Available online at www.sciencedirect.com

ScienceDirect

Procedia Computer Science 125 (2018) 698–708

Procedia Computer Science

www.elsevier.com/locate/procedia

6th International Conference on Smart Computing and Communications, ICSCC 2017, 7-8 December 2017, Kurukshetra, India

Public integrity auditing for shared dynamic cloud data

Shubham Singh[a], Surmila Thokchom[b]

[a]*Dept. of Computer Science and Engineering, NIT Meghalaya, Shillong-793003, India*
[b]*Dept. of Computer Science and Engineering, NIT Meghalaya, Shillong-793003, India*

Abstract

Cloud computing is an important storage platform being researched nowadays. It provides various services to its users. Among them, one of the salient service offered is cloud storage which makes data outsourcing a rising trend. But the major concern associated is the integrity and seclusion of outsourced data. Users require their data to be secure from any modification or unauthorized access. Therefore someway to verify whether the data is intact or not, without retrieving, should exist. This boosts the need of secure remote data auditing. This paper proposes an auditing scheme based on vector commitment, identity based ring signature and group key agreement protocol, emanated on bilinear pairing. An experimental analysis of the proposed scheme, later in the end, shows that when compared with its pertinent schemes, the proposed scheme is also efficient.

Peer-review under responsibility of the scientific committee of the 6th International Conference on Smart Computing and Communications

Keywords: Cloud computing; public integrity auditing; vector commitment; ring signature; group key agreement protocol.

1. Introduction

Cloud computing can be defined as a network based computing which provides shared processing data & resources to its user when required. As per NIST, it is a model which enables pervasive, on-demand access to resources being shared that can be rapidly provisioned & released with minimum management effort [29]. It provides a user various capabilities for storing their data at the cloud server & processing it when required. This motivates organizations to outsource their data to an external storage server & improve the storage constraints of local devices, and enables them

[a] Shubham Singh. Tel.: +91-9027627808.
E-mail address: ShubhamSinghCMR@nitm.ac.in

[b] Surmila Thokchom. Tel.: +91-9458177016.
E-mail address: Surmila.Thokchom@nitm.ac.in

1877-0509
Peer-review under responsibility of the scientific committee of the 6th International Conference on Smart Computing and Communications
10.1016/j.procs.2017.12.090

to have more focus on their core competencies. Cloud user can access the data anytime, when required, from any part of the world but in some cases like hardware failure etc. the server may return an invalid result. Thus data integrity becomes the biggest concern for the cloud users as they no longer have a physical control over their outsourced data. Therefore to assure whether the data is secure or not, a way to verify its integrity and accessibility must exist for the users.

Some solutions have been put forward for assuring the integrity & availability of data stored at a faraway server. Authors in the references [2], [28], [10], [24], [25], [35], [37] and [32] proposes dynamic scheme which focuses on instances where only the owner can modify the stored data. Applications [19], [20] and [21], where cloud assistance is used as a cooperation platform, multiple group users shares the code and can access, revise and run it anytime anywhere. Such type of collaborative network makes remote auditing schemes impracticable where only the data owner can modify the data. It will cause a lot of computation and communication overhead to data owner and are inappropriate for him. If integrity verification can be done by person other than data owner, that is, by third party auditor, then the scheme is publicly verifiable. The scheme in [38] designs polynomial authentication tags and uses proxy tag update technique to support public auditing but the data confidentiality of group users is not considered. This means that the scheme supports data update & integrity checking for plaintext, not for cipher text. Yet no solution addresses the issue of public integrity checking with group user modification.

The dearth of these schemes prompts us to propose a reliable as well as an efficient way for remote data auditing. To the end, a construction is proposed which applies vector commitment over the database and supports group data encryption & decryption during its modification using group key agreement protocol [36]. Identity based ring signatures [39] are used to protect the anonymity of the signer.

1.1. Our Contribution

This paper put forwards a method for efficient public integrity auditing which is based on the scheme in the reference [27]. The issues of public integrity auditing were further studied and vector commitment, from the existing scheme [27], is incorporated with identity based ring signature to put forward an efficient public data integrity checking scheme. And in the end, a performance evaluation of the proposed scheme shows that it is more efficient than the existing scheme.

2. Related Work

Availability, integrity & confidentiality are the key attributes of data stored at cloud server. Serious work has been done looking for a way to securely outsource local data to faraway storage server and its remote auditing. In the papers [2] & [28], homomorphic authentication scheme is used by the authors to decrease the communication and computation cost. Later, deviants of these schemes are drafted to refine their efficiency like allowing public data auditing [35], [34], [37] and data update [24], [25].In the ref. [4] a scheme is proposed that supports user revocation. But it is constructed on the conjecture that there exists no collusion, neither it occurs, between the revoked user and the cloud server. It assumes that an exclusive authenticated channel exist between entities. Yuan & Yu proposed a dynamic auditing scheme in [38] which uses proxy tag update method and is built on polynomial authentication tags but doesnt considers ciphertext store. Benabbas et al. [8] proposes a verifiable database scheme but the problem is that public verifiability is not supported in it.

Authors puts forward a new way in the ref. [16] to build a database that is verifiable using vector commitment that supports public verifiability. This scheme assumes outsourced database to be of fixed size with the client having the ability to obtain information about the outsourcing function beforehand. Backes et al. presents a scheme in [5] having properties which eliminates this assumption. Group signature was first introduced in the ref. [17]. This signing method allows each member of the group to have a secret key and sign a message. Only the group manager knows the identity of actual signer, who is a trusted entity, and thus, in this way, this form of signing confirms signers anonymity. This signature type has been studied in the references [18] [15] [14] [3] [13] [33]. The authors have proposed a group signature which supports verifier local revocation in the paper [9]. In the proposed scheme, revocation information is sent to the signature verifier in user revocation. However, an initialization procedure is needed to specify a group in this scheme which may not be feasible under some conditions.