**INTRODUCTION**

PUBLIC cloud storage service becomes increasingly popular due to cost reduction and good data usability for users. This trend has prompted users and corporations to store (unencrypted) data on public cloud, and share their cloud data with others. Using a cloud for high-value data requires the user to trust the server to protect the data from unauthorized disclosures. This trust is often misplaced, because there are many ways in which confidential data leakage may happen, e.g. these data breaches reported [1], [2], [3], [4], [5], [6]. To counteract data leakage, one of the most promising approaches is client-side encryption/decryption. Concretely, client-side encryption allows senders to encrypt data before transmitting it to clouds, and decrypt the data after downloading from clouds. In this way, clouds only obtain encrypted data, thus making server-side data exposure more difficult or impossible. At the same time, as a crucial functionality of cloud storage, flexible file sharing with multiple users or a group of users must be fully supported. However, existing client-side encryption solutions suffer from more or less disadvantages in terms of security, efficiency and usability. Known Client-Side Encryption Solutions. We review existing solutions and point out their limitations.

\_ **Limited support or no support.** Many cloud storage providers, including Google Drive and Drop box, do not provide support for client-side encryption. They adopt server-side encryption for files stored, TLS for data at transit, and two-factor authentication for user authentication. Apple I Cloud supports end-to end encryption for sensitive information, e.g., I Cloud Keychain, Wi-Fi passwords. For other data uploaded to I Cloud, only server encryption is adopted.

\_ **Password-Based Solutions.** Some products [7], [8], [9] use symmetric encryption (typically AES) to encrypt users’ data and then upload ciphertexts to clouds. However, in these schemes, the cryptographic keys are derived from a password/ passphrase or even a 4-digit PIN. Relying on such low entropy is considered unsafe [10]. Worse still, most password-based solutions only deal with

the case of single-user file encryption and decryption, and do not provide any file sharing mechanism. Notably, [7] allows users to generate a share link for each password-protected file. However, users must manually send the share link through one channel, and password to all receivers through another secure channel, which is inconvenient and brittle.

\_ **Hybrid Encryption Scheme.** The cloud adopts a key encapsulation mechanism (KEM) and a data encapsulation mechanism (DEM), so called the KEM-DEM setting. Many public cloud service providers, including Amazon [11], Tresor it [12], and Mega [13], adopt the RSA-AES paradigm. Users generate RSA key pairs and apply for certificates from the providers, who build and maintain a Public Key Infrastructures (PKI). Users encrypt data under fresh sampled AES keys, which are further encrypted under all recipients’ RSA public keys. This file sharing mechanism is inflexible and inefficient. A sender needs to obtain and specify the public keys of all receivers during encryption. Even worse, the size of the cipher text and encryption workload are proportional to the number of recipients, resulting in greater bandwidth and storage costs and more user expenditure.

Limitations of the Existing Solutions. Three drawbacks exist in above-mentioned solutions: 1) comparatively poor security, 2) coarse-grained access control, inflexible and inefficient file sharing, and 3) poor usability. The first two are easy to see and we now elaborate the usability issue. Typically, users use different terminals to upload files, including desktop, Web and mobile applications [14]. However, almost all the existing solutions require additional software or plugins, thus limiting users’ devices and platforms. When switching to a new device, users need to repeat the boring installation process, which greatly increases users’ burden thus decreases usability.