Chapter 60
Cloud Auditor Loyalty Checking Process Using Dual Signature

Divya Thakur
Samrat Ashok Technological Institute (SATI), India

ABSTRACT

We apply dual signature method. Providing security to the data from auditor during remote data possession checking by applying dual signature. Basically dual signature is a mechanism that is used to provide security during secure electronic transition protocol. The function of dual signature is to provide authenticity and integrity of the data. It links two message wished for two different recipient. In the case of providing security from auditor we use this methodology because it works on the basic of providing two links for two different recipients. In the case of dual signature customer wants to send order information to the trader and payment information to the bank. Here we use two links but not for the purpose of secure transaction but for the purpose of secure information exchange in remote possession checking.

INTRODUCTION

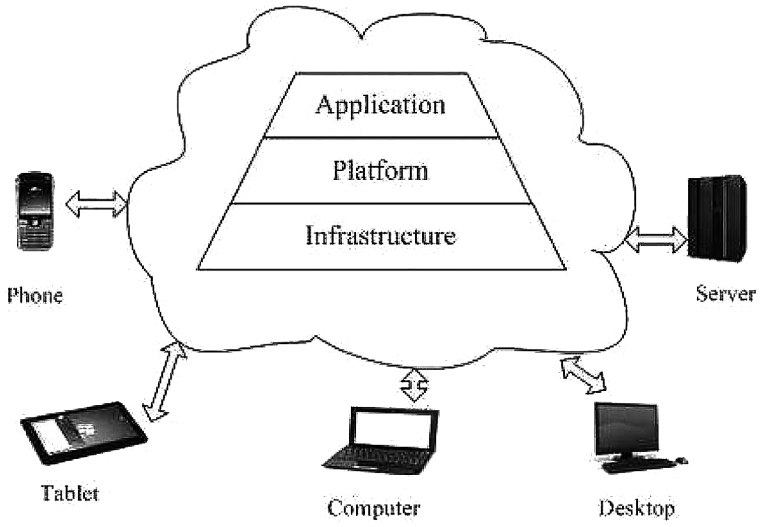
Since cloud provides greater storage capacity in virtual environment so mostly organizations use cloud to store their data without leaving a copy in their local device. However along with many benefits of cloud computing, it also brings new summons to create security (A. Atayero and O. Feyisetan 2011) and reliable data storage and ensuring the integrity of the data stored in the cloud is one of them. This is because data loss could happen in any infrastructure, no matter how high degree of reliability the cloud service provider commit to the user.

Here author are taking about dual signature based method (B. J. Brodkin, N. W. Cloud, S. Risks, C. Computing and G. A. Engine 2008) that is a technique under digital signature it provides two links for transaction purpose.

Digital signatures are a fundamental technique for verifying the authenticity of a digital message. The Significance of digital signatures in cryptography is also amplified by their use as building blocks for more complex cryptographic protocols. Recently, we have seen several pairing based signature schemes that are both practical and have added structure which has been used to build other primitives ranging

DOI: 10.4018/978-1-5225-8176-5.ch060

Figure 1. Cloud computing logical diagram



from Aggregate Signatures to Oblivious Transfer. Ideally, for such a fundamental cryptographic primitive we would like to have security proofs from straightforward, static complexity assumptions.

Now by improving this technique we can apply it to provide security from static assumptions for new signature schemes as well as pre-existing schemes. Providing new proofs for these existing schemes serve a meaningful sanity check as well as new insight into their security. This kind of security check is valuable not only for schemes proven in the generic group model, but also for signatures that require extra checks to rule out trivial breaks since these subtleties can easily be missed at first glance. Although users can use the traditional remote data possession checking method to check the integrity of their outsourced data, the two-party based checking method could not fully meet the properties of cloud computing for the following reasons: First, the users have to be online to conduct the checking procedure, which is feasible in many cases for example the user is travelling on the ocean; Second, the users' computation and communication resources are limited and it will take much of the users' resource to conduct the checking procedures themselves (C. C. Basics 2009).

Therefore, third-party auditing becomes the natural choice for auditing the cloud storage, which has been widely adopted. A third-party auditor (TPA), who owns expertise and capabilities, can do a more efficient and unbiased work. For the third-party auditing, it allows a third- party auditor to auditing the integrity of data in the cloud on behalf of the users. Recently, a number of auditing protocols were proposed to meet all kinds of properties: public auditing, privacy-preserving, high efficiency and so on. There some existing auditing protocols in terms of the type of cryptography, the data dynamics, the costs of communication and computation, the need for challenge-updating (G. Ateniese, K. Fu, M 2005).

In Cloud Computing, the remotely stored electronic data might not only be accessed however additionally updated by the clients, e.g., through block modification, deletion, insertion, etc. Unfortunately, the state of the art within the context of remote data storage mainly target static data files and therefore the importance of this dynamic data updates has received limited attention. According to the role of the verifier within the model, all the schemes out there fall into two categories: private confirmable and public confirmable. Achieving higher efficiency, schemes with private verifiability impose computational burden