INTERNATIONAL JOURNAL OF APPLIED SCIENCE ENGINEERING AND MANAGEMENT

ISSN2454-9940www.ijsem.org

Vol 17, Issuse.2 April 2023

ISSN: 2454-9940

INTERNATIONAL JOURNAL OF APPLIED SCIENCE ENGINEERING AND MANAGEMENT

E-Mail :
editor.ijasem@gmail.com
editor@ijasem.org

www.ijasem.org

INTERNATIONAL JOURNAL OF APPLIED SCIENCE ENGINEERING AND MANAGEMENT

ISSN2454-9940www.ijsem.org

Vol 17, Issuse.2 April 2023

A Privacy-Preserving and Untraceable Group Data Sharing Scheme in Cloud computing

1.M. PRATHYUSHA, 2. P. SRI HARSHITHA, 3. D. HARI KRISHNA, 4. V. MOHANA

Article Info

Received: 09-01-2023 *Revised: 10 -02-2023* *Accepted: 22-03-2023*

OBJECTIVE:

We propose a novel privacy-preserving mechanism that supports public auditing on shared data stored in the cloud. Recent studies have been worked to promote the cloud computing evolve towards the internet of services. Subsequently, security and privacy issues are becoming key concerns with the increasing popularity of cloud services.

DOMAIN: Cloud computing

Abstract and introduction:

In this paper, we propose a novel privacy-preserving mechanism that supports public auditing on shared data stored in the cloud. In particular, we exploit ring signatures to compute verification metadata needed to audit the correctness of shared data. With our mechanism, the identity of the signer on each block in shared data is kept private from public verifiers, who are able to efficiently verify shared data integrity without retrieving the entire file. In addition, our mechanism is able to perform multiple auditing tasks simultaneously instead of verifying them one by one.The propose system, a privacy-preserving public auditing mechanism for shared data in the cloud. We utilize ring signatures to construct homomorphism authenticators, so that a public verifier is able to audit shared data integrity without retrieving the entire data, yet it cannot distinguish who is the signer on each block.

1 Asst. Professor, Department of Computer Science and Engineering

2,3,4, Student, Department of Computer Science and Engineering

QIS College of Engineering and Technology Ongole

To improve the efficiency of verifying multiple auditing tasks, we further extend our mechanism to support batch auditing. There are two interesting problems we will continue to study for our future work. One of them is traceability, which means the ability for the group manager to reveal theidentity of the signer based on verification metadata in some special situations.AES is associate degree unvarying instead of Feistel cipher. It‟s supported „substitution–permutation network‟. It contains of a series of joined operations, a number of that involve exchange inputs by specific outputs and other involve shuffling bits around.Interestingly, AES performs all its computations on bytes instead ofbits. Hence, AES treats the 128 bits of a plaintext block as sixteen bytes. These sixteen bytes square measure organized in four columns and 4 rows for process as a matrix

PROPOSED SYSTEM:

The propose system, a privacy-preserving public auditing mechanism for shared data in the cloud. We utilize ring signatures to construct homomorphism authenticators, so that a public verifier is able to audit shared data integrity without retrieving the entire data, yet it cannot distinguish who is the signer on each block.

To improve the efficiency of verifying multiple auditing tasks, we further extend our mechanism to support batch auditing. There are two interesting problems we will continue to study for our future work. One of them is traceability, which means the ability for the group manager to reveal theidentity of the signer based on verification metadata in some special situations.

Stands for "Simple Mail Transfer Protocol." this can be the protocol used for causation e-mail over the web. Your e-mail shopper uses SMTP to send a message to the mail server, and also the mail server uses SMTP to relay that message to the proper receiving mail server. Basically, SMTPcould be a set of commands that certifyand direct the transfer of electronic message. Once configuring the settingsfor your e-mail program, you always ought to set the SMTP server to your native net Service Provider's SMTP settings. However, the incoming mail server (IMAP or POP3) ought to be setto your mail account's server, whichcan differ than the SMTP server.

INTERNATIONAL JOURNAL OF APPLIED SCIENCE ENGINEERING AND MANAGEMENT

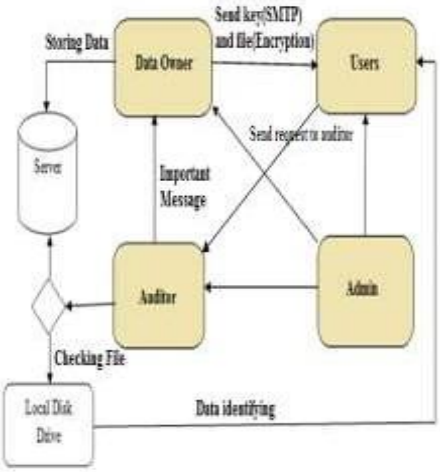
ISSN2454-9940www.ijsem.org

Vol 17, Issuse.2 April 2023

ADVANTAGES:

- The proposed system can perform multiple auditing tasks simultaneously They improve the efficiency of verification for multiple auditing tasks.
  - ➢ High security provide for file sharing.
  - ➢ Admin has control deleting users
  - ➢ Users can send request to auditor.

SYSTEM ARCHITECTURE:



HARDWARE AND SOFTWARE SPECIFICATION:

Software Requirement:

- Language - Java(JDK 1.7)
- OS - Windows 7 32bit
- MySql Server
- NetBeans IDE 7.1.2

Hardware Requirement :

i. 1 GB RAM

i. 80 GB Hard Disk

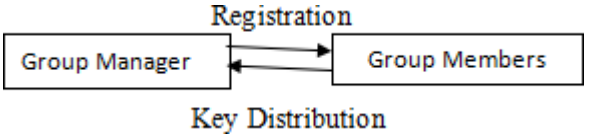
i. Above 2GHz Processor

i. Data Card

Module:

1. User Registration:

For the registration of user with identity ID the group manager randomly selects a number. Then the group manager adds into the group user list which will be used in the traceability phase. After theregistration, user obtains a private key which will be used for group signature generation and file decryption.



2. Public Auditing:

Homomorphic authenticators are unforgeable verification metadata generated from individual data blocks, which can be securely aggregated in such a way to assure an auditor that a

ISSN2454-9940www.ijsem.org

Vol 17, Issuse.2 April 2023

linear combination of data blocks is correctly computed by verifying only the aggregated authenticator. Overview to achieve privacy-preserving public auditing, we propose to uniquely integrate the Homomorphic authenticator with random mask technique. In our protocol, the linear combination of sampled blocks in the server‟s response is masked with randomness generated by a pseudo random function (PRF). The proposed scheme is as follows:

- Setup Phase
- Audit Phase

3. Sharing Data:

The canonical application isdata sharing. The public auditing property is especially useful when we expect the delegation to be efficient and flexible. The schemes enable a content provider to share her data in a confidential and selective way, with a fixed and small ciphertext expansion, by distributing to each authorized usera single and small aggregate key.

4. Integrity Checking:

Hence, supporting data dynamics for privacy-preserving public risk auditing is also of paramount importance. Now we show how our main scheme can be adapted to build upon the existing work to support data dynamics, including block level operations of modification, deletion and insertion. We can adopt this technique in our design to achieve privacy-preserving public risk auditing with support of data dynamics. The user download the particular file not download entire file.

LITERATURE SURVEY:

1. QoS Support for End Users of I/O-intensive Applications Using auditing Shared Storage Systems. Author: Xuechen Zhang ECE Department Wayne State Universities Trans. Kei Davison Alamos National Laboratory Parallel and Distributed Systems, vol. 21, no. 11, pp. 1586-1594, Nov. 2010.

We consider the problem of constructing an erasure code for storage over a network when the data sources are distributed. Specifically, we assume that there are n storage nodes with limited memory and k < n sources generating the data. We want a data collector, who can appear

anywhere in the network, to query any k storage nodes and be able to retrieve the data. We introduce Decentralized Erasure Codes, which are linear codes with a specific randomized structure inspired by network coding on random bipartite graphs. We show that decentralized erasure codes are optimally sparse, and lead to reduced communication, storage and computation cost over random linear coding.

2. Repair Locality from a Combinatorial Perspective. Author: Anyu Wang and Zhifang ZhangKey Laboratory of Mathematics Mechanization, IEEE Dec.2014.

3.

Plutus is a cryptographic storage system that enables secure file sharing without placing much trust on the file servers. In particular, it makes novel use of cryptographic primitives to protect and share files. Plutus features highly scalable key management while allowing individual users to retaindirect control over who gets access to their files. We explain the mechanisms in Plutus to reduce the number of cryptographic keys exchanged between users by using file groups, distinguish file read and write access, handle user revocation efficiently, and allow an untrusted server to authorize file writes. We have built a prototype of Plutus on OpenAFS. Measurements of this prototype show that Plutus achieves strong security with overhead comparable to systems that encrypt all network traffic.

3. On the Effective Parallel Programming of Multi-core Processors.Author: Prof.dr.ir. H.J. Sips Technische Universities Delft, promotor Prof.dr.ir. A.J.C. van Gemund Technische Universities Delft Prof.dr.ir. H.E. Bal. 7December 2010.

Availability is a storage system property that is both highly desired and yet minimally engineered. While many systems provide mechanisms to improve availability– such as redundancy and failure recovery – how to best configure these mechanisms is typically left to the system manager. Unfortunately, few individuals have the skills to properly manage the trade-offs involved, let alone the time to adapt these decisions to changing conditions. Instead, most systems are configured statically and with only a cursory understanding of how the configuration will impact overall

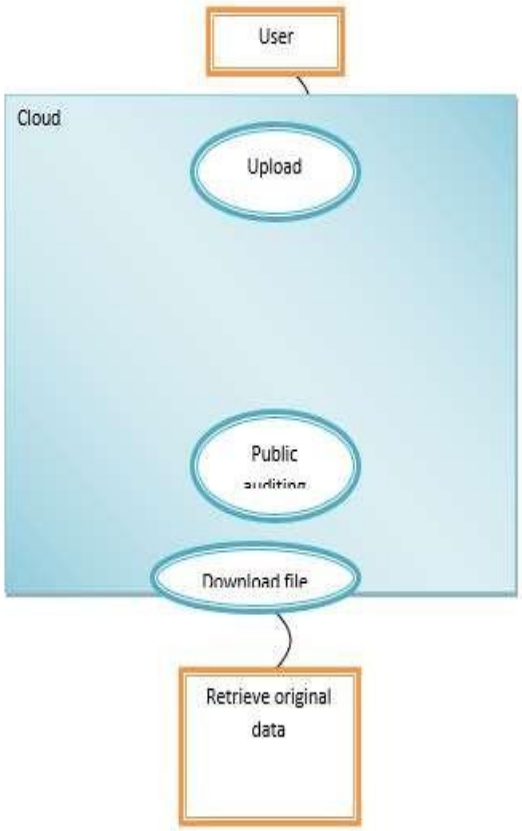
performance or availability. While this issue can be problematic even for individual storage arrays, it becomes increasingly important as systems are distributed – and absolutely critical for the wide area peer-to-peer storage infrastructures being explored. This paper describes the motivation, architecture and implementation for a new peer-to-peer storage system, called Total Recall that automates the task of availability management. In particular, the Total Recall system automatically measures and estimates the availability of its constituent host components, predicts their future availability based on past behavior, calculates the appropriate redundancy mechanisms and repair policies, and delivers user-specified availability while maximizing efficiency.

4. Parallel Reed/Solomon Coding on Multicore Processors.

Author:Peter Sobs Institute of Computer Engineering University of LuebeckLuebeck, Germany. 2010 EEE DOI 10.1109/SNAPI.2010.16

This paper sketches the design ofPAST, a large-scale, Internet-based, global storage utility that provides scalability, high availability, persistence and security. PAST is a peer-to-peer Internet application and is entirely selforgaining. PAST nodes serve as access points for clients, participate in the routing of client requests, and contribute storage to the system. Nodes are not trusted, they may join the system at any time and may silently leave the system without warning. Yet, the system is able to provide strong assurances, efficient storage access, load balancing and scalability.

DFD Level 0:

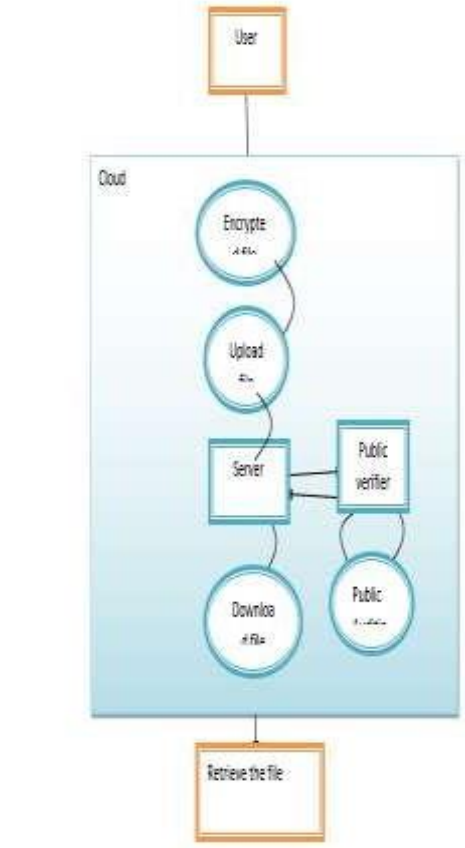


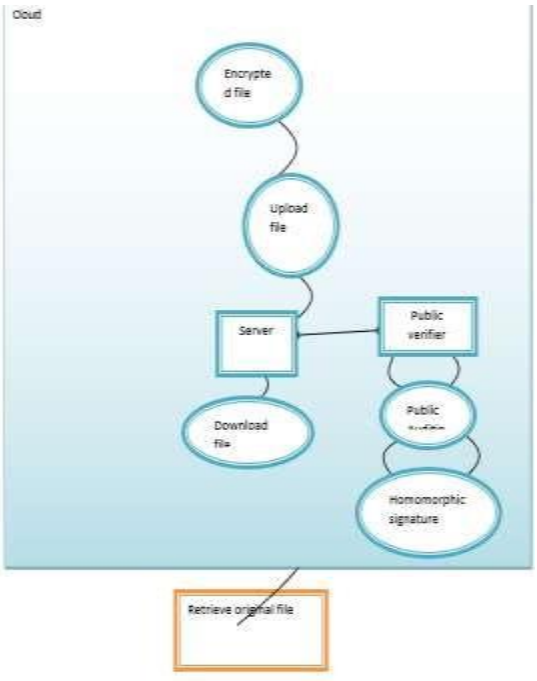
INTERNATIONAL JOURNAL OF APPLIED SCIENCE ENGINEERING AND MANAGEMENT

ISSN2454-9940www.ijsem.org

Vol 17, Issuse.2 April 2023

DFD 1:





Future work:

As a response, erasure codingas an alternative to backup has emerged as a method of protecting against drive failure.Raid just does not cut it in the age of high-capacity HDDs. The larger a disk's capacity, thegreater the chance of bit error.And when a disk fails, the Raid rebuild process begins, during which there isno protection against a second (or third) mechanism failure. So not only has the risk of failure during normal operation grown with capacity, it is much higher during Raid rebuild, too. Also, rebuild times were once measured in minutes or hours, but disk transfer rates have not kept pace with the rate of disk capacity expansion, so large Raid rebuilds can now take days or even longer.

INTERNATIONAL JOURNAL OF APPLIED SCIENCE ENGINEERING AND MANAGEMENT

ISSN2454-9940www.ijsem.org

Vol 17, Issuse.2 April 2023

CONCLUSION:

In this paper, we present a secure and collusion-resistant proxy re-encryption protocol and an untraceable and faulttolerant OCLT-ORAM protocol for group data sharing in a cloud storage scheme. Based on key exchange, the proposed approach can efficiently generate the users conference key, which can be used to protect the security of shared data and prevent malicious user collusion with other users. In addition, security of shared group data in the cloud and access control are achieved with respect to the proxy re-encryption technique. Moreover, according to the operation algorithms and the novel OCLT storage structure, our OCLT- ORAM protocol can support untraceability of address sequencesand efficiency in data storage. Fault- tolerant and tamper protection features are accomplished with respect to pointer tuples. The sufficient security proof indicates the security of our protocol. The experimental comparison results could be considered as validation of the performance of our protocol, making it substantially more convincing.

REFERENCES:

[1] J. Yu, K. Ren, C. Wang, and V. Varadharajan, “Enabling cloud storage auditing with key-exposure

resistance," Information Forensics and Security, IEEE Transactions on, vol.10, no. 6, pp. 1167–1179, 2015.

[2] R. S. Bali and N. Kumar, "Secure clustering for efficient data dissemination in vehicular cyberphysical systems," Future Generation Computer Systems, pp. 476–492, 2016.

[3] S. Zarandioon, D. D. Yao, and V. Ganapathy, "K2c: Cryptographic cloud storage with lazy revocation and anonymous access," in International Conference on Security and Privacy in Communication Systems. Springer, 2011, pp. 59–76.

[4] C. Wang, Q. Wang, K. Ren, and W. Lou, "Privacy-preserving public auditing for data storage security in cloud computing," in 2010 proceedings ieee infocom. IEEE, 2010, pp. 1–9.

[5] M. Ali, R. Dhamotharan, E. Khan, S. Khan, A. Vasilakos, K. Li, and A. Zomaya, "Sedasc: Secure data sharing in clouds," IEEE Systems Journal, vol. 11, no. 2, pp. 395–404, 2017.