Ensuring Public Verifiability and Data Dynamics Security in Cloud Computing

[1] C. Manikandan and [2] P. Ahathiya,
[1] Final M.E., CSE, [2] Assistant Professor. Dept. of CSE,
Dhanalakshmi Srinivasan Engineering College, Perambalur-621212.

Abstract

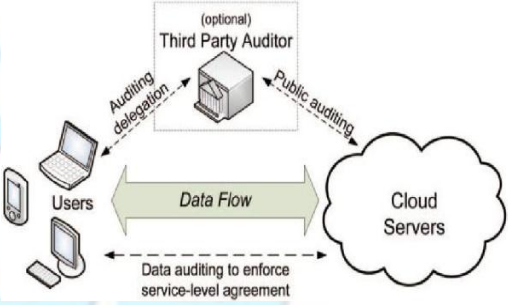
The flexible distributed storage integrity auditing mechanism is utilize the homomorphic token and distributed erasure-coded data. It moves the application software and databases to the centralized large data centers , where the management of the data and services may not be fully trustworthy .Cloud Service Provider (CSP),address domain will identifies these threats, it can come from two different sources internal and external attacks. In internal attacks, a CSP can be self-interested, untrusted and possibly malicious .In external attacks, data integrity threats may come from outsiders who are beyond the control domain of CSP, for the economically motivated attackers. It allows users to audit the cloud storage with very lightweight communication and computation cost. The proposed scheme is highly efficient and resilient against Byzantine failure ,malicious data modification attack, and even server colluding attacks. The cloud data are dynamic in nature, the proposed design further supports secure and efficient dynamic operations on outsourced data, including block modification, deletion, and append.

Index Terms- Data integrity,dependable distributed storage,error localization, datadynamics,csp

I. INTRODUCTION

The Cloud service provider owns and administers the physical infrastructure on which the cloud services are provided. Site owners provide the service to their respective users via sites that are hosted by the cloud service provider. Cloud tenant running a collection of the virtual appliances that are hosted on the cloud infrastructure, the services are provided to the end users through the public internet. moving data into the cloudoffers great convenience to users since they don’t have to care about the complexity of direct hardware management.One of the key issues is to effectively detect any unauthorized data modification and corruption, possibly due to server compromise or random Byzantine failures. The main scheme for ensuring cloud data storage is presented in this section.The first part of the section is devoted to a review of basic tools from coding theory that is needed in the scheme for file distribution across cloud servers.Then, the homomorphic token is introduced. The token computation functions are considering belongs to a family of universal hash function, chosen to preserve the homomorphic properties, which can be perfectly integrated with the verification of erasure coded data.Simple storage service, Elastic Compute cloud both are internet based online services do provide huge amounts of storage space and customizable computing resources,this computing platform shift, however is eliminating the responsibility of local machines for data maintenance at the same time.Cloud infrastructure are much more powerful and reliable than personal computing devices, broad range of both internal and external threats for data integrity still exist.

To propose an effective and flexible distributed storage verification scheme with explicit dynamic data support to ensure the correctness and availability of users’ data in the cloud.To rely on erasure correcting code in the file distribution preparation to provide redundancies and guarantee the data dependability against Byzantine servers, where a storage server may fail in arbitrary ways.



II. LITERATURE REVIEW

A model for provable data possession (PDP)[1] that allows a client that has stored data at an untrusted server to verify that the server possesses the original data without retrieving it. The model generates probabilistic proofs of possession by sampling random sets of blocks from the server, which drastically reduces I/O costs.In a proof-of-retrievability system,[2] The first one is privately verifiable and builds elegantly on pseudorandom functions (PRFs); the second allows for publicly verifiable proofs and is built from the signature scheme of Boneh,Lynn, and Shacham in bilinear groups.The multiple-replica provable data possession (MR-PDP)[3] a provably-secure scheme that allows a client that stores a file in a storage system to verify through a challenge-response protocol that each unique replica can be produced at the time of the challenge and that the storage system uses times the storage required to store a single replica.Protocols are privacy-preserving[4], in that they never reveal the data contents to the auditor. The solution removes the burden of verification from the customer, alleviates both the customer's and storage service's fear of data leakage, and provides a method for independent arbitration of data retention contracts. In a proof-of-retrievability system, a data storage center must prove to a verifier that he is actually storing all of a client's data. The central challenge is to build systems that are both efficient and provably secure|that is, it should be possible to extract the client's data from any prover that passes a verification check. The create the first compact and provably secure proof of retrievability systems.It allows for compact proofs with just one authenticator value|in practice this can lead to proofs with as little as 40 bytes of communication.

To present two solutions with similar structure. The first one is privately verifiable and builds elegantly on pseudorandom functions (PRFs); the second allows for publicly verifiable proofs and is built from the signature scheme of Boneh,Lynn, and Shacham in bilinear groups. Both solutions rely on homomorphic properties to aggregate a proof into one small authenticator value. A growing number of online service providers offer to store customers' photos, email, system backups, and other digital assets. Currently, customers cannot make informed decisions about the risk of losing data stored with any particular service provider, reducing their incentive to rely on these services.It argue that third party auditing is important in creating an online service oriented economy, because it allows customers to evaluate risks, and it increases the efficiency of insurance based risk mitigation.To describe approaches and system hooks that support both internal and external auditing of online storage services, describe motivations for service providers and auditors to adopt these approaches, and list challenges that need to be resolved for such auditing to become a reality. Cloud Computing has been envisioned as the next generation architecture of IT Enterprise. In contrast to traditional solutions, where the IT services are under proper physical,logical and personnel controls, Cloud Computing moves the application software and databases to the large data centers, where the management of the data and services may not be fully trustworthy.

This unique attribute it poses many new security challenges which have not been well understood. It focus on cloud data storage security, which has always been an important aspect of quality of service. To ensure the correctness of users' data in the cloud, To propose an effective and flexible distributed scheme with two salient features, opposing to its predecessors. By utilizing the homomorphic token with distributed verification of erasure-coded data, The scheme achieves the integration of storage correctness insurance and data error localization, the identification of misbehaving server(s). Unlike most prior works, the new scheme further supports secure and efficient dynamic operations on data blocks, including: data update, delete and append. Extensive security and performance analysis shows that the proposed scheme is highly efficient and resilient against it, malicious data modification attack, and even server colluding attacks.Cloud Computing has been envisioned as the next-generation architecture of IT Enterprise. It moves the application software and databases to the centralized large data centers, where the management of the data and services may not be fully trustworthy.

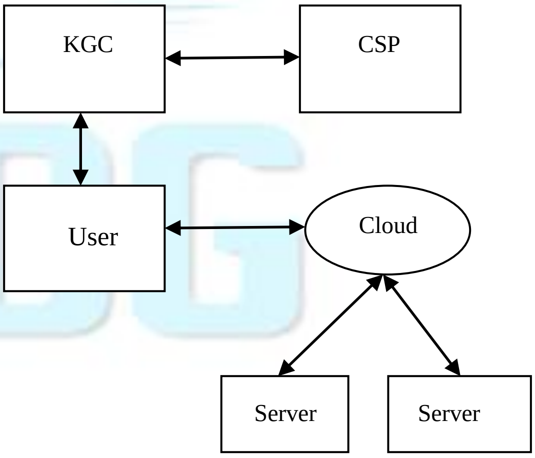


Fig.2. The proposed framework schema of Byzantine Failures.

III. PROPOSED METHODOLOGY

To propose an effective and flexible distributed scheme with explicit dynamic data support, including block update, delete, and append.

a) KGC(Key Generation Center)

- To generate attribute based public key and private key.

b) Pseudo Random Permutation

- It's a technique to pick up the attribute.

To rely on erasure-correcting code in the file distribution preparation to provide redundancy parity vectors and guarantee the data dependability. To achieves the key updation process in server side.

Adversary Model

The adversary model has to capture all kinds of threats towards the cloud data integrity. Due to cloud data do not reside at user's local site but at cloud service providers address domain. It desire to move data that has not been or is rarely accessed to a lower tier of storage than agreed for monetary reasons, but it may also attempt to hide a data loss incident due to management errors, Byzantine failures and so on.For external attacks, data integrity threats may come from outsiders .And also the data while store on the storage center it can check for the previous data similarly to that stored one and make a replace for it. This functions made for some software version updations.

Token Precomputation

Data storage correctness and data error localization simultaneously, this scheme entirely relies on the pre-computed verification tokens. The main idea is before file distribution the user pre-computes a certain number of short verification tokens on individual vector, each token covering a random subset of data blocks. Upon receiving challenge, each cloud server computes a short "signature" over the specified blocks and returns them to the user. The values of these signatures should match the corresponding tokens precomputed by the user.

File Retrieval and Error Recovery

User can reconstruct the original file by downloading the data vectors from the servers, assuming that they return the correct response values. Verification scheme is based on random spot-checking, so the storage correctness assurance is a probabilistic one.By choosing system parameters appropriately and conducting enough times of verification, can guarantee the successful file retrieval with high probability. The newly recovered blocks can then be redistributed to the misbehaving servers to maintain the correctness of storage.

Key Generation Center(KGC)

A Key generation center can be consumed by the user does not have the time, feasibility or resources to perform the storage correctness verification.Cloud consumer can optionally delegate this task to an independent third party auditor, it makes the cloud storage securable.KGC should accept consumers data and it generates a key to store in the cloud.It 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. Users rely on the Cloud Server for cloud data storage and maintenance. And also dynamically interact with the Cloud Server to access and update the stored data for various application purposes. The users may resort to KGC for ensuring the storage security of the outsourced data,while hoping to keep the data private.

In most of time it behaves properly and does not deviate from the prescribed protocol execution.During providing the cloud data storage based services, for their own benefits the Cloud Server might neglect to keep or deliberately delete rarely accessed data files which belong to ordinary cloud users.The Cloud Server may decide to hide the data corruptions caused by server hacks or Byzantine failures to maintain reputation.It is in the business of auditing, is reliable and independent, and thus has no incentive to collude with either the Cloud Server or the users during the auditing process.It should be able to efficiently audit the cloud data storage without local copy of data and without bringing in additional on-line burden to cloud users.

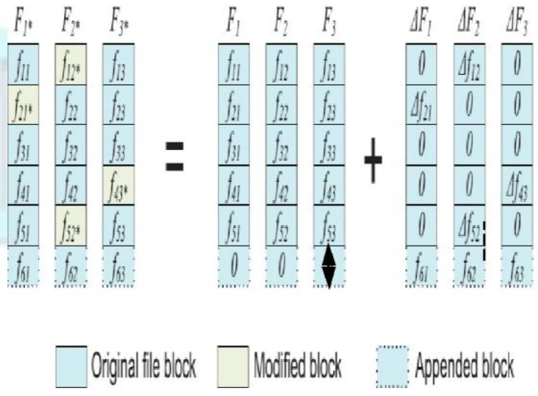


Fig.3.Logical representation of data dynamics including block update,append and delete

IV. RESULTS AND DISCUSSIONS

The experimental results and performance evaluation on the three combination of partition and grouping on the data storing blocks are illustrated in Fig. 3 where blocks denote results of 1) Blue block represents original block of data storage with a nodal one of 2)White block represents modified block stacking through data storage.Appended block represents nodal form of data.An effective and flexible distributed scheme with explicit dynamic data support eventually and also it performs reduce the storage space in cloud for better performing.Through detailed security and extensive experiment results

V. Conclusion and Future Work

To achieve the assurances of cloud data integrity and availability and enforce the quality of dependable cloud storage service for users, To propose an effective and flexible distributed scheme with explicit dynamic data support, including block update, delete, and append. Through detailed security and extensive experiment results. This scheme is highly efficient and resilient to Byzantine failure, malicious data modification attack, and even server colluding attacks. In future this scheme achieves the integration of storage correctness insurance and data error localization. whenever data corruption has been detected during the storage correctness verification across the distributed servers, can almost guarantee the simultaneous identification of the misbehaving servers.

References

[1] M. Arrington, “Gmail Disaster: Reports of mass Email Deletions,”htt p://www.tech-crunch.-com/2006/12/2 8/gmail disaster reports-of-mass-email -deletions,Dec. 2006.

[2] G. Ateniese, R. Burns, R. Curtmola, J. Herring,L. Kissner, Z.Peterson, and D. Song, “Provable Data Possession at Untrusted Stores,” Proc. 14th ACM Conf. Computer and Comm. Security (CCS’07), pp. 598-609, Oct. 2007.

[3] G.Ateniese,R.D. Pietro, L.V. Mancini, and G. Tsudik, “Scalable and Efficient Provable Data Possession,” Proc. Fourth Int’l Conf.Security and Privacy in Comm. Netowrks (SecureComm ’08), pp. 1-10,2008.

[4] Amazon.com,“Amazon Web Services (AWS)“http://aws.amazon.com”,2009.

[5] Amazon.com,“AmazonS3 Availability Event:July20,2008,”http://status. aws. ama zon .com/s3-20080720.html, July 2008.

[6] A. Juels and B.S. Kaliski Jr., “PORs: Proofs of Retrievability for Large Files,” Proc. 14th ACM Conf. Computer and Comm. Security(CCS ’07), pp. 584-597, Oct. 2007.

[7] J.Kincaid,“Media Max/The Linkup Closes Its Doors,”http://www.techcru nch.Com/2008/07/10/-media max the linkup-closesits-doors,July 2008.

[8] B. Krebs, “Payment Processor Breach May Be LargestEver,”http://voices .washingtonpost.com/securityfix/2009 /01/payment_processor_breach_may _b. ht ml , Jan. 2009.

[9] K. Ren, C. Wang, and Q. Wang, “Security Challenges for the Public Cloud,”IEEE Internet Computing, vol. 16, no. 1, pp. 69-73,2012.

[10] Sun Microsystems, Inc., “Building Customer Trust in Cloud Computing with Transparent Security,”https:// www.sun.com/offers/details/-sun_tran sparency.xml, Nov. 2009.

[11] M.A. Shah, M. Baker, J.C. Mogul, and R. Swaminathan, “Auditing to Keep Online Storage Services Honest,” Proc. 11th USENIX Workshop Hot Topics in Operating Systems (HotOS ’07), pp. 1-6, 2007.

[12] M.A. Shah, R. Swaminathan, and M. Baker, “Privacy-Preserving Audit and Extraction of Digital Contents,” Cryptology ePrint Archive, Report 2008/186, http://eprint.iacr.org, 2008.

[13] C. Wang, Q. Wang, K. Ren, and W. Lou, “Ensuring Data Storage Security in Cloud Computing,” Proc. 17th Int’l Workshop Quality ofService (IWQoS ’09), pp. 1-9, July 2009.

[14] S.Wilson,“AppengineOutage,”http://www.cio weblog.com/50226711/appengine-outage. php, June 2008.

[15] Q. Wang, C. Wang, J. Li, K. Ren, and W. Lou, “Enabling PublicVerifiability and Data Dynamics for Storage Security in Cloud Computing,” Proc. 14th European Conf. Research in Computer Security (ESORICS ’09), pp. 355-370, 2009.