User Study A - Key

Part I. Build the threat model of the above system using framework A. Fill in the result of applying each step of framework A below.

Step 1: **Start time:** **Finish time:**

List the components in the system:

- Store a file.
- Pay servers for storage periodically.
- Retrieve a file and pay for the service.

List participants:

- Clients.
- Servers.

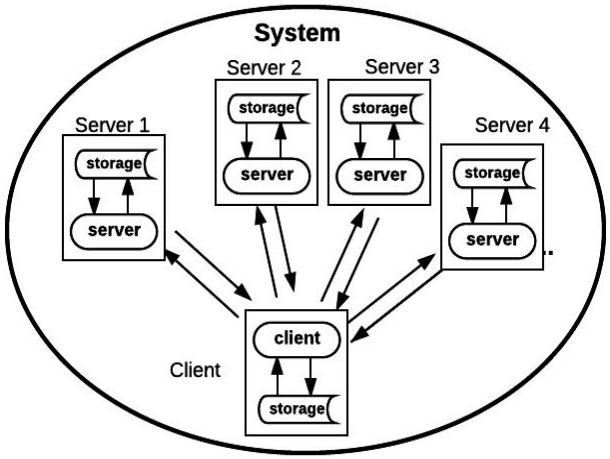
List assets of value:

- Files.
- Payments or currency

Assumptions and external dependencies:

(no need to rewrite them, just read them again)

Draw the DFD (data flow diagram) of the system's components.



The three activities in the system have the same network model, the difference is in the eschanged messages as follows:
- **Store a file:** client and servers exchange file storage requests and file fragments.
- **Rewarding storage:** client and servers exchange proofs of storage and payments periodically.
- **File retrieval:** client sends a retrieval rqeuests, receive file fragments from servers and then sends them payments.

Step 2: **Start time:** **Finish time:**

Possible threats:

- Corruption of files stored: invalid files are stored at the server, or server discards clients files, receive corrupted files, etc.
- Denial of service: interrupt the operation of the system, no one can store or retrieve files, or pay for the service.
- Information disclosure: someone tracks the requests issued by a client and read the content of its files, etc.
- A client obtains correct file retrieval/storage service but pays less or does not pay at all.
- A server obtains payments without doing all the work required to store or retrieve files.

Step 3: **Start time:** **Finish time:**

(The participant is not provided this sheet until later and is asked not to edit earlier pages)

Description of threat scenarios for:

Service theft / file retrieval (client retrieves file without paying)

(1) A client receives correct file fragments but does not pay or send invalid payments.
(2) A client colludes with a server to send a corrupted fragment to avoid paying the servers (or even set his own server and store a corrupted file fragment there).