Chapter 17
Smarter Data Availability Checks in the Cloud:
Proof of Storage via Blockchain

Aydin Abadi
University College London, UK

ABSTRACT

Cloud computing offers clients flexible and cost-effective resources. Nevertheless, past incidents indicate that the cloud may misbehave by exposing or tampering with clients' data. Therefore, it is vital for clients to protect the confidentiality and integrity of their outsourced data. To address these issues, researchers proposed cryptographic protocols called "proof of storage" that let a client efficiently verify the integrity or availability of its data stored in a remote cloud server. However, in these schemes, the client either has to be online to perform the verification itself or has to delegate the verification to a fully trusted auditor. In this chapter, a new scheme is proposed that lets the client distribute its data replicas among multiple cloud servers to achieve high availability without the need for the client to be online for the verification and without a trusted auditor's involvement. The new scheme is mainly based on blockchain smart contracts. It illustrates how a combination of cloud computing and blockchain technology can resolve real-world problems.

INTRODUCTION

The importance of cloud computing is swiftly growing. The cloud is receiving increasing attention (Luxner, 2021, March 15; Abadi, 2017), as it enables ubiquitous access to a pool of configurable computing resources that can be scaled up, on demand. It offers elastic and cost-effective storage and computation resources to clients. It has been drawing the attention of individuals and businesses as a vital game-changing technology. There are various benefits for businesses to use the cloud, such as cost flexibility, business scalability, and increased collaboration with external partners (Berman et al., 2012). Nevertheless, the cloud is susceptible to data security breaches such as exposing confidential data, data

DOI: 10.4018/978-1-7998-7712-7.ch017

tampering, and denial of service. Thus, it cannot be fully trusted, and it is crucial for the clients who use the cloud to protect the security of their own data.

To address these issues, researchers have proposed Proof of Storage (PoS). It is an interesting cryptographic protocol that allows a client (e.g., a computer system acting on behalf of a party) to efficiently verify the integrity or availability of its data that is stored in a remote cloud server, which is not necessarily trusted (Kamara, 2013). In general, PoS schemes can be classified into two distinct categories; namely, Proofs of Retrievability (PoR) (proposed by Juels and Kaliski, 2007) and Proofs of Data Possession (PDP) (proposed by Ateniese et al., 2007). The former variant offers a stronger security guarantee than the latter, because a PoR scheme guarantees that the entire file is available whereas a PDP scheme guarantees that only a portion of a file remains intact in a remote server. The schemes that offer stronger security guarantees (i.e., PoR) are the main focus of this chapter. Since, in traditional PoR schemes, a client has to either perform the verification itself or delegate it to a fully trusted third-party, researchers proposed *outsourced* PoR schemes that let a client delegate the verifications, without having to fully trust a single entity. An efficient outsourced PoR scheme has recently been put forward by Abadi and Kiayias (2021, March 4). The scheme uses the decentralised nature of the blockchain (and smart contracts) to eliminate the involvement of a single trusted third-party. It allows a client to outsource its data to a single server, and lets the client delegate the verification of its data availability to a smart contract, which can periodically check data availability on the client's behalf.

In this chapter, it will be shown how we can improve upon the state-of-the-art outsourced PoR. In particular, a new variant of the PoR that lets a client store and distribute replicas of its sensitive data among *multiple cloud servers,* is discussed. The new PoR variant does not require the client to be always available to perform data availability checks itself. Instead, a smart contract efficiently performs the checks, on the client's behalf, and pays the servers if they successfully prove to the smart contract that the data is available. In the new scheme, the time intervals between two consecutive verifications can have different sizes which makes this scheme more flexible. To do that, it will be shown how the "chained time-lock puzzle" scheme, that is used in the scheme proposed by Abadi and Kiayias (2021, March 4), can be modified to support different size, time intervals. The modified chained time-lock puzzle scheme will be used in the multi-server outsourced PoR protocol. Thus, there are two primary properties that the multi-server outsourced PoR scheme offers, compared with the state-of-the-art PoR protocol, i.e., supporting (a) multiple cloud servers, and (b) allowing different size time intervals. The proposed scheme is mainly based on symmetric-key primitives that leads to an efficient implementation. The scheme imposes low costs, especially at the verification phase, while preserving all appealing features of the state-of-the-art protocol.

RELATED WORK

PoS is a cryptographic protocol that has been studied for over a decade. It allows a client to efficiently check the integrity or availability of its data stored in a remote cloud server that can potentially be malicious. PoR schemes ensure that the server maintains knowledge of the client's *entire* outsourced data, whereas PDP schemes only ensure the server is storing most of the client's data. Moreover, each PoR and PDP scheme can be grouped into two categories; namely, publicly and privately verifiable. In the former group, everyone without knowing a secret key can verify proofs, while the latter category requires a verifier to have the knowledge of a secret key. The PoR notion was first put forward and de-