Comparative Study on Decentralized Cloud Collaboration (DCC)

Nikethan Selvanathan[1*], Guhanathan Poravi[2]

Cloud collaboration is a billion-dollar industry, for sharing and co-authoring files, in which the files are uploaded to a remote storage. In the current age of information technology, cloud collaboration expects to see a significant amount of growth, as more organizations look to leverage the benefits of the industry specifically in the areas of flexibility, cost-efficiency and security. However, despite the indisputable benefits provided by collaboration services, there are several inherent weaknesses such as high server costs for service providers, illegal data mining in trust-based architecture, security loopholes, and unethical government surveillance. Thus, decentralization (removal of client-server architecture) will mitigate these traditional server expenses, data failure and outage, as well as the increment of security, and privacy of data.

In this paper, we describe about cloud collaboration, their impacts on adaption, existing research background relation to decentralized cloud collaboration, and proposing solutions using decentralized architecture. In particular, we propose an innovative approach, implementing client-side application, distributed storage, blockchain, and peer-to-peer (P2P) protocol.

We propose client-side application which standardizes client side encryption (asymmetric encryption), file sharding, block exchange protocol, version control, and multiuser real-time collaboration through P2P communication to allow collaborators to store, share, and co-author without third party reliance. The distributed storage consists of storage space contributed by volunteer nodes to store collaborators data. As generally data availability is a function of probability in a decentralized network, we propose a novel design using RAID mechanism, and node failure management to improve fault tolerance. The blockchain act as a distributed data management platform to store contracts of volunteers, and generalized Merkle DAG challenges, which data verifiers (miners) can use to ensure data integrity of data in other nodes though challenge-response technique. The P2P protocol maintain consensus in decentralized network between client-side application, distributed storage, and blockchain, by creating a distributed network with efficient message routing and other desirable qualities to improve fault tolerance of the network.

[1]Informatics Institute of Technology, 55, Ramakrishna Road, Wellawatte, Sri Lanka.[*]nikethan.2014272@iit.ac.lk
[2]Informatics Institute of Technology, 55, Ramakrishna Road, Wellawatte, Sri Lanka