Volume : 2 | Issue : 11 | Nov 2013 • ISSN No 2277 - 8160



Research Paper | Engineering

Providing Dynamic Data Stoage and Indirect Mutual Trust in Clouds

E. Christo Paul — PG Scholar, Computer Science and Engineering, Srinivasan Engineering College

S. Saravanakumar — Assistant Professor, Computer Science and Engineering, Srinivasan Engineering College

ABSTRACT

Currently, the amount of sensitive data produced by many organizations is outpacing their storage ability. The management of such huge amount of data is quite expensive due to the requirements of high storage capacity and qualified personnel. Storage-as-a-Service (SaaS) offered by cloud service providers (CSPs) is a paid facility that enables organizations to outsource their data to be stored on remote servers. Thus, SaaS reduces the maintenance cost and mitigates the burden of large local data storage at the organization's end. A data owner pays for a desired level of security and must get some compensation in case of any misbehavior committed by the CSP. On the other hand, the CSP needs a protection from any false accusation that may be claimed by the owner to get illegal compensations. In this paper, we propose a cloud-based storage scheme that allows the data owner to benefit from the facilities offered by the CSP and enables indirect mutual trust between them. The proposed scheme has four important features: First one, it allows the owner to outsource sensitive data to a CSP, and perform full block-level dynamic operations on the outsourced data, i.e., block modification, insertion, deletion, and append. Second one, it ensures that authorized users (i.e., those who have the right to access the owner's file) receive the latest version of the outsourced data. Next one, it enables indirect mutual trust between the owner and the CSP. Last one, it allows the owner to grant or revoke access to the outsourced data. We discuss the security issues of the proposed scheme. Besides, we justify its performance through theoretical analysis and experimental evaluation of storage, communication, and computation overheads.

KEYWORDS : Outsourcing data storage, dynamic environment, mutual trust, access control

I.INTRODUCTION

Cloud computing has received considerable attention from both academia and industry due to a number of important advantages including: cost effectiveness, low management overhead, immediate access to a wide range of applications, flexibility to scale up and down information technology (IT) capacity, and mobility where customers can access information wherever they are, rather than having to remain at their desks. Cloud computing is a distributed computational model over a large pool of shared-virtualized computing resources (e.g., storage, processing power, memory, applications, service and network bandwidth).Cloud service Provider(CSPs) offer different classes of services

Storage-as-a-Service (SaaS), Application-as-a-Service, and Platform-as-a-Service that allow organizations to concentrate on their core business and leave the IT operations to experts. In the current era of digital world, different organizations produce a large amount of sensitive data including personal information, electronic health records, and financial data. SaaS offered by CSPs is an emerging solution to mitigate the burden of large local data storage and reduce the maintenance cost via the concept of outsourcing data storage. Through outsourcing data storage scenario, data owners delegate the storage and management of their data to a CSP in exchange for pre-specified fees metered in GB/month. Such outsourcing of data storage enables owners to store more data on remote servers than on private computer systems. Moreover, the CSP often provides better disaster recovery by replicating the data on multiple servers across multiple data centers achieving a higher level of availability. Thus, many authorized users are allowed to access the remotely stored data from different geographic locations making it more convenient for them. Since the owner physically releases sensitive data to a remote CSP, there are some concerns regarding confidentiality, integrity, and access control of the data. In some practical applications, data confidentiality is not only a privacy concern, but also a juristic issue. For example, in e-Health applications inside the USA the usage and exposure of protected health information should meet the policies admitted by Health Insurance Portability and Accountability Act (HIPAA), and thus keeping the data private on the remote storage servers is not just an option, but a demand. The confidentiality feature can be guaranteed by the owner via encrypting the data before outsourcing to remote servers.

Main contributions. Our contributions can be summarized in two main points.

1) The design and implementation of a cloud-based storage scheme that has the following features:

a) It allows a data owner to outsource the data to a remote CSP, and perform full dynamic operations at the block-level, i.e., it supports operations such as block modification, insertion, deletion, and append
b) It ensures the newness property, i.e., the authorized users receive the most recent version of the data
c) It establishes indirect mutual trust between the data owner and the CSP since each party resides in a different trust domain
d) It enforces the access control for the outsourced data

2) We discuss the security features of the proposed scheme. Besides, we justify its performance through theoretical analysis and experimental evaluation of storage, communication, and computation overheads.

II RELATED WORK

Existing research close to our work can be found in the areas of integrity verification of outsourced data, Cryptographic file systems in distributed networks, and access control of outsourced data.

Based on proxy re-encryption have introduced a secure distributed storage protocol. In their protocol, a data owner encrypts the blocks with symmetric data keys, which are encrypted using a master public key. The data owner keeps a master private key to decrypt the symmetric data keys. Using the master private key and the authorized user's public key, the owner generates proxy re-encryption keys. A semi-trusted server then uses the proxy re encryption keys to translate a cipher text into a form that can be decrypted by a specific granted user, and thus enforces access control for the data.

Discussion. Some aspects related to outsourcing data storage are beyond the setting of both PDP and POR, e.g., enforcing access control, and ensuring the newness of data delivered to authorized users. Even in the case of dynamic PDP, a verifier can validate the correctness of data, but the server is still able to cheat and return stale data to authorized users after the auditing process is done.

III.OUR SYSTEM AND ASSUMPTIONS

System components and relations. The cloud computing storage model considered in this work consists of four main components as illustrated in Fig. 1: (i) a data owner that can be an organization generating sensitive data to be stored in the cloud and made available for

controlled external use; (ii) a CSP who manages cloud servers and provides paid storage space on its infrastructure to store the owner's files and make them available for authorized users; (iii) authorized users – a set of owner's clients who have the right to access the remote data; and (iv) a trusted third party (TTP), an entity who is trusted by all other system components, and has expertise and capabilities to detect and specify dishonest parties.

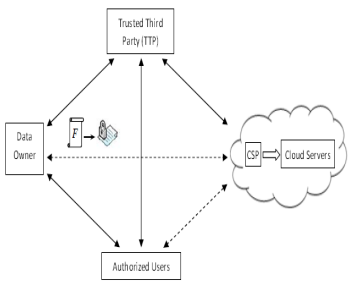

Fig. 1: Cloud computing data storage system model.

In Fig. 1, the relations between different system components are represented by double-sided arrows, where solid and dashed arrows represent trust and distrust relations, respectively. For example, the data owner, the authorized users, and the CSP trust the TTP. On the other hand, the data owner and the authorized users have mutual distrust relations with the CSP. Thus, the TTP is used to enable indirect mutual trust between these three components. There is a direct trust relation between the data owner and the authorized users.

IV.SYSTEM PRELIMINARIES

4.1 Lazy Revocation

The proposed scheme in this work allows the data owner to revoke the right of some users for accessing the outsourced data. In lazy revocation, it is acceptable for revoked users to read (decrypt) unmodified data blocks.

4.2 Key Rotation

Key rotation is a technique in which a sequence of keys can be generated from an initial key and a master secret key. The sequence of keys has two main properties: (i) only the owner of the master secret key is able to generate the next key in the sequence from the current key, and (ii) any authorized user knowing a key in the sequence is able to generate all previous versions of that key. In other words, given the i-th key Ki in the sequence, it is computationally infeasible to compute keys K_l for l > i without having the master secret key, but it is easy to compute keys K_j for j < i.

Whenever a user's access is revoked, the data owner generates a new key in the sequence (rotating forward). Let ctr indicate the index/version number of the current key in the keys sequence. The owner generates the next key by exponentiating Kctr with the master secret key d: Kctr+1 = Kdctr mod N. Authorized users can recursively generate older versions of the current key by exponentiating with the public key component e: Kctr-1 = Kectr mod N (rotating backward). The RSA encryption is used as a pseudorandom number generator; it is unlikely that repeated encryption results in cycling, for otherwise, it can be used to factor the RSA modulus N.

4.3 Broadcast Encryption

Broadcast encryption (bENC) allows a broadcaster to encrypt a message for an arbitrary subset of a group of users. The users in the subset are only allowed to decrypt the message. However, even if all users outside the subset collude they cannot access the encrypted message. Such systems have the collusion resistance property, and are used in many practical applications including TV subscription services and DVD content protection.

4.4 Block Status Table

The block status table (BST) is a small dynamic data structure used to reconstruct and access file blocks outsourced to the CSP. The BST consists of three columns: serial number (SN), block number (BN), and key version (KV). SN is an indexing to the file blocks. It indicates the physical position of each block in the data file. BN is a counter used to make a logical numbering/indexing to the file blocks.

V.EXPERIMENTAL EVALUATION

In this section we experimentally evaluate the computation overhead the proposed scheme brings to a cloud storage system that has been dealing with static data with only confidentiality requirement.

The experiments are conducted using .NET on a system with an Intel(R) Xeon (R) 2-GHz processor and 3GB RAM running Windows XP. Algorithms (hashing, broadcast encryption, digital signatures, etc.) are implemented using MIRACL library version 5.5.4. For a 128-bit security level, bENC uses an elliptic curve with a 256-bit group order. In the experiments, we utilize SHA-256, 256-bit BLS signature, and Barreto-Naehrig (BN) [50] curve defined over prime field GF(p) with p = 256 bits and embedding degree = 12 (the BN curve with these parameters is provided by the MIRACL library). To evaluate the computation overhead on the owner side due to dynamic operations, we perform 100 different block operations from which 50% are executed following revocations (this percent is higher than an average value in practical applications).

Scalability (i.e., how the system performs when more users are added) is an important feature of cloud storage systems. The access control of the proposed scheme depends on the square root of the total number of system users.

To identify the dishonest party in the system in case of disputes, the TTP verifies two signatures (F and T), computes combined hashes for the data (file and table), and compare the computes hashes with the authentic values (THTTP and FHTTP). Thus, the computation overhead on the TTP side is about 10.77 seconds. Through our experiments, we use only one desktop computer to simulate the TTP and accomplish its work. In practice, the TTP may choose to split the work among a few devices or use a single device with a multi-core processor which is becoming prevalent these days, and thus the computation time on the TTP side is significantly reduced in many applications.

VI.CONCLUSIONS

Outsourcing data to remote servers has become a growing trend for many organizations to alleviate the burden of local data storage and maintenance. In this work we have studied different aspects of outsourcing data storage: block-level data dynamic, newness, mutual trust, and access control.

We have proposed a cloud-based storage scheme which supports outsourcing of dynamic data, where the owner is capable of not only archiving and accessing the data stored by the CSP, but also updating and scaling this data on the remote servers. The proposed scheme enables the authorized users to ensure that they are receiving the most recent version of the outsourced data. Moreover, in case of dispute regarding data integrity/newness, a TTP is able to determine the dishonest party. The data owner enforces access control for the outsourced data by combining three cryptographic techniques: broadcast encryption, lazy revocation, and key rotation. We have studied the security features of the proposed scheme.

REFERENCES

[1] C. Wang, Q. Wang, K. Ren, and W. Lou, "Privacy-preserving public auditing for data storage security in cloud computing," in INFOCOM, 2010, pp. 525–533. | | [2] W. Wang, Z. Li, R. Owens, and B. Bhargava, "Secure and efficient access to outsourced data," in Proceedings of the 2009 ACM workshop on Cloud computing security, ser. CCSW '09. ACM, 2009, pp. 55–66. | | [3]. C. Erway, A. Kupu, C. Papamanthou, and R. Tamassia, "Dynamic provable data possession," in CCS'09: Proceedings of the 16th ACM Conference on Computer and Communications Security, New York, NY, USA, 2009, pp. 213–222. | | [4].G. Ateniese, R. D. Pietro, L. V. Mancini, and G. Tsudik, "Scalable and efficient provable data possession," in SecureComm '08: Proceedings of the 4th International Conference on Security and Privacy in Communication Netowrks, New York, NY, USA, 2008, pp.1–10. | | [5]. G. Ateniese, R. Burns, R. Curtmola, J. Herring, L. Kissner, Z. Peterson, and D. Song, "Provable data possession at untrusted stores," in CCS '07: Proceedings of the 14th ACM Conference on Computer and Communications Security, New York, NY, USA, 2007,pp. 598–609. | | [6].M. J. Atallah, K. B. Frikken, and M. Blanton, "Dynamic and efficient key management for access hierarchies," in Proceedings of the 12th ACM Conference on Computer and Communications Security, ser. CCS '05. ACM, 2005, pp. 190–202. | | [7]. M. Kallahalla, E. Riedel, R. Swaminathan, Q. Wang, and K. Fu, "Plutus: Scalable secure file sharing on untrusted storage," in Proceedings of the FAST 03 Conference on File and Storage Technologies. USENIX, 2003. | | [8]. D. Boneh, B. Lynn, and H. Shacham, "Short signatures from the weil pairing," in ASIACRYPT '01: Proceedings of the 7th International Conference on the Theory and Application of Cryptology and Information Security, London, UK, 2001, pp. 514–532. |