Enabling Reliable Keyword Search in Encrypted Decentralized Storage with Fairness

ABSTRACT:

Block chain has led the trend of decentralized applications and shown great use beyond cryptocurrencies. Decentralized storage such as Storj and Sia leverages block chain to establish an open platform for sharing economy, which provides private andreliable file-outsourcing services. However, the ubiquitous keyword search function over encrypted files is yet to be supported. Toenable this function, we first apply searchable encryption techniques to the decentralized setting. But this primitive can hardly ensurethe service integrity. The reason is that decentralized storage commonly faces severe threats from both clients and service peers.Service peers may return partial or incorrect results, while clients may intentionally slander the service peers to avoid payments. Toaddress these threats, we utilize the smart contract to record the logs of encrypted search (aka evidence) on the block chain, and devise a fair protocol to handle disputes and issue fair payments. Using a dynamic-efficient searchable encryption scheme as aninstantiation, we craft a concrete scheme that preserves encrypted search capability and enforces ecosystem healthiness, so thatservice peers are incentivized to make real efforts and jointly guarantee service reliability. We implement our scheme in Python andSolidity, and test its search performance and transaction costs on Ethereum.

SYSTEM REQUIREMENTS:

HARDWARE REQUIREMENTS:

- System : Pentium i3 Processor.
- Hard Disk : 500 GB.
- Monitor : 15’’ LED
- Input Devices : Keyboard, Mouse
- Ram : 4 GB

SOFTWARE REQUIREMENTS:

- Operating system : Windows 10.
- Coding Language : Java
- Web Framework : Flask

REFERENCE:

C. Cai, J. Weng, X. Yuan and C. Wang, "Enabling Reliable Keyword Search in Encrypted Decentralized Storage with Fairness," in IEEE Transactions on Dependable and Secure Computing, vol. 18, no. 1, pp. 131-144, 1 Jan.-Feb. 2021, doi: 10.1109/TDSC.2018.2877332.