International Journal of Technology, Leadership and Sciences (IJTLS)
ISSN: 3107-9083 www.ijtls.com Paper ID: TLS-26/V2/I2-017
DOI: https://doi.org/10.5281/zenodo.19125256

ENHANCING CLOUD STORAGE SECURITY AND RELIABILITY THROUGH NETWORK CODING

[#1]**G. LAKSHMI,** ***Associate Professor,***
[#2]**KALAGURA UDAY KIRAN,** ***B.Tech Student,***
[#3]**GOLLENA PRASANNALAXMI,** ***B.Tech Student,***
[#4]**BARLA SAMATHA,** ***B.Tech Student,***
[#5]**PINDI SAINITHIN,** ***B.Tech Student,***
Department of AIML,
TRINITY COLLEGE OF ENGINEERING AND TECHNOLOGY, PEDDAPALLY, TG.

ABSTRACT: Cloud computing enables users to connect their data to servers located in different parts of the world, allowing them to access their data from anywhere, regardless of their storage capacity. Users are able to access their data freely and without limitations through these services. By utilizing secure cloud storage, a customer can guarantee the accuracy of the information they share with a third party. We investigate the feasibility of using secure network coding techniques for cloud storage of dynamic data. In order to build dynamic data storage systems for the cloud, this research compares and contrasts various secure network coding approaches. Decoding dynamic data becomes much easier with the SHA algorithm. Data from the pre-processor is read and encrypted using methods that are based on the Ceaser Cipher. Moving the encrypted files to a cloud service is a step in the process.

Keywords: Cloud storage, Dynamic data, Network coding.

1. INTRODUCTION

"Cloud computing" refers to the practice of accessing and making use of shared computing resources, such as data storage and processing, through an Internet-based network. The name comes from the fact that complex system diagrams commonly include cloud-shaped symbols. A user's data, apps, and tasks can be "cloud-computing" transferred to distant machines. When you use cloud computing, a remote third party hosts and controls your computer

systems and applications. Various state-of-the-art server infrastructures and software applications are accessible to consumers through these services.

One main goal of cloud computing is to tap into the processing power of older, more conventional HPC and supercomputer systems, which are commonly used by institutions like universities and the military. Supporting massively multiplayer online role-playing games (MMORPGs), streamlining data storage, managing financial portfolios, and providing personalized content are all part of the plan. A phenomenon known as "cloud computing" occurs when several inexpensive personal computers linked to the internet divide and conquer the task of data processing. All that talk about IT infrastructure up there is actually just a bunch of interconnected systems. If you want your cloud computing to run more smoothly, you should look into virtualization strategies.

An example would be the inability to store large amounts of data or do sophisticated calculations on a smartphone due to slow processing or insufficient storage space. The option to delegate these duties to a remote server in the cloud is always available to the user. People use cloud servers when they contract with an outside company to store their data. In order to create room for new data, a faulty cloud server could delete less frequently used client files. One secure method of cloud storage is two-party protocols, which connect the client and server. Their presence can reveal if the server is faithfully preserving the client's data in its unaltered state. Secure cloud storage protocols (SSCS) and dynamic storage security standards (DSCS) are available for outsourced data storage. Customers lose access to static data, such as backup and archive files, after the first outsourcing.

Users are able to update their information at any time with dynamic data, which enhances the overall picture. Determining the research and action objectives is the primary focus of the project. Nodes outside of the sender and receiver may combine received packets to form a new packet in a network coding scheme. When comparing scalability, efficiency, and performance, the aforementioned techniques outperform store-and-forward routing. They are nevertheless vulnerable to intrusion attempts from intermediary websites that use bogus packets.

The recipient of these packets may have difficulty deciphering the file sent by the source node. To prevent these types of attacks, Secure Network Coding (SNC) approaches assign a unique tag to each packet after the source has been confirmed. Message authentication codes (MACs) and homomorphic signatures are utilized to construct these markers of authenticity.

An intermediary node can combine all incoming data packets with their identifiers into a single packet thanks to the homomorphic characteristic.

2. LITERATURE SURVEY

Secure Cloud Storage with Data Dynamics using Provable Data Possession.

The authors Ateniese et al. advocated for PDP, or verified data ownership. The client-specific sections of the file are separated. Message Authentication Codes (MACs) and similar security tags are subsequently applied to each block. Final step: client-side transmission of blocks and associated labels. It is common practice for clients to request that the server verify the authenticity of a predetermined number of randomly selected blocks during audits.

The server will send a proof (answer) to the client after receiving the challenge and the stored data. The majority of your file should be recoverable if your proof is sufficient. Additionally, Ateniese et al. discuss publicly verifiable information, which allows clients to choose an unbiased auditor. Any TPA worth their salt needs the correct public key in order to conduct an audit. To validate the server's proof, only the client with the secret key and privacy-preserving processes can do so.

Secure Cloud Storage with Data Dynamics using Proofs of Retrievability.

Proofs of Retrievability (POR) was developed by Juels and Kaliski (year) to guarantee that all blocks in static data files could be located. According to Shacham and Waters, before sending the compressed file blocks to the server, you should check them. If you wish to edit or remove a single block, the server may likely need to process many blocks concurrently.

Additional proof-of-retrievability (POR) approaches have been introduced as a direct consequence of the work of Juels and Kaliski. While some of these tools work better with static data, the majority of them allow you to edit data before sending it out. The DSCS protocol is defined formally here. This protocol, which may be a PDP/POR system, aims to guarantee data retrieval as its primary function. Both the client and a TPA are capable of doing the check.

3. METHODOLOGY

The development of distributed storage systems based on network encoding has facilitated the transfer of client data across numerous locations. However, reducing the bandwidth required to repair computers remains their primary objective. Through the research mentioned below, we want to address the issue, "Can we build a cloud storage system that

efficiently and securely manages dynamic data on a single storage server?" Here, we'll zero in on the SNC protocol's potential applications. Data that is dynamic can undergo changes such as the addition of new data, the deletion of existing data, or the introduction of new formulas. There are times when you'll need to store data by appending it to the end of an existing file. While static data remains unchanged, dynamic data can be changed at any time by users. These programs often add new and old data to existing databases to make it more secure.

Existing System

- The majority of up-to-date dynamic point-of-sale (PoS) systems generate an identifier that, when combined with the uploader's secret key, can confirm the uploader's identity. Client-side cross-user deduplication prevents the creation of duplicate tags when many users make changes to a file without seeing the original. The dynamic point-of-sale (PoS) systems would be useless in this case.
- The client-side Proof of Ownership approach to cross-user deduplication was established by Halevi et al. Without access to a cloud server, dynamic Proof of Stake (PoS) systems make it difficult to build the Merkle tree.
- An improved method of ownership tracking has been proposed by Pietro and Sorniotti.
- Clients now have a better option for removing duplicates from encrypted data, thanks to Xu et al. Due to the deterministic nature of their proof process, however, each file also contains a brief proof. Users can successfully finish the verification procedure without the file if they have this proof.

Proposed System

- Deduplicatable dynamic Proof of Storage (deduplicatable dynamic PoS) has never been investigated before, as far as we are aware, in a single paper. The requirement for hidden tags and the variety of structural types give rise to challenges, which this novel concept addresses.A novel authenticated structure called the Homomorphic Authenticated Tree (HAT) was developed to reduce communication costs throughout the proof-of-storage and deduplication phases while maintaining constant CPU costs. Compared to other popular structures, such as the Merkle tree and the skip list, this one is unique.
- Integrity checks, dynamic operations, and user-wide deduplication are all tasks that the HAT system is capable of doing at all times.The Dey-PoS structure was the first to be proposed and utilized for deduplicatable dynamic Proof of Stake (PoS). It offers a plethora of options for updating and verifying. We demonstrate the robustness of this design through extensive theoretical and experimental testing, all based on the random

International Journal of Technology, Leadership and Sciences (IJTLS)
ISSN: 3107-9083 www.ijtls.com Paper ID: TLS-26/V2/I2-017
DOI: https://doi.org/10.5281/zenodo.19125256

oracle model.

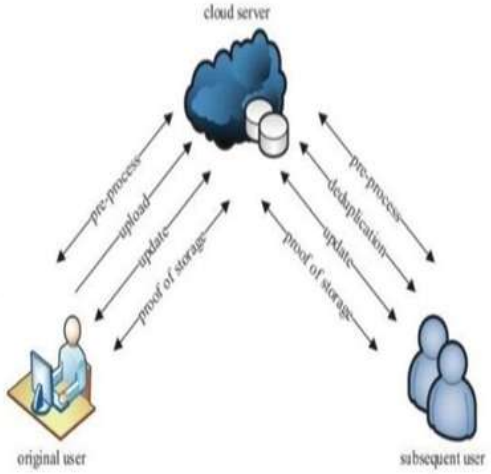

Fig.1. System Architecture

Data Owner

The data owner can transfer the data to a remote server by utilizing the File Blocks block in this module. Prior to storing them in the cloud, the data owner takes extra precautions by encrypting the File Blocks. By modifying the expiration date, the data custodian can modify the file-blocking method. It is possible that the data owner can alter certain protected data file blocks. To further restrict access to the data's File Blocks, the administrator can establish permissions.

Cloud Server

Data storage and infrastructure management in the cloud are the responsibilities of the cloud provider. To ensure the security of their data stored in the cloud, data owners employ encryption. Those with authorization can now access this data more easily. Users must retrieve the desired encrypted data File Blocks from the cloud and decode them on their personal computers before they may access the shared data File Blocks.

Third Party

The knowledge and approval of the data owner, a "third party auditor" (TPA) can examine or supervise outsourced data if they have the appropriate expertise to do so. For digital forensics, updating old private keys, or verifying the legitimacy of your cloud infrastructure, this auditing service is essential.

End User

Data saved in the cloud can be accessed in several ways, depending on the user's permissions and degree of expertise. Downloading the desired file blocks is the last step after searching

International Journal of Technology, Leadership and Sciences (IJTLS)
ISSN: 3107-9083 www.ijtls.com Paper ID: TLS-26/V2/I2-017
DOI: https://doi.org/10.5281/zenodo.19125256

for them using content keywords. Other steps include requesting specific file blocks, requesting the download of a file block together with its security key, and so on.

4. RESULTS

Fig 2: Home Page

Fig 3: Cloud login page

Fig 4: Registration Page

International Journal of Technology, Leadership and Sciences (IJTLS)
ISSN: 3107-9083 www.ijtls.com Paper ID: TLS-26/V2/I2-017
DOI: https://doi.org/10.5281/zenodo.19125256

Fig 5: User Details Page

Fig 6: User Login Page

Fig 7: File Name Page

International Journal of Technology, Leadership and Sciences (IJTLS)
ISSN: 3107-9083 www.ijtls.com Paper ID: TLS-26/V2/I2-017
DOI: https://doi.org/10.5281/zenodo.19125256

Fig 8: Verify Page

Fig 9: File Upload Page

Fig 10: File View Page

International Journal of Technology, Leadership and Sciences (IJTLS)
ISSN: 3107-9083 www.ijtls.com Paper ID: TLS-26/V2/I2-017
DOI: https://doi.org/10.5281/zenodo.19125256

Fig 11: File Details Page

Fig 12: Download Page

5. CONCLUSION

The information that is stored in the cloud can be updated by project users. In order to ensure that no unauthorized parties can access the data, the user's input is converted into discrete units using procedures that prioritize security. When material that has already been posted is reuploaded, deduplication is used to remove duplicate data. In order for users to access their own data stored in the cloud, the data owner must provide them with a secret key. The app will make cloud storage accessible to many individuals.

REFERENCES

1. B. Sengupta and S. Ruj, “Publicly verifiable secure cloud storage for dynamic data using secure network coding,” in ACM Asia Conference 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. X.

Song, “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 Communications Security, 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. Küpçü, 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.