Innovative Approaches To Public Auditing And Data Dynamics In The Cloud

N. BhagyaLakshmi [1], G. Jahnavi[2], J. Bala Divya[3], V. Sri Sai Likhitha[4]

MTech, Computer Science & Engineering, Bapatla Women's Engineering College, Bapatla, India[1]

BTech, Computer Science & Engineering, Bapatla Women's Engineering College, Bapatla, India[2-4]

Abstract: In order to highlight the need of effective integrity checks, this article delves into the topic of public auditing for encrypted data kept on cloud servers. The main objective is to enable data dynamics, which includes additions, changes, and removals. By means of a meticulous examination of current auditing protocols, we pinpoint the primary element placing constraints on data dynamics concerning costs. To address this difficulty, we introduce a novel public auditing methodology that aims to accomplish data dynamics at a substantially faster rate than existing techniques. Our novel challenge-response technique significantly lowers the cost of computation for motivation: Data security and integrity are becoming more and more of a problem as cloud servers are used for data storage. In order to ensure that the encrypted information on cloud servers is trustworthy, public audits is essential. Nevertheless, the inefficiencies of current auditing techniques make it difficult to effectively manage data dynamics including additions, deletions, and revisions.

Keywords: Cloud computing, data dynamics, and public auditing.

I. INTRODUCTION

Data security and integrity issues have been brought up by the growing reliance on cloud servers for data storage. To guarantee the reliability of the stored data, public auditing for encrypted data on cloud servers is essential. Nevertheless, current auditing systems are unable to effectively manage data dynamics, including additions, deletions, and revisions. This underscores the necessity for a novel approach that may expedite the auditing procedure, save expenses, and preserve data confidentiality and integrity in unreliable cloud settings.

High computing costs and extended verification durations are caused by inefficiencies in managing data dynamics in the public auditing systems for encrypted data on cloud servers that are currently in place.

II. BACKGROUND AND RELATED WORK

ARMBRUST ET AL. (2010):
Utilizing the knowledge from the groundbreaking work on cloud computing by Armbrust et al., our study seeks to address the changing opportunities and problems in this field. By investigating the most recent developments and their effects on many elements of cloud services, we want to improve knowledge of and utilization in relation to cloud computing.

He offered a thorough analysis of computing, emphasizing its importance and possibilities. Our research draws inspiration from their core thoughts in line with this landmark work. Our goal is to present an updated analysis of the status of cloud computing, considering the most recent advancements and trends.

Our study will use a variety of cloud computing-related methods and techniques, with a basic reference being the work of Armbrust et al. These algorithms will contribute to the general knowledge and development of cloud computing by helping to analyse and optimize cloud architecture, data storage, and resource management. Building on the groundbreaking work of Armbrust et al., our project has multiple benefits. It offers a modern perspective on cloud computing, accounting for the most recent advancements and difficulties. Researchers, practitioners, and decision-makers in the field of cloud computing will find this revised viewpoint useful, allowing them to fully utilize cloud services and make well-informed judgments.

The suggested method for our project will act as an expansion and improvement of the ideas and guidelines given by Armbrust et al. (2010). It will consider a thorough examination of cloud computing concepts, algorithms, and best practices in line with the quickly evolving cloud service market. We hope to contribute to the progress of this important topic by utilizing this basis to offer a solid and current framework that solves the changing security, scalability, and efficiency concerns of cloud computing systems.

III. METHODOLOGY

A. EXISTING SYSTEM:

Public auditing for data kept on cloud servers has difficulties in effectively managing data dynamics in the current system. The present procedures frequently lead to drawn-out auditing procedures that incur significant computing expenses for Third-Party Auditors (TPAs). These restrictions make it more difficult and expensive to promptly confirm the Precision of information stored in the cloud Servers. Moreover, especially in untrusted cloud settings, current systems can find it difficult to achieve the ideal balance between security and performance, which could compromise data integrity and privacy.

B. Proposed System:

We include a novel public auditing methodology in the proposed system that is intended to achieve data dynamics at a substantially faster rate than earlier approaches. Our novel challenge-response protocol improves the speed of result verification in the auditing process by significantly lowering the computing cost for Third-Party Auditors (TPAs). It is noteworthy that the suggested strategy maintains data integrity and privacy while maintaining low computing costs by striking a balance between performance and security. This is especially important when dealing with an untrusted cloud environment.
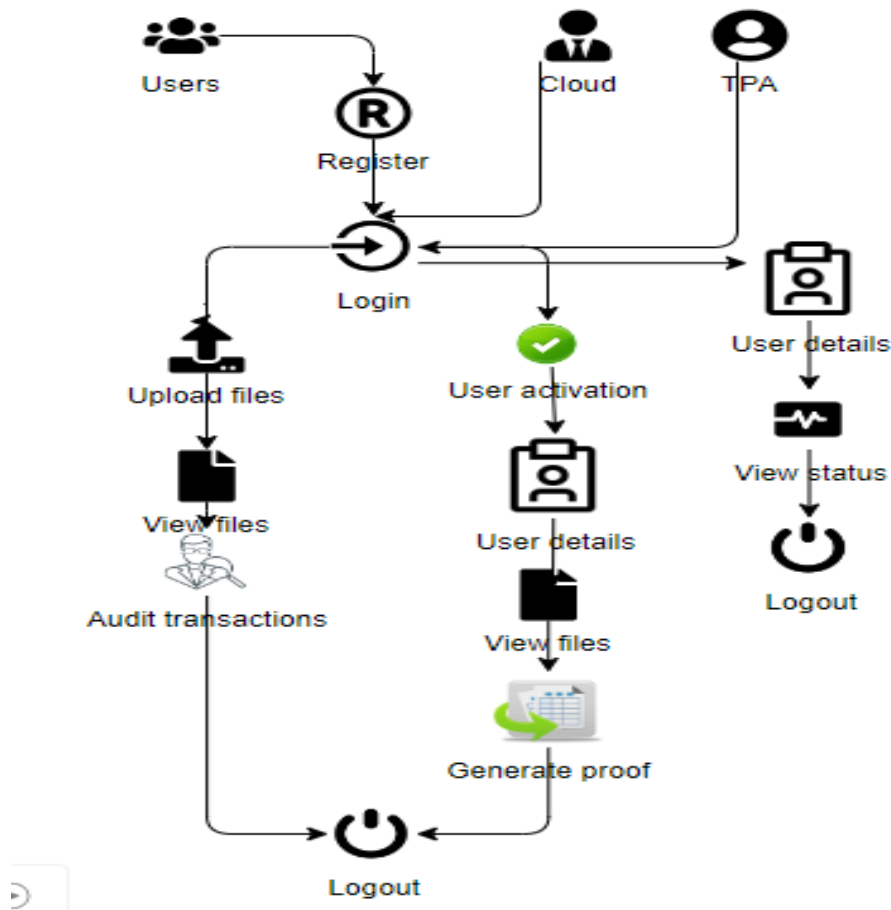
C. Architecture:

Fig 1: System Architecture

D. Result:
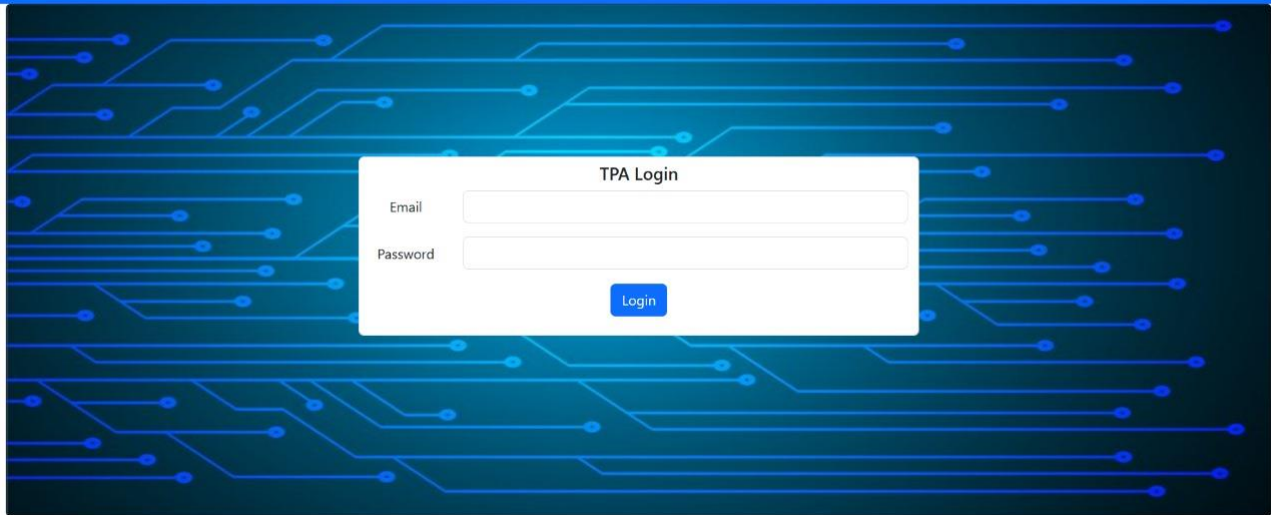
IV. CONCLUSION

As a result, this article has addressed the urgent requirement for effective integrity checks while also delving into the important area of public auditing for encrypted data kept on cloud servers. We have determined the main element restricting data dynamics in terms of cost efficiency by carefully examining the auditing procedures that are already in place. We have responded to this difficulty by launching a novel public auditing program that speeds up data dynamics

and drastically lowers Third-Party Auditors' (TPAs') calculation expenses. Especially in untrusted cloud settings, our technique not only ensures low computational cost but also maintains data integrity and privacy by striking a healthy balance between performance and security. Thorough performance and security assessments have shown the efficacy of our methodology, constructing a strong foundation for preserving data integrity.

REFERENCES

[1]. Armbrust, M., Fox, A., Griffith, R., Joseph, A. D., Katz, R., Konwinski, A., ... & Zaharia, M. (2010). A view of cloud computing Communications of the ACM, 53(4), 50-58.
[2]. Ren, K., Wang, C., & Wang, Q. (2012). Security challenges for the public cloud. IEEE Internet Computing, 16(1),69-73.
[3]. Song, D., Shi, E., Fischer, I., & Shankar, U. (2012). Cloud data protection for the masses. Computer, 45(1), 39-45.
[4]. Wei, L., Zhu, H., Cao, Z., Dong, X., Jia, W., Chen, Y., & Vasilakos, A. V. (2014). Security and privacy for storage and computation in cloud computing. Information sciences, 258, 371-386.
[5]. Ateniese, G., Burns, R., Curtmola, R., Herring, J., Kissner, L., Peterson, Z., & Song, D. (2007, October). Provable data possession at untrusted stores. In Proceedings of the 14th ACM conference on Computer and communications security (pp. 598-609).
[6]. Ateniese, G., Di Pietro, R., Mancini, L. V., & Tsudik, G. (2008, September). Scalable and efficient provable data possession. In Proceedings of the 4th international conference on Security and privacy in communication networks (pp. 1-10).
[7]. Juels, A., & Kaliski Jr, B. S. (2007, October). PORs: Proofs of retrievability for large files. In Proceedings of the 14th ACM conference on Computer and communications security (pp. 584-597).
[8]. Shacham, H., & Waters, B. (2008, December). Compact proofs of retrievability. In International conference on the theory and application of cryptology and information security (pp. 90-107). Springer, Berlin, Heidelberg.
[9]. Erway, C. C., Kupc¸¨u, A., Papamanthou, C., & Tamassia, R. (2015). ¨ Dynamic provable data possession. ACM Transactions on Information and System Security (TISSEC), 17(4), 1-29.
[10].   Wang, Q., Wang, C., Ren, K., Lou, W., & Li, J. (2010). Enabling public auditability and data dynamics for storage security in cloud computing. IEEE transactions on parallel and distributed systems, 22(5), 847-859.
[11].   Zhu, Y., Wang, H., Hu, Z., Ahn, G. J., Hu, H., & Yau, S. S. (2011, March). Dynamic audit services for integrity verification of outsourced storages in clouds. In Proceedings of the 2011 ACM Symposium on Applied Computing (pp.1550-1557).

BIBILOGRAPHY

Mrs.N. BaghyaLakshmi M.Tech, Asst. Professor Dept of CSE BWEC, Andhra Pradesh, India

G. Jahnavi (B. Tech) Student, Dept of CSE, BWEC, Andhra Pradesh, India.

J. Bala Divya (B. Tech) Student, Dept of CSE, BWEC, Andhra Pradesh, India.

V. Sri Sai Likhitha (B. Tech) Student, Dept of CSE, BWEC, Andhra Pradesh, India.