INTEGRITY AUDITING FOR MULTI-COPY IN CLOUD STORAGE BASED ON RED-BLACK TREE

E AMARNATH REDDY[1], V RAMESH[2], Dr J REDDEPPA REDDY[3]

1,2 & 3, Associate Professor, CSE department, Brilliant Institute of Engineering & Technology, Hyderabad, TS.

ABSTRACT

With the rapid development of cloud storage, cloud users are willing to store data in the cloud storage system, and at the same time, the requirements for the security, integrity, and availability of data storage are getting higher and higher. Although many cloud audit schemes have been proposed, the data storage overhead is too large and the data cannot be dynamically updated efficiently when most of the schemes are in use. In order to solve these problems, a cloud audit scheme for multi-copy dynamic data integrity based on red-black tree full nodes is proposed. This scheme uses ID-based key authentication, and improves the classic Merkel hash tree MHT to achieve multi-copy storage and dynamic data manipulation, which improves the efficiency of real-time dynamic data update (insertion, deletion, modification). The third-party audit organization replaces users to verify the integrity of data stored on remote cloud servers, which reduces the computing overhead and system communication overhead. The security analysis proves that the security model based on the CDH problem and the DL problem is safe. Judging from the results of the simulation experiment, the scheme is safe anf efficient.

1. INTRODUCTION

In the face of increasing user management and sharing needs, the emergence of cloud computing and cloud storage provides a new scheme for it. Users can obtain sufficient storage capacity at a lower price, and at the same time, highly concentrated computing resources greatly improve computing power. Usually when people use cloud storage services, they upload their data to the cloud and store it on a remote cloud server. In order to save local storage resources, the local copy will be deleted. There are two hidden dangers in this way.

One is the lack of control over the confidentiality and integrity of the data and the other is that it is difficult to recover the data if the local copy is deleted. In order to solve these problems, the researchers proposed that users can encrypt data before outsourcing and sending it to a remote cloud server. People also think of improving the availability and recoverability of data by storing multiple copies of the original data. Suppose that part of the users' data is damaged, only one copy of the data is needed to restore the data correctly, and it remains unchanged with the data in the cloud .

Ateniese et al. proposed the concept of provable data possession (PDP). Users can effectively verify the integrity of cloud server data without retrieving the entire file, and based on homomorphic linear verification,

they proposed an effective and proved a secure PDP scheme, but the scheme it proposes is only for static data. In the case of increasing data, dynamic operation of data is also a key research point of later researchers . Wang et al. proposed a dynamic data scheme based on Merkle hash tree. Luo et al. used the Shamir secret sharing concept to improve the authentication tag based on polynomials. Barsoum et al. extended the PDP model and proposed a map-based provable multi-copy dynamic data possession (MB-PMDDP) scheme. Users can dynamically manipulate data and store fewer copies. Security is guaranteed, but any insert and delete operations will result in the need to recalculate the label and the position of the operation block, which will incur high calculation costs. Subsequently, the scheme was proposed, which greatly improved the method of dynamic update efficiency.

At the same time, Yang et al. proposed a public cloud audit scheme for dynamic update of user data and revocation of user data, but it did not solve the problem of dynamic revocation at any time. Min et al. proposed an integrity verification scheme based on spatiotemporal chaos, which supports dynamic data analysis, blinding information, and preventing third parties from leaking user data privacy. Min et al. proposed a data integrity verification scheme based on a binary balanced tree. The efficiency of data update has been greatly improved, and it also provides us with a research direction.

2. LITERATURE SURVEY

TITLE: ‘‘Light-weight and privacy-preserving secure cloud auditing scheme for group users via the third party medium,’’

ABSTRACT: To verify the integrity of cloud data, many cloud storage auditing schemes have been proposed. However, most of them incur a lot of computation overhead for users when data authenticators are generated or the data integrity is verified, which inevitably brings in heavy burdens to resource-constrained users. To overcome this problem, we propose a cloud storage auditing scheme for group users, which greatly reduces the computation burden on the user side. In our scheme, we introduce a Third Party Medium (TPM) to perform time-consuming operations on behalf of users. The TPM is in charge of generating authenticators for users and verifying data integrity on behalf of users. In order to protect the data privacy against the TPM, we blind data using simple operations in the phase of data uploading and data auditing. The user does not need to perform time-consuming decryption operations when using cloud data. We set an expiration time of the authorization to make sure only the TPM who possesses the authorization within valid period is able to upload data to the cloud and challenge the cloud data. The security proof and the performance analysis show that our proposed scheme is secure and efficient.

TITLE: ‘Cloud and IoT based smart architecture for desalination water treatment,’’

ABSTRACT: Increasing water demand and the deteriorating environment has continuously stressed the requirement for new technology and methods to attain optimized use of resources and desalination management, converting seawater into pure drinking water. In this age, the Internet of Things use allows us to optimize a series of previously complicated processes to perform and required enormous resources. One of these is optimizing the management of water treatment. This research presents an implementable water treatment model and suggests smart environment that can control water treatment plants. The proposed system gathers data and analysing to provide the most efficient approach for water desalination operations. The desalination framework integrates smart enabling technologies such as Cloud Portal, Network communication, Internet of Things, Sensors powered by solar energy with ancient water purification as part of seawater's desalination project. The proposed framework incorporates the new-age technologies, which are essential for efficient and effective operations of desalination systems. The implemented desalination dual membrane framework uses solar energy for purifying saline water using ancient methods to produce clean water for drinking and irrigation. The desalination produced 0.47 m3/l of freshwater from a saline concentration of 10 g/l, consuming 8.31 KWh/m3 energy for production from the prototype implementation, which makes desalination process cost effective.

TITLE: ‘‘CGP: Cluster-based gossip protocol for dynamic resource environment in cloud,’

ABSTRACT: Since the recent past, cloud computing is developing as a solution to expansive calculation and information storage issues in the form of services. It gives a stage to ask for computational assets with "on interest payments per use arrangement". It thus opens ways to getting to boundless assets with negligible equipment and programming at the customers' end. This paper goes for the advancement of a cloud administration's provisioning structure by building up a dynamic load-balancer for the cloud. In this article, a framework and protocol for the resource environment in the cloud have proposed. Distributed Hash Table (DHT) protocol has been utilized for a service query to perform a job agreed by the user. For load balancing, gossip protocol has been used for inter/intra-cluster gossip. For inter-cluster gossip, the load is balanced among the leaders of every cluster. The proposed protocol uses the inter-cloud resource management, where a leader is selected from the cloud that interacts to other cloud and decides on virtual machine (VM) migration. The decision about job allocation is not acknowledged by a single machine, which generates the scalable architecture of the proposed protocol. The protocol considers the current load situation and decides at the time of request submission. This protocol is adaptable, reliable and scalable and supports green computing by utilizing server solidification.

3. EXISTING SYSTEM

In this protocol, they used the rank characteristics of the Merkel hash tree to verify the data, but all its copies are existing on a cloud storage server, the performance of multiple copies is meaningless. To solve this problem, Li et al. proposed to deliver all copies to different cloud storage servers, and audit the integrity of all copies through homomorphic verifiable tags

Other aspects, such as privacy protection and data deduplication , have also been studied in remote data integrity auditing. Although the batch update storage of multiple copies can be achieved, the audit cost has always been high and the efficiency is not high. Therefore, in this article, we explore how to optimize the storage structure and reduce dynamic operation overhead, so as to design an effective dynamic multi-copy integrity audit scheme.

DISADVANTAGES OF EXISTING SYSTEM

The first limitation that we can extend is rank characterestics due to which there is a storage overhead. And the second limitation is data deduplication, which allows users to enable the changes.

PROPOSEDSYSTEM

A. DYNAMIC STORAGE STRUCTURE RED-BLACK TREE

In order to establish a more complete cloud storage service system, we use the red-black tree data structure for data storage. Compared with the balanced binary tree, although the red-black tree algorithm has the same time complexity, its statistical performance is higher. For dynamic data update, the traditional tree storage structure requires a lot of queries and adjustment operations in the worst case. If the data is stored in the data structure of the red-black tree, because it is not strictly balanced, its query ability is slightly weaker, but its insertion and deletion capabilities are completely stronger than the balanced binary tree. In our scheme, each copy corresponds to a red-black tree with a complete node and is stored in the CSP, and the data block copy in each copy corresponds to a node value, which is stored in the TPA. According to the node value of the binary tree, the location of the data block can be verified, which greatly reduces the verification path and improves the system efficiency. Here, the red-black tree stored in the CSP is abbreviated as C-RBTree, and the red-black tree stored in the TPA is abbreviated as T-RBTree.

B. CONSTRUCTION OF OUR PROPOSAL

In the program, the review process is divided into two phases: the setup phase and the verification phase. The previous phase is some preparations, including: KeyGen, ReplicaGen and TagGen. The system setting is mainly for the user. The user generates a public key and a private key pair through the KeyGen algorithm, and then performs other pre-processing tasks through ReplicaGen and TagGen. The latter phase includes three algorithms: ChalGen, ProofGen and VerifyProof. At this stage, users, CSP, and TPA will participate to perform data verification. In the ChalGen algorithm, the TPA sends verification challenge information to the CSP, and then the CSP responds in the ProofGen algorithm to prove the integrity of the stored data. In the final Verify Proof algorithm, TPA audits the proof and sends the audit results to the user by TPA.

C. DYNAMIC OPERATION VERIFICATION

For each data change operation, the user will send a request to the CSP to run the dynamic operation. After receiving the request, the CSP will dynamically update the data. According to the user's request, it will implement operations such as modification, insertion, and deletion.

4.SYSTEM ARCHITECTURE .

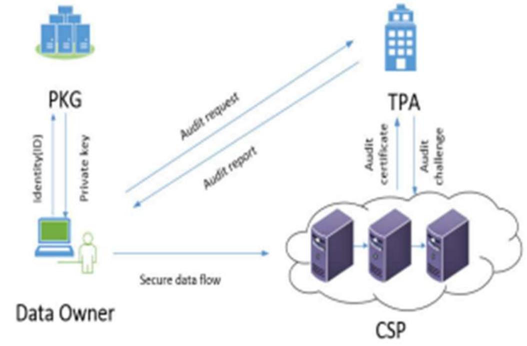
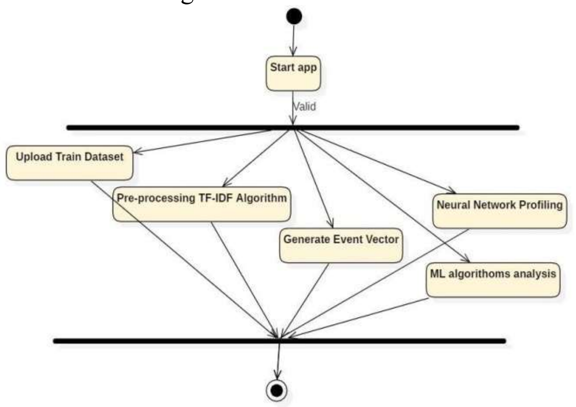


FIGURE 1. The system model of the data integrity auditing.

Activity Diagram

A graphical representation of the work process of stepwise exercises and activities with support for decision, emphasis and simultaneousness, used to depict the business and operational well-ordered stream of parts in a framework furthermore demonstrates the general stream of control.



5. SYSTEM IMPLEMENTATION

There are 4 modules:

1. TPA
2. PKG

3. User
4. Cloud

TPA:-

- Login
- T-RBT Details
- Audit Request
- Download Request
- Logout

User:-

- Register
- Login
- Upload Files
- My Files
- My Profile
- Audit Files
- Logout

Cloud:-

- Login
- C-RBT Details
- Audit Challange
- Logout

PKG:-

- Login
- User Details
- User Request
- Logout

6.1 TYPES OF TESTING

■Unit testing

Unit testing involves the design of test cases that validate that the internal program logic is functioning properly, and that program inputs produce valid outputs. All decision branches and internal code flow should be validated. It is the testing of individual software units of the application .it is done after the completion of an individual unit before integration. This is a structural testing, that relies on knowledge of its construction and is invasive. Unit tests perform basic tests at component level and test a specific business process, application, and/or system configuration. Unit tests ensure that each unique path of a business process performs accurately to the documented specifications and contains clearly defined inputs and expected results.

■Integration testing

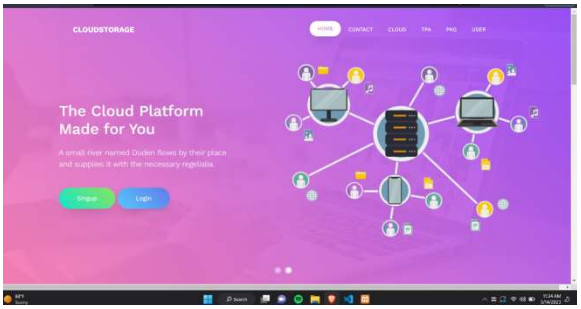
Integration tests are designed to test integrated software components to determine if they actually run as one program. Testing is event driven and is more concerned with the basic outcome of screens or fields. Integration tests demonstrate that although the components were individually satisfaction, as shown by successfully unit testing, the combination of components is correct and consistent. Integration testing is specifically aimed at exposing the problems that arise from the combination of components.

■Functional test

Functional tests provide systematic demonstrations that functions tested are available as specified by the business and technical requirements, system documentation, and user manuals.

Functional testing is centered on the following items:

7.RESULTS



The Cloud Platform Made for You

A small river named Duden flows by their place and supplies it with the necessary regelialia.

fig.7. 1 uploading of dataset

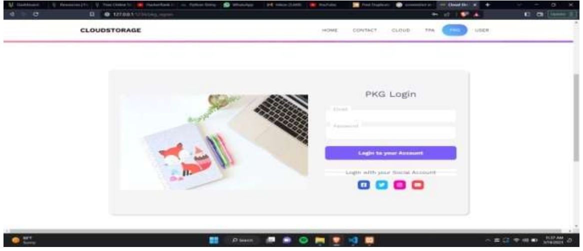
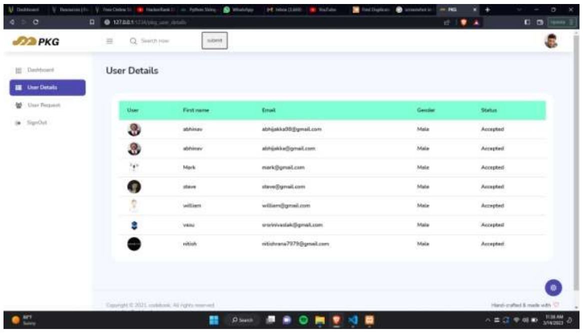


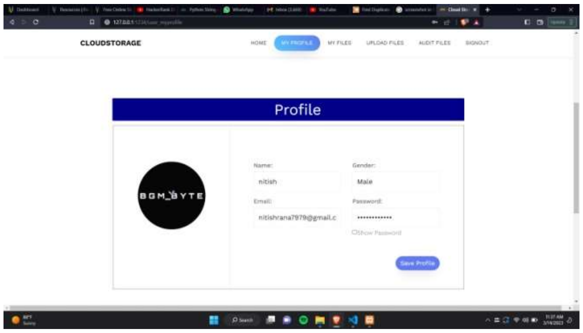
fig.7.2 dataset loaded



User Details

User	First name	Email	Gender	Status
	abhinav	abhijakka98@gmail.com	Male	Accepted
	abhinav	abhijakka@gmail.com	Male	Accepted
	Mark	mark@gmail.com	Male	Accepted
	steve	steve@gmail.com	Male	Accepted
	william	william@gmail.com	Male	Accepted
	vasu	srinivasdak@gmail.com	Male	Accepted
	nitish	nitishrana7979@gmail.com	Male	Accepted

fig.7.3 user details



Name: nitish

Gender: Male

Email: nitishrana7979@gmail.c

Password: •••••••••••••

☐ Show Password

8. CONCLUSION & FUTURE WORK

This paper proposes an effective multiple copies data integrity verification scheme based on red-black tree in cloud storage. It supports dynamic operations on multiple copies, which can improve efficiency. In terms of data storage, the red-black tree data structure storage is adopted to effectively improve data storage efficiency and simplify data update operations. The theoretical analysis of our scheme also proves the security of the scheme. The experimental results also show that our scheme is superior to other comparative schemes in terms of computational cost, storage cost, and communication cost. The experimental analysis demonstrate that our scheme achieves desirable security and efficiency.

REFERENCES

[1] W. Shen, J. Yu, H. Xia, H. Zhang, X. Lu, and R. Hao, ‘‘Light-weight and privacy-preserving secure cloud auditing scheme for group users via the third party medium,’’ J. Netw. Comput. Appl., vol. 82, pp. 56–64, Mar. 2017.

[2] M. Alshehri, A. Bhardwaj, M. Kumar, S. Mishra, and J. Gyani, ‘‘Cloud and IoT based smart architecture for desalination water treatment,’’ Environ. Res., vol. 195, Apr. 2021, Art. no. 110812, doi: 10.1016/ j.envres.2021.110812.

[3] S. Srivastava, S. Saxena, R. Buyya, M. Kumar, A. Shankar, and B. Bhushan, ‘‘CGP: Cluster-based gossip protocol for dynamic resource environment in cloud,’’ Simul. Model. Pract. Theory, vol. 108, Apr. 2021, Art. no. 102275, doi: 10.1016/j.simpat.2021.102275.

[4] K. He, J. Chen, Q. Yuan, S. Ji, D. He, and R. Du, ‘‘Dynamic group-oriented provable data possession in the cloud,’’ IEEE Trans. Dependable Secure Comput., early access, Jul. 2, 2019, doi: 10.1109/TDSC.2019.2925800.

5] M. Kumar, M. Alshehri, R. AlGhamdi, P. Sharma, and V. Deep, ‘‘A DE-ANN inspired skin cancer detection approach using fuzzy C-means clustering,’’ Mobile Netw. Appl., vol. 25, no. 4, pp. 1319–1329, Aug. 2020, doi: 10.1007/s11036-020-01550-2.

[6] L. Zhou, A. Fu, G. Yang, H. Wang, and Y. Zhang, ‘‘Efficient certificateless multi-copy integrity auditing scheme supporting data dynamics,’’ IEEE Trans. Dependable Secure Comput., early access, Aug. 4, 2020, doi: 10. 1109/TDSC.2020.3013927.

[7] C. Dhasarathan, M. Kumar, A. K. Srivastava, F. Al-Turjman, A. Shankar, and M. Kumar, ‘‘A bio-inspired privacy-preserving framework for healthcare systems,’’ J. Supercomput., early access, Mar. 19, 2021, doi: 10.1007/ s11227-021-03720-9.

[8] L. Krithikashree and S. Manisha, ‘‘Audit cloud: Ensuring data integrity for mobile devices in cloud storage,’’ IEEE Trans. Depend. Sec. Comput., pp. 1–5, Sep. 2018, doi: 10.1109/ICCCNT.2018.8493963.