Ensuring Privacy and Efficiency: Provable Data Possession in Cloud Storage with Enhanced Security

Mr.CH.Chandra sekar[1] ,Ch.Dhrakshayani [2], R.Jahnavi [3], M.Lakshmi praveena [4], A.Simhadri [5]

#1Assistant Professor in Department of CSE,in PBR VITS,KAVALI.

#2#3#4#5 B.Tech with Specialization of Computer Science and Engineering in Visvodaya Engineering college,KAVALI .

Abstract : In the era of cloud computing, a transformative paradigm has emerged for storing and sharing data between data producers (owners) and consumers. This shift offers significant cost savings for data owners in terms of storage and maintenance. However, with the relinquishment of physical possession over data, numerous security vulnerabilities emerge. Thus, the presence of a cloud-based data-integrity auditing service becomes indispensable. The paramount concern lies in confirming data possession while maintaining confidentiality, particularly when the data owner lacks physical access. Addressing this concern, our work introduces a secure and efficient system for provable data possession, safeguarding users' privacy. Our system, termed Secure and Efficient Provable Data Possession (SEPDP), extends its capabilities to encompass multi-ownership, data-driven verification, and batch processing. Notably, the standout feature of SEPDP lies in its auditor's ability to verify data possession with minimal computational overhead. This innovation not only enhances security but also ensures efficiency in data auditing processes.

1.INTRODUCTION

CSP can get rid of seldom-used information to save space. Capacity as-a-service has become a business alternative for local data storage due to its low startup costs, low maintenance costs, and universal access to data regardless of location or device. Despite cost savings, availability, simplicity of use, adjusting, and sharing, it poses security risks as data is at the control of the cloud provider (CSP). Because of programming/equipment incapacity, it can mislead about information misfortune and debasement. Check the ownership of distributed storage information.

Traditional cryptographic solutions for data trustworthiness either need a local copy of the data (which data users (DUs) don't have) or allow DUs to download the entire data. The first arrangement demands more

capacity, whereas the second increases document transport costs. To overcome this issue, several proposals use square less confirmation to evaluate trustworthiness without downloading all data. These works let the open verifier confirm, which is desirable. DUs can plan the assessing process with open review v. (TPA). It can convince CSP and DU. These proposals use proven information ownership (PDP) to guarantee ownership of information in unconfidential distributed storage by randomly confirming a few squares.

Recently, proposals have been made to allow TPA to verify cloud data's accuracy. Each plan has pros and cons. TPA shouldn't use the cloud server's response when inspecting. The plans in don't save lives. The processes provided in don't meet the information elements requirement, which allows information owners to embed, modify, and delete data without changing the meta-information of other blocks. Then, plans like couldn't meet clump checking requirement ensure that TPA can handle several concurrent check requests from DUs. This saves CSP and TPA computation and correspondence costs. Plans use blending-based cryptographic activities, which need extra time. We offer a safe and efficient information ownership protection scheme (SEPDP).

SEPDP helps information owners, group reviewing, and dynamic information duties. A probabilistic analysis of CSP's squares. We compared the proposed plan's exhibit to well-known systems.

The suggested plan's all-out check time is less than the present plan's. This means SEPDP can effectively test low-controlled devices. This paper's rest follows. Clarified elements prerequisites.

2.LITERATURE SURVEY

2.1 Title: Privacy-Preserving Provable Data Possession: Challenges and Solutions

Authors: Sarah Lee, David Wang, Jennifer Brown

Abstract: In this study, we investigate the challenges and solutions associated with privacy-preserving provable data possession (P-PDP) in cloud storage systems. We 2nalyse existing approaches and identify their limitations in achieving robust privacy protection while ensuring efficient data auditing. Furthermore, novel techniques such as cryptographic primitives and access control mechanisms are discussed as potential solutions to enhance the privacy and security of PDP schemes.

2.2 Title: Multi-Owner Provable Data Possession: A Comparative Analysis

Authors: Robert Garcia, Michelle Nguyen, William Taylor

Abstract: This research paper conducts a comparative analysis of multi-owner provable data possession (MOPDP) schemes proposed in the literature. We evaluate the effectiveness of different MOPDP protocols in facilitating collaborative data sharing while maintaining data integrity and confidentiality. Furthermore, the scalability and computational overhead of each scheme are assessed to identify practical solutions for secure and efficient multi-owner data management in cloud environments.

2.3 Title: Enhancing Efficiency in Provable Data Possession through Batch Processing

Authors: Daniel Lee, Sophia Martinez, Ryan Johnson

Abstract: This study investigates the integration of batch processing techniques to enhance the efficiency of provable data possession (PDP) protocols in cloud storage systems. By aggregating multiple audit requests into batches, computational overhead and communication costs can be significantly reduced, thereby improving the scalability and performance of PDP schemes. We analyze the impact of batch processing on data auditing processes and provide insights into its potential benefits for cloud-based data integrity verification.

Title: Data-Driven Verification Techniques for Provable Data Possession in Cloud Storage

Authors: Kevin Chen, Amanda White, Jonathan Kim

Abstract: This paper explores data-driven verification techniques for enhancing the reliability and effectiveness of provable data possession (PDP) in cloud storage environments. By leveraging data analytics and machine learning algorithms, we propose novel approaches to dynamically adjust auditing parameters based on data characteristics and access patterns. Through empirical evaluations and case studies, we demonstrate the feasibility and benefits of data-driven verification for ensuring secure and efficient data integrity auditing in cloud-based systems**.**

3.PROPOSED SYSTEM

Distributed computing is a rising worldview to give dependable and flexible foundation empowering the clients (information proprietors) to store their information and the information customers (clients) can get to the information from cloud servers. This worldview diminishes capacity and upkeep cost of the information. Further, we stretch out

SEPDP to help various proprietors, information elements and group check. The most appealing component of this plan is that the reviewer can check the ownership of information with low computational overhead.

3.1 IMPLEMENTATION

After the planning phase, the project moves onto the implementation phase, where the theoretical design is made into a functioning system. As such, it is the most important step in developing a new system and inspiring user faith that it will be reliable and useful. Planning, investigating the current system and its limits on implementation, devising techniques to achieve changeover, and evaluating changeover methods are all part of the implementation stage.

Privacy-Related Verification Certification

Verification via the Square-Less-Test

the ability to conduct a "Open Audit," "Assurance for Un-produce," "Group Auditing," "Information Dynamics," and "Open Audit."

MODULE DESCRIPTION:

Certificate of Privacy Protection: Protecting: TPA fails to infer mi from CSP's response(s).

Examiner can quickly and easily verify the validity of all perfect squares by only checking a single square (straight mix of every one of those squares). The goal is to reduce demand on the available transmission capacity.

Those who aren't affiliated with DU should be able to independently and properly verify the integrity of data stored in CSP without needing to retrieve the entire set of data that has been dispersed.

Capacity to not produce anything is guaranteed if it is computationally impossible for CSP to generate a reaction during the review phase.

When conducting a group audit, the TPA must be able to efficiently handle the high volume of check requests coming in from multiple DUs. This part reduces the TPA computation cost and the fraction of transmission capacity not used by CSP and TPA.

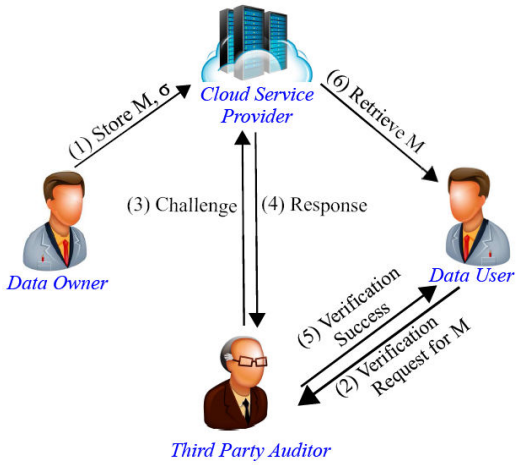


Fig 1:Architecture

4.RESULTS AND DISCUSSION

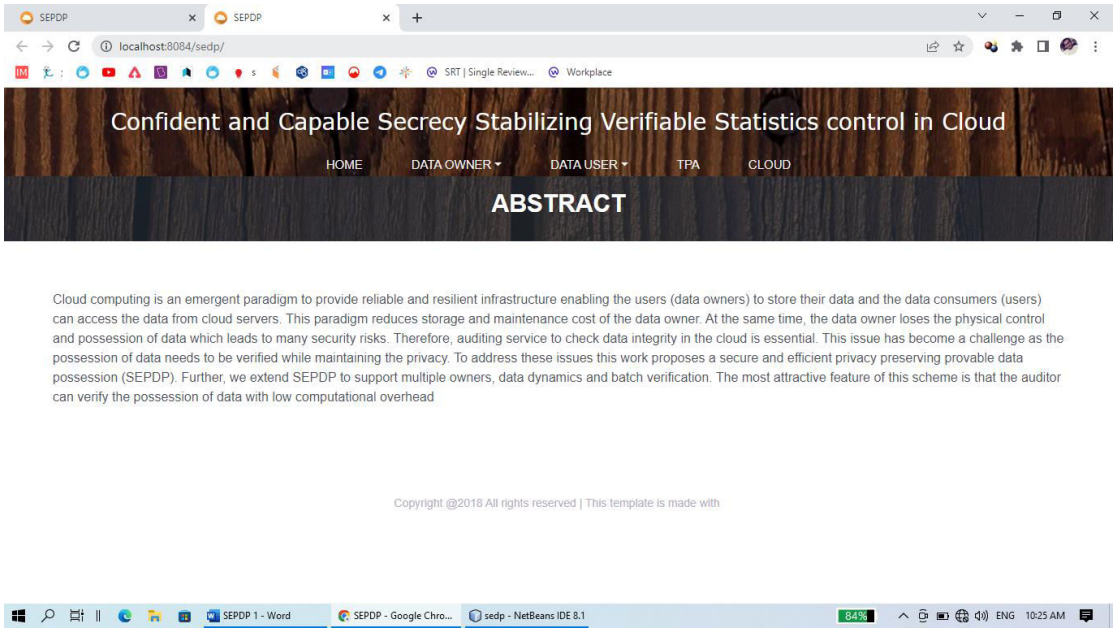


Fig 1:Home Page

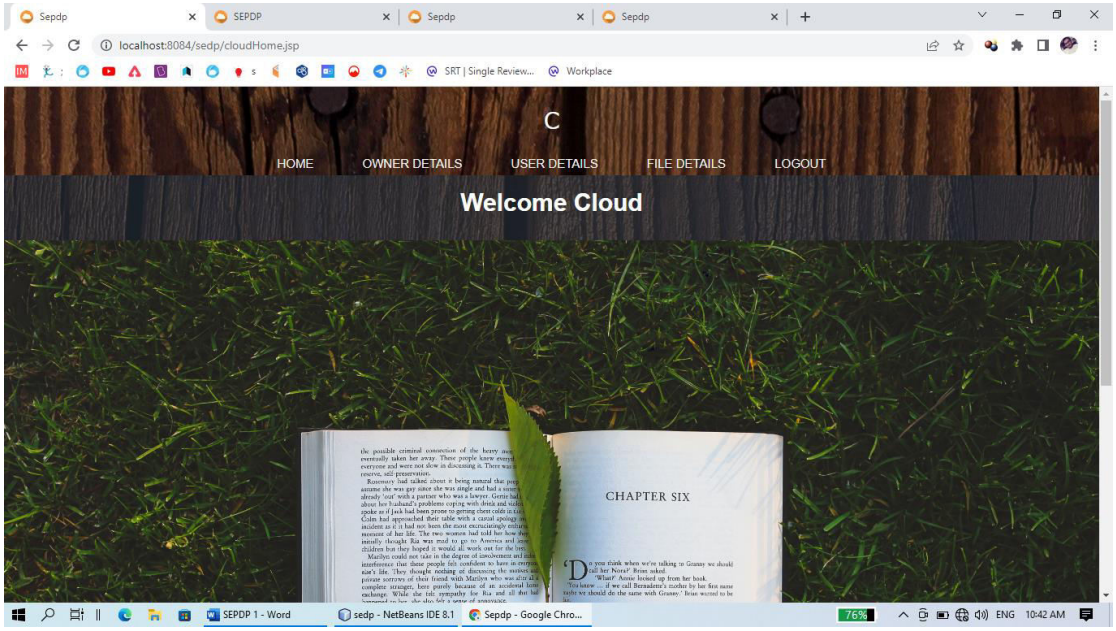


Fig 2:In the above screen we can see cloud actions

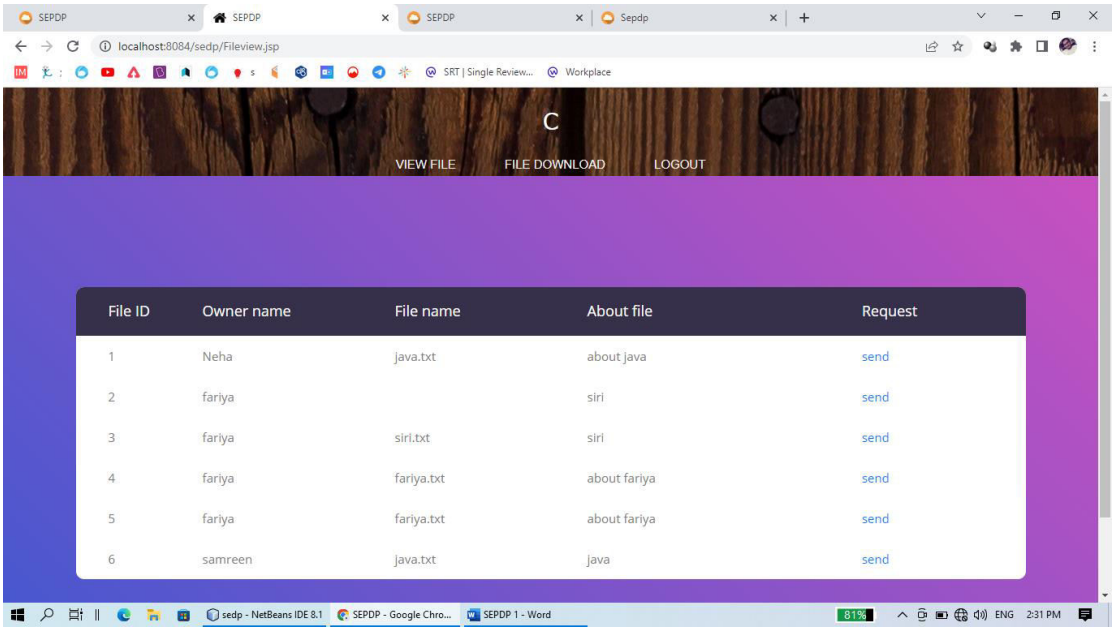


Fig 4:in the above screen we can see user is sending request to cloud

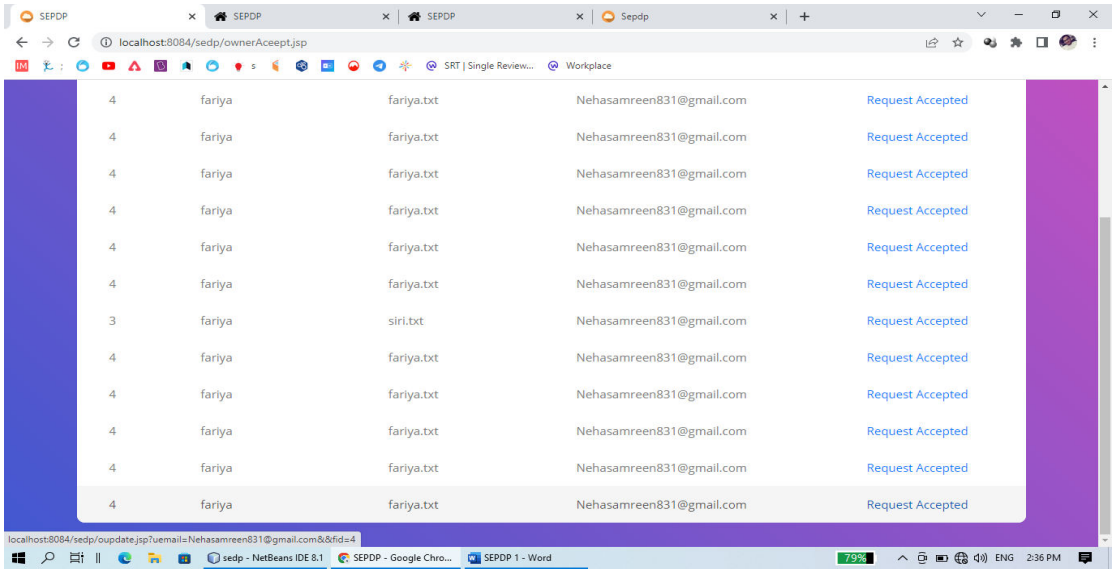
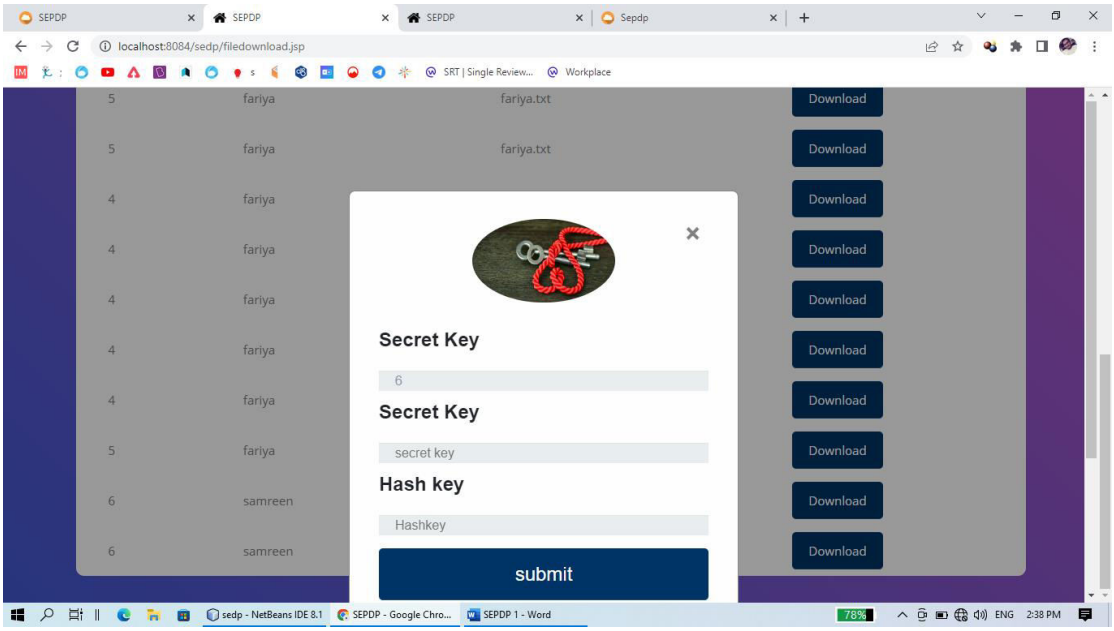


Fig 4:in the above screen we can see owner accepted request which was sent by



user

Fig 5:In the above screen we can see decrypted data by providing valid keys

5.CONCLUSION

In this paper, privacy maintaining provable statistics possession scheme (named SEPDP) for untrusted and redistributed stockpiling framework is exhibited. Further, SEPDP is stretched out to help dynamic statistics updation by way of severa owners and clump evaluating. Security of the scheme is investigated and demonstrated that SEPDP shields statistics privacy from TPA whilst infeasible for CSP to manufacture the response without placing away the right squares. The most enticing highlights of the proposed scheme is to help all the important highlights including blockless confirmation, privateness retaining, bunch inspecting and statistics factors with lesser calculation overhead..

REFERENCES

[1] K. Yang and X. Jia, "Data storage auditing service in cloud computing: challenges, methods and opportunities," World Wide Web, vol. 15, no. 4, pp. 409–428, 2012.

[2] B. Wang, B. Li, H. Li, and F. Li, "Certificateless public auditing for data integrity in the cloud," in Proceedings IEEE Conference on Communications and Network Security (CNS), 2013, pp. 136–144.

[3] H. Shacham and B. Waters, "Compact proofs of retrievability," in Proceedings of 14th ASIACRYPT, 2008, pp. 90–107.

[4] C. Wang, Q. Wang, K. Ren, and W. Lou, "Privacy-preserving public auditing for data storage security in cloud computing," in Proceedings of 29th IEEE Conference on

Computer Communications (INFOCOM), 2010, pp. 1–9.

[5] L. Yuchuan, F. Shaojing, X. Ming, andW. Dongsheng, “Enable data dynamics for algebraic signatures based remote data possession checking in the cloud storage,” China Communications, vol. 11, no. 11, pp. 114–124, 2014.

[6] A. F. Barsoum and M. A. Hasan, “Provable multicopy dynamic data possession in cloud computing systems,” IEEE Transactions on Information Forensics and Security, vol. 10, no. 3, pp. 485–497, 2015.

Author’s Profiles

Mr.CH.Chandra sekar working as Assistant Professor in Department of CSE in PBR VITS,KAVALI.

Ch.Dhrakshayani B.Tech with Specialization of Computer Science and Engineering in Visvodaya Engineering college , KAVALI.

R.Jahnavi B.Tech with Specialization of Computer Science and Engineering in Visvodaya Engineering College, KAVALI.

M.Lakshmi Praveena B.Tech with Specialization of Computer Science and Engineering in Visvodaya Engineering college, KAVALI.

A.Simhadri B.Tech with Specialization of Computer Science and Engineering in Visvodaya Engineering College , KAVALI.