Presentation #2

Haron Taher
Anthony Vasquez

Project Vision Summary:

Guard-Cloud is a user-friendly web application designed to provide secure, end-to-end encrypted file sharing and editing. By encrypting files both in transit and at rest, Guard-Cloud ensures the highest level of protection for sensitive data. With an intuitive interface and straightforward features, it is easy for users of all backgrounds to securely upload, download, manage, and share files. Everything from drag-and-drop uploads to advanced file management is engineered to be as seamless and efficient as possible.

Beyond its core file operations, Guard-Cloud offers several robust security and administrative features. Decryption of files happens exclusively on the client side, meaning that no unauthorized user (including server administrators) can read file contents without the proper encryption keys.

Overall, Guard-Cloud is an ideal solution for individuals and organizations seeking a simple yet powerful way to protect their confidential files. Its closed system setup option adds an extra layer of control for businesses that prefer to keep their data on a private network, while still offering the flexibility of running on the open web. By combining robust encryption mechanisms with an intuitive design, Guard-Cloud delivers peace of mind and convenience for anyone looking to securely store, share, and manage important files online.

Outline:

- The user accesses the web app from their browser.
- The user is prompted to log in or create an account on initial start up.
- File manager web app presented to the user after logging in.
- The user has the options of uploading files, managing files, downloading files, deleting files, and sharing files.
- If the user wants to upload a file, they can do so from a dialogue box or drag and drop.
    - File is uploaded to the working directory in the file system.
- If the user wants to download a file, they can do so from a dialogue box or context menu.
- If the user wants to delete a file, it is removed from the file system completely.
    - Whole directories can be deleted as well.
- If the user wants to share a file, they must provide the identity of the user(s) to share the file with.
- The user can share whole directories or folders.
- Files in transit between the client and the server are encrypted.
- Files stored on the remote server are encrypted.
- Decryption of files happens on the client.

- The user can view information about files from the web app.
    - Date of creation
    - Date of upload
    - Date last modified
    - File hash (SHA, MD5, etc.)
    - Other information
- The user can manage the properties and locations of files within the file system.
    - Applying tags.
    - Renaming files.
    - Move actions.
    - Copy actions.
        - Copying has the option to keep access permissions from the original file.
- The user can search and filter files by name and properties using the search function.
- Some restrictions apply to file uploads.
    - File size limit.
    - File hash matches known malware.
- If a shared file is deleted, access to the file is lost for all users.
    - This does not apply to copies of the file.
- The server application can be set up as a closed system or on the open web.
    - If the server is closed, it can be only accessed by authorized users on the local network.
- The user can delete their account.
    - On account deletion, all data owned by that account is destroyed.
- Server admins can view account activity and encrypted files in the remote server.
    - Server admins may decrypt files with the associated key, but this activity is not regulated or monitored by the server program, and is therefore not recommended.