PRIVACY & DATA INTEGRITY FOR SECURE CLOUD STORAGE

Almas Ansari¹, Prof. Chetan Bawankar²
¹ (Student, M.Tech Dept. Computer Science & Engineering J.D. College of Engineering, Nagpur, India)
² (Asst. Prof Dept. Computer Science & Engineering J.D. College of Engineering, Nagpur, India)

ABSTRACT: Cloud computing is clearly one of today’s most enticing technology areas due, at least in part, to its cost-efficiency and flexibility. However, despite the surge in activity and interest, there are significant, persistent concerns about cloud computing that are impeding momentum and will eventually compromise the vision of cloud computing as a new IT procurement model. In this paper, we characterize the problems and their impact on adoption. In addition, and equally importantly, we describe how the combination of existing research thrusts has the potential to alleviate many of the concerns impeding adoption. In particular, we argue that with continued research advances in trusted computing and computation-supporting encryption, life in the cloud can be advantageous from a business intelligence standpoint over the isolated alternative that is more common today. A third party service provider, stores & maintains data, application or infrastructure of Cloud user. Relinquishing the control over data and application poses challenges of security, performance, availability and privacy. Security issues in Cloud computing are most significant among all others. Information Technology (IT) auditing mechanisms and framework in cloud can play an important role in compliance of Cloud IT security policies. In this paper, we focus on cloud security audit mechanisms and models.

1. INTRODUCTION

Today, the 14th largest software company by market capitalization (Salesforce.com) operates almost entirely in the cloud, the top five software companies by sales revenue all have major cloud offerings, and the market as a whole is predicted to grow to $160B by 2011 (source: Merrill Lynch). Yet, despite the trumpeted business and technical advantages of cloud computing, many potential cloud users have yet to join the cloud, and those major corporations that are cloud users are for the most part putting only their less sensitive data in the cloud. Lack of control in the cloud is the major worry. One aspect of control is transparency in the cloud implementation - somewhat contrary to the original promise of cloud computing in which the cloud implementation is not relevant. Transparency is needed for regulatory reasons and to ease concern over the potential for data breaches. Because of today’s perceived lack of control, larger companies are testing the waters with smaller projects and less sensitive data. In short, the potential of the cloud is not being realized.

When thinking about solutions to cloud computing’s adoption problem, it is important to realize that many of the issues are essentially old problems in a new setting, although they may be more acute. For example, corporate partnerships and offshore outsourcing involve similar trust and regulatory issues. Similarly, open source software enables IT departments to quickly build and deploy applications, but at the cost of control and governance. Finally, virtual machine attacks and Web service vulnerabilities existed long before cloud computing became fashionable. Indeed, this very overlap is reason for optimism; many of these “cloud problems” have long been studied and the foundations for solutions exist.

Third-party data control: The legal implications of data and applications being held by a third party are complex and not well understood. There is also a potential lack of control and transparency when a third party holds the data. Part of the hype of cloud computing is that the cloud can be implementation independent, but in reality regulatory compliance requires transparency into the cloud. All this is prompting some companies to build private clouds to avoid these issues and yet retain some of the advantages of cloud Computing.

II. LITERATURE REVIEW

Data outsourcing in Cloud Computing is fast becoming economically viable for large enterprises. In fact, this data outsourcing is ultimately retrieving user’s control over its own data and does not provide any assurance on data integrity and availability. On behalf of cloud user, a third party auditor (TPA) who has resources and experience that a user does not have can be emplaced to audit the integrity of large data storage. But user data privacy is still exposed to a TPA, which is required to be secured against unauthorized leakage. Wang and Sherman et al. [2] have proposed a public auditing system of data storage security by developing a
privacy preserving auditing protocol. By which auditor can audit without having knowledge of user’s data contents. Wang and Sherman also proposed a batch auditing protocol where multiple auditing tasks from different users can be performed simultaneously by a TPA.

Cloud computing provides development, delivery, and consumption of IT services over a distributed network environment. These services are interdependent on each other and failure of one service can cause unavailability of other service resulting loss of revenue, damaging reputation of the enterprise providing services and unreliability over the cloud. To minimize the risks of cloud outages, there is a dire need for ‘cloud governance’ model that could control and manage cloud-based services and storage.

In this paper[8], Zhiyun and Meina et al. have proposed a cloud based governance model that securely manages and controls the implementation of cloud services according to recognized policies, service management policies and their audit procedures. Elements of operational governance model includes: Authentication, i.e. enforcement of identity and access management system. Authorization, it enables implementation of a role-based authorization model. Audit, the collection of information related to the compliance of cloud security and service management policies. Monitoring, the preparation of individual and aggregate data transaction reports, summaries and graphs.

Juels et al. [11] describe a “proof of retrievability” (PoR) model, where spot-checking and error-correcting codes are used to ensure both “possession” and “retrievability” of data files on remote archive service systems. However, the number of audit challenges a user can perform is fixed a priori, and public auditability is not supported in their main scheme. Although they describe a straightforward Merkle-tree construction for public PoRs, this approach only works with encrypted data.

III. PROBLEM DEFINITION

A. The System and Threat Model

We consider a cloud data storage service involving three different entities, as illustrated in Fig. 1: the cloud user (U), who has large amount of data files to be stored in the cloud; the cloud server (CS), which is managed by cloud service provider (CSP) to provide data storage service and has significant storage space and computation resources (we will not differentiate CS and CSP hereafter); the third party auditor (TPA), who has expertise and capabilities that cloud users do not have and is trusted to assess the cloud storage service security on behalf of the user upon request.

B. Design Goals

Fig. 1: The architecture of cloud data storage service

We consider a cloud data storage service involving three different entities, as illustrated in Fig. 1: the cloud user (U), who has large amount of data files to be stored in the cloud; the cloud server (CS), which is managed by cloud service provider (CSP) to provide data storage service and has significant storage space and computation resources (we will not differentiate CS and CSP hereafter); the third party auditor (TPA), who has expertise and capabilities that cloud users do not have and is trusted to assess the cloud storage service security on behalf of the user upon request.
To enable privacy-preserving public auditing for cloud data storage under the aforementioned model, our protocol design should achieve the following security and performance guarantee:

1) Public auditability: to allow TPA to verify the correctness of the cloud data on demand without retrieving a copy of the whole data or introducing additional on-line burden to the cloud users;
2) Storage correctness: to ensure that there exists no cheating cloud server that can pass the audit from TPA without indeed storing users’ data intact;
3) Privacy-preserving: to ensure that there exists no way for TPA to derive users’ data content from the information collected during the auditing process;
4) Batch auditing: to enable TPA with secure and efficient auditing capability to cope with multiple auditing delegations from possibly large number of different users simultaneously;
5) Lightweight: to allow TPA to perform auditing with minimum communication and computation overhead.

**IV. THE PROPOSED SCHEMES**

In the introduction we motivated the public auditability with achieving economies of scale for cloud computing. This section presents our public auditing scheme for cloud data storage security. We start from the overview of our public auditing system and discuss two straightforward schemes and their demerits. Then we present our main result for privacy-preserving public auditing to achieve the aforementioned design goals. Finally, we show how to extent our main scheme to support batch auditing for TPA upon delegations from multiusers. Our public auditing system can be constructed from the above auditing scheme in two phases, Setup and Audit:

- **Setup**: The user initializes the public and secret parameters of the system by executing KeyGen, and preprocess the data file F by using SigGen to generate the verification metadata. The user then store the data file F at the cloud server, delete its local copy, and publish the verification metadata to TPA for later audit. As part of pre-processing, the user may alter the data file F by expanding it or including additional metadata to be stored at server.

- **Audit**: The TPA issues an audit message or challenge to the cloud server to make sure that the cloud server has retained the data file F properly at the time of the audit. The cloud server will derive a response message from a function of the stored data file F by executing GenProof. Using the verification metadata, the TPA verifies the response via VerifyProof.

**V. ALGORITHM**

A public auditing scheme consists of four algorithms (KeyGen, SigGen, GenProof, VerifyProof).

- **KeyGen**: key generation algorithm that is run by the user to setup the scheme.
- **SigGen**: used by the user to generate verification metadata, which may consist of MAC, signatures or other information used for auditing.
- **GenProof**: run by the cloud server to generate a proof of data storage correctness.
- **VerifyProof**: run by the TPA to audit the proof from the cloud server.

**VI. FLOWCHART**

User

Web Proxy: Login or Transaction

Enterprise

Identity & Access Platform

Delegated Authentication

Cloud Computing Platform

Strong (2-factor/3-factor)

MAC Services

Enterprise
VII. CONCLUSION

In this paper, we propose a privacy auditing system for data storage security in Cloud Computing. We utilize the homomorphic authenticator and random masking to guarantee that TPA would not learn any knowledge about the data content stored on the cloud server during the efficient auditing process, which not only eliminates the burden of cloud user from the tedious and possibly expensive auditing task, but also alleviates the users’ fear of their outsourced data leakage. Considering TPA may concurrently handle multiple audit sessions from different users for their outsourced data files, we further extend our privacy-preserving public auditing protocol into a multi-user setting, where TPA can perform themultiple auditing tasks in a batch manner, i.e., simultaneously. Extensive analysis shows that the proposed schemes are provably secure and highly efficient.

REFERENCE: