Final Year Project Showcase Batch-2019
Year 2023

	Department: Software Engineering Programme: Bachelor of Engineering
1	**Project Idea: (Cloud3 – A secure decentralized cloud storage)** In the age of the Internet, having a secure, decentralized file-sharing and storage system is essential. The idea is to create a web-based system named Cloud3 that maintains the privacy of user data, offers decentralized storage, and enables simple file management over decentralized networks. The solution offers the user an intuitive GUI and API to save his data on IPFS while utilizing various pinning services. Additionally, users are given the option to pin, unpin, and securely share their encrypted files with other users.
2	**Process** Certainly, let's dive into a bit more detail for each of the components and processes mentioned in the system: **Authentication Process:** **Sign Up:** When a user joins the system, they must sign up by providing their public key. The system generates a random nonce and sends it to the user. The user uses their Web3 Wallet to sign the nonce with their private key and sends the signature back to the backend. The backend decrypts the signature using the stored public key and checks it against the stored nonce. If the signature is valid, a new nonce is generated, and stored, and the user is notified of successful sign-up. **Login:** To log in, users provide their public key. The stored nonce is sent to the user, who signs it with their private key and sends the signature back to the backend. Upon successful verification, a new nonce is generated, and the user is logged in. **Key Management Store (KMS):** A browser extension called KMS is used to locally store users' public and private keys securely. Users set up their accounts by creating a strong password and receive a secret recovery key for password recovery. KMS also allows users to generate new key pairs or import existing ones. **File Upload:** After a successful login, users can upload files. The system ensures end-to-end encryption by performing encryption on the client-side using the Advanced Encryption Standard (AES). The AES key for the file is sent to the KMS, which encrypts it using the user's public key. This double encryption ensures that only the user can decrypt the AES key. A random verification ID (UUID) is generated and, along with the encrypted AES key, stored locally. If the user doesn't complete the upload process immediately, they can resume it later using the AES key from their local storage. The encrypted file, encrypted AES key, and additional metadata such as the verification ID and parent folder ID are sent to the backend. The backend uploads the file to the InterPlanetary File System (IPFS) and stores it there. Metadata about the file and activities related to it, like the last modified time and pinning services, are stored in a database. The file's hash (CID - Content Identifier) from IPFS is stored on the blockchain for immutability.

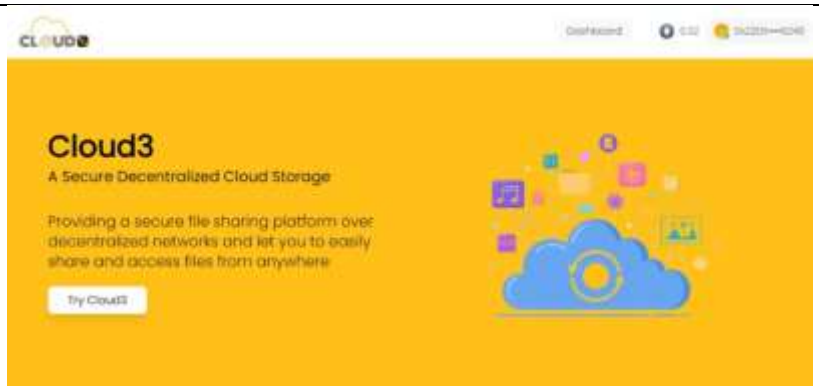
	File View: When a user requests to view a specific file, the system fetches the file's CID from the database. The encrypted AES key associated with the CID is retrieved from the blockchain. Using this key, the system decrypts the file and presents it to the user. **Verification of Non-Verified Files:** If a user fails to complete the upload process and verify their files within 24 hours, the system deletes those unverified files from IPFS and the database. Users are given the option to verify these files within this time frame, ensuring that only verified files are retained. **Share File:** Users can share files with specific recipients of their choice. When a user selects a file to share, the system retrieves the file's CID and the recipient's public key from the database. The encrypted AES key associated with the file is fetched from the blockchain. The system then decrypts this AES key using the user's private key, re-encrypts it with the recipient's public key, and stores this information on the Ethereum Blockchain's smart contract. A notification is sent to the recipient. **Unshare File:** Users can revoke access to shared files by re-encrypting the AES key, but this time excluding the recipient they want to unshare with. This process ensures that files are securely unshared with specific individuals. **Move to Trash:** When a user decides to delete a file, the same unsharing process is followed to revoke access from all shared individuals. The file is then marked as "trashed" in the database, indicating it's in the trash but not yet permanently deleted. **Delete File:** When a user permanently deletes a file from the trash, access is completely revoked. A Boolean field "exists" in the blockchain is set to false, and the entry for the file is removed from the database. Additionally, the file is unpinned from IPFS, ensuring that no one can access it. **Pinning File:** The system integrates various pinning services (e.g., Pinata, Web3.storage, Filebase, NFT.storage, Estuary) for redundancy and higher availability. Users have the option to choose whether they want to pin their files on multiple services, ensuring data availability even if one service experiences downtime.
3	**Outcome** The outcome of cloud3 is in two parts 1. **Cloud3 Website:** The outcome is the most user-friendly website which provides the following features: • The user manages his files himself and no third-party or cloud3 has access to the files of the user. • The system instructs the user to first install the Cloud3-KMS extension before proceeding if it is not installed. • Users sign up and log into the system using web3 wallet with one click functionality.

	• Users can create a folder or upload their files directly in any format. The system encrypts it on frontend. The system keeps the encryption key also in an encrypted format and this is achieved using KMS. • Users can share files with other users in a secure fashion. • Users can revoke shared access to files from other users. • Users can delete files using the unpin functionality of IPFS. • Users can pin files using different pining services like Pinata, web3.storage etc. • Users can access their own and shared files in unencrypted form. • Users can view files and download it • Users can star the files to make them favorites and access them easily. • Users can search the files or folders by their name. • Users can update their username and email. • Users can view the storage details. • Users can view the non-verified files. • Users can view their transaction details such as hash and their status • Users can verify the files within 24 hours of upload, if not verified at the time of upload. **2. Cloud3-KMS** Cloud3-KMS is a browser extension that helps the user to manage his keys. Features provided in the KMS to the users include: • Users can create a new account which requires the user to add his password and then the secret phrase is provided to the user. • Users can import existing accounts by providing the secret phrase. • In case the user forgets the password, they can create a new password by providing the secret phrase. • The secret phrase is revealed when the correct password is provided. • Users can create new keys, which will be generated using the secret phrase • Users can provide their existing keys. • By providing the correct password, the private key for some specific public key is exported
4	**Evidence (Theoretical Basis)** Our project "**Cloud3**" is a center of attraction for all those who are concerned about their data privacy, and immutability. Even though technology is progressing day by day, there are still threats to data privacy. Even if we have large storage platforms such as Google and Microsoft, we are facing data privacy and availability issues because of their centralized approach. Decentralized platforms such as IPFS solves these problems but fails to provide confidentiality as data is stored in unencrypted form. The background study proves that well-known centralized storage Google got attacked in past years and many users became the victims and lost their Gmail credentials. Moreover, these centralized storage platforms do customer marketing by analyzing our activity patterns and data. All this poses a risk to data security and urges the need for a secure decentralized system for storing and sharing data. Cloud3 combines the benefits of decentralization, encryption, and cloud storage where decentralization gives data availability plus immutability, encryption gives confidentiality and the cloud provides remote management and sharing of files. To accomplish our objectives, we have developed a web-based system that allows users to securely store their data on a decentralized platform. For this, we have used blockchain along with IPFS. The files of the users will be stored in the encrypted format on IPFS, while other application data

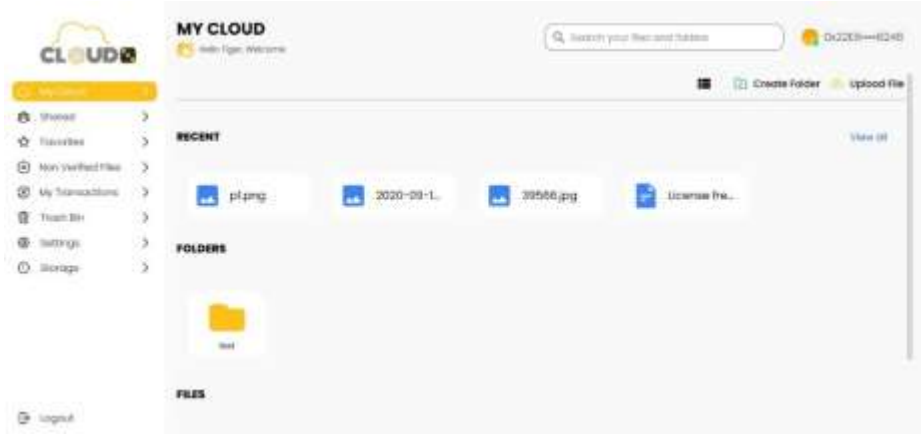
	will be stored on Blockchain, so Cloud3 is both secure and decentralized. In addition, various pinning services have been integrated so that files can be pinned at multiple locations. In this way, data will always be available to users. Our major finding is how to provide maximum transparency to users so that no unencrypted file is stored anywhere and ensures no third-party intervention. We have provided this by bringing all encryption logic to the client side. We also found a way to balance security and usability by providing a Key Management Store for users to manage their keys. In short, Cloud3 is an advanced invention in data security.
5	**Competitive Advantage or Unique Selling Proposition**
a	**Attainment of any SDG** **SDG#09: Industry, innovation, and infrastructure:** We are contributing to the blockchain industry, innovating the way files are stored by using IPFS, cryptography and Blockchain and working on decentralized infrastructure which is also achieved using IPFS and Blockchain. This is necessary for the region to safeguard data, ensure compliance with regulations, and foster economic growth while aligning with sustainability goals.
b	**Process Improvement which Leads to Superior Product or Cost Reduction, Efficiency Improvement of the Whole Process** Currently, we have two competitors in the market 1. Auguron (a mobile application) 2. Storj (a command line interface-based system) **Existing Systems** But as the above chart depicts, these two competitors are lacking in some crucial features that cloud3 provides and hence become our USPs. **Issues in Existing Systems** 1. **Truly Decentralized System:** Auguron is partly decentralized. They store user's data only on their nodes If their nodes are failed due to any reason, the user's data becomes completely unavailable. 2. **Anonymity:** Storj ask the users to provide their email address using which they can track the user's activity and impact user's privacy 3. **Ease of Use:** Storj and Auguron both are not user-friendly. Storj provides a command line interface and user can operate it by providing relevant commands

System	Truly Decentralized	No Third Party Administration	Anonymity	Ease of Use	User Understandability	Secure
Auguron (Mobile App)	✗	✓	✓	✗	✓	✓
Storj (Uplink CLI)	✓	✓	✗	✗	✗	✓
Cloud3	✓	✓	✓	✓	✓	✓

	which is very difficult for a naive user. On the other hand, Auguron demands the user to manage his keys by himself. 4. **User Understandability:** Storj has a very complex architecture and their target market is limited to the technical people only. **How Cloud3 solves the above issues:** 1. **Truly Decentralized System:** Cloud3 brings decentralization by integrating various pining services. When user uploads the data, the data is by default pinned on the IPFS nodes of Cloud3, but this storage is not limited to only Cloud3 nodes. We extended the storage boundaries and provide the user with the option to pin their data on the nodes of multiple pinning services just by one click. 2. **Anonymity:** Cloud3 is equipped with web3 login mechanism so that user is not forced to provide his email address or password and thus maintains the anonymity and user's privacy. 3. **Ease of Use:** Cloud3 is a user-friendly system that provides users with a key management extension to manage their keys. 4. **User understandability:** For the systems that provide privacy, it is very important that user understands what is going on. The target market of Cloud3 ranges from highly technical people to a naive users. All actions are performed on button clicks. The UI is simple and understandable.
6	**Target Market** The target market of Cloud3 can be any industry, group or individuals who wants privacy of their data. For industries, the system is useful in a way that employees can store and share their trade secrets securely. For a naive user, cloud3 is easy to use and provides the utmost privacy to his crucial data.
7	**Team Members**	Darakhshan. darakhshan704@gmail.com Farzeen Zehra. farzeenzehra.fz@gmail.com Maha Javed. mahajaved986@gmail.com Sheikh Muhammad Ahsan Tariq. ahsantariq792@gmail.com
8	**Supervisor Name**	Miss Asma Khan asmakhan@neduet.edu.pk
9	**Pictures (If any)**	**Cloud3 Website** **Main Page:**

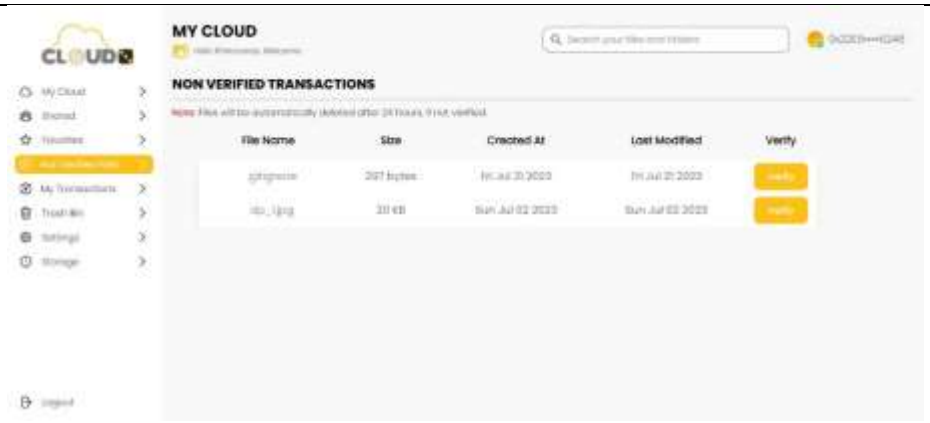


Dashboard:

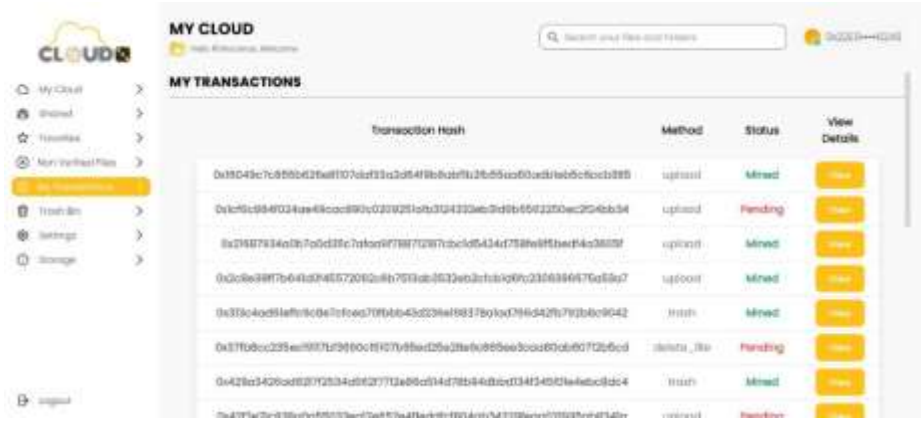


Shared Files Page:

Non-verified Files:

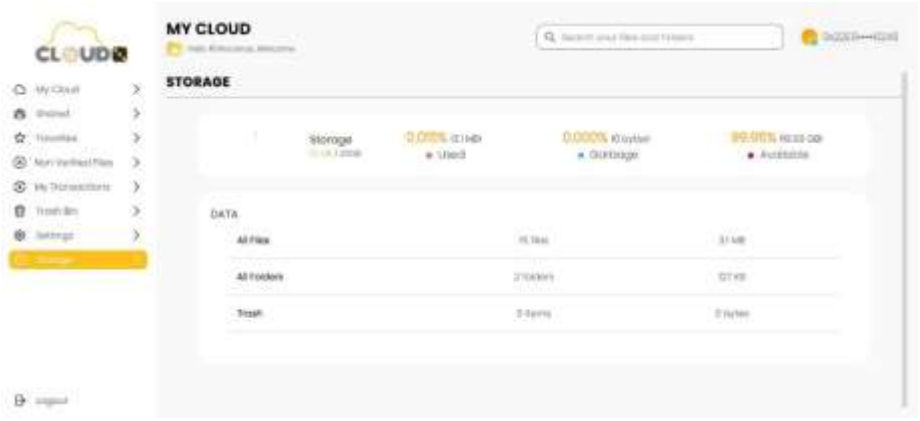


Transactions Page:

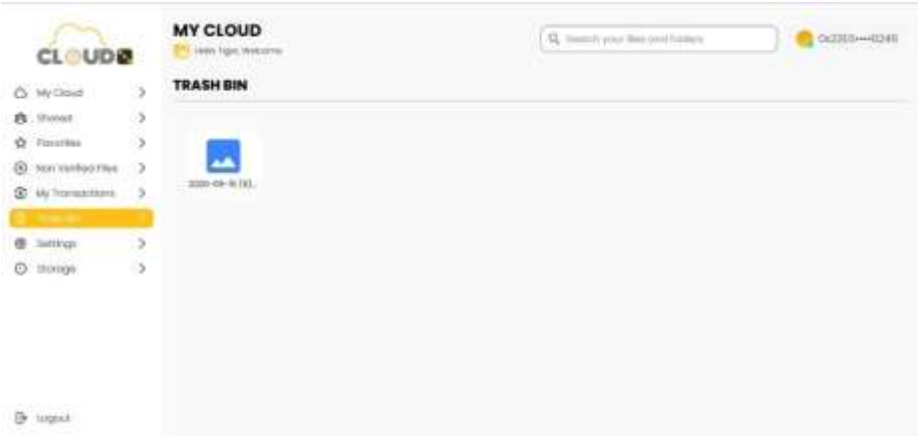


Settings Page:

Storage Page:

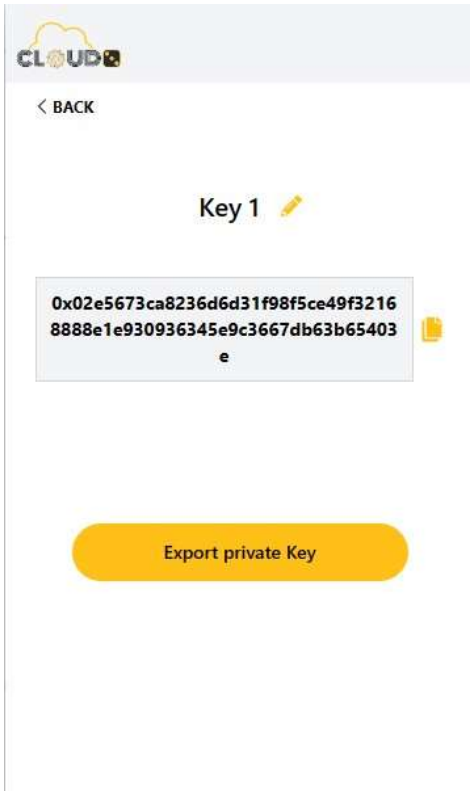


Trash Page:

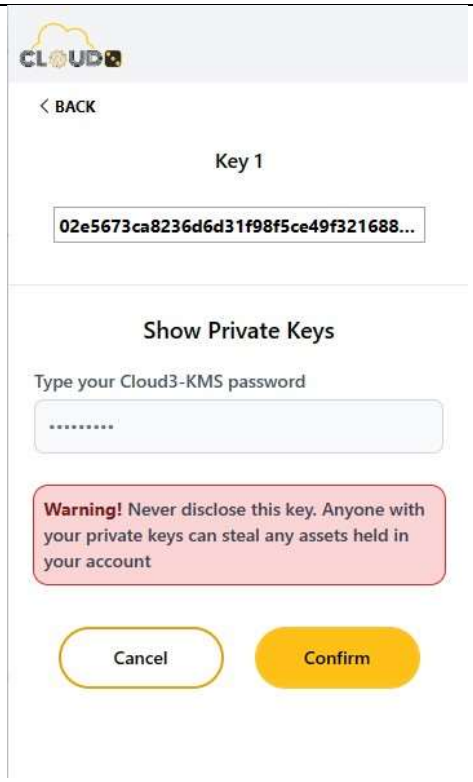


Favorites Page:

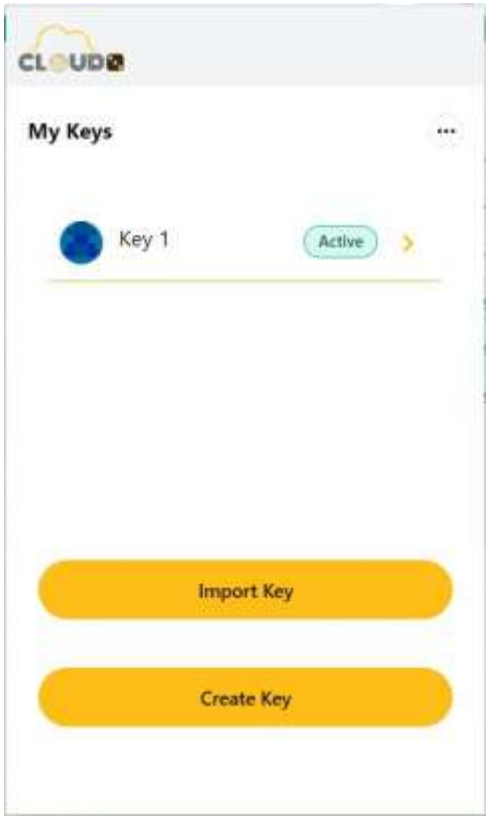
Cloud3-KMS:
Key Details:



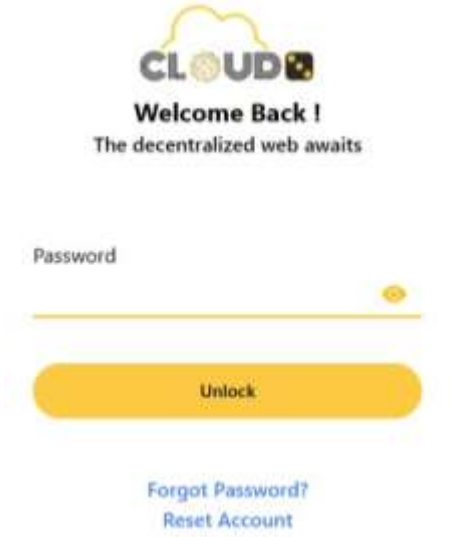
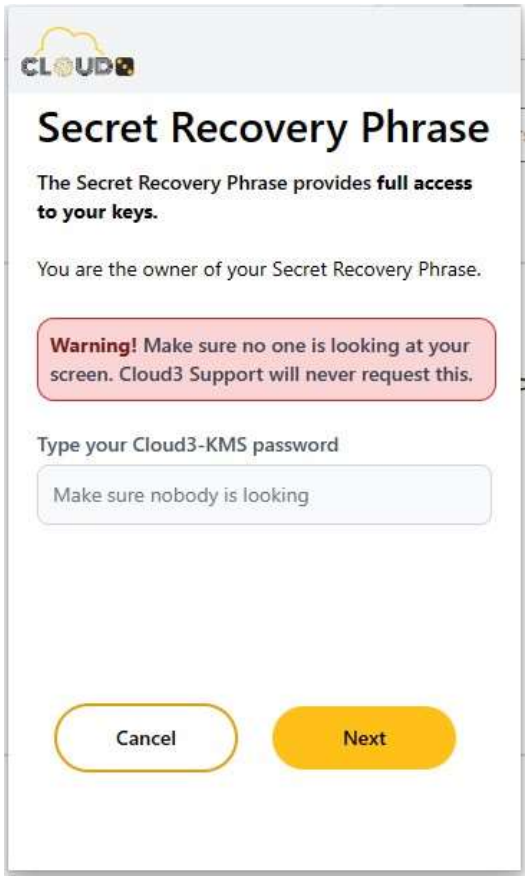
Export Key:



Keys Page:



KMS login:

		 **Secret Recovery Page:** 
10	**Video (If any)**	https://drive.google.com/drive/folders/1Ldv0LH9xtGTIRuDLu1vnhJuwYiDLFA0Z