Journal of Network and Computer Applications 66 (2016) 17–32

Contents lists available at ScienceDirect

Journal of Network and Computer Applications

journal homepage: www.elsevier.com/locate/jnca

Review

Comparative analysis of cloud data integrity auditing protocols

Neenu Garg *, Seema Bawa

Department of Computer Science and Engineering, Thapar University, Patiala, India

ARTICLE INFO

Article history:
Received 14 May 2015
Received in revised form
22 December 2015
Accepted 14 March 2016
Available online 15 March 2016

Keywords:
Cloud computing
Data integrity
Data integrity auditing
Third party auditing

ABSTRACT

In this paper, various protocols for data integrity auditing in cloud computing have been analyzed. The system models and threat models for data integrity auditing have been presented. Brief reviews on mathematical and cryptographic methods used to devise data integrity auditing protocols have been done. A comparative analysis of existing data integrity auditing protocols chronologically first, based on development methods is presented. Further, a specific analysis based on security methods, storage overheads, computation cost and communication cost is comprehended and presented in tabulated form. A comprehensive view of desirable properties of these protocols is presented later. Finally, the challenges in the composition of a dynamic data integrity auditing protocol for cloud computing environment have been highlighted.

Contents

* Corresponding author.
E-mail address: neenu.garg@thapar.edu (N. Garg).

http://dx.doi.org/10.1016/j.jnca.2016.03.010
1084-8045/

1. Introduction

Cloud computing is defined as a model for enabling ubiquitous, convenient, on-demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction (Mell and Grance, 2011). Services catered by cloud computing are software as a service (SaaS), platform as a service (PaaS) and hardware as a service (HaaS) Huth and Cebula (2015). Amazon, Google, Microsoft, IBM are key companies in cloud computing. At present a lot of users outsource their data to the websites hosted by these companies. According to IDC the overall expenditure on software, storage structures, and licensed business by the public cloud service providers will escalate at a 21.9% Compound Annual Growth Rate (CAGR) to $12.2 billion in 2016 (Iacono, 2015). Lending data storage space is pivotal service of cloud computing. This service allows business organizations and individuals to shift their data from personal data centers to cloud based data servers. Moving data into the cloud servers lends much contentment to organizations and individuals since they need not to anguish about the management of complex hardware systems. However, once the ownership of data is dropped, it brings security and privacy issues with data. Without data security, success of cloud computing is abridged. Maintaining data integrity is one of the vital security concerns.

By outsourcing data, the data owner gave right to cloud service provider to perform any operation on data. Hence data owner suffers from loss of possession of data. Possession of data states the control of data which means that if data is on local systems then data owner has full control over any operation performed on data including block deletion, modification, and insertion. But if the data is on cloud storage server then cloud provider has all the power to control any operation performed on the data. Cloud provider can stop any operation on data, process any operation incorrectly and may produce incorrect results. The major problem with loss of data possession is that the cloud provider can hide such mistakes from data owner for some benefits. The cloud server may also face internal and external security issues including components failure, administration problems, and software bugs which can harm data owner's critical data.

This third party data controlling has endangered data integrity and thereby hindering successful adoption of cloud environment by individuals and organizations (Chow et al., 2009). Checking data integrity when accessed is common for assuring data possession, but considering the amount of data stored at cloud, checking data integrity when accessed is not efficient. Moreover it is inapropos to let cloud providers or the data owners to audit data integrity as there is no guarantee for neutral auditing. Also, in these complex, voluminous data storage systems, the data may be refurbished from time to time and the prior data auditing protocols devised for static data archives may not be appropriate for data auditing in present scenario. Here in this scenario an authoritarian auditing service is required to audit data integrity in cloud periodically. In recent years checking data integrity at remote server without having to access whole data has gained much attention of researchers.

1.1. Our contributions

In this paper the various data integrity auditing protocols have been studied. Our main contributions are as follows:

a. The various system models and threat models for outsourcing data in cloud have been discussed.
b. The mathematical and cryptographic background concepts used in realizing a data integrity auditing protocol are also reviewed briefly.
c. A detailed analysis of these protocols, chronological first based on development methods is presented.
d. A comparative analysis of these protocols on the basis of security methods, storage overheads, computation costs, communication cost and requirements fulfilled is conferred in tabular form.
e. The challenges for actualizing an efficient data integrity auditing protocol have been highlighted.

1.2. Organization

In Section 2, the public auditing system model and private auditing system model for data integrity auditing and threats to public data auditing have been discussed. Section 3 provides details of mathematical and cryptographic methods used frequently in data integrity auditing protocols. In Section 4 a detail analysis of some existing data integrity auditing protocols has been given followed by a performance analysis based on security methods, storage overheads, computation cost and communication cost. In Section 5 few basic requirements to be fulfilled by data auditing protocols have been specified. Section 6 discusses some challenging issues in designing an efficient data integrity protocol. Finally we wrap this survey in Section 7.

2. Various models for data integrity auditing in cloud

During recent years the issue of data auditing in cloud computing has scored more significance and a number of protocols have been suggested by many researchers. There are various models of a auditing protocol. The first one discusses the various entities and their roles in the auditing system. The second one highlights the threats to the auditing system. These two models are discussed below:

2.1. System models

Few prior auditing protocols allow only data owners to audit data integrity. Such systems involving data owner and cloud server is termed as private auditing system. Role of two entities in private auditing system is explained below: