International Journal of Future Innovative Science and Engineering Research (IJFISER)
Volume - 2, Issue - I ISSN (Online): 2454- 1966

Research Manuscript Title

SECURE ERASURE CODE TECHNIQUES USING SOFTWARE AS A SERVICE

[1]Dr.P.Sumitra, [2]P.Kaladevi

Assistant Professor, M.Phil Scholar,
Department of Computer Science & Applications
Vivekanandha college of Arts and Science for Women,
Elayampalayam, Tiruchengode.

E-Mail: **deviselvamct@gmail.com**

March – 2016

www.istpublications.com

SECURE ERASURE CODE TECHNIQUES USING SOFTWARE AS A SERVICE

[1]Dr.P.Sumitra, [2]P.Kaladevi

Assistant Professor, M.Phil Scholar,
Department of Computer Science & Applications
Vivekanandha college of Arts and Science for Women,
Elayampalayam, Tiruchengode.

E-Mail: **deviselvamct@gmail.com**

ABSTRACT

Cloud storage enables users to remotely store their data and make the on-demand high quality cloud applications without the burden of local hardware and software management. Though the benefits of the cloud storage are made clear such a service is also relinquishing users physical possession of their outsourced data, which inevitably poses new security risks toward the correctness of the data in cloud. A flexible distributed storage integrity auditing mechanism(SIAM), utilizing the homomorphic token and distributed erasure-coded data. The design allows users to audit the cloud storage with very lightweight communication and computation cost. The auditing result not only ensures strong cloud storage correctness guarantee, but also simultaneously achieves fast data error localization the identification of misbehaving server. Considering the cloud data are dynamic in nature, the design further supports secure and efficient dynamic operations on outsourced data, including block modification, deletion, and append. Analysis shows that the scheme is highly efficient and resilient against Byzantine failure, malicious data modification attack, and even server colluding attacks**.**

Keywords *- Cloud Storage, SIAM, Erasure code data and Homomorphic token, Byzantine failure*

1. INTRODUCTION

Cloud Computing means "Internet based Computing." The Internet is commonly visualized as clouds. Hence the term “cloud computing” for computation done through the Internet .It is a technology that uses the internet and central remote servers to maintain data and application. Computing is a general term for anything that involves delivering hosted services over the Internet the services are broadly divided into three categories: Infrastructure-as-a-Service, Platform as a- Service and Software-as-a-Service. Infrastructure as a service sometimes referred as hardware as a service. IaaS includes storage, hardware, servers and networking components. IaaS Provides user computing resources and storage comprised with many servers as an on demand and “pay per use” service: Data Centre, Bandwidth, Private Line Access, Servers and Server tool itself is hosted in the Cloud and accessed through a browser .With PaaS, developers can build Web applications without installing any tools on their computers. PaaS room. Platform as a service (PaaS) model provides a platform for creating applications. PaaS solutions are essentially development platforms for which the development bundles all stack components (hardware, infrastructure, storage) together with database, security, workflow, user interface, and other tools that allow users to create and host powerful business applications, web sites, and mobile apps kind of cloud computing provides development environment as a service. The consumer can use the middleman’s equipment to develop his own program and deliver it to the users through Internet and servers. The consumer controls the applications that run in the environment, but

does not control the operating system, hardware or network infrastructure on which they are running Software as a service (SaaS) cloud providers install and operate application software in the cloud and cloud users access the software from clients. SaaS can be defined through five key ideas: (i)services are fully managed and hosted(ii) have regular recurring payments(iii) allow for anytime and anywhere access (iv)have multiple tenants on servers(v) don't require installation of specialized software. SaaS is software that owned, delivered and managed remotely by one or more providers and that is offered in a pay-per-use manner .SaaS in simple terms can be defined as "Software deployed as a hosted service and accessed over the Internet." SaaS clouds provide scalability and also shifts significant burdens from subscribers to providers, resulting in a number of opportunities for greater efficiency. Public cloud services are characterized as being available to clients from a third party service provider via the Internet.

The term "public" does not always mean free, even though it can be free or fairly inexpensive to use. A public cloud does not mean that a user's data is publicly visible; public cloud vendors typically provide an access control mechanism for their users. Public clouds provide an elastic, cost effective means to deploy solutions. A private cloud offers many of the benefits of a public cloud computing environment, such as being elastic and service based.

The difference between a private cloud and a public cloud is that in a private cloud-based service, data and processes are managed within the organization without the restrictions of network bandwidth, security exposures and legal requirements that using public cloud services might entail. In addition, private cloud services offer the provider and the user greater control of the cloud infrastructure, improving security and resiliency because user access and the networks used are restricted and designated.

A community cloud is controlled and used by a group of Organizations that have shared interests, such as specific security requirements or a common mission. The members of the community share access to the data and applications in the cloud. A community cloud is controlled and used by a group of Organizations that have shared interests, such as specific security requirements or a common mission. The members of the community share access to the data and applications in the cloud.

An [3] effective and flexible distributed storage verification scheme with explicit dynamic data support to ensure the correctness and availability of user's data in the cloud. Erasure correcting code in the file distribution preparation to provide redundancies and guarantee the data dependability against Byzantine servers a storage server may fail in arbitrary ways. Construction reduces the communication and storage overhead as compared to the traditional replication-based file distribution techniques. By using the homomorphic token with distributed verification of erasure coded data achieves corruption has been detected during the storage correctness verification and guarantee the simultaneous localization of data errors.

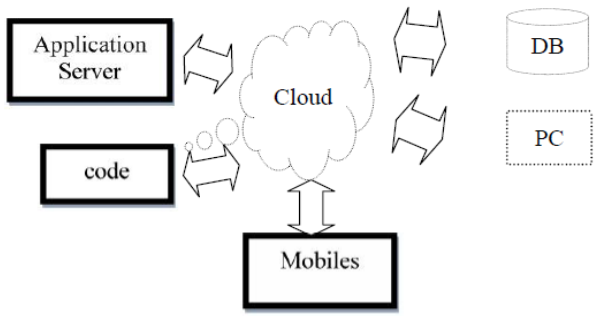

Fig.1. Cloud Computing Environment

Contribution can be summarized as the following three aspects1) Compared to many of its predecessors which only provide binary results about the storage status across the distributed servers scheme achieves the integration of storage correctness insurance and data error localization the identification of misbehaving servers. 2) Unlike most prior works for ensuring remote data integrity the new scheme further supports secure and efficient dynamic operations on data blocks including update, delete, and append. 3) The experiment results demonstrate the proposed scheme is highly efficient. Extensive security analysis shows our scheme is resilient against Byzantine failure, malicious data modification attack and even server colluding attacks.

2. RELATED WORK

HAIL: High-Availability and Integrity Layer (HAIL) [1] a distributed cryptographic system that allows a set of servers to prove to a client that a stored file is intact and retrievable. A strong formal adversarial model for HAIL. The two basic approaches to client verification of file availability and integrity. The HAIL is a remote-file integrity checking protocol that offers efficiency, security, and modelling improvements over straight forward multi-server application of POR protocols.
HAIL manages file integrity and availability across a collection of server's independent storage services. It makes use of PORs as building blocks by which storage resources can be tested and reallocated when failures are detected. HAIL does so in that transcends the basic single-server design of PORs and instead exploits both within-server redundancy and cross-server redundancy. POR protocol that only supports a limited number of challenges and high corruption rates are quickly. HAILS only provide assurance for static files.

Dynamic Data Provable Possession

The provable data possession (PDP) model, the client pre-processes the data and then sends it to an untrusted server for storage. while keeping a small amount of meta-data. A definitional framework and efficient constructions for dynamic provable data possession (DPDP) which extends the PDP model to support provable updates on the stored data is provided. A DPDP scheme is to an outsourced file systems and version control systems. The integrity of data stored at untrusted servers is prevented. Data (often represented as a file F) is pre-processed by the client and metadata used for verification purposes is produced. The file is then sent to an untrusted server for storage, and the client may delete the local copy of the file. The client keeps some information to check server responses later. The server proves the data has not been tampered with by responding to challenges sent by the client. PDP scheme apply only to the static (or append only) files.

Practical Byzantine Fault Tolerance and Proactive Recovery

BFT can be used to build highly available systems that tolerate Byzantine faults. A proactive recovery mechanism that allows the replicated system to tolerate any number of faults over the lifetime of the system. The most important optimization is the use of symmetric cryptography to authenticate messages. Detection of denial-of-service attack sailed at increasing the window and detects when the state of replica is corrupted by an attacker is provided. BFT have two important properties.

(i)Intersection

(ii) Availability.

Properties enable the use of quorums as a reliable memory for protocol information. Replicas write information to a quorum and they collect quorum certificates, which are sets with one message from

each element in a quorum saying that it stored the information. These certificates are proof that the information has been reliably stored and will be reflected in later reads. Reads from the reliable memory obtain the information stored by all the elements in a quorum and pick the latest piece of information. BFT does not rely on synchrony to provide safety.

Multiple Data Provable Data Possession

` Multiple-replica provable data possession (MR-PDP) [4] extends previous work on data possession proofs for a single copy of a file in client/server storage system. And verify through a challenge-response protocol that each unique replica can be produced at the time of the challenge and the storage system uses t times the storage required to store a single replica. The problem of creating multiple unique replicas of a file in a distributed storage system is gained. Replica Maintenance, file checking and can generate further replicas on demand is reduced. Generation of further replicas on demand is little expensive.

Drawbacks

There is no high security provided in the Cloud server for data safety. The main drawback is there is no backup process and data safety. General encryption schemes protect data confidentiality, but also limit the functionality of the storage system because few operations are supported over encrypted data constructing a secure storage system that supports multiple functions is challenging .when the storage system is distributed and has no central authority. Storing data in a third party cloud system causes serious concern on data confidentiality.

3. PROPOSED SYSTEM

An effective distributed data verification and data retrieval mechanism is implemented. It provides assurance to the integrity and availability of the data uploaded into the cloud. The uploaded data is divided into blocks and stored in different servers. By this data availability can be assured using erasure corrected code. The algebraic property of erasure code helps to retrieve the lost or modified data. Unreliable servers which perform these data block modifications are identified by tokens by using challenge response auditing mechanism. Third Party Auditor (TPA) performs this data error localization process identification of misbehaving servers. The client's uploaded data will be encrypted by the cloud server and this prevents TPA from accessing the data. Erasure coding (EC) is a method of data protection in which data s broken into fragments expanded and encoded with redundant data pieces and stored across a set of different locations such as disks, storage nodes or geographic locations. Erasure coding creates a mathematical function to describe a set of numbers so they can be checked for accuracy and recovered if one is lost to as polynomial interpolation or oversampling this is the key concept behind erasure codes. Erasure coding can be useful with large quantities data and any applications or systems that need to tolerate failures, such as disk array systems, data grids, distributed storage applications, object stores and archival storage. One common current use case for erasure coding is object based cloud storage.

Advantages

(i) One way to provide data robustness is to replicate a message such that each storage server stores a copy of the message. It is very robust because the message can be retrieved as long as one storage server survives

(ii) The encryption scheme supports encoding operations over encrypted messages and forwarding operations over encrypted and encoded messages. The tight integration of encoding, encryption, and

forwarding makes the storage system efficiently meet the requirements of data robustness, data confidentiality, and data forwarding

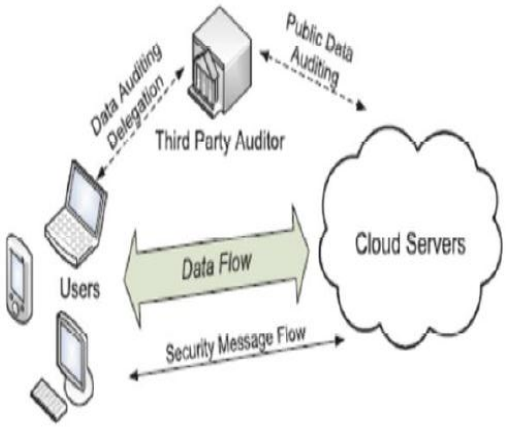

Fig 2. Secure Cloud Storage System

4. EXPERIMENTAL RESULTS

Servers are required to operate only on specified rows in each challenge-response execution. The storage correctness challenge Scheme would be undermined even if those modified blocks are covered by the specified rows Action must be taken to maintain replicas despite failure; otherwise, all replicas will be lost.

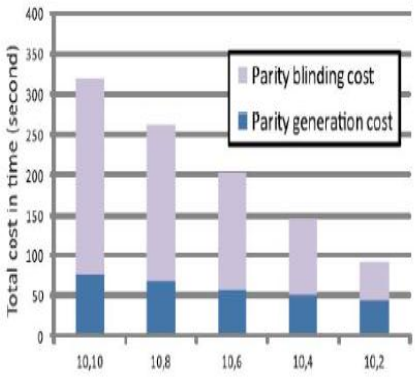

Fig 3. Challenge-response execution.

5. CONCLUSION

Threshold proxy re-encryption scheme and integrate it with a decentralized erasure code such that a secure distributed storage system is formulated. The distributed storage system not only supports secure and robust data storage and retrieval, but also a user forward his data in the storage servers to another user without retrieving the data back. The main technical contribution is that the proxy re-encryption scheme supports encoding operations over encrypted messages as well as forwarding operations over

encoded and encrypted message. It is fully integrates encrypting, encoding, and forwarding mechanism of the data blocks.

REFERENCES

[1] K.D. Bowers, A. Juels, and A. Oprea, "HAIL: A High-Availability and Integrity Layer for Cloud Storage," Proc.ACM Conf. Computer and Comm. Security (CCS '09), pp. 187-198, 2009.

[2] M. Bellare, R. Canetti, and H. Krawczyk, "Keying Hash Functions for Message Authentication," Proc. 16th Ann. Int'l Cryptology Conf.Advances in Cryptology (Crypto'96), pp. 1-15, 1996.

[3] M. Bellare, O. Goldreich, and S. Goldwasser, "Incremental Cryptography: The Case of Hashing and Signing," Proc. 14thAnn. Int'l Cryptology Conf. Advances in Cryptology (CRYPTO '94),pp. 216-233, 1994.

[4] R. Curtmola, O. Khan, R. Burns, and G. Ateniese, "MR-PDP: Multiple-Replica Provable Data Possession," Proc. IEEE 28th Int'lConf. Distributed Computing Systems (ICDCS '08), pp. 411-420, 2008.

[5] C. Erway, A. Kupcu, C. Papamanthou, and R. Tamassia,"Dynamic Provable Data Possession," Proc. 16th ACM Conf.Computer and Comm. Security (CCS '09), pp. 213-222, 2009.

[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.S. Plank, S. Simmerman, and C.D. Schuman, "Jerasure: A Libraryin C/C++ Facilitating Erasure Coding for Storage Applications Version 1.2," Technical Report CS-08-627, Univ. of Tennessee, Aug. 2008

[8] M. Castro and B. Liskov, "Practical Byzantine Fault Tolerance and Proactive Recovery," ACM Trans. Computer Systems, vol. 20, no. 4, pp. 398-461, 2002.

[9] Q. Wang, C. Wang, K. Ren, W. Lou, and J. Li, "Enabling Public Auditability and Data Dynamics for Storage Security in Cloud Computing," IEEE Trans. Parallel and Distributed Systems, vol. 22, no. 5, pp. 847-859, 2011.

[10]George Nychis, Argyro Andreou, Deepti Chheda, and Alexander Giamas, "Analysis of Erasure Coding in a Peer to Peer Backup System, "IEEE Trans. on information networking,2008.