers in other regions. These services provide users with unrestricted access to their data for free. A client can verify the accuracy of the information they have provided to a third party by employing secure cloud storage technologies. We investigate whether or not dynamic data may be stored safely in the cloud using secure network coding techniques. In this research, we evaluate the efficacy of various secure network coding techniques for developing cloud-based dynamic data storage solutions. The SHA algorithm simplifies the process of removing dynamic data during decoding. The information from the pre-processor is parsed and encrypted using algorithms inspired by the Ceaser Cipher. The technique includes uploading the encrypted data to the cloud.*

Keywords: cloud storage, dynamic data, network coding

I. INTRODUCTION

Cloud computing refers to the practice of utilizing data processing and storage capabilities that are made available across a network, most commonly the Internet. The diagrams of complex systems are commonly represented by a cloud-shaped symbol, hence the name. The term "cloud computing" refers to the practice of offloading a user's information, applications, and tasks to remote servers. Through cloud computing, both computer systems and their associated software are hosted and maintained remotely by an external source. Many cutting-edge server infrastructures and software applications are made available to users via these services. The primary objective of cloud computing is to leverage the processing capacity of conventional supercomputers and high-performance computing systems often employed by the military and academic organizations. Financial portfolio management, individualized content delivery, simplified data storage, and supporting MMORPG functionality are all examples of these aims. The term "cloud computing" refers to the practice of distributing data processing tasks among a large group of inexpensive personal computers (PCs) connected via the internet. The aforementioned IT infrastructure is in fact an interconnected system of systems. Virtualization techniques are frequently used to improve the efficiency of cloud computing. A smartphone with a weak processor or inadequate storage capacity, for instance, would be unable to do complex calculations or store large amounts of data. The user always has the option of outsourcing these tasks to a remote server in the cloud. When users outsource the task of storing their data to a third party service provider, they turn to cloud servers to do so. In order to free up capacity, a malicious cloud server can remove infrequently accessed client data. Two-party protocols between the client and the server are one example of a secure cloud storage approach that can reveal whether or not the server is maintaining the client's data in its original, unaltered form. Secure cloud storage protocols for static data (called SSCS) and secure cloud storage protocols for dynamic data (called DSCS) categorize the protocols used for outsourced data storage. When it comes to static data like backup and archive information, the customer is locked out after the first outsourcing. Dynamic data allows users to update their information whenever they see fit, leading to a more complete image. Ultimately, the purpose of this project is to define the research and action objectives. Nodes other than the sender and receiver often combine the packets they have received to create a new packet as part of a network coding scheme. The aforementioned methods outperform store-and-forward routing in terms of performance, efficiency, and scalability. Intermediate sites that send forged packets can still compromise them. There is a potential that the receiver of such packets will have problems deciphering the file that was sent by the source node. Protecting

IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
Impact Factor: 7.301
Volume 3, Issue 1, September 2023

against such attacks, Secure Network Coding (SNC) techniques assign a unique tag to each packet after the source has been validated. Message authentication codes (MACs) and homomorphic signatures are used to create these indicators of authenticity. An intermediary node can consolidate all incoming data packets and their associated identifiers into a single packet using the homomorphic property.

II. LITERATURE SURVEY

Secure Cloud Storage with Data Dynamics using Provable Data Possession.

Proven data ownership (PDP) was proposed by Ateniese et al. The file is broken up into chunks that are owned by the client. After that, a Message Authentication Code (MAC) or other form of security tag is generated for each block. At last, the client transmits the blocks and their associated labels. The client submits a challenge to the server during an audit, requesting that the server verify the integrity of a predetermined number of randomly selected blocks. The server takes the challenge and the stored information and returns a proof (response) to the client. If your proof is convincing, you can count on recovering the vast majority of your file. The concept of public verifiability is also brought up by Ateniese et al., which means the client has the option of selecting an independent auditor. An audit can be performed by any Third-Party Auditor (TPA) who has access to the necessary public key. Only the client, equipped with the secret key and privacy-preserving methods, can verify the server's proof.

Secure Cloud Storage with Data Dynamics using Proofs of Retrievability.

Juels and Kaliski introduce proofs of Proofs of retrievability (POR) are a scheme developed by Juels and Kaliski (year) to guarantee that all blocks in static data files may be retrieved. According to Shacham and Waters, verifying the compressed file's blocks before uploading them to the server is crucial. It is likely that you may observe the server deleting or updating many blocks in order to remove or modify a single block correctly. More proof-of-retrievability (POR) schemes have been presented as a direct result of the work done by Juels and Kaliski. While some of these programs are better suited to static data, most can be used to make modifications to data before outsourcing is ever initiated. Here we present a formal definition of the DSCS protocol. The protocol under consideration may be a PDP/POR scheme whose primary objective is to guarantee data retrieval. The person doing the checking could be the client himself or a TPA.

III. METHODOLOGY

Network encoding-based distributed storage systems have been developed to facilitate the dissemination of client data over numerous locations. However, they still have as their primary purpose the decrease in bandwidth required to resolve computer issues. We hope to answer the question, "Can we build a cloud storage system that efficiently and securely manages dynamic data on a single storage server?" by doing the research outlined here. We will focus on how the SNC protocol's techniques may be applied in this context. Data that can be altered in any way, including additions, deletions, and modifications, is considered dynamic. In some cases, you might want to work with data that can only be saved by appending it to the end of an existing file. While static data is fixed in its current state, dynamic data can be altered in any way the user desires. These programs typically safeguard both existing data and newly created data by incorporating it into existing databases.

Existing System

Most modern dynamic Point-of-Sale (PoS) systems use the uploader's secret key to generate an identification that may be used to verify the uploader's identity. When many users are making changes to a file without having access to the original, client-side cross-user deduplication is used to ensure that no new tags are created. The dynamic Point-of-Sale (PoS) systems would be rendered useless in this scenario.

Proof of Ownership is a client-side approach developed by Halevi et al. for cross-user deduplication. Building the Merkle tree without the assistance of a cloud server is a challenging requirement in dynamic Proof of Stake (PoS) systems.

Pietro and Sorniotti have suggested an improved system of ownership documentation.

IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
Impact Factor: 7.301
Volume 3, Issue 1, September 2023

Xu et al. present a new client-side method for deduplicating encrypted data. However, they use a deterministic proof mechanism in their method, therefore each file also comes with a deterministic brief proof. With this evidence, users can successfully complete the verification procedure without physically possessing the file.

Proposed System

This work presents the first investigation into deduplicatable dynamic Proof of Storage (deduplicatable dynamic PoS), to the best of our knowledge. This innovative idea solves problems caused by a wide variety of structure types and the need for secret tags.The Homomorphic Authenticated Tree (HAT) is an innovative authenticated structure designed to keep CPU costs constant while reducing communication expenses during the proof-of-storage and deduplication phases. When compared to other tried and true structures like the skip list and the Merkle tree, this one stands out as unique.

Cross-user deduplication, dynamic operations, and integrity checks are all features that can be reliably supported by the HAT system at all times.Dey-PoS is the first suggested and implemented deduplicatable dynamic Proof of Stake (PoS) structure, and it supports a wide variety of update and verification methods. To demonstrate the robustness of this architecture, we apply the random oracle model and conduct thorough theoretical and experimental analyses of its performance.

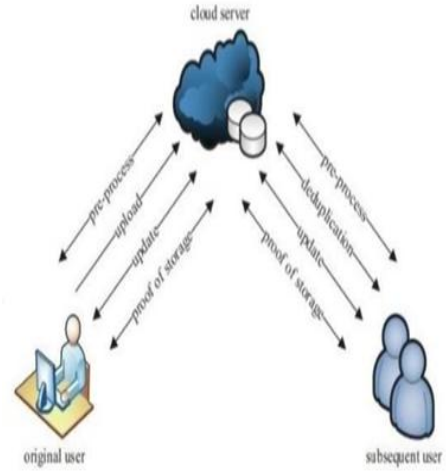


Fig.1. **System Architecture**

Data Owner

The owner of the data transfers it to a remote server using the File Blocks block in this module. The data owner encrypts the File Blocks before storing them in the cloud for added safety. The data custodian can alter the file-blocking approach by adjusting the expiration date. To some extent, secured data file blocks may be editable by the data's owner. In addition, the data's administrator can decide who or what can access the data's File Blocks by setting permissions.

Cloud Server

Data storage services are provided by the cloud provider, who is responsible for maintaining the cloud infrastructure. Encryption is used by data owners to ensure the security of their cloud-based data storage. This streamlines access to this information for authorized individuals. The only way for data users to access the shared data File Blocks is to retrieve the desired encrypted data File Blocks from the cloud and decode them locally.

Third Party

A "Third party auditor" (TPA) is a person who has the authority to review or oversee outsourced data and the necessary expertise to do so with the knowledge and consent of the data owner. If you need to verify the authenticity of your cloud infrastructure, conduct digital forensics investigations, or replace your old private keys, then you need this auditing service.

IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
Impact Factor: 7.301
Volume 3, Issue 1, September 2023

End User

Depending on the user's access rights and level of expertise, the data stored in the cloud can be used in a variety of ways. Searching for file blocks using content keywords, requesting individual file blocks, asking download of a file block along with its associated security key, and eventually downloading the requested file blocks are all examples of these actions.

IV. RESULTS

Home Page

Cloud login page

IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
Impact Factor: 7.301
Volume 3, Issue 1, September 2023

Registration Page

User Details

User Name	Email	DOB	Contact	State	Country	Authentication
vanu	vanu@gmail.com	2016-05-13	9090909090	Telangana	India	Activate
Susmitha Yarmala	susmitha.yarmala@gmail.com	2016-05-15	9080009090	Telangana	India	Activate
durga laxmi	durga@gmail.com	2016-05-14	9783456745	Telangana	India	Activate
akanksha	akanksha@gmail.com	2016-05-15	7899424566	Telangana	India	Activate
devi	devi@gmail.com	2016-05-13	9647746372	Telangana	India	Activate
likitha	likitha@gmail.com	2016-05-13	8389424566	Telangana	India	Activate
vijay kumar	vijayn@gmail.com	2016-05-14	9441079139	Telangana	India	Activate
dheeraj	dheeraj@gmail.com	2016-05-13	9999999999	Telangana	India	Activate
dheeraj	dheeraj@gmail.com	2016-05-13	9999999999	Telangana	India	Activate
shiva	shiva@gmail.com	2016-05-14	9898989898	Telangana	India	Activate
mohan	mohan@gmail.com	2016-05-14	8389424566	Telangana	India	Activate
Susmitha Yarmala	susmitha.yarmala@gmail.com	2016-05-14	8389424566	Telangana	India	Activate

User Details Page

User Login Page

IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
Impact Factor: 7.301
Volume 3, Issue 1, September 2023

File Name Page

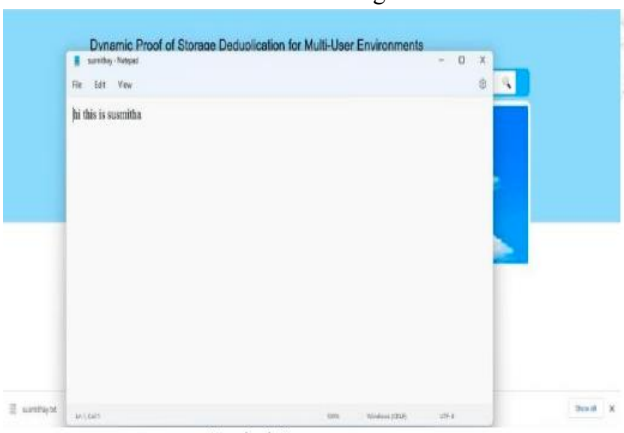
Verify Page

File Upload Page

IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
Impact Factor: 7.301
Volume 3, Issue 1, September 2023

File View Page

File Details Page



Download Page

Download Page

V. CONCLUSION

The users of the project have the option to edit the information stored in the cloud. In order to prevent unwanted access to the data, algorithms are used to convert the user's input into discrete units. Deduplication is the process of removing redundant data that results when content is reuploaded after already having been uploaded. Users need to use a secret

IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
Impact Factor: 7.301
Volume 3, Issue 1, September 2023

key given to them by the data owner in order to access their submitted data stored in the cloud. By taking advantage of this program, a large number of people will have access to cloud storage for their data.

REFERENCES

[1] B. Sengupta and S. Ruj, "Publicly verifiable secure cloud storage for dynamic data using secure network coding," in ACM AsiaConference on Computer and Communications Security, 2016, pp. 107–118.

[2] G. Ateniese, R. C. Burns, R. Curtmola, J Herring, L. Kissner, Z. N. J. Peterson, and D.XSong, "Provable data possession at untrusted stores," in ACM Conference on Computer and Communications Security, 2007, pp. 598–609.

[3] Juels and B. S. Kaliski, "PORs: Proofs of retrievability for large files," in ACM Conference on Computer and CommunicationsSecurity, 2007, pp. 584–597.

[4] H. Shacham and B. Waters, "Compact proofs of retrievability," Journal of Cryptology, vol. 26, no. 3, pp. 442–483, 2013.

[5] C. Erway, A. K¨upc¸¨u, C. Papamanthou, and R. Tamassia, "Dynamic provable data possession," ACM Transactions on Information and System Security, vol. 17, no. 4, pp. 15:1– 15:29, 2015