Chapter 10
Data Security Issues and Solutions in Cloud Computing

Abhishek Majumder
Tripura University, India

Sudipta Roy
Assam University, India

Satarupa Biswas
Tripura University, India

ABSTRACT

Cloud is considered as future of Information Technology. User can utilized the cloud on pay-as-you use basis. But many organizations are stringent about the adoption of cloud computing due to their concern regarding the security of the stored data. Therefore, issues related to security of data in the cloud have become very vital. Data security involves encrypting the data and ensuring that suitable policies are imposed for sharing those data. There are several data security issues which need to be addressed. These issues are: data integrity, data intrusion, service availability, confidentiality and non-repudiation. Many schemes have been proposed for ensuring data security in cloud environment. But the existing schemes lag in fulfilling all these data security issues. In this chapter, a new Third Party Auditor based scheme has been proposed for secured storage and retrieval of client's data to and from the cloud service provider. The scheme has been analysed and compared with some of the existing schemes with respect to the security issues. From the analysis and comparison it can be observed that the proposed scheme performs better than the existing schemes.

INTRODUCTION

Cloud Computing is a new computing model that distributes the computation on a resource pool. The resource pool which contains a large amount of computing resources offers services to the clients. These services are provided to the cloud users as utility services. The utility services are generally described as XaaS (X as a Service) where X can be software, platform or infrastructure.

Many organizations deal with the storage, retrieval and maintenance of huge amount of

DOI: 10.4018/978-1-4666-8387-7.ch010

data. In traditional computing environment, the organization has to maintain an infrastructure for storing the data. With the use of cloud computing services, the organization gets relieved from the burden of maintaining the infrastructure. But, when the cloud clients are storing their data, users are unaware of its physical storage location. As a result, one of the biggest concern of cloud computing is its data security. It is not clear how safe the client's data is and ownership of data is also unclear when these services are used. Cloud service providers claim that the stored data are completely safe. But, it is too early to comment on the reliability issues claimed by them. The stored data may suffer from damage during data transition to or from the cloud service provider by intrusion. Therefore, data security is the prime threat of modern technological era that each of the cloud service providers are facing. Data security involves encrypting the data as well as ensuring that suitable policies are imposed for sharing those data. The issues which need to be considered for ensuring data security in cloud environment are: data integrity, data intrusion, service availability, confidentiality and non-repudiation (Mahmood, 2011; Alzain et al., 2012; You et al., 2012).

For ensuring data security in cloud environment many schemes have been proposed. Varalakshmi et al., (2012), proposed a third party broker based scheme. Here a third party broker has been introduced to reduce the computational burden on client side and to increase the security of the system by not relying on the cloud service provider. The third party broker performs the activities of partitioner, hash key generator, encryptor, decryptor, local database manager and verifier. S. Kumar et al., (2011), proposed a meta data encryption based scheme for checking the integrity of stored data. In this scheme the verifier creates the meta data and encrypts it to reduce the computational overhead on the client side. At the time of integrity checking the verifier compares the decrypted meta data with the stored meta data. P. Kumar et al., (2011), proposed a hidden markov model and clustering based approach for intrusion detection in cloud environment. The scheme uses a data mining techniques for securing the cloud computing network. Hemant et al., (2011), proposed a governance body based scheme for solving the security issues of cloud computing. In this scheme all the transaction between the cloud server and the clients goes through the central server or governance body. Double encryption is used on each transaction. Shuai Han et al. proposed a third party auditor (TPA) scheme for ensuring data storage security in cloud computing. In this scheme, the cloud service performs additional functionality of TPA for making the system more trustful. Alzain et al., (2011) proposed Multi-clouds Database Model (MCDB). The model has been developed for handling data security issues in multi cloud environment. A redundancy based approach (Alzain et al., 2012) has been proposed for improving the security of MCDB model. The scheme uses Shamir's secret sharing algorithm (Shamir, 1979) and triple modular redundancy (TMR) to enhance the security of MCDB model.

In this chapter a new Third Party Auditor based scheme has been proposed. The entities used in the scheme are: Client/Data owner, Third Party Auditor (TPA) and Cloud Service Provider (CSP). It uses Whirlpool hash algorithm (Stallings, 2006) to maintain data integrity. A comparative study of the proposed scheme has been carried out with respect to some of the existing schemes. It has been observed that the proposed scheme performs better than the existing schemes.

The organization of the chapter is as follows. Next section discusses different data security issues. Various data security models, a Third Party Auditor based scheme and its comparison with other existing schemes have been discussed in the subsequent sections.