Copyright Work Details

Title: DecenDS – Decentralized Storage System

1. Preface

Decentralized data storage represents a rudimentary shift in the efficiency and economics of enormous-scale storage. Eliminating centralized control allows users to store and share data without relying or trusting on a third-party storage provider. Decentralization mitigates the risk of knowledge failures and outages while simultaneously increasing the security and privacy of object storage. It also allows economic processes to optimize for less expensive storage at a greater rate than any single provider could afford. Even Though there are some ways to build such a system, there are some specific responsibilities any given implementation should address. We introduce a Plug-n-Play framework for considering these responsibilities and for building our distributed storage network. Additionally, we'll describe an initial concrete implementation for the entire framework.

2. Objectives of the proposed work:

1. To enable easy use of Decentralized Data Storage
2. To create one-stop solution Renter and user to share and use data storage effectively.
3. To Provide Easy-to-Use and light weight solution that can even work on mobile devices.

3. Concept Deployed

Decentralized Storage System

The decentralized storage system is a horizontally scalable object store that distributes and stores encrypted data shards across a global network of nodes. The system is designed with modular components that have specific tasks, ensuring robustness, performance, reliability, and economy compared to traditional centralized cloud storage solutions. The decentralized architecture aligns naturally with the decentralized architecture of the Internet, providing better privacy and security. Here, we intend on creating android application to rent out a space on android device to decentralized network for which the will be paid in crypto currency. Below are few roadblocks and proposed method to overcome them.

To ensure rich access management features, each file is encrypted with a unique key, rather than using a single key for all files. This enables users to share access to specific files while maintaining encryption details for other files. The metadata regarding the encryption, along with other metadata about the file, such as its path, is stored securely and reliably in a metadata storage system. The metadata is encrypted using a hierarchical encryption scheme based on BIP32, allowing for subtree sharing without sharing the parent nodes and for sharing some files without sharing others.

AES: Advanced Encryption Standard, is a symmetric encryption algorithm used for encrypting and decrypting data. AES works by taking a block of plaintext and applying a series of mathematical operations to it to produce a block of ciphertext. The algorithm uses a fixed block size of 128 bits and supports key sizes of 128, 192, or 256 bits.

AES will be used in our system to encrypt keys to access files using CID such that files cannot be even accessed by creator of system nor anyone else except intended user.

Sharding:

Data loss is an ever-present risk in any distributed storage system. While there are many potential causes for file loss, storage node churn (storage nodes joining and leaving the network) is the largest leading risk by a significant degree compared to other causes. Network session time in many real world systems range from hours to mere minutes. While there are many other ways data might get lost, such as corruption, malicious behavior, bad hardware, software error, or user initiated space reclamation, these issues are less serious than full node churn. We expect node churn to be the dominant cause of data loss in our network.

Distribution:

Client : A user or application that will upload or download data from the network.

IPFS : A publicly available interplanetery file system will be used to host the files on network. IPFS (InterPlanetary File System) is a distributed file system that aims to create a global, peer-to-peer network for storing and sharing files in a decentralized and efficient manner. It uses content-addressed hyperlinks to create a permanent, tamper-evident, and cryptographically verified record of each file, and it is designed to enable fast and reliable distribution of large files with minimal bandwidth usage. IPFS is an open-source project and is being developed by a ıunity of developers around the world, with applications in areas such as content ɔution, version control, and decentralized web applications.

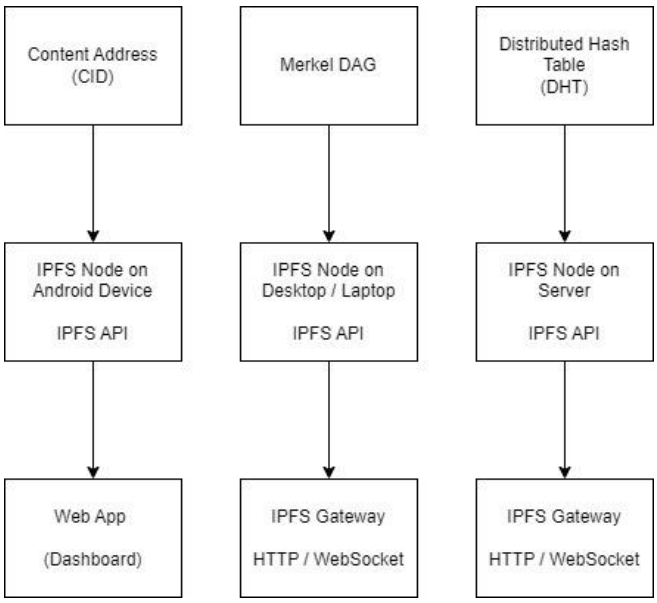

Figure 1 IPFS Architecture

Dashboard:

Easy to use web-app will be developed in order to provide ease of usage, because even state-of-the-art systems will be rendered useless if they are difficult to use. Thus Easy to use dashbord will be controlling all the features such as file upload, file download, statistics management and payment checkout for renter.

Owners and Authors of this work are:

1. Ms. Ayushi Nandeshwar
2. Ms. Shivyani Rathod
3. Mr. Swapnil Londhe
4. Mr. Yash Deshmukh
5. Mrs. Deepali Mahesh Gohil