Chapter 32
CoPS – Cooperative Provenance System with ZKP using Ethereum Blockchain Smart Contracts

Navya Gouru
https://orcid.org/0000-0001-9321-1461
GITAM (Deemed to be University), Visakhapatnam, India

NagaLakshmi Vadlamani
GITAM (Deemed to be University), Visakhapatnam, India

ABSTRACT

The redesign of cloud storage with the amalgamation of cooperative cloud and an immutable and unhackable distributed database blockchain thrives towards a strong CIA triad and secured data provenance. The conspiracy ideology associated with the traditional cloud has economized with cooperative cloud storage like Storj and Sia, decentralized storage, which allows renting the unused hard drive space and getting monetary compensation in an exchange with cryptocurrency. In this article, the authors explain how confidentiality, integrity and availability can be progressed with cooperative cloud storage along with tamper-proof data provenance management with ethereum smart contracts using zero-knowledge proof (ZKP). A contemporary architecture is proposed with regards to storing data on the cooperative cloud and collecting and verifying the provenance data from the cloud and publishing the provenance data into blockchain network as transactions.

1. INTRODUCTION

The emergence of cloud computing has a profound impact on the business world which includes organizations and industries of different magnitude. The invent of centralized cloud, has been a boon for data storage by providing immeasurable benefits to consumers like cost-effective, scalability, flexibility,

DOI: 10.4018/978-1-7998-5351-0.ch032

high-profit edge as well as environmentally friendly, simultaneously as a bane as it comes with threats like outages, possible downtime and security risk. Though storage of data in cloud has proved to be cost-effective when compared with traditional data storage but the datacenters, which are the heart for cloud storage come with inflated cost tag, for cloud providers, consumers and users as billions of dollars are used every quarter for infrastructures like networking devices, physical servers, electricity just for sustainment and business extension. In this regard, data storage has been evolving from centralized to a decentralized cloud. Cooperative cloud storage is a decentralized cloud platform where users are connected over a peer-to-peer network, which is more resistant to hack, agile and economical when compared to traditional data-center based cloud storage. In Cooperative cloud storage, users' data is safeguarded on numerous nodes, which are hosted by the participating nodes who rent their vacant hard drive space cooperating the cloud and there exists a centralized control only for orchestration between users and hosts. Cooperative cloud is a trust-less system based between the client and the host. storj (Wilkinson et al., 2016) is an example of cooperative cloud that is end-to-end encrypted and agile because of its peer-to-peer technology with higher availability rate. Sia (Vorick and Champine, 2014). is another example of cooperative cloud which stores data in a decentralized and secure way without the server farms. Unlike storj, Sia uses their own cryptocurrency called Siacoin. Data provenance cites the process of discovering and record keeping the ancestry of data and its evolution between databases. Secured data provenance in a centralized cloud can uncover access violation but to establish such a secured provenance data is still a penetrating issue. Also, apart from tracking provenance data, it should guarantee integrity and should be accurate as provenance data may contain sensitive information.

The blockchain is a distributed network and a fault tolerant hyper ledger, which is shared by each and every participant in the network, but no singleton has the control. Blockchain would profoundly change the business approach across several industries and the list of applications and uses cases using Blockchain technology is viable. Bitcoin, (Nakamoto, 2008). a decentralized digital currency is one of the best-known implementations of the blockchain. Bitcoin uses blockchain technology across a wide decentralized network of computers to securely verify, confirm and record the transaction. Miners are special nodes who process and confirm the transactions. The decentralized architecture of blockchain can assure data provenance where every node in blockchain network can participate to track and safeguard the data provenance with assured privacy in the cooperative cloud environment. Even in terms of the payment mechanisms, online payments are used between the providers and consumers for centralized cloud storage services, which are not private or secure hence information about the payee and payer can be hacked. In the cooperative cloud, the payments between providers and consumers are made in cryptocurrency, which is pseudonymous. Cryptocurrency puts the power in people hands avoiding payment fees to banks, transaction fees, tax fees, credit card fees, which shows Blockchain is the future.

In this paper, the authors proposed Cooperative Provenance System CoPS, a data provenance architecture, which is based on blockchain for tamper-proof data operations in the cooperative cloud while reinforcing confidentiality, integrity and availability all the time. CoPS record the data transactions made in the cooperative cloud where there is no role for trusted middlemen and validation of provenance data is done by smart contracts that are built on ethereum blockchain. Authorized nodes verify the collected data provenance before publishing it to the blockchain. The authorization between the blockchain nodes accessing the verification script which resides on CoPS server is done with Zero-knowledge proof to protect against unauthorized users.