Security and Mutual Trust in Cloud Computing Storage Systems

Shaik Meer Subhan Ali, Ch. Sekhar
Vignan’s Institute of Engineering & Technology, Duvvada, Visakhapatnam, AP, India

Abstract

One important service provided by the cloud computing systems is Storage as a service. This service is provided to the clients to store the critical, complex and huge data of the clients in the remote servers. In this context the security and mutual trust play a very important role. This paper deals with the various aspects related to security and the mutual trust of the CSP and clients of the data stored in the cloud storage systems.

Keywords

Storage as a Service, Mutual Trust, Remote Servers

Introduction

In the complex business world the data that is generated by the organizations is increasing day by day. It may be difficult for the organizations to maintain the data in the storage facilities they own. Sometimes the overheads for the maintenance of the data storage devices become unbearable for the business houses. The local management of such huge amount of data is problematic and costly due to the requirements of high storage capacity and qualified personnel. As the data is stored elsewhere, which is under the control of somebody else, there are certain concerns about the safety, security, privacy and mutual trust. The confidentiality of the data can be guaranteed by the owner through encryption of the data file before entering in to an agreement with the outside storage service providers.

Storage-as-a-Service (SaaS), Application-as-a-Service, and Platform-as-a-Service that allow organizations to concentrate on their core business and leave the IT operations to experts. In the current era of digital world, different organizations produce a large amount of sensitive data including personal information, electronic health records, and financial data. SaaS offered by CSP’s is an emerging solution to mitigate the burden of large local data storage and reduce the maintenance cost via the concept of outsourcing data storage. Through outsourcing data storage scenario, data owners delegate the storage and management of their data to a CSP in exchange for pre-specified fees metered in GB/month. Such outsourcing of data storage enables owners to store more data on remote servers than on private computer systems. Moreover, the CSP often provides better disaster recovery by replicating the data on multiple servers across multiple data centers achieving a higher level of availability. Thus, many authorized users are allowed to access the remotely stored data from different geographic locations making it more convenient for them. Since the owner physically releases sensitive data to a remote CSP, there are some concerns regarding confidentiality, integrity, and access control of the data.

In some practical applications, data confidentiality is not only a privacy concern, but also a juristic issue. The unauthorized users, including the CSP, are unable to access the data since they do not have the decryption key. This general solution has been widely incorporated into existing schemes which aim at providing data storage security on untrusted remote servers. On the other hand, the CSP needs to be safeguarded from a dishonest owner, who attempts to get illegal compensations by falsely claiming data corruption over cloud servers. This concern, if not properly handled, can cause the CSP to go out from the business. In this work, we propose a scheme that addresses important issues related to outsourcing the storage of data, namely dynamic data, mutual trust, newness, and access control. The remotely stored data can be updated and scaled by authorized users, and owner. After updating, authorized users should receive the latest version of the data (newness property), that is a technique is required to detect whether the received data is stale. Mutual trust between the CSP and the data owner is another important issue, which is addressed in the proposed scheme. A mechanism is introduced to determine the dishonest party. Last but not least, the access control is considered, which allows the owner to grant or revoke access rights to the outsourced data.

There are four components in this cloud computing model, (i) a data owner can collect a sensitive data for outsourcing and make it available for controlled use (ii) CSP who manage owners file and make it available for authorized users (iii) set of users who should receive the latest version of the data (newness property), (iv) a TTP has capabilities to detect / specify dishonest parties.

![Fig. 1: Cloud Computing Storage System Model](image-url)

The Mutual trust between the data owner and the CSP is another issue and that is addressed in this scheme. A mechanism is introduced to determine the dishonest party, from any side is detected and the responsible party is identified. Access control is also provided by the model which allows the owner to grant access or to revoke access rights to the outsourced data. In the existing schemes discussed, access control techniques assume the existence of the data owner and the storage servers in the same trust domain. Such system, no longer holds when the data is outsourced to a remote CSP. This scheme addresses important issues related to outsourcing the storage of data over the cloud storage systems. Especially these issues dynamic data, newness, mutual trust, and access control are addressed by this scheme. The cloud computing storage model considered in this scheme as shown in figure.

In this work the authorized user will do the auditing process of the data received from the CSP and we resort to the TTP only to resolve disputes that may arise regarding data integrity and newness. Outsourcing, updating and accessing of data owner file consists of m blocks. For Confidentiality owner encrypt the data using AES algorithm to protect the outsourced data from CSP and TTP before sending to cloud server, the owner and authorized...
user can interact with the CSP to perform block level operations (insert, delete and append) on the file, the AU and owner can any time interact with the CSP and access the encrypted outsourced data and decrypt using a secret key of their own and this lead to Integrity of data. Newness is receiving most recent version of outsourced data is an important requirement of cloud based storage system. Access control defines only authorized user is allowed to access the outsourced data. Revoked user cannot read new or update block but he can able to read old data. The CSP is untrusted, and the confidentiality and integrity of data may be in risk, for economic incentives and maintaining a data, the CSP may hide the loss of data, the data owner and AU may also falsely accuse that data integrity over the cloud servers has been violated or recent modification issued by the owner is not done on the data.

The architecture of the security is visualized as follows.

The following assumptions are considered to evaluate the data privacy of the proposed system.
1. The data owner and users have mutual distrust relation with cloud service provider.
2. Trusted third party helps to make the indirect mutual trust between authorized user and data owner with cloud service provider.
3. Public cloud model is considered for storage of outsourced data in data centers

The data owner has a file (F) consisting of m blocks of equal size. Since the data is storing on remote data center, for confidentiality all the blocks are encrypted using symmetric data encryption algorithm before sending to the cloud server.

**Conclusion**

In this paper we have discussed various related to the security and mutual trust in cloud computing storage systems.

**References**


Shaik Meer Subhan Ali, Vignan’s Institute of Engineering & Technology, Duvvada, Visakhapatnam, AP, India.
Ch. Sekhar, Vignan’s Institute of Engineering & Technology, Duvvada, Visakhapatnam, AP, India.