WWW.IJRPR.COM

International Journal of Research Publication and Reviews

Journal homepage: www.ijrpr.com ISSN 2582-7421

Ensuring Data Security in Cloud Using an Efficient Merkel Based Data Auditing Protocol

R. Rahul[1], Mr. Arun M[2]

[1] UG Student, Sri Krishna Adithya College of Arts And Science

[2]MCA., (P. hD), Assistant Professor, Department of Computer science Sri Krishna Adithya College of Arts and Science, Coimbatore -42.

A B S T R A C T

With the widespread adoption of cloud storage, users benefit from cost-effective remote data storage and flexible data sharing. Due to the partial trust in Cloud Service Providers (CSP), various cloud auditing schemes have been developed to ensure data security and integrity. Researchers have designed an efficient sampling verification algorithm, optimized for auditing, and introduced a dynamic auditing function for data updates. However, these existing schemes face security risks such as user identity disclosure, denial of service attacks, and single-manager power abuse.

We propose the use of Merkel-based Message Authentication Codes (MACs) to enhance public auditability in cloud data storage. This approach allows a trusted external audit party to assess the risk of outsourced data, saving computation resources for data owners and providing a transparent, cost-effective method for building trust in the cloud. Additionally, we aim to improve user interactions between data owners and the cloud server. Our work outlines necessary approaches, system requirements, and addresses challenges for establishing a publicly auditable, secure cloud storage service.

1. INTRODUCTION

Our high-level architecture for cloud data storage consists of four entities: the data owner, user, cloud server (CS), and a trusted third-party auditor (TPA). The TPA is an expert entity responsible for assessing the security of cloud storage on behalf of the data owner. The data owner, who could be an individual or an enterprise, relies on the cloud server for remote data storage and maintenance, benefiting from availability, low cost, and on-demand sharing among trusted users.

In this single writer/many readers scenario, only the data owner can update the data stored on the CS, while users can only read files. Ensuring publicly auditable secure cloud data storage is essential since the data owner no longer has physical control over the data. Therefore, the data owner may employ a TPA for auditing to verify data security while keeping data private from the TPA.

The TPA, being reliable and independent, audits the cloud data without needing a local copy or imposing additional burdens on the data owner. It's crucial to prevent any data leakage during this process. We also consider potential adversaries like malicious outsiders, who might attack cloud storage servers, and a semi-trusted CS, which may neglect or delete data for its benefit. Our architecture assumes basic security mechanisms, such as preloaded public/private key pairs, to ensure secure communication with minimal overhead.

2. LITERATURE REVIEW

System analysis will be conducted to evaluate whether the design of the information system can adapt to organizational policies and user requirements while addressing the weaknesses of the current system. This chapter discusses the existing system, the proposed system, and highlights the system requirements.

To protect data integrity, traditional cryptographic methods, such as public key encryption, can be utilized. In this approach, data owners maintain a small number of keys locally for the files to be outsourced to the cloud. When the data owner retrieves a file, they can verify its integrity by recalculating the key of the received file and comparing it to the precomputed value. This method allows data owners to ensure the correctness of the received data from the cloud. However, it does not guarantee the integrity of the other outsourced data unless all data is downloaded and verified by the owner. This limitation indicates that while traditional methods are beneficial for verifying individual files, they fall short in ensuring the overall integrity of all stored data in the cloud.

Our proposed system aims to address these limitations by providing a more comprehensive solution. In addition to using cryptographic methods, we will incorporate advanced auditing techniques to verify the integrity of all data stored in the cloud without requiring the data owner to download all files. This

will significantly reduce the burden on data owners and improve the reliability of the cloud storage system. By combining traditional cryptographic methods with modern auditing techniques, our system will ensure a higher level of data security and integrity, making it more robust and trustworthy for users.

3. MODELING AND ANALYSIS

The main focus of the modeling and analysis is to provide a detailed report on the modeling. In this section, we present the graphs and charts to show the analysis and the glimpse of our research work. This contains very useful information regarding the modeling of the research. In this we have made a website named 'ENSURING DATA SECURITY IN CLOUD USING AN EFFICIENT MERKEL BASED DATA AUDITING PROTOCOL'

Flow Chart

The flow chart shows the methodology of the system and how it works and operates It also shows all the possible action which are performed by the user. It shows the flow of action which is performed by the user on the system. Flowchart is as follows:-

Figure 1:-It indicates the flow of actions

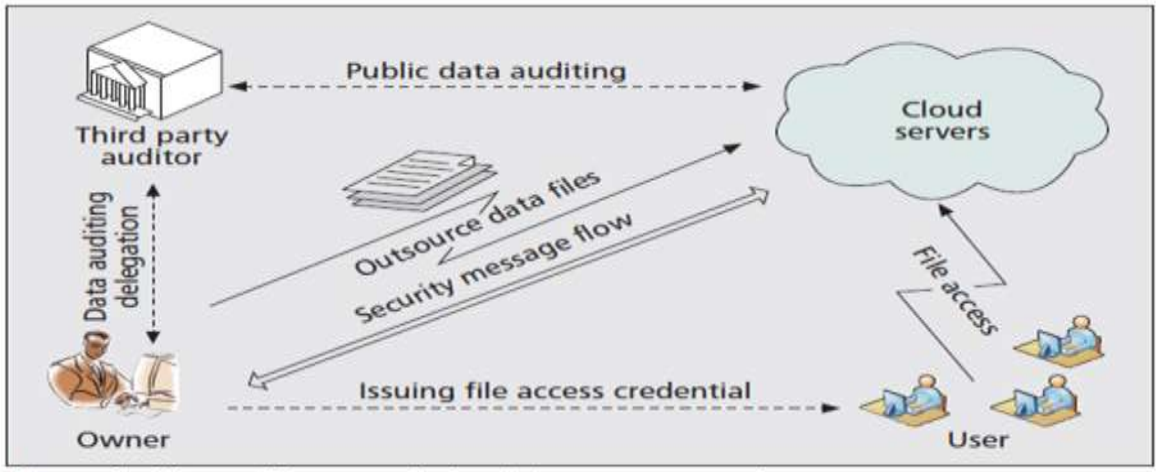

Figure 1. *The architecture of cloud data storage service.*

Figure 1: Flowchart for depicting the flow of operations.

4. DRAWBACKS

Because cloud data can be vast, retrieving all data for verification is impractical for data owners. Delegating this task to a TPA introduces high auditing costs and risks data privacy. Therefore, efficient module design is crucial.

Module Design

Minimize Auditing Overhead: The auditing process must not impose significant overhead on the cloud server. This includes minimizing I/O costs for data access and bandwidth costs for data transfer. Extra burdens on the data owner should be minimized, allowing them to enjoy cloud storage without concerns about auditing correctness.

Protect Data Privacy: Data privacy protection is essential in service level agreements for cloud storage. A public auditing protocol must not compromise the owner's data privacy. TPAs should audit cloud data storage efficiently without needing a local copy or accessing the data content.

Support Data Dynamics: Cloud storage services often require dynamic data updates. The auditing protocol should support this feature, ensuring data integrity even with frequent updates.

Support Batch Auditing: Efficient auditing is necessary for large-scale cloud storage services. TPAs should handle multiple auditing tasks from different owners quickly and cost-effectively. This capability ensures the scalability of public auditing services, even with numerous data owners.

5. RESULT AND DISCUSSION

Feasibility Assessment: Define the problem, develop criteria for choosing solutions, propose possible solutions, estimate costs and benefits, and recommend actions.

Requirement Analysis: Specify high-level capabilities, functional requirements, and performance requirements, refining initial planning details to characterize system features.

External Design: Conceive, plan, and specify externally observable characteristics like user displays, report formats, and data links.

Internal Design: Develop and specify the internal structure, processing details, algorithms, data structures, and test plans, providing blueprints for implementation, testing, and maintenance.

Detailed Design: Focus on algorithmic details, data representation, and interconnections among data structures.

Coding: Translate detailed designs into source code using appropriate programming languages.

Debugging: Remove errors from programs to ensure they are error-free.

Maintenance: Load the system into use and modify it according to user requirements, including enhancements and problem resolution.

6. CONCLUSION

Cloud computing is the next-generation enterprise IT architecture, moving applications and databases to large internet-based data centers, which introduces new security challenges in software, data security, recovery, privacy, and legal compliance. In this work, we focus on cloud data storage security by presenting a network architecture to describe, develop, and evaluate secure storage issues. We suggest cryptographically desirable properties for public auditing services to ensure dependable cloud storage security. Our in-depth analysis examines existing data storage security methods, and our proposed algorithm overcomes their limitations, providing enhanced security and reliability.

7. REFERENCES

[1] M. Armbrust et al., ``Above the clouds: A Berkeley view of cloud computing," Univ. California, Berkeley, Berkeley, CA, USA, Tech. Rep. UCBEECS-2009-28, 2009.

[2] Cloud Security Alliance. (2017). Security Guidance for Critical Areas of Focus in Cloud Computing. [Online]. Available: https:// cloudsecurityalliance.org/download/securityguidance-v4/

[3] Cloud Security Alliance. (2018). Top Threats to Cloud Computing: Deep Dive. [Online]. Available: http://www.cloudsecurityalliance.org

[4] J. Xu and E.-C. Chang, ``Towards efcient proofs of retrievability," in Proc. ACM Symp. Inf., Comput. Commun. Secur., 2012, pp. 7980.

[5] K. Ren, C.Wang, and Q.Wang, ``Security challenges for the public cloud," IEEE Internet Comput., vol. 16, no. 1, pp. 6973, Jan./Feb. 2012.

[6] J.Wang, X. Chen, X. Huang, I. You, and Y. Xiang, ``Verifiable auditing for outsourced database in cloud computing," IEEE Trans. Comput., vol. 64, no. 11, pp. 32933303, Nov. 2015.

[7] F. Chen, T. Xiang, Y. Yang, and S. S. M. Chow, ``Secure cloud storage meets with secure network coding," IEEE Trans. Comput., vol. 65, no. 6, pp. 19361948, Jun. 2016.

[8] G. Ateniese et al., ``Provable data possession at untrusted stores," in Proc. ACM Conf. Comput. Commun. Secur., 2007, pp. 598609.

[9] H. Shacham and B. Waters, ``Compact proofs of retrievability," in Proc. Int. Conf. Theory Appl. Cryptol. Inf. Secur., 2008, pp. 90107.

[10] K. Yang and X. Jia, ``An efcient and secure dynamic auditing protocol for data storage in cloud computing," IEEE Trans. Parallel Distrib. Syst., vol. 24, no. 9, pp. 17171726, Sep. 2013.