**[Designing Dropbox Let's design a file hosting service like Dropbox or Google Drive. Cloud file storage enables users to store their data on remote servers. Usually, these servers are maintained by cloud storage providers and made available to users over a](https://www.evernote.com/shard/s395/nl/71011483/87343f87-0934-4789-8e37-fe0e3e194fd6)Designing Dropbox (Concepts are Isolated)**

Let's design a file hosting service like Dropbox or Google Drive. Cloud file storage enables users to store their data on remote servers. Usually, these servers are maintained by cloud storage providers and made available to users over a network (typically through the Internet). Users pay for their cloud data storage on a monthly basis.  Similar Services: OneDrive, Google Drive Difficulty Level: Medium

**1. Why Cloud Storage?**

Cloud file storage services have become very popular recently a**s they simplify the storage and exchange of digital resources among multiple devices**. The shift from using single personal computers to using multiple devices with different platforms and operating systems such as smartphones and tablets each with portable access from various geographical locations at any time, is believed to be accountable for the huge popularity of cloud storage services. Following are some of the top benefits of such services:

**Availability:** The motto of cloud storage services is to **have data availability anywhere, anytime. Users can access their files/photos from any device whenever and wherever they like.**

**Reliability and Durability:** Another benefit of cloud storage is that it offers 100% reliability and durability of data. **Cloud storage ensures that users will never lose their data by keeping multiple copies of the data stored on different geographically located servers.**

**Scalability:** Users will never have to worry about getting out of storage space. With cloud storage you have unlimited storage as long as you are ready to pay for it.

**Why users won't  have to worry about getting out of storage space.**

**How does cloud storage ensures space never runs out.**

**They keep large amount of space reserved.**

If you haven’t used [dropbox.com](http://dropbox.com/) before, we would highly recommend creating an account there and uploading/editing a file and also going through the different options their service offers. This will help you a lot in understanding this chapter.

**2. Requirements and Goals of the System**

💡 **You should always clarify requirements at the beginning of the interview. Be sure to ask questions to find the exact scope of the system that the interviewer has in mind.**

What do we wish to achieve from a Cloud Storage system? Here are the top-level requirements for our system:

1. Users should be able to upload and download their files/photos from any device.
2. Users should be able to share files or folders with other users.
3. Our service should support automatic synchronization between devices, i.e., after updating a file on one device, it should get synchronized on all devices.
4. The system should support storing large files up to a GB.
5. ACID-ity is required. Atomicity, Consistency, Isolation and Durability of all file operations should be guaranteed
6. **What is in-depth meaning of ACID on file operations..**
7. Our system should support offline editing. **Users should be able to add/delete/modify files while offline**, and **as soon as they come online, all their changes should be synced to the remote servers and other online devices.**

**Extended Requirements**

* The system should support snapshotting of the data, so that users can go back to any version of the files.

**Data snapshotting - maintaining file versions implementation. Data deduplication will apply here.  hbase or cassandra for storing metadata.**

**Need consistency - hbase should be ideal. Maintain file versions by storing metadata as compound entities.**

**3. Some Design Consideration**

* **We should expect huge read and write volumes.**
* **Read to write ratio is expected to be nearly the same.**
* Internally, **files can be stored in small parts or chunks (say 4MB); this can provide a lot of benefits i.e.** **all failed operations shall only be retried for smaller parts of a file.** **If a user fails to upload a file, then only the failing chunk will be retried.**
* **How will amazon s3 buckets look like when storing in amazon s3.**
* **Another advantage can be large number of files can be uploaded to google cloud/s3 in parallel, faster uploads.**
* We can **reduce the amount of data exchange by transferring updated chunks only**.
* By removing duplicate chunks, we can save storage space and bandwidth usage.
* Keeping a local copy of the metadata (file name, size, etc.) with the client can save us a lot of round trips to the server.
* Metadata - **url of file chunks on amazon s3, this metadata is kept on local filesystem as well, to avoid fetching this information from remote database.**
* **For small changes, clients can intelligently upload the diffs instead of the whole chunk.**

**what if changes are split in two chunks, both chunks will be reuploaded.**

**chunk itself is stored  in small hashes, upload parts of chunk whose hash does not match.**

**Merkle tree useful in this scenario..??**

**4. Capacity Estimation and Constraints**

* Let’s assume that we have 500M total users, and 100M daily active users (DAU).
* Let’s assume that on average **each user connects from three different devices.**
* On average if a **user has 200 files/photos, we will have 100 billion total files.**
* Let’s assume that **average file size is 100KB, this would give us ten petabytes of total storage.**

100B \* 100KB => 10PB

* Let’s also assume that we will have one million active connections per minute.

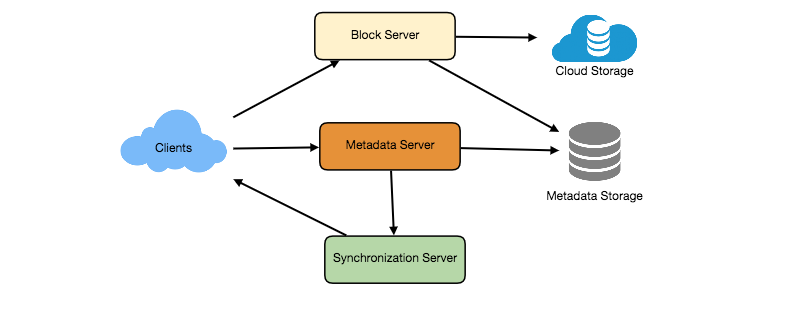
**One million users are active sending requests to the load balancer.**

**5. High Level Design**

The user will specify a folder as the workspace on their device. **Any file/photo/folder placed in this folder will be uploaded to the cloud, and whenever a file is modified or deleted, it will be reflected in the same way in the cloud storage**. The user can specify similar workspaces on all their devices and any modification done on one device will be propagated to all other devices to have the same view of the workspace everywhere.

At a high level, we need to store files and their metadata information like File Name, File Size, Directory, etc., and who this file is shared with. So, we need some servers that can help the clients to upload/download files to Cloud Storage and **some servers that can facilitate updating metadata about files and users. We also need some mechanism to notify all clients whenever an update happens so they can synchronize their files.**

As shown in the diagram below, Block servers will work with the clients to upload/download files from cloud storage and **Metadata servers will keep metadata of files updated in a SQL or NoSQL database.** **Synchronization servers will handle the workflow of notifying all clients about different changes for synchronization.**



                                                                                  High level design for Dropbox

**Block server connecting supplying information to  cloud storage and metadata storage (file block hashes) (retried chunks in case of failure to upload)**

**6. Component Design**

Let’s go through the major components of our system one by one:

**a. Client**

The Client Application monitors the workspace folder on the user’s machine and syncs all files/folders in it with the remote Cloud Storage. The client application will work with the storage servers to upload, download, and modify actual files to backend Cloud Storage. The client also interacts with the remote Synchronization Service to handle any file metadata updates, e.g., change in the file name, size, modification date, etc.

Here are some of the essential operations for the client:

1. Upload and download files.
2. Detect file changes in the workspace folder.
3. **Handle conflict due to offline or concurrent updates.** **(Atomicity??) (multiple users writing to same file resulting in conflict with local copy of metadata , offline update causing conflict with local copy of  metadata)**

**How do we handle file transfer efficiently?** As mentioned above, we can break each file into smaller chunks so that we transfer only those chunks that are modified and not the whole file. Let’s say we divide each **file into fixed sizes of 4MB chunks**. We can statically calculate what could be an optimal chunk size based on 1) **Storage devices we use in the cloud** to optimize space utilization and input/output operations per second (IOPS) 2) Network bandwidth 3) Average file size in the storage etc. **In our metadata, we should also keep a record of each file and the chunks that constitute it. (Individual chunk urls, that are uploaded to amazon s3)**

**Should we keep a copy of metadata with Client?** Keeping a local copy of metadata not only enable us to do offline updates but also saves a lot of round trips to update remote metadata.

**Metadata changes communicated to synchronization server which updates remote database and then updates are written to response queue.**

**How can clients efficiently listen to changes happening with other clients?** One solution could be that the clients periodically check with the server if there are any changes. The problem with this approach is that we will have a delay in reflecting changes locally as clients will be checking for changes periodically compared to a server notifying whenever there is some change. If the client frequently checks the server for changes, it will not only be wasting bandwidth, as the server has to return an empty response most of the time, but will also be keeping the server busy. Pulling information in this manner is not scalable.

A solution to the above problem could be to usewa HTTP long polling. **With long polling the client requests information from the server with the expectation that the server may not respond immediately. If the server has no new data for the client when the poll is received, instead of sending an empty response,** the server holds the request open and waits for response information to become available. Once it does have new information, the server immediately sends an HTTP/S response to the client, completing the open HTTP/S Request. Upon receipt of the server response, the client can immediately issue another server request for future updates.

**Maintains a long poll with  notification server, in case of any update in response queue, clients poll response queue for messages and messages/updates are evicted on poll from queue. (Eviction is good as it helps on clearing queue of messages which are not required otherwise it will have to be dequeued periodically and there won't be optimium space utilization in queue (unnecessary messages remaining in queue which are not required)(Why kafka can't be used as message queueing service  - log retention ?? + too many topics (topics should be broad / generic otherwsie there will be too many topics)**

Based on the above considerations, we can divide our client into following four parts:

I. **Internal Metadata Database** w**ill keep track of all the files, chunks, their versions, and their location in the file system.**

**chunks + differences - mapped to versions**

II. **Chunker** will split the files into smaller pieces called chunks. It will also be responsible for 1)reconstructing a file from its chunks. Our 2) chunking algorithm will detect the parts of the files that have been modified by the user and only transfer those parts to the Cloud Storage; this will save us bandwidth and synchronization time.

III. **Watcher** will monitor the local workspace folders and notify the Indexer (discussed below) of any action performed by the users, e.g. when users create, delete, or update files or folders. Watcher also listens to any changes happening on other clients that are broadcasted by Synchronization service.

**Will generate events corresponding to different actions**

**Watcher maintains a long poll connection with the synchronization service, and get notified of events, data written to response queue.**

IV. **Indexer** will process the events received from the Watcher and (**local software/service on client to update internal metadata database**) update the internal metadata database with information about the chunks of the modified files. Once the chunks are **successfully submitted/downloaded to the Cloud Storage, the Indexer will communicate with the remote Synchronization Service**

**(messages are written in request queue)(microservice which polls request queue and updates remote metadata database, can do the job of writing response data to response queue as well )** **to broadcast changes to other clients and update remote metadata database**.

Graphical user interface, application

Description automatically generated

**WHow should clients handle slow servers?** **Clients should exponentially back-off if the server is busy/not-responding. Meaning, if a server is too slow to respond, clients should delay their retries and this delay should increase exponentially.**

**Should mobile clients sync remote changes immediately?** Unlike desktop or web clients, **mobile clients usually sync on demand (when users opens file on a mobile device)to save user’s bandwidth and space.(there is always resource constraint on mobile device in terms of bandwith, number of connections which can remain open)**

**(long poll is not advisable on resource constrained devices)**

**b. Metadata Database**

The Metadata Database is responsible for maintaining the versioning and metadata information about files/chunks, users, and workspaces. The Metadata Database can be a relational database such as MySQL, or a NoSQL database service such as DynamoDB. Regardless of the type of the database, the Synchronization Service **should be able to provide a consistent view of the files using a database (same metadata of a file)(metadata is consistent in cassandra across replicas - different replicas giving inconsistent data view)**, especially if more than one user is working with the same file simultaneously. Since NoSQL data stores do not support ACID properties in favor of scalability and performance, we need to incorporate the support for ACID properties programmatically in the logic of our Synchronization Service in case we opt for this kind of database. However, **using a relational database can simplify the implementation of the Synchronization Service as they natively support ACID properties.**

The metadata Database should be storing information about following objects:

1. Chunks
2. Files
3. User
4. Devices
5. Workspace (sync folders)

**c. Synchronization Service**

The Synchronization Service is the component that processes file updates made by a client and applies these changes to other subscribed clients. It also synchronizes clients’ local databases with the information stored in the remote Metadata DB. The Synchronization Service is the most important part of the system architecture due to its critical role in managing the metadata and synchronizing users’ files. Desktop clients communicate with the Synchronization Service to either obtain updates from the Cloud Storage or send files and updates to the Cloud Storage and, potentially, other users. If a client was offline for a period, it polls the system for new updates as soon as they come online. When the Synchronization Service receives an update request, it checks with the Metadata Database for consistency and then proceeds with the update. Subsequently, a notification is sent to all subscribed users or devices to report the file update.

The Synchronization Service should be designed in such a way that it transmits less data between clients and the Cloud Storage to achieve a better response time. To meet this design goal, the Synchronization Service can employ a differencing algorithm to reduce the amount of the data that needs to be synchronized. Instead of transmitting entire files from clients to the server or vice versa, we can just transmit the difference between two versions of a file. Therefore, only the part of the file that has been changed is transmitted. This also decreases bandwidth consumption and cloud data storage for the end user. As described above, we will be dividing our files into 4MB chunks and will be tranferring modified chunks only. Server and clients can calculate a hash (e.g., SHA-256) to see w22

**(which  chunks need to provided to block server, after applying differencing algorithm, this information is communicated by synchronization service)**

**(other clients will dowlnoad only modified chunks as per differencing algorithm)**

hether to update the local copy of a chunk or not. On the server, if we already have a chunk with a similar hash (even from another user), we don’t need to create another copy, we can use the same chunk. This is discussed in detail later under Data Deduplication.

To be able to provide an efficient and scalable synchronization protocol we can consider using a communication middleware between clients and the Synchronization Service. The messaging middleware should provide scalable message queuing and change notifications to support a high number of clients using pull or push strategies. This way, multiple Synchronization Service instances can receive requests from a global request [Queue](https://en.wikipedia.org/wiki/Message_queue), and the communication middleware will be able to balance its load.

**d. Message Queuing Service**

An important part of our architecture is a messaging middleware that should be able to handle a substantial number of requests. A scalable Message Queuing Service that supports asynchronous message-based communication between clients and the Synchronization Service best fits the requirements of our application. The Message Queuing Service supports asynchronous and loosely coupled message-based communication between distributed components of the system. The Message Queuing Service should be able to efficiently store any number of messages in a highly available, reliable and scalable queue.

The Message Queuing Service will implement two types of queues in our system. The Request Queue is a global queue and all clients will share it. Clients’ requests to update the Metadata Database will be sent to the Request Queue first, from there the Synchronization Service will take it to update metadata. The Response Queues that correspond to individual subscribed clients are responsible for delivering the update messages to each client. Since a message will be deleted from the queue once received by a client, we need to create separate Response Queues for each subscribed client to share update messages.

A picture containing text

Description automatically generated

**Message Queueing Service in Dropbox -  How to implement the same**

**e. sdee Storage**

Cloud/Block Storage stores chunks of files uploaded by the users. Clients directly interact with the storage to send and receive objects from it. Separation of the metadata from storage enables us to use any storage either in the cloud or in-house.

Graphical user interface, application

Description automatically generated

Detailed component design for Dropbox

**7. File Processing Workflow**

The sequence below shows the interaction between the components of the application in a w when **Client A updates a file that is shared with Client B and C, so they should receive the update too. If the other clients are not online at the time of the update, the Message Queuing Service keeps the update notifications in separate response queues for them until they come online later.**

1. Client A uploads chunks to cloud storage.
2. Client A updates metadata and commits changes.
3. Client A gets confirmation and notifications are sent to Clients B and C about the changes.
4. Client **B and C receive metadata changes and download updated chunks (download happens from cache/block server directly)**

**8. Data Deduplication**

Data deduplication is a technique used for eliminating duplicate copies of data to improve storage utilization. It can also be applied to network data transfers to reduce the number of bytes that must be sent. For each new incoming chunk, we can calculate a hash of it and compare that hash with all the hashes of the existing chunks to see if we already have the same chunk present in our storage.

We can implement deduplication in two ways in our system:

**a. Post-process deduplication**

With post-process deduplication, new chunks are first stored on the storage device and later some process analyzes the data looking for duplication. The benefit is that clients will not need to wait for the hash calculation or lookup to complete before storing the data, thereby ensuring that there is no degradation in storage performance. Drawbacks of this approach are 1) We will unnecessarily be storing duplicate data, though for a short time, 2) Duplicate data will be transferred consuming bandwidth.

**b. In-line deduplication**

**Alternatively, deduplication hash calculations can be done in real-time as the clients are entering data on their device. If** our system identifies a chunk that it has already stored, only a reference to the existing chunk will be added in the metadata, rather than a full copy of the chunk. This approach will give us optimal network and storage usage. **(scans chunk table for new chunks added by client, their urls, if new chunks are present, metadata is updated in different devices mobile, desktop and chunks asre downloaded via urls obtained from metadata database)**

**9. Metadata Partitioning**

To scale out metadata DB, we need to partition it so that it can store information about millions of users and billions of files/chunks. We need to come up with a partitioning scheme that would divide and store our data in different DB servers.

**1. Vertical Partitioning:** We can partition our database in such a way that we store tables related to one particular feature on one server. For example, we can store all the user related tables in one database and all files/chunks related tables in another database. Although this approach is straightforward to implement it has some issues:

1. Will we still have scale issues? What if we have trillions of chunks to be stored and our database cannot support storing such a huge number of records? How would we further partition such tables?
2. Joining two tables in two separate databases can cause performance and consistency issues. How frequently do we have to join user and file tables?

**2. Range Based Partitioning:** What if we **store files/chunks in separate partitions based on the first letter of the File Path? In that case, we save all the files starting with the letter ‘A’ in one partition and those that start with the letter ‘B’ into another partition and so on. This approach is called range based partitioning. We can even combine certain** **less frequently occurring letters into one database partition.** **We should come up with this partitioning scheme statically so that we can always store/find a file in a predictable manner.**

The main problem with this approach is that it can lead to unbalanced servers. For example, if we decide to put all files starting with the letter ‘E’ into a DB partition, and later we realize that we have too many files that start with the letter ‘E’, to such an extent that we cannot fit them into one DB partition.

**3. Hash-Based Partitioning:** In this scheme we take a hash of the object we are storing and based on this hash we figure out the DB partition to which this object should go. In our case, we can take the hash of the ‘FileID’ of the File object we are storing to determine the partition the file will be stored. Our hashing function will randomly distribute objects into different partitions, e.g., **our hashing function can always map any ID to a number between [1…256], and this number would be the partition we will store our object.**

**This approach can still lead to overloaded partitions, which can be solved by using**[**Consistent Hashing**](https://www.educative.io/collection/page/5668639101419520/5649050225344512/5709068098338816)**.** **(By adding a node - keys will redistribute instead of  redistributing across all nodes)**

**10. Caching**

We can have two kinds of caches in our system. To deal with hot files/chunks we can introduce a cache for Block storage. We can use an off-the-shelf solution like [Memcached](https://en.wikipedia.org/wiki/Memcached) that can store whole chunks with its respective IDs/Hashes and B**lock servers before hitting Block storage can quickly check if the cache has desired chunk. Based on clients’ usage pattern we can determine how many cache servers we need. A high-end commercial server can have 144GB of memory; one such server can cache 36K chunks.**

**Which cache replacement policy would best fit our needs?** When the cache is full, and we want to replace a chunk with a newer/hotter chunk, how would we choose? Least Recently Used (LRU) can be a reasonable policy for our system. Under this policy, we discard the least recently used chunk first. Load Similarly, we can have a cache for Metadata DB.

**11. Load Balancer (LB)**

We can add the Load balancing layer at two places in our system: 1) Between Clients and Block servers and 2) Between Clients and Metadata servers. Initially, a simple Round Robin approach can be adopted that distributes incoming requests equally among backend servers. This LB is simple to implement and does not introduce any overhead. **Another benefit of this approach (round robin) is if a server is dead, LB will take it out of the rotation and will stop sending any traffic to it**. A problem with Round Robin LB is, it won’t take server load into consideration. If a server is overloaded or slow, the LB will not stop sending new requests to that server. To handle this, a more intelligent LB solution can be placed that periodically queries backend server about their load and adjusts traffic based on that.

**12. Security, Permissions and File Sharing**

One of the primary concerns users will have while storing their files in the cloud is the privacy and security of their data, especially since in our system users can share their files with other users or even make them public to share it with everyone. To handle this, we will be storing the permissions of each file in our metadata DB to reflect what files are visible or modifiable by any user.

**metadata contains file permissions + metadataDB file chunks information**

|  |  |
| --- | --- |
|  |  |
|  |  |

**Multithreaded Batch Upload of  Chunks - Chunker**

Drop box long poll architecture Analogous-

For receiving song published

------------------------------------------------

public static void main(String[] args) {

        ConfigurableApplicationContext ctx = SpringApplication.run(Application.class, args);

        AmazonSQS sqs = ctx.getBean(AmazonSQS.class);

        AmazonCloudSearchDomainClient cloudSearchDomainClient = ctx.getBean(AmazonCloudSearchDomainClient.class);

        ExecutorService executorService = Executors.newFixedThreadPool(PARALLEL\_WORKER\_THREADS);

        final String queueUrl = sqs.getQueueUrl(QUEUE\_NAME).getQueueUrl();

        executorService.submit(() -> {

            while (true) {

                consumeMessagesFromQueue(queueUrl, sqs, cloudSearchDomainClient);

            }

        });

    }

    private static void consumeMessagesFromQueue(final String queueUrl, final AmazonSQS sqs, final AmazonCloudSearchDomainClient cloudSearchDomainClient){

        ReceiveMessageRequest receiveMessageRequest = new ReceiveMessageRequest()

                .withQueueUrl(queueUrl)

                .withWaitTimeSeconds(LONG\_POLLING\_INTERVAL\_SECONDS);

        List<Message> messages = sqs.receiveMessage(receiveMessageRequest).getMessages();

        System.out.println("Messages received: " + messages.size());

        messages.forEach(message -> {

            try {

                System.out.println("Message: " + message.getBody());

                ObjectMapper mapper = new ObjectMapper();

                TypeReference<HashMap<String, String>> typeRef

                        = new TypeReference<HashMap<String, String>>() {};

                Map<String, String> map = mapper.readValue(message.getBody(), typeRef);

                final String songID = map.get("id");

                final String documentsContent = String.format(BATCH\_OPERATION\_TEMPLATE, songID, message.getBody());

                System.out.println("Batch: " + documentsContent);

                UploadDocumentsRequest request = new UploadDocumentsRequest();

                request.setContentType(ContentType.Applicationjson);

                request.setDocuments(new StringInputStream(documentsContent));

                request.setContentLength((long) documentsContent.getBytes().length);

                cloudSearchDomainClient.uploadDocuments(request);

            } catch (IOException e) {

                throw new RuntimeException(e);

            }

            sqs.deleteMessage(new DeleteMessageRequest(queueUrl, message.getReceiptHandle()));

        });

    }

}

For writing to sqs

----------------------------

public void onSongPublished(final Song newSong) {

    final SendMessageRequest messageRequest =

            new SendMessageRequest(queueName, newSong.toJson());

    sqsClient.sendMessage(messageRequest);

}

<https://docs.aws.amazon.com/AWSSimpleQueueService/latest/SQSDeveloperGuide/sqs-short-and-long-polling.html>