**how to develop a secure cloud storage**

Developing a secure cloud storage solution involves several steps, including:

1. Data Encryption: Encrypt the files before uploading them to the cloud. This can be done using a variety of encryption algorithms, such as AES or RSA.
2. Key Management: Implement a secure key management system to ensure that only authorized users can access the encrypted files. This can be done using a key management service or by implementing a custom key management system.
3. Access Control: Implement access controls to ensure that only authorized users can access the files. This can be done using role-based access control or by implementing a custom access control system.
4. Authentication: Implement strong authentication mechanisms to ensure that only authorized users can access the files. This can be done using multi-factor authentication or by implementing a custom authentication system.
5. Data Backup: Regularly backup the data to ensure that it can be recovered in case of data loss or corruption.
6. Data Integrity: Implement mechanisms to ensure data integrity, such as hashing, signature or digital certificate.
7. Steganography: As previously discussed, you can use steganography to embed user's files within other files. This will make it difficult for an attacker to identify the presence of the hidden message.
8. Security monitoring and audit: Regularly monitor the cloud storage system for any suspicious activity and perform security audits to identify and fix vulnerabilities.

It is important to note that developing a secure cloud storage solution requires a comprehensive approach that involves multiple layers of security. It is important to keep the system updated and to comply with relevant laws and regulations.

**suggest some research paper or github implementation**

Here are a few research papers and Github implementations related to steganography and secure cloud storage:

1. Research Paper: "A Survey of Steganography Techniques" by S. Singh and R. Kaur: This paper provides an overview of various steganography techniques and their applications.
2. Research Paper: "Steganography in Cloud Computing: A Survey" by S. Singh and R. Kaur: This paper provides an overview of steganography techniques used in cloud computing and their security challenges.
3. GitHub Implementation: "Steganography-Python": This is a Python implementation of various steganography techniques, including LSB, DCT and DWT.
4. GitHub Implementation: "CloudStego": This is a Java implementation of steganography techniques for cloud storage.
5. GitHub Implementation: "AES-Encryption-in-Cloud-Storage": This is an implementation of AES encryption for cloud storage using the AWS SDK.
6. GitHub Implementation: "Steganography-JPEG-Python": This is a Python implementation of steganography in JPEG images using the LSB technique.
7. GitHub Implementation: "Cloud-Steganography-Java": This is a Java implementation of steganography for cloud storage, including encryption, compression and data hiding.

It is important to note that these are just examples, and it is important to carefully evaluate the security and compliance of any open source solution before using it in a production environment.