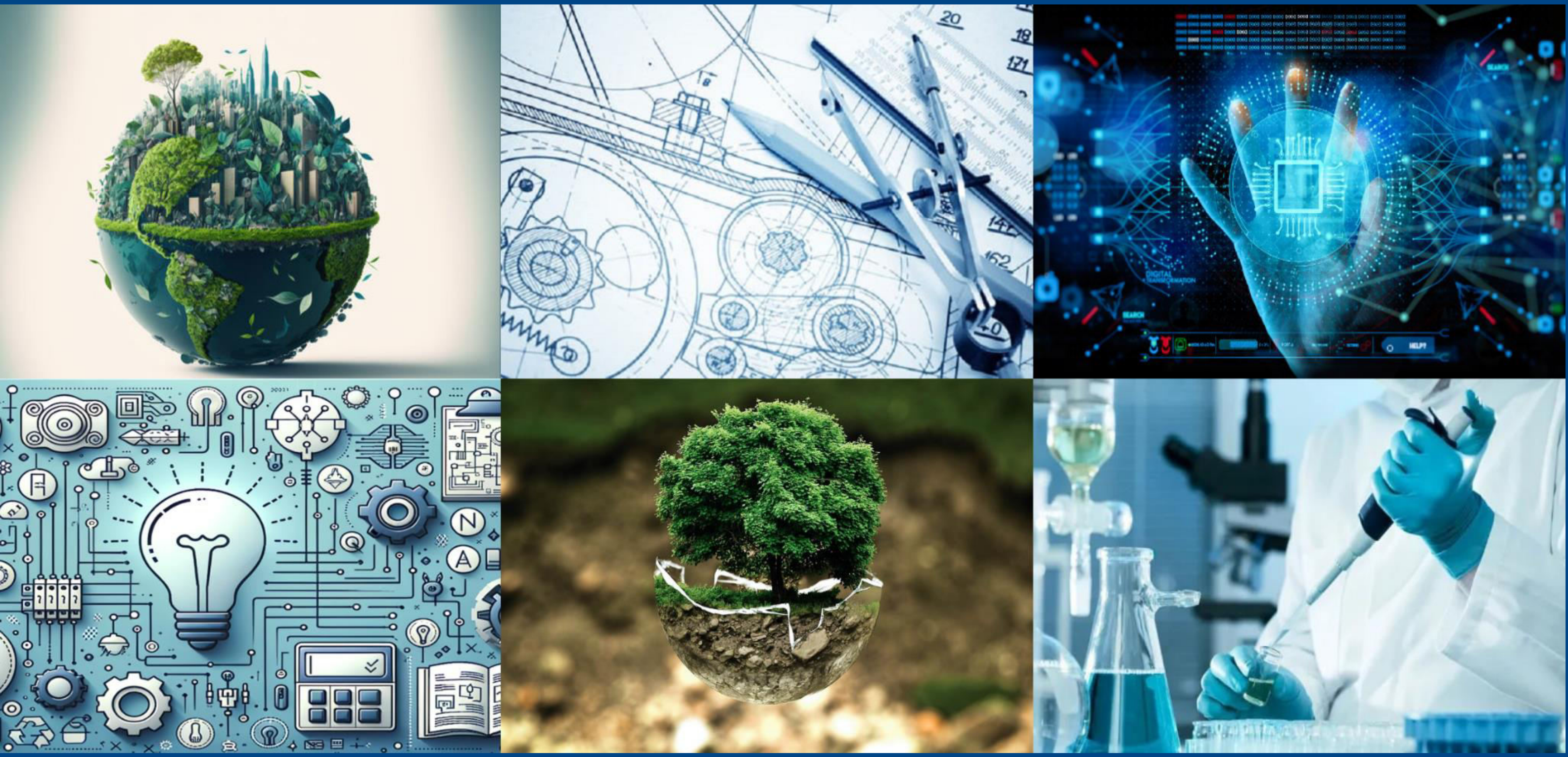
ISSN: 2582-7219

International Journal of Multidisciplinary Research in Science, Engineering and Technology

(A Monthly, Peer Reviewed, Refereed, Scholarly Indexed, Open Access Journal)



Impact Factor: 8.206

Volume 8, Issue 3, March 2025

www.ijmrset.com ✉ ijmrset@gmail.com ☎ +91 6381 907 438 ☎ +91 63819 07438

© 2025 IJMRSET | Volume 8, Issue 3, March 2025| DOI: 10.15680/IJMRSET.2025.0803274

ISSN: 2582-7219 | www.ijmrset.com | Impact Factor: 8.206| ESTD Year: 2018|

International Journal of Multidisciplinary Research in Science, Engineering and Technology (IJMRSET)

(A Monthly, Peer Reviewed, Refereed, Scholarly Indexed, Open Access Journal)

Public Auditing and Secured Management for Cloud Storage

Dr. D.J. Samatha Naidu, K. Venkata Ramya, S.Shereen

Professor, Dept. of MCA, APGCCS, New Boyanapalli, Rajampet, A.P, India

Assistant Professor, Dept. of MCA, APGCCS, New Boyanapalli, Rajampet, A.P, India

PG Student, Dept. of MCA, APGCCS, New Boyanapalli, Rajampet, A.P, India

ABSTRACT: Cloud computing is an evolving technology that provides data storage and highly fast computing services at a very low cost. All data stored in the cloud is handled by their cloud service providers or the caretaker of the cloud. The data owner is concerned about the authenticity and reliability of the data stored in the cloud as the data owners. Data can be misappropriated or altered by any unauthorized user or person. This paper desire to suggest a secure public auditing scheme applying third party auditors to authenticate the privacy, reliability, and integrity of data stored in the cloud. This proposed auditing scheme composes the use of the AES-256 algorithm for encryption, SHA-512 for integrity check and RSA- 15360 for public-key encryption. And perform data dynamics operation which deals with mostly insertion, deletion, and, modification.

I. INTRODUCTION

Cloud computing has become a popular information technology service by providing huge amount of resources (eg.. storage and computing) to end users based on their demands. Among all cloud computing services, cloud storage is the most popular. Since the volume of data in the world is increasing rapidly, saving cloud storage becomes essential. One of the key reasons that causes storage waste is duplicate data storage. Multiple users may save same files or different files containing same pieces of data blocks at the cloud. Obviously, duplicate data storage at the cloud introduces a big waste of storage resources. Data De-duplication provides a promising solution to this issue. In a de-duplication scheme, the CSP can cooperate with the cloud user to first check whether a pending uploaded file has been saved already or not, and then provide the user whose pieces of file data are checked duplicate a way to access the file without storing another copy at the cloud. However, since the CSP cannot be fully trusted. the cloud users may suffer from some security and privacy issues. Notably, a semi trusted CSP may modify, tamper or delete the uploaded data driven by some profits. The damage of de-duplicated data could cause huge loss to all related users (eg., data owners and holders). Thus, the integrity of the data stored at the cloud should be verified, especially for duplicate data storage with de-duplication. Several Proof of Irretrievability (POR) schemes have been proposed to address the issue of integrity check on cloud data storage in recent decade. In such schemes, a user adds verification tags along with a file. During the verification, the user creates a random challenge and sends it to the CSP: the CSP has to use all the data in user's corresponding files it stored as inputs to compute a response back to the user.The user then checks the integrity of the stored file by verifying the response. However, existing POR solutions mainly aim to improve the performance at the user side and assume that the CSP has infinite computation and storage resources.

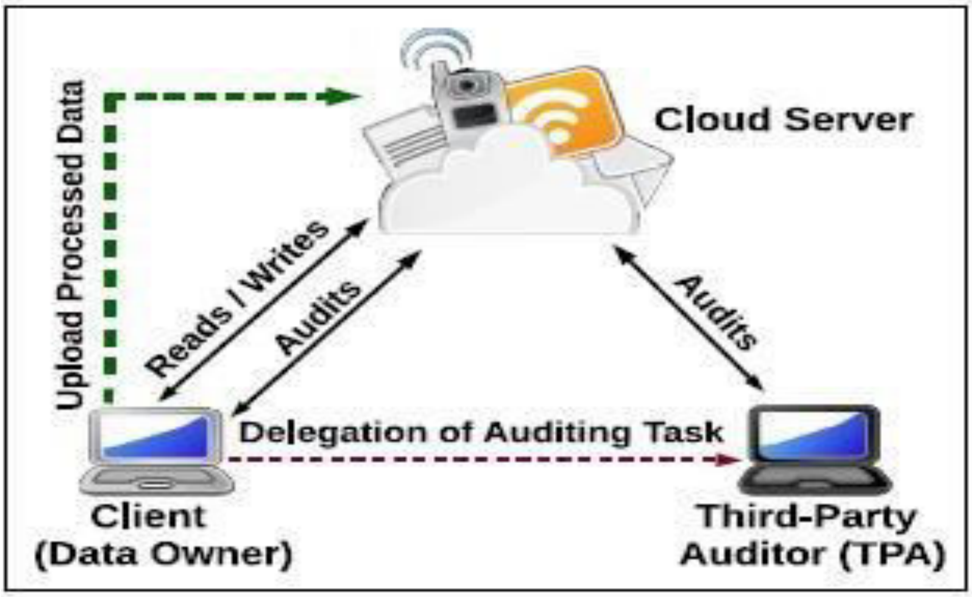


Figure 1: System Architecture

Public auditing and secure management in cloud storage systems focus on ensuring data integrity, privacy, and transparency while maintaining secure access controls and compliance. In such a system, users (data owners) encrypt their data before uploading it to the cloud, ensuring privacy and preventing unauthorized access. The cloud service provider securely stores the encrypted data, employs encryption techniques like AES-256 for data at rest, and uses key management systems to safeguard encryption keys. Public auditing enables third-party auditors to verify the integrity of stored data without accessing its contents by leveraging cryptographic proofs such as Proof of Data Possession (PDP) or Proof of Retrievability (PoR), ensuring that the provider has not tampered with the data. Access to data is tightly controlled through role-based access control (RBAC) and multi-factor authentication (MFA), and comprehensive, tamper-evident audit logs are maintained to track all actions on the data, ensuring accountability. These logs can be periodically reviewed by auditors to ensure compliance and transparency. Overall, the architecture combines strong encryption, secure data management practices, cryptographic integrity proofs, and transparent auditing to create a robust and trusted cloud storage environment.

II. LITERATURE REVIEW

[1] L. Moreau, J. Freire, J. Futrelle, R. McGrath, J. Myers, and P. Paulson, “The open provenance model: an overview,” in International Provenance and Annotation Workshop, LNCS, vol. 5272, Salt Lake City, Utah, 17-18 June 2008, **pp. 323–326.**

The Open Provenance Model (OPM) was introduced to represent data provenance, process documentation, data derivation, and data annotation. Provenance is well understood in the context of art or digital libraries, where it respectively refers to the documented history of an art object, or the documentation of processes in a digital object’s life cycle.

Interest for provenance in the “e-science community is also growing, since provenance is perceived as a crucial component of workflow systems that can help scientists ensure reproducibility of their scientific analyses and processes.

[2] J. Freire, D. Koop, E. Santos, and C. Silva, “Provenance for computational tasks: A survey,” IEEE Computing in Science and Engineering, vol. 10, no. 3, pp. 11–21, 2008.

Since then, OPM has been widely adopted and extended by various research groups [9]. Freire et al. surveyed diverse models of provenance management but did not discuss the use of provenance for security.The problem of systematically capturing and managing provenance for computational tasks has recently received significant attention because of its relevance to a wide range of domains and applications. The authors give an overview of important concepts related to provenance management, so that potential users can make informed decisions when selecting or designing a provenance solution.

[3] P. McDaniel, "Data provenance and security," IEEE Security and Privacy, vol. 9, no. 2, pp. 83–85, 2011
McDaniel addressed that accurate, timely, and detailed provenance information leads to good security decisions. One of the unanticipated consequences of the Internet age is a pervasive loss of context. Information is often filtered, sampled, repackaged, condensed, or altered to suit any number of purposes. Over time, the entropy of these processes causes information to lose its essential validity. This column argues the needs, applications, and challenges of providing greater access to data provenance in information systems.

[4] S. Rajbhandari, I. Wootten, A. Ali, and O. Rana, "Evaluating provenance- based trust for scientific workflows," in 6th IEEE International Symposium on Cluster Computing and the Grid, vol. 1, Singapore, 16-19 May 2006, pp. 365–372

Provenance has been used to verify trust, trustworthiness, or correctness of information in many research areas. Rajbhandari et al. examined how provenance information is associated with a workflow in a Bio-Diversity application. Provenance is the documentation concerning the origin of a result generated by a process, and provides explanations about who, how, what resources were used in a process, and the processing steps that occurred to produce the result. Such provenance information is important to improve a scientist's ability to judge and place certain amount of trust on the generated data.We illustrate how provenance information associated with a workflow can be used to evaluate trust. This work is based on several use cases from a Bio-Diversity application. We also propose a simple architecture to illustrate our trust framework.

III. METHODOLOGY OF PROPOSED SURVEY

The Software Development Life Cycle (SDLC) is a series of stages that provide a structured approach to the software development process. It encompasses understanding the business requirements, eliciting needs, converting concepts into functionalities and features, and ultimately delivering a product that meets business needs. A proficient software developer should possess adequate knowledge to select the appropriate SDLC model based on project context and business requirements. Therefore, it is essential to select the right SDLC model tailored to the specific concerns and requirements of the project to ensure its success. To explore more about choosing the right SDLC model, you can follow this link for additional information. Furthermore, to delve deeper into software lifecycle testing and SDLC stages, follow the highlighted links here. The exploration will cover various types of SDLC models, their benefits, disadvantages, and when to use them. SDLC models can be viewed as tools to enhance product delivery. Therefore, understanding each model, its advantages, disadvantages, and the appropriate usage is crucial to determine which one suits the project context.
Types of Software developing life cycles (SDLC)

- Waterfall Model
- V-Shaped Model
- Evolutionary Prototyping Model
- Spiral Method (SDM)
- Iterative and Incremental Method

IV. CONCLUSION AND FUTURE WORK

In this work, we provided a new user authentication scheme in which a legal user In this work, we have proposed a secure cloud storage protocol for dynamic data (DSCS I) based on a secure network coding (SNC) protocol. To the best of our knowledge, this is the first SNC- based DSCS protocol that is secure in the standard model and enjoys public verifiability. We have discussed some challenges while constructing an efficient DSCS protocol from an SNC protocol. We have also identified some limitations of an SNC-based secure cloud storage protocol for dynamic data. However, some of these limitations follow the underlying SNC protocol used. A more efficient SNC protocol can give us a DSCS protocol with better efficiency. We have also identified certain SNC protocols suitable for append-only data and constructed an efficient DSCS protocol (DSCS II) for append only data. We have shown that DSCS II overcomes some limitations of DSCS I. Finally, we have provided prototype implementations of DSCS I and DSCS II in order to show their practicality and compared the performance of DSCS I with that of an SNC-based secure cloud storage for static data and that of DPDP.

REFERENCES

1. M. E. Porter, Competitive Strategy: Techniques for Analyzing Industries and Competitors. Free Press,1980.
2. A. R. Deshpand and H. Gatingon, “Competitive analysis,” Marketing Letters, 1994.
3. B. H. Clark and D. B. Montgomery, “Managerial Identification of Competitors,” Journal of Marketing,1999.
4. W. T. Few, “Managerial competitor identification: Integrating the categorization, economic and organizational identity perspectives,” Doctoral Dissertaion, 2007.
5. M. Bergen and M. A. Peteraf, “Competitor identification and competitor analysis: a broad Based managerial approach,” Managerial and Decision Economics, 2002.
6. J. F. Porac and H. Thomas, “Taxonomic mental models in competitor definition,” The Academy of Management Review, 2008.
7. M.-J. Chen, “Competitor analysis and interfirm rivalry: Toward a theoretical integration,” Academy of Management Review, 1996.
8. R. Li, S. Bao, J. Wang, Y. Yu, and Y. Cao, “Cominer: An effective algorithm for mining competitors from the web,” in ICDM, 2006.
9. Z. Ma, G. Pant, and O. R. L. Sheng, “Mining competitor relationships from online news: A Network based approach,” Electronic Commerce Research and Applications, 2011.
10. R. Li, S. Bao, J. Wang, Y. Liu, and Y. Yu, “Web scale competitor discovery using mutual Information,” in ADMA, 2006.
11. G. Yang, J. Yu, W. Shen, Q. Su, Z. Fu, and R. Hao, ``Enabling public auditing for shared data in cloud storage supporting identity privacy and traceability," J. Syst. Softw., vol. 113, pp. 130139, Mar. 2016. doi: 10.1016/j.jss.2015.11.044.

INTERNATIONAL JOURNAL OF MULTIDISCIPLINARY RESEARCH IN SCIENCE, ENGINEERING AND TECHNOLOGY

| Mobile No: +91-6381907438 | Whatsapp: +91-6381907438 | ijmrset@gmail.com |

www.ijmrset.com