Slik Safe Encryption Overview

Technical White Paper

Arpit Agarwal
arpit@sliksafe.com

Charvi Agarwal
charvi@sliksafe.com

Version 1 Published Nov 27, 2021

Contents

Introduction 3
Threat Model 3
Security by Simplicity 3
Cloud Storage 4
Decentralized File Storage.....5
Ransomware Protection 5
Folder Sharing 5
Multi-Device Support.....6
Key Recovery 8
Personalized Search.....8
Encryption Algorithms 8
Quantum Safe Cryptography.....9
Conclusion.....9

Introduction

Slik Safe is a decentralized, end-to-end-encrypted files backup and sharing platform. It allows users to backup their files on the decentralized web powered by the blockchain[1]. Since, the blockchain is an open and decentralized storage solution, Slik provides a mechanism to encrypt their file system before uploading it to the cloud. This enables the user to be in complete control of their data, while giving them the option of sharing it with others, while ensuring end-to-end encryption. Slik also enables the user to search their documents and files locally, without ever compromising ownership of their data. We start by describing our thread model and then describe components of our security and privacy system.

Threat Model

We consider a powerful adversary that can eavesdrop and corrupt all network communication between the individual clients and between the client and Slik servers. We also assume that the adversary can corrupt all data stored for the user by either unauthorized modifications or deletions.

Such an adversary would be able to control local networks (e.g., owners of wireless networks or administrators of enterprise networks) as well as large segments of the Internet (e.g., a nation state). Our threat model also treats Slik and its service providers as adversaries to ensure that they are unable to see any plaintext client data.

Security by Simplicity

"*The worst enemy of security is complexity. This has been true since the beginning of computers, and it's likely to the true for the foreseeable future"*

- A Plea for Simplicity: You can't secure what you don't understand.
Bruce Schneier, 1999

Slik's core innovation is a set of simple cryptographic protocols that exclusively use symmetric encryption. We have worked hard to simplify our protocols so that they are easy to understand, analyze, and implement. Our simplified protocols were designed to

[1] The blockchain is a peer-to-peer network with built in economic incentives.

achieve privacy at scale, which along with our distributed system, enable Slik to scale to virtually any number of users worldwide.

Cloud Storage

We store all files end-to-end-encrypted in the cloud with keys that only exist on your devices, therefore, nobody other than you, and people you share your files with, can access the decrypted data. We store the encrypted files on the cloud in a geographically replicated decentralized storage to ensure your files are safe and always accessible. We describe our cloud storage protocol below:

Protocol 1: Cloud Storage Protocol

We use `orange` for keys, `red` for plaintexts, and `green` for ciphertexts. All keys are 256-bits.

User Key Generation

1. The client generates a uniform random `User Key`.

File Upload

1. The client generates a uniform random `Folder Key`, and a uniform random `File Key` for each file in the folder.
2. The client encrypts the `File` with `File Key` and encrypts the `File Key` with `Folder Key` using symmetric encryption to obtain `Encrypted File`, and `Encrypted File Key`.
3. The client encrypts `Folder Key` with `User Key` using symmetric encryption to obtain `Encrypted Folder Key`.
4. The client uploads `Encrypted File`, `Encrypted File Key` and `Encrypted Folder Key` to the Slik server.

File Download

1. The client downloads `Encrypted File, Encrypted File Key` and `Encrypted Folder Key` from the Slik server.
2. The client decrypts the `Encrypted Folder Key` with `User Key` to get `Folder Key`.
3. The client decrypts the `Encrypted File Key` using `Folder Key` to get the `File Key`.
4. The client decrypts the `Encrypted File` with `File Key` to get `File`.

Decentralized File Storage

All files stored by users on Slik are stored on a geographically distributed decentralized storage. Each file is first encrypted using Protocol 1, as described above. After that, the file is broken down into small chunks of variable size and distributed over a network of nodes all around the world[2]. Since those files are encrypted and chunked on your client before being distributed, they are always secure.

Ransomware Protection

As an extra layer of protection, all your encrypted files are also stored on an immutable blockchain using the IPFS protocol[3]. This safeguards your data from unauthorized modifications and deletions by malicious actors.

Folder Sharing

We allow users to share folders of files with other users and allow them to view the files in the shared folders. Every folder is encrypted with a `Folder Key` that only exists on

[2] Storj DCS (https://www.storj.io/how-it-works)

[3] IPFS (https://ipfs.io/#how), the InterPlanetary File System.

the user device(s). To share a folder with another user, the user needs to share the `Folder Key` and the `Encrypted Folder`. The `Encrypted Folder` is shared directly through the Slik server. However, the `Folder Key` only exists on the user's device(s). We encode the `Folder Key` using an ephemeral public key of the person receiving the `Encrypted Folder.` We describe our folder sharing protocol below:

Protocol 2: Folder Sharing Protocol

Suppose a user Alice wants to share a folder with another user Bob. They will proceed as follows:

1. Alice shares `Encrypted Folder` with Bob using the Slik server. The folder is encrypted with `Folder Key`.

2. Alice will generate a one-time `Sharing Key` and encrypt the `Folder Key` with `Sharing Key` using symmetric encryption. Alice shares the `Encrypted Folder Key` with Bob using the Slik server.

3. Alice encodes the `Sharing Key` using an ephemeral public key of Bob to obtain `Encrypted Sharing Key` and shares it with Bob using Slik server.

4. Bob decrypts the `Encrypted Sharing Key` using the corresponding private key to obtain `Sharing Key`. Bob then decrypts the `Encrypted Folder Key` to obtain `Folder Key.`

5. Bob decrypts the `Encrypted Folder` with `Folder Key` to retrieve the plaintext `Folder`.

Multi-Device Support

Slik seamlessly supports multiple user devices without compromising security and user experience. We allow users to securely enroll multiple devices and our system securely

synchronizes the files across all user devices. We describe our multi-device synchronization protocol below:

Protocol 3: Multi-Device Synchronization Protocol

Device Enrollment

1. To enroll the first device, a user, say Alice, will sign up for Slik and create an account. During this process, the Slik app will perform User Key Generation, described in Protocol 1, on this device to generate `User Key`.

2. To enroll all subsequent devices:

    2.1. Alice uses any of her already enrolled device(s) to generate a one-time `Enroll Key`, encrypts the `User Key` with `Enroll Key` using symmetric encryption, and shares this `Encrypted User Key` with the new device using the Slik server.

    2.2. Alice encodes the `Enroll Key` as a QR code and physically shares it with her new device.

    2.3. Alice's new device retrieves the `Encrypted User Key` from the Slik server, decodes the QR code and obtains the `Enroll Key`, and uses it to decrypt the `Encrypted User Key` to obtain `User Key`.

State Synchronization

1. Alice's device with a newly created `File`, is encrypted using `File Key`. The `File Key` is encrypted using `Folder Key` which is encrypted by `User Key` using symmetric encryption to obtain `Encrypted Folder Key`, `Encrypted File Key`, and `Encrypted File`.

2. Alice's device then shares the encrypted data with all of Alice's device using Slik server.

3. All Alice's devices will decrypt the `Encrypted Folder Key` using the `User Key` to obtain `Folder Key`. and decrypt the `Encrypted File Key` using the `Folder Key` to obtain the `File Key`.

4. All Alice's devices then decrypt the `Encrypted File` with `File Key` to retrieve the plaintext `File`.

Key Recovery

As the encryption keys are only present on the user's device(s), Slik provides a recovery mechanism if the user loses a device. If the user still has access to at least one of their devices that was enrolled to use Slik, they can use that device to enroll a new device. If the user do not have access to any of their devices enrolled in Slik, we provide a seed phrase at the install time, which could be used to recover the encryption keys.

Personalized Search

Slik allows users to search files using date, time, and other metadata in files. Our search system exclusively uses files that you own or that are shared with you to generate a personalized search experience. All the data and search indices remain on your client and no information from the client is shared with anybody.

Encryption Algorithms

Slik employs authenticated symmetric encryption. We use AES block cipher in Galois Counter Mode (GCM) with 256-bit key for all of our encryption operations

Quantum Safe Cryptography

Files and documents have a long life and many times are passed across generations and decades. Slik uses Quantum safe cryptography to ensure that your files are secure even against a future adversary with currently known quantum computing capabilities.

Conclusion

In this white paper, we present a technical overview of security and privacy system that Slik has developed. Our system allows users to store their files in the cloud and share them with other people, while their files remain end-to-end encrypted. Our system supports multiple devices per user and is quantum-safe. We provide a personalized search experience without sharing your data with anybody else. Our cryptographic protocols are designed with “security by simplicity” mindset, which makes our protocols easy to understand, analyze, and implement.