A Measurement Based Comparison of Centralized and Decentralized Storage Services

Akshay Raghavan
raghavan9@wisc.edu
University of Wisconsin-Madison

Dante Smith
dsmith67@wisc.edu
University of Wisconsin-Madison

Abstract:

The internet is undergoing a revolution - centralized services are being replaced by distributed and peer to peer alternatives. One such service that is becoming prominent today is the data storage network. Decentralized storage eliminates middlemen to provide cheaper and more private storing of data. This paper tries to analyze if there are actually merits to using or migrating to distributed storage networks such as Internxt and Stroj over popular and proven cloud service providers like Dropbox and Google Drive. Therefore we measure, analyze and compare properties such as performance, reliability, security and cost between centralized and decentralized options to aid users in making informed decisions.

Introduction:

Overview:

We are in an age of content creation and user content is becoming ubiquitous as mobile devices and storage services are becoming widespread and cheaper. Users are constantly looking for cheaper services with capabilities such as security and reliability to store their data. One popular option nowadays is personal cloud storage services provided by organizations like Google, Microsoft, Amazon, etc. When users opt for these services, they store their personal files on the companies' servers and often forgo privacy concerns. Moreover, the big players in the cloud storage arena often dictate prices and customers are forced to comply.

There is an emergent market for decentralized storage that mitigates these issues. When a user file is uploaded to such a network, typically it is encrypted and broken up into multiple pieces often called chunks and stored in numerous nodes. Privacy is inherent as the file is encrypted and distributed to different providers. Any provider with spare space can sign up with such a network, providing an open market system where pricing is determined by demand and supply. This ensures the best possible price for the customers.

As we can see, the distributed P2P file storage seems to be an appealing alternative to personal cloud storage services but important questions need to be addressed as to its performance and reliability. Hence in this paper, we try to quantify these properties and compare the services provided by decentralized and centralized network storage providers.

Research Problem:

To conduct a quantitative comparison between centralized and decentralized data storage networks with regards to performance, reliability, cost, and security.

Related Work:

Internxt: Experience what's next [18]

The Internxt whitepaper elaborates on the objective of creating a decentralized internet by developing decentralized applications such as Internxt Drive, Internxt Mail, and Internxt photos disrupting the status quo that is the age of cloud services like

Google Drive and Dropbox. Internxt achieves this by designing an efficient underlying P2P network called the XCore that enables users to sell their surplus resources to others looking to host data more privately and securely. The network rewards users who share their resources with INXT tokens providing a financial motive to adopt and remain in the network.

A file is encrypted, sharded, and distributed to multiple nodes when uploaded to the network thus ensuring inherent security and privacy. The network contains two main agents - the bridge and the hosts. Like Napster, the bridge tracks the list of active hosts with the amount of shared resources. Thus, it plays a vital role in load balancing a dynamic system of hosts by deciding the number and destination of chunks. The decentralized network also establishes a proof of availability to associate the shards with their data owner. When retrieving a file from the Internxt network, the corresponding chunks are fetched, combined, and decrypted before sending to the data owner.

Storj: A Decentralized Cloud Storage Network Framework [9]

The Storj white paper describes in detail the importance of having a decentralized storage solution, the challenges and constraints that Storj's design must work within, and how those challenges are resolved in the design of Storj. The paper breaks down Storj into its separate components, including the storage nodes themselves, the peer-to-peer communication and discovery, redundancy, metadata, encryption, audits and host reputation, data repair, and payments.

In Storj, files are broken into segments upon upload. Each segment represents an erasure share since Storj uses erasure codes to handle redundancy. Each of the segments is sent to a participating node in the system. Data is encrypted before it leaves the client's computer and remains encrypted when on the remote storage node, so the storage node is not aware of the contents of the information it stores. The peers in the network communicate with each other to find segments of a file using a distributed hash table, and lookup of the segments is sped up using a decentralized caching service.

Benchmarking Personal Cloud Storage [4]

The paper discusses the methodology for benchmarking performance and identifying the architecture and capabilities of personal cloud storage services such as Google Drive, Dropbox, and Amazon Cloud Drive. The authors identify the data center placement, capabilities like compression, deduplication, and delta encoding, as well as performance metrics such as start-up time, duration, and network overhead by active measurements of different workloads. The paper provided a comprehensive comparison of various centralized storage services and inspired our research.

Storage management and caching in PAST, a large-scale, persistent peer-to-peer storage utility [1]

The authors present a self-organizing overlay network of storage nodes called PAST for distributed peer-to-peer persistent storage of user data. PAST uses Reed-Solomon codes for redundancy, a caching mechanism for improved performance, smart cards for security, and statistical assignment of files to nodes for efficient load balancing. The paper provided insights into how P2P storage works and the metrics significant in comparing decentralized storage options.

Bitcoin: A Peer-to-Peer Electronic Cash System [17]

This paper was essential to learn how contemporary block-chains work, achieve

distributed consensus using proof-of-work, and validate transactions in a trustless environment. Studying how Bitcoin's blockchain worked gave us a foundation to understand other blockchains like the ones used by Internxt and Storj.

Description of Methods & Techniques:

Selecting storage options to study:

To compare different internet storage options, we measured and analyzed file transfers to the following providers:
Centralized services: Google Drive and Dropbox
Decentralized services: Storj and Internxt

We chose Google Drive and Dropbox because of their efficiency and popularity in the personal cloud storage space. The user-friendly interface, eloquent documentation, and cost persuaded us to proceed with Storj and Internxt. Internxt and Storj provide 2 GB and 150 GB of free storage upon signing up, enabling us to experiment with the production software instead of the testnet.

We also tested the BitTorrent File System (BTFS), but it is technically impossible to upload a file to the BTFS testnet due to code bugs. Uploading to BTFS requires BTT tokens to be converted to sufficient WBTT network tokens, and the conversion API results in a segmentation fault. Experimenting with Siacoin was difficult due to insufficient documentation, prohibitive blockchain synchronization time, and an incomplete testnet system. The Filecoin testnet and documentation were very helpful, but it takes practically hours to successfully upload to the network due to the blockchain consensus algorithm [12]. Also, the network does not allow retrieval of a file before 24 hours of file upload.

The Measurement experiments:

We used the following dataset (Table 1) mimicking current internet storage workloads to measure various metrics for our study. 200 KB was chosen to be a representative file size of a several page long PDF document; 2 MB was a representative of a photo, and 2 GB is a representative file size for a video. We performed each experiment 10 times to avoid statistical noise for all the selected storage options.

Experiment #	Size	Operation
1	200 KB	Upload
2	200 KB	Download
3	2 MB	Upload
4	2 MB	Download
5	2 GB	Upload
6	2 GB	Download

Table 1: Description of experiments

We also developed Python scripts to automate packet capturing and file transfers, eliminate human errors, and extract precise timings.

Description of Data:

We perform active measurement by uploading and downloading files described in Table 1 to collect the following statistics.

- Total upload time
  We calculate the total upload time as the sum of
  - Time before file upload
  - File transfer time

  The time before file upload captures the time for:
  - Location of prospective receivers
  - Encryption
  - Chunking

- Total download time
  The total download time is the sum of
  - Time before file download
  - File transfer time

  The time before file download captures the time for calculation of the location of required file chunks
- Total network overhead
  The total network overhead is the total number of bytes transferred to/from the network to facilitate the required operation, including the actual data, control information, and redundant chunks.
- Number of contacted servers
  This gives insight into the distribution and redundancy mechanism employed by the network.
- The geographic location of servers
  This highlights the availability of network nodes and the efficiency of distribution. We expect the file chunks to be spread closer to the data owner for quicker retrieval.

We also discuss about other factors listed below:

- Security
  - Data encryption on transit and at rest
  - Encryption mechanism
  - Malware/Virus detection
- Privacy
  - User information collected by the service
  - Physical location and possibility of user content access
- Sharding and redundancy
  - Size of file chunks
  - Number of redundant copies
  - Redundancy mechanism
- Cost

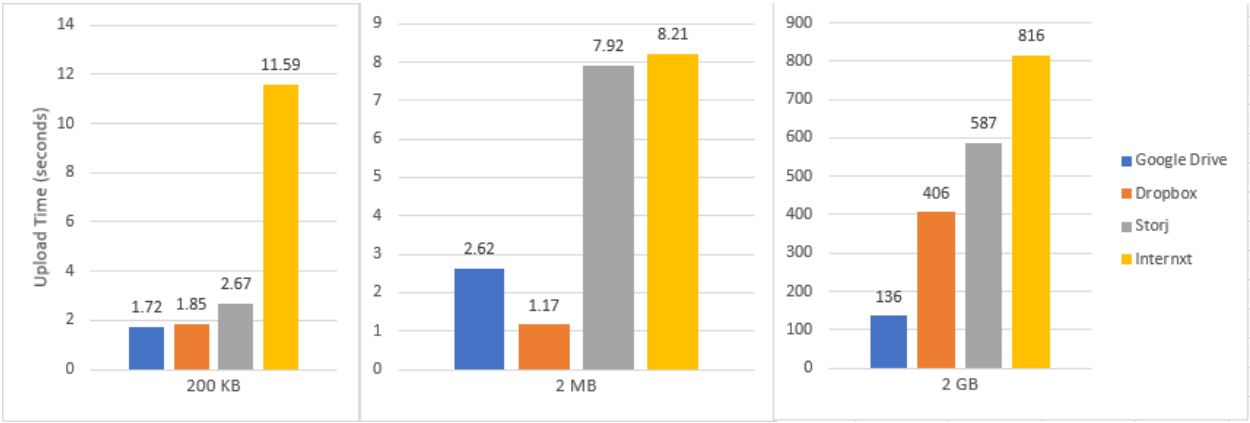

Figure 1: Time to upload files (in seconds) once the connections are established for each of the 4 services.

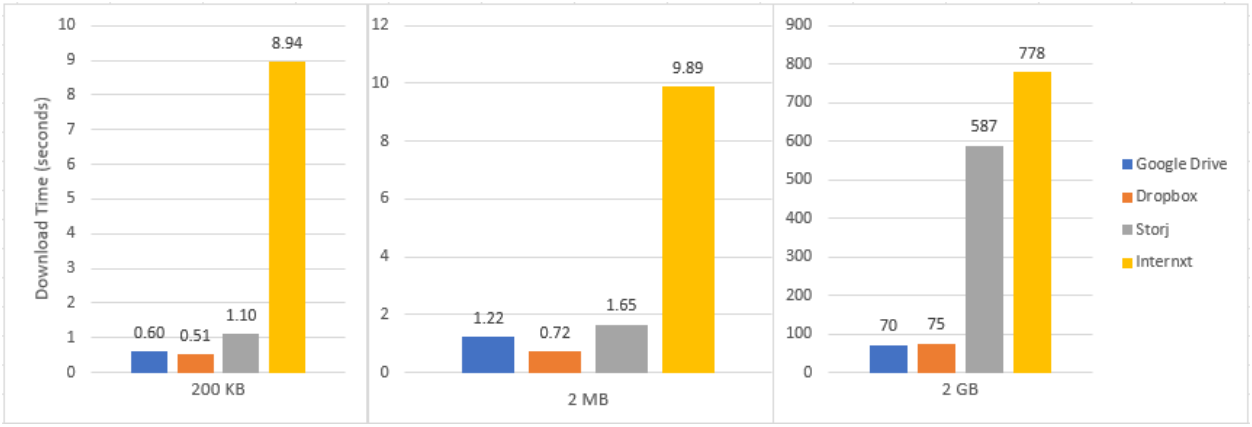

Figure 2: Time to upload files (in seconds) once the connections are established for each of the 4 services.

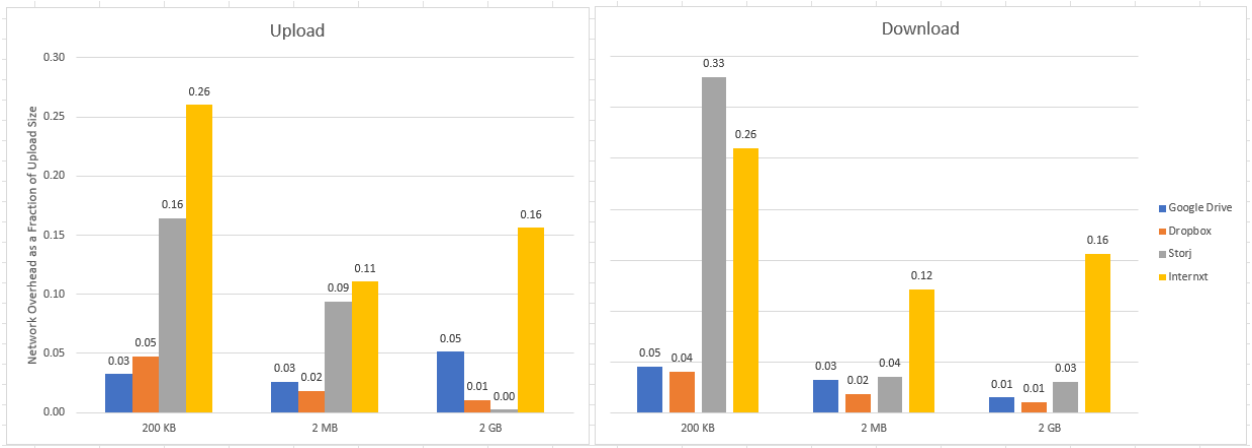

Figure 3: Extra data (overhead) sent over the network when uploading and downloading files from each of the 4 services tested.

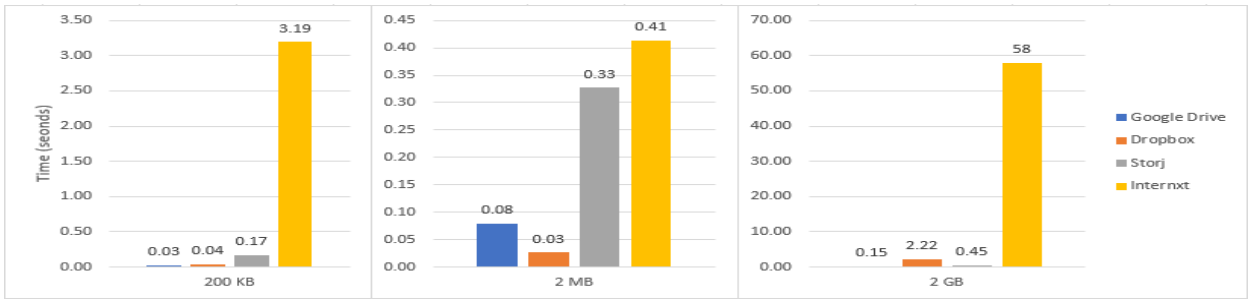

Figure 4 : Time taken to establish connections when uploading files.

Figure 5 : Time taken to establish connections when downloading files.

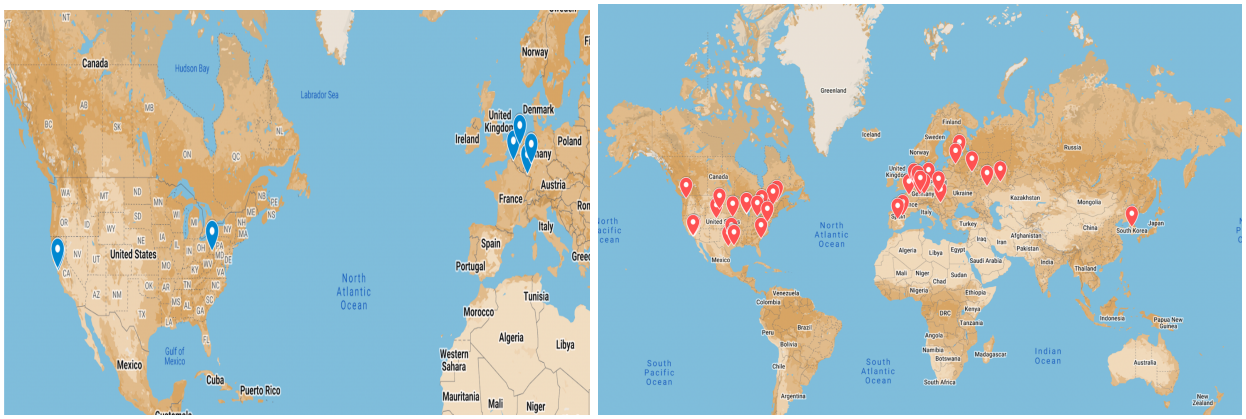

Figure 6: Geolocations of data uploaded to decentralized services. Internxt on the left, Storj on the right.

Property	Google Drive	Dropbox	Internxt	Storj	Winner
Upload time (seconds)	2.62	1.17	8.21	7.92	Dropbox
Download time (seconds)	1.22	0.72	9.89	1.65	Dropbox
Network overhead (Fraction)	0.03	0.02	0.115	0.065	Dropbox
Cost ($/TB/month)	4.99	4.99	4.49	4	Stroj

Table 2: Summary of quantitative results for the 2MB workload for the considered storage services.

Evaluation and results :

Following the dataset and techniques mentioned in the previous section, we conducted active measurements by uploading files of different sizes and extracting useful information from the captured packet traces. The results are graphically displayed in Figures 1 - 6. Figure 1 shows that the centralized storage services are much faster in terms of upload time than the decentralized options. Figure 2 shows that the centralized options again are better in download speed, although for smaller files, Storj is actually performing close to the centralized options. Figure 3 shows that there is generally more overhead data sent over the network when using the decentralized storage options. Figures 4 and 5 shows that there is more time taken to establish the necessary connections for upload and download when using decentralized options, and notably Internxt takes much longer. Finally Figure 6 shows how the geographic distribution of upload files is much more widespread with Storj than with Internxt. We cannot see the distribution of data on Google Drive or Dropbox after sending to the edge server, so that is why geolocations of data stored using those services are not shown.

In summary, Google Drive and Dropbox perform incredibly well when it comes to latency, network overhead, and startup times. Decentralized storage services encrypt, shard, replicate and distribute the file to various storage nodes and are expected to take longer than their centralized counterparts. As expected, Internxt has longer startup times, and surprisingly Storj starts up very quickly.

Storj replicates data chunks and distributes them to a large number of nodes (approx. 100) when compared to Internxt (approx. 12). Moreover, out of the 12 storage nodes, most of them belong to the Internxt organization. When uploading files to Storj, there were approximately 100 TCP connections established, compared to approximately 40 TCP connections established when downloading files. This difference is most likely due to the erasure code redundancy that Storj uses and it is possible that the k/n ratio used to encode the test files is actually the 40/100 we observe when testing. This allows Storj to select the 40 fastest peers to retrieve the file segments and might contribute to the low latency as compared with Internxt. We can therefore conclude that Storj provides better redundancy and file durability compared to Internxt.

Redundancy:

Redundancy is important for storage services to provide user data durability and disaster recovery. We discuss how redundancy is achieved in various storage options below:

Google Drive:

Google Drive breaks data into subfile chunks as large as a gigabyte and calculates a checksum for data integrity before storage. Drive encrypts the shards at the storage level with a unique data encryption key (DEK) [13], replicates them using erasure coding for backup and disaster recovery, and distributes them across the storage system to achieve 99.999999999% durability [14] (the famous eleven 9s). The data chunks are also named randomly to make them unreadable to the human eye. An attacker who wants to access customer data would need to know and be able to access all of the storage chunks that correspond to the data and all of the encryption keys that correspond to the chunks. In addition to storage system-level encryption, data is also encrypted using a separate device-level AES-256 key before storing it in hard disk and solid state drives. The number of file chunks used by the Colossus File System, the successor to the Google file system used by Drive, could not be found in any official Google documentation.

Dropbox:

Dropbox breaks files into chunks of up to 4MB and uses a SHA256 hash value to identify the chunks. This hash value is part of the set of metadata that describes a chunk. The Dropbox architecture at a high level can be divided among control servers that store the metadata to locate files upon request, and the data storage servers that store the chunk. Dropbox owns the control servers, and Amazon EC2/S3 are used for the data storage servers. Redundant copies of metadata are stored across servers within a data center in an N+2 availability model. During outage events, users can still access the latest copy of their synced files from their Dropbox folder on their computer. Changes made during the outage will not be lost once connectivity is restored

Internxt:

Internxt encrypts user data, splits into chunks, and distributes it across numerous Internxt P2P network nodes. It also uses SHA-256 for integrity and proof of availability to verify the existence of user data. Although the white paper describes the chunk size to be 2MB, there is limited information on the number of replicas and the redundancy mechanism used.

Storj:

Storj is built to be resilient to the storage failures that affect centralized services, and to the phenomenon of node churn. This is where participating nodes in the network stop participating, whether due to hardware failures or simply withdrawing from the system. Storj uses redundancy thresholds, and when the amount of redundancy of a file goes below the threshold, then the necessary data for the missing pieces is regenerated and replaced. The key element of Storj's redundancy mechanism are erasure codes, where a block of data that is s bytes can be broken into n erasure shares and only any k of those erasure shares are needed to recover the original data. Each of the erasure shares is approximately s/k bytes large. During upload, files are encoded to a higher than necessary k/n ratio. The extra redundancy allows for lookups from the fastest peers when downloading files.

Privacy:

Privacy becomes a huge concern when using public cloud storage due to the following reasons:

- Data resides physically in the storage providers' data centers
- Collection of personal user information
- Sharing data or content with third parties for advertising purposes
- Accessing private user content when required by law

Decentralized storage options typically don't suffer from these limitations. This section elaborates on the privacy considerations of the four chosen storage providers.

Google Drive:

Google Drive collects vast amounts of user data for various reasons. Below is a non-exhaustive list of collected information as reported by Google [15]

- Name
- Email address
- Phone number
- File contents (including content inside Google Docs and Sheets to provide spam filtering and virus/malware detection).
- Usage statistics (to improve performance, reliability, and security).
- Purchase histories on Google Drive
- Location data (for geographic relevance and anomaly detection).

Google Drive reportedly does not share user information and content with third parties for advertisements. Google also mentions its obligation to reveal consumer content and data when required by the law. These problems could be overcome (to a certain extent) by

- Encrypting content before uploading to Google Drive
- Password protecting documents
- Limiting data shared with Google using the privacy settings in My Account tab.

Dropbox:

Dropbox does have access to user files, but limits employee access to those systems. There is a firewall to limit access to only authorized administrators. Dropbox also keeps records of access requests to data centers and production servers. Dropbox collects the following information on its users [7]:

- Name
- Email Address
- Phone Number
- Payment Information (i.e. credit card on file)
- User's physical address
- File usage/collaborators/sizes
- How users share/edit/view/create/move files

Internxt:

Internxt is fundamentally more private compared to public clouds due to its design. As user data is encrypted, sharded, and stored at numerous network nodes, accessing user content is impossible. Internxt uses a Bridge to store

chunk-node associations. According to the whitepaper, the bridge seems to be a centralized agent (like Napster) instead of using a distributed data store like Chord [20] and therefore raises questions about the actual privacy and security of data.

Storj [9]:

Storj provides a level of privacy due to its decentralized nature. Peers on a network lookup where information is stored on a distributed hash table. Each peer is unaware of the file or the metadata for the file that they store on the node. There is little incentive for malicious actors to search for data on Storj because the files are segmented across dozens of nodes and the segments are HMAC-SHA256 encrypted.

Security:

Security and trust are other user concerns when data is stored in an external system. In this section, we discuss in detail how each service provides security.

Google Drive:

Google Drive takes immense responsibility for preventing attacks and storing user content securely[16]. Drive uses Captchas to prevent misuse and checks for malware, viruses, and phishing attempts in files shared from outside the user organization. Irrespective of the login method (Web, App, API, etc.), Google Drive requires credentials to access content and notifies users upon anomalous logins. The data is encrypted at rest using 128-bit or 256-bit AES keys and uses TLSv1.2 for secure network transmission. This means a random hacker cannot read user content even if they have access. But since Google owns the AES encryption keys, a Google employee can potentially access private user data.

Dropbox [5][8]:

Data in transit is protected using Secure Sockets Layer (SSL)/Transport Layer Security (TLS), which will create a secure tunnel protected by 128-bit or higher AES encryption. To prevent man-in-the-middle attacks, an authentication of Dropbox front end servers is performed via public certificates held by the client. An encrypted connection is required before the transfer of files to ensure secure delivery to and from Dropbox servers. Data at rest is encrypted using 256-bit AES. Data is fragmented and each block of data is encrypted.

Internxt:

Internxt uses AES256 to encrypt files and SHA256 for data integrity. There is no single point of attack as the files are distributed across the network. Although it seems like Internxt provides appreciable security, there are concerns about the ownership of the Bridge node. If Bridge is a centralized unit owned by Internxt, it becomes vulnerable to attacks and data access by Internxt employees.

Storj:

Data is split into segments across nodes, with each segment representing an erasure share of the file. Each segment will typically have a different encryption key. Data is encrypted before it ever leaves the customer source computer. Storj uses authenticated encryption so that the user can be aware if there is any tampering with their data. Encryption schemes that are supported include AES-GCM and Secretbox ciphers. From experiment results, Storj uses TLSv1.3 for encrypted communication, rather than the TLSv1.2 that other services used.

Cost:

Google Drive [14]:

- Google Drive provides 15GB of free usage for all the users.
- The cheapest individual option is $9.99/month for 2TB storage.

Dropbox [6]:

- Dropbox Basic is free, but users can only store 2 GB
- $9.99/month for 2 TB is the cheapest individual option

Internxt [19]:

- Internxt provides 2GB free data upon signing up to their network.
- The cheapest option in their plan is priced at $8.99/month for 2TB of data storage.

Storj [10]:

- A free account gives users 150 GB per month
- $4/month for a TB if users need more than 150 GB in a month.

The results are summarized in Table 2. When it comes to privacy, security, and durability, Storj seems to be the best option although the centralized options still provide high durability guarantees.

Conclusion:

Internet-based storage is growing tremendously, with numerous centralized and decentralized options that consumers are unaware of. This study exposes the readers to four services - Google Drive, Dropbox, Storj, and Internxt and compares performance, cost, privacy, security, and durability using active measurements. Google Drive and Dropbox perform well in terms of file transfer times and network overhead for different workloads. The decentralized options provide better privacy and security, but there are a few caveats for Internxt. All services have strong file durability guarantees owing to the duplication within the network (either in P2P nodes or in data centers). Storj provides 150GB of free storage upon signup and a reasonable price thereon. If file transfer performance is not a concern, consumers can experiment with decentralized options like Storj to get better privacy, security, and cost.

The research helped us learn about how centralized, decentralized, and P2P storage services operate under the hood. It also helped us appreciate the immense potential of active measurements in understanding networking systems. We also had the opportunity to learn useful Python tools like the subprocess module and gained the experience of using APIs to talk to remote services like Google Drive, Storj, and Dropbox. We also understood how to automate packet capturing and analyze packet traces to extract useful information. Apart from learning the advantages and disadvantages of contemporary storage options, the study also enhanced our writing and research capabilities.

References:

[1] Peter Druschel Anthony Rowstron. 2001. Storage management and caching in PAST, a large-scale, persistent peer-to-peer storage utility. SOSP ’01: Proceedings of the eighteenth ACM symposium on Operating systems principles (Oct. 2001), 188–201. https://doi.org/10.1145/502034.502053

[2] Idilio Drago, Marco Mellia, Maurizio M. Munafo, Anna Sperotto, Ramin Sadre, and Aiko Pras. 2012. Inside dropbox: understanding personal cloud storage services. In Proceedings of the 2012 internet measurement conference. 481–494.

[3] Sanjay Ghemawat, Howard Gobioff, and Shun-Tak Leung. 2003. The Google file system. In Proceedings of the nineteenth ACM symposium on Operating systems principles. 29–43.

[4] Marco Mellia Herman Slatman Idilio Drago, Enrico Bocchi and Aiko Pras. 2013. Benchmarking Personal Cloud Storage. IMC ’13: Proceedings of the 2013 conference on Internet measurement conference (Oct. 2013), 205–212. https://doi.org/10.1145/2504730.2504762

[5] Dropbox Inc. 2022. Dropbox Business: Shared responsibility: Working together to keep your data secure. https://aem.dropbox.com/cms/content/dam/dropbox/www/en-us/business/solutions/solutions/Shared_Responsibility_Guide.pdf
[6] Dropbox Inc. 2022. Dropbox Plans: Secure cloud storage—and so much more. https://www.dropbox.com/plans
[7] Dropbox Inc. 2022. Dropbox Privacy Policy. https://www.dropbox.com/privacy
[8] Dropbox Inc. 2022. How Dropbox keeps your files secure. https://help.dropbox.com/security/how-security-works
[9] Storj Labs Inc. 2018. Storj Whitepaper V3. https://www.storj.io/whitepaper
[10] Storj Labs Inc. 2022. Storj Pricing. https://www.storj.io/pricing
[11] Protocol Labs. 2017. Filecoin: A Decentralized Storage Network. https://filecoin.io/filecoin.pdf
[12] Protocol Labs. 2022. Lotus Docs: Deal States. https://lotus.filecoin.io/tutorials/lotus/store-and-retrieve/store-data/#deal-states
[13] Google LLC. 2022. Default Encryption at rest. https://cloud.google.com/docs/security/encryption/default-encryption
[14] Google LLC. 2022. Google Cloud Storage: Frequently Asked Questions. https://cloud.google.com/storage/docs/faq
[15] Google LLC. 2022. How Drive protects your privacy and keeps you in control. https://support.google.com/drive/answer/10375054?hl=en
[16] Google LLC. 2022. Is Google Drive secure? https://support.google.com/drive/answer/141702?hl=en
[17] Satoshi Nakamoto. 2009. Bitcoin: A Peer-to-Peer Electronic Cash System. https://bitcoin.org/bitcoin.pdf
[18] Internxt Universal Technologies SL. 2018. Internxt: Experience what's next. https://neironix.io/documents/whitepaper/8e5a53c88a24b00efa677ef442c57063.pdf
[19] Internxt Universal Technologies SL. 2022. Internxt: Plans for Individuals. https://internxt.com/pricing
[20] Ion Stoica, Robert Morris, David Karger, M Frans Kaashoek, and Hari Balakrishnan. 2001. Chord: A scalable peer-to-peer lookup service for internet applications. ACM SIGCOMM computer communication review 31, 4 (2001), 149–160.