SECURE CLOUD STORAGE WITH DATA DYNAMICS USING SECURE NETWORK CODING TECHNIQUES

G.RANI
Assistant Professor
Department of CSE
rani.g550@gmail.com
Teegala Krishna Reddy Engineering College, Hyderabad

PINDI PALLAVI
Department of CSE
pindi.pallavireddy@gmail.com
Teegala Krishna Reddy Engineering College, Hyderabad

CIRIPANGI RISHIKA
Department of CSE
rishikaraj026@gmail.com
Teegala Krishna Reddy Engineering College, Hyderabad

USHAKOLA SAITEJA
Department of CSE
ushakolasaiteja9@gmail.com
Teegala Krishna Reddy Engineering College, Hyderabad

Abstract- In the age of cloud computing, cloud users with limited storage can outsource their data to remote servers. These servers, in lieu of monetary benefits, offer retrievability of their clients' data at any point of time. Secure cloud storage protocols enable a client to check integrity of outsourced data. In this work, we explore the possibility of constructing a secure cloud storage for dynamic data by leveraging the algorithms involved in secure network coding. We show that some of the secure network coding schemes can be used to construct efficient secure cloud storage protocols for dynamic data. In this we use SHA algorithm for deleting the dynamic data and it is used for decrypt data. By using Ceaser Cipher techniques the pre-processor data will divided in to blocks, and the data will encrypted. The Encrypted data will uploaded to cloud.

I. INTRODUCTION

Cloud computing is the use of computing resources (hardware and software) that are delivered as a service over a network (typically the Internet). The name comes from the common use of a cloud-shaped symbol as an abstraction for the complex infrastructure it contains in system diagrams. Cloud computing entrusts remote services with a user's data, software and computation. Cloud computing consists of hardware and software resources made available on the Internet as managed third-party services. These services typically provide access to advanced software applications and high-end networks of server computers. The goal of cloud computing is to apply traditional supercomputing, or high- performance computing power, normally used by military and research facilities, to perform tens of trillions of computations per second, in consumer-oriented applications such as financial portfolios, to deliver personalized information, to provide data storage or to power large, immersive computer games. The cloud computing uses networks of large groups of servers typically running lowcost consumer PC technology with specialized connections to spread data- processing chores across them. This shared IT infrastructure contains large pools of systems that are linked together. Often, virtualization techniques are used to maximize the power of cloud computing. For example, a client having a smart phone with a low-performance processor or limited storage cannot accomplish heavy computation or store large volume of data. Under such circumstances, she can delegate her computation/storage to the cloud server. In case of storage outsourcing, the cloud server stores massive data on behalf of its clients (data owners). However, a malicious cloud server can delete some of the client's data (that are accessed infrequently) to save some space. Secure cloud storage protocols (two-party protocols between the client and the server) provide a mechanism to detect if the server stores the client's data untampered. Based on the nature of the outsourced data, these protocols are classified as: secure cloud storage protocols for static data (SSCS) and for dynamic data (DSCS). For static data, the client cannot change her data after the initial outsourcing (e.g., backup/archival data). Dynamic data are more generic in that the client can modify her data as often as needed.

Scope of the Project

In a network coding protocol each intermediate node (except sender/receiver nodes) on a network path combines incoming packets to output another packet. These protocols enjoy higher throughput, efficiency and scalability than the store-and-forward routing, but they are prone to pollution attacks by malicious intermediate nodes injecting invalid packets. These packets produce more such packets downstream, and the receiver might not finally decode the file sent by the sender node. Secure network coding (SNC) protocols use cryptographic techniques to prevent these attacks: the sender authenticates each packet by attaching a small tag to it. These authentication tags are generated using homomorphic message authentication codes (MACs) or homomorphic signatures. Due to homomorphic property, an intermediate node can combine incoming packets into a packet and its tag.

Literature survey

Secure Cloud Storage with Data Dynamics using Provable Data Possession.

Ateniese et al introduce provable data possession (PDP) where the client (data owner) splits the data file into blocks, computes an authentication tag (e.g., MAC) for each block, and uploads the blocks along with their tags. During an audit, the client asks the server to prove the integrity of a predefined number of random blocks (challenge). The server computes a proof (response) based on the challenge and the stored data, and sends it to the client. A valid proof ensures retrievability of almost all blocks in the file. Ateniese et al also introduce the notion of public verifiability where the client can delegate the auditing task to a third party auditor. The TPA with the knowledge of the public key can perform an audit. For privately verifiable schemes, only the client having the secret key can verify the proof sent by the server.

Secure Cloud Storage with Data Dynamics using Proofs of Retrievability.

Juels and Kaliski introduce proofs of retrievability (POR) for static data file that ensures retrievability of all of its blocks. According to Shacham and Waters, the underlying idea is to encode the file with an erasure code, authenticate the blocks of the encoded file, and upload them on the server. With this technique, the server has to delete/modify a considerable number of blocks to actually delete/modify a single block — which can be detected with high probability. Following the work by Juels and Kaliski, several POR schemes have been proposed. Some of these schemes are designed for static data, and the rest allow the client to modify data after the initial outsourcing. We define a DSCS protocol as follows. It can be a PDP/POR protocol based on the retrievability guarantee of data. The client (or a TPA) can be the verifier.

III Methodology

Network coding techniques have been used to construct distributed storage system where the client's data are disseminated across multiple servers. However, they primarily aim to reduce the repair bandwidth when some of the servers fail. On the other hand, we explore whether we can exploit the algorithms involved in an SNC protocol to construct an efficient and secure cloud storage protocol for dynamic data (for a single storage server). Although dynamic data are generic in the sense that they support arbitrary update (insertion, deletion and modification) operations, append-only data (where new data corresponding to a data file are inserted only at the end of the file) find numerous applications as well. These applications primarily maintain archival as well as current data by appending the current data to the existing datasets.

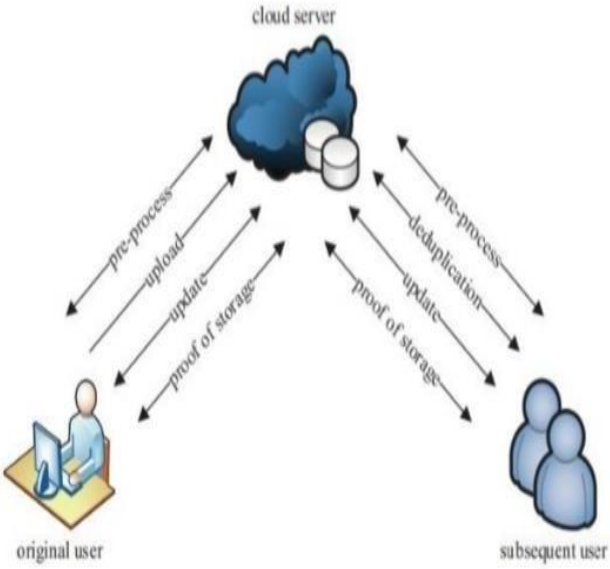
Existing System

- In most of the existing dynamic PoSs, a tag used for integrity verification is generated by the secret key of the uploader. Thus, other owners who have the ownership of the file but have not uploaded it due to the cross-user deduplication on the client-side, cannot generate a new tag when they update the file. In this situation, the dynamic PoSs would fail.
- Halevi et al. introduced the concept of proof of ownership which is a solution of cross user deduplication on the client-side. It requires that the user can generate the Merkle tree without the help from the cloud server, which is a big challenge in dynamic PoSs.
- Pietro and Sorniotti proposed another proof of ownership scheme which improves the efficiency.
- Xu et al. proposed a client-side deduplication scheme for encrypted data, but the scheme employs a deterministic proof algorithm which indicates that every file has a deterministic short proof. Thus, anyone who obtains this proof can pass the verification without possessing the file locally.

Proposed System

- To the best of our knowledge, this is the first work to introduce a primitive called deduplicatable dynamic Proof of Storage (deduplicatable dynamic PoS), which solves the structure diversity and private tag generation challenges.
- In contrast to the existing authenticated structures, such as skip list and Merkle tree, we design a novel authenticated structure called Homomorphic Authenticated Tree (HAT), to reduce the communication cost in both the proof of storage phase and the deduplication phase with similar computation cost.
- Note that HAT can support integrity verification, dynamic operations, and cross-user deduplication with good consistency.
- We propose and implement the first efficient construction of deduplicatable dynamic PoS called Dey-PoS, which supports unlimited number of verification and update operations. The security of this construction is proved in the random oracle model, and the performance is analyzed theoretically and experimentally.

IV ARCHITECTURE



System Architecture

V RESULTS

Home Page

Registration Page

Cloud login page

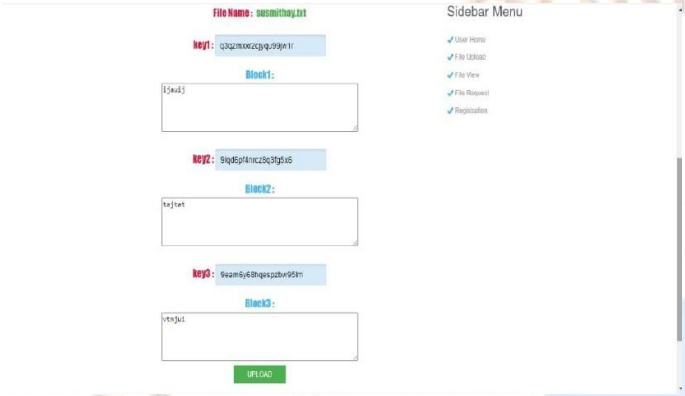
User Details

User Name	Email	DOB	Contact	State	Country	Authentication
vasu	vasu@gmail.com	2018-05-13	9090909090	Telangana	India	Activate
Susmitha Yarmala	susmitha.yarmala@gmail.com	2018-05-15	9090909090	Telangana	India	Activate
durga laxmi	durga@gmail.com	2018-05-14	9783456745	Telangana	India	Activate
akanksha	akanksha@gmail.com	2018-05-15	7809424566	Telangana	India	Activate
devi	devi@gmail.com	2018-05-13	9647746372	Telangana	India	Activate
likitha	likitha@gmail.com	2018-05-13	8309424566	Telangana	India	Activate
vijay kumar	vijays@gmail.com	2018-05-14	9441079139	Telangana	India	Activate
dheeraj	dheeraj@gmail.com	2018-05-13	9999999999	Telangana	India	Activate
dheeraj	dheeraj@gmail.com	2018-05-13	9999999999	Telangana	India	Activate
shiva	shiva@gmail.com	2018-05-14	9898989898	Telangana	India	Activate
mohan	mohan@gmail.com	2018-05-14	8309424566	Telangana	India	Activate
Susmitha Yarmala	susmitha.yarmala@gmail.com	2018-05-14	8309424566	Telangana	India	Activate

User Details Page

User Login Page

File Upload Page



File Name Page

File View Page

Verify Page

File Details Page

Download Page

Conclusion:

This project allows the users to modify the data that is stored in the cloud. By using the algorithms the original data of user is converted into blocks so that is can be secured from the others. If the existed content is uploaded again, it gives deduplication and user can view his/heruploaded data in the cloud by using secret key provided by the data owner. This project allowsthe multi users to upload and stores their data in the cloud.

II. 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.XSong, "Provable data possession at untrusted stores," in ACM Conference on Computer and Communications Security, 2007, pp. 598–609.

[3] A. 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. 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.