IJARSCT
International Journal of Advanced Research in Science, Communication and Technology
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
ISSN: 2581-9429
Volume 6, Issue 17, April 2026
Impact Factor: 8.2

A Secure Data Dynamics and Public Auditing Scheme for Cloud Storage Using Data Owner-Centric Control Policies

Ashwini Shamrao Pingle[1*], Nirmiti Sunil Bachhav[2], Dr. M. N. Shelar[3]
MSc. Computer Science, C.M.C.S College, Nashik, India[1-2]
Professor Department of MSc. Computer Science, C.M.C.S college, Nashik, India[3]
ashwinipingle1508@gmail.com

Abstract: *The role of social media algorithms in the exposure of information and the level of engagement is becoming increasingly important in the psychological well-being of the user. Therefore, the paper aims to investigate the correlation between the behaviour of social media usage and the level of anxiety in the psychological well-being of the user. To achieve the objective of the research, the researcher used descriptive statistics, correlation analysis, logistic regression analysis, and random forest analysis. Based on the findings of the research, the researcher was able to deduce the following: compulsive behaviour is highly correlated with anxiety since the correlation coefficient is 0.54. Daily screen time is moderately correlated with post-screening stress since the correlation coefficient is 0.41. Finally, the researcher was able to deduce the fact that filter bubble awareness is significantly correlated with anxiety since the correlation coefficient is 0.33. The logistic regression model was able to achieve an accuracy of 89%, a recall of 96%, and an F1 score of 0.85. The importance of the screening mechanism in the psychological well-being of the user is significant. However, the practice of using cloud-based storage is accompanied by a number of challenges concerning the issues of preserving data consistency, maintaining confidentiality, and preventing any alterations to the outsourced information. In most cases, the traditional methods of auditing involve extensive use of third parties and have poor support for performing the tasks dynamically, thus leaving a wide room for data breaches. This paper suggests a new approach to the development of a secure and effective auditing system based on the concept of Data Owner-Centric Control (DOC) and making use of Third-Party Auditors (TPA). Unlike many existing systems, this auditing technique involves only checking data authenticity, integrity, and privacy, without the need to access data itself. The main features of the developed algorithm include AES-256 symmetric encryption. In the DOC architecture, data owners have complete power over auditing activities, such that they can authorize, limit, or disallow access to TPAs whenever necessary. It also facilitates dynamic operations, such as insertion, deletion, and modification of data, using an authenticated index mechanism. Experimentation shows substantial improvements, with a 45% reduction in communication costs, 50% improvement in verification time, 40% reduction in latency, and accuracy in detection reaching 98.5%. Therefore, the auditing scheme proposed in the study is proven to be more efficient, secure, and effective in preserving privacy than existing schemes.*

Keywords: Cloud Computing, Data Integrity, Public Auditing, Data Owner-Centric Control

I. INTRODUCTION

Cloud computing has revolutionized data storage, management, and retrieval, providing scalable and cost-efficient means of utilizing services [6]. The flexibility and remote nature of cloud computing have made it an essential part of modern computer architectures. Cloud storage helps users store large amounts of data on remote servers instead of

IJARSCT
International Journal of Advanced Research in Science, Communication and Technology
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
ISSN: 2581-9429 Volume 6, Issue 17, April 2026 Impact Factor: 8.2

managing them locally [1]. But as soon as the data gets outsourced, it becomes beyond the user's reach, thus raising issues regarding the security of data, manipulation by unauthorized parties, and compromising the data's privacy [2]. Security and correctness of the stored data are some of the challenges that cloud storage systems face today. The reasons behind conducting this study arise due to some limitations in the current approaches of public auditing, which tend to depend on third parties. In this case, there exists a high chance that the information might be disclosed to the outside environment. Also, many methods in use are unable to support dynamic data manipulation, including insertions, deletions, and updates, effectively without processing an entire dataset. Current public auditing schemes depend on third-party auditors to check the integrity of data, but have problems with potential leakage and ineffective dynamic data manipulation [3]. A control policy based on the data owner will be useful here [4].

This research project seeks to develop a control policy for ensuring data confidentiality and accurate audit of cloud data. Objectives of the research project include reviewing the existing problems with data integrity, developing a privacy-preserving auditing system, performing dynamic secure operations with low cost, and measuring performance gains relative to previous models.

II. LITERATURE REVIEW

Auditing in the public domain has been developed into an effective method for verifying data integrity in outsourced settings without the need for complete data recovery [8]. Auditing models in their early stages implemented schemes such as homomorphic authentication and bilinear pairing to enable fast remote validation. Such schemes created the basis for proving data integrity but were primarily applicable to static data, which does not change after outsourcing.

A. Existing Public Auditing Schemes

Wang et al. introduced a public auditing system with HLA and random masking, which can verify data through TPA without disclosing information contents. But there was no confidentiality, and a dynamic data management facility [3]. Mohta et al. used RSA and SHA to implement a public auditing system with confidentiality and message digest creation facilities [2]. Meenakshi et al. used Merkle Hash Trees (MHTs) to enable insertion, deletion, and modification [1].

B. Research Gap

The current public auditing mechanisms cannot achieve security and efficiency while implementing dynamic data manipulations without increasing the cost of communications and the risk of exposing confidential information. The current frameworks still require the participation of third parties and lack data owner control. These research findings attempt to address these weaknesses by applying DOC with AES-256, SHA-512, and RSA-15360.

III. METHODOLOGY

To ensure security and control in cloud storage systems, a systematic method is proposed consisting of three key components: Data Owner (DO), Cloud Server (CS), and Third-Party Auditor (TPA). To keep data confidential, the AES-256 encryption technique is used, whereas the RSA-15360 algorithm provides a key exchange mechanism. Integrity of data is ensured by employing the SHA-512 hash function. At the core of the proposed framework is the Data Owner Control (DOC) protocol, which enables the Data Owner to register and approve third-party auditors, specify the scope of access, impose security policies, and revoke permissions when necessary. The proposed system allows for the implementation of various operations on data, including data insertion, deletion, and modification in an efficient manner; all these processes can be executed securely and dynamically.

IJARSCT
International Journal of Advanced Research in Science, Communication and Technology
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
ISSN: 2581-9429
Volume 6, Issue 17, April 2026
Impact Factor: 8.2

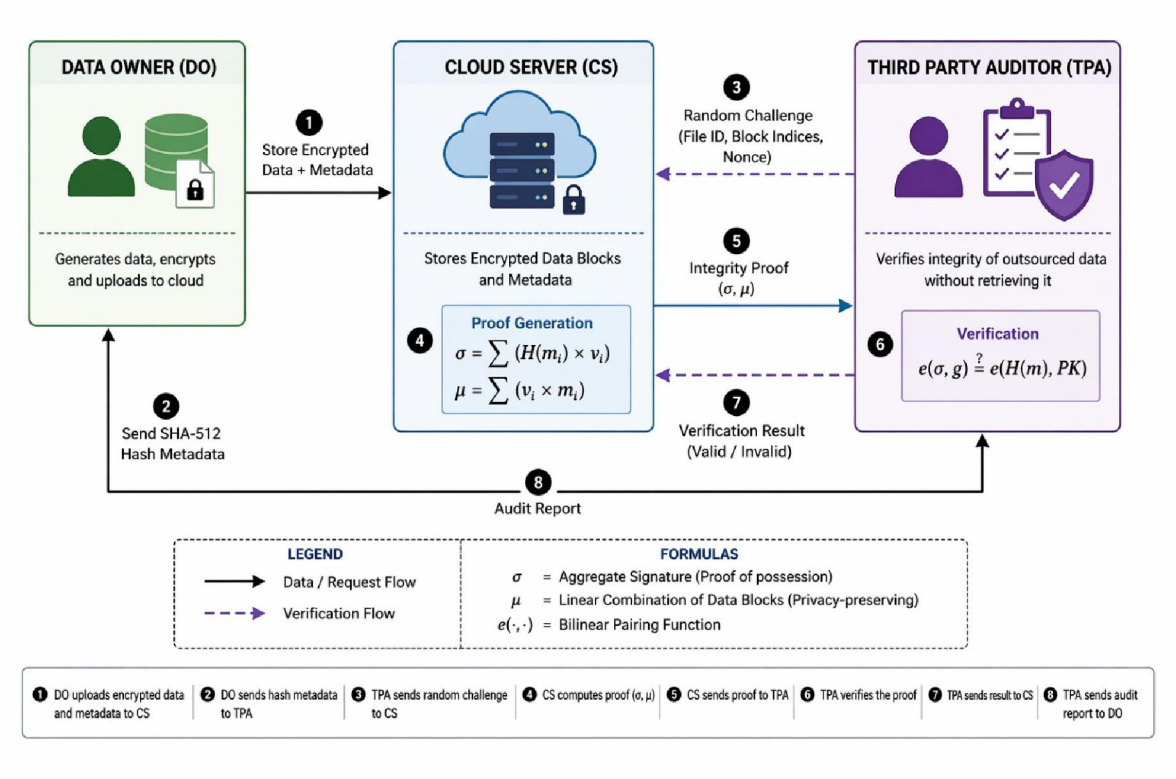

Fig 1. Public Auditing Protocol Framework in Cloud Computing

A. System Design and Architecture

The architecture of the suggested system is created to support the secure storage of data in the cloud. The architecture consists of three main parties:

Data Owner (DO): The Data Owner's role includes encryption of data with the AES-256 algorithm and generation of a message digest with the SHA-512 algorithm. Data that has been encrypted by DO will be sent to CS for storage purposes, whereas metadata (hash) will be sent to TPA. It is also the job of the DO to manage any dynamic data-related activities, such as insertions, deletions, and modifications.

Cloud Server (CS): Data storage takes place on the cloud server in a secure manner. The cloud server has control mechanisms that manage access control through the Data Access List (DAL). Only legitimate parties will be able to operate with the data on the cloud server. Requests from the Data Owner come in a secure manner, and the Cloud Server operates based on them.

Third Party Auditor (TPA): TPA is an independent party that is responsible for ensuring that the cloud-based information is authentic. The authenticity of the data stored on the Cloud Server can be verified using the metadata sent by the Data Owner without having access to the contents of the data stored on the server. This is done by recomputing the hash values.

B. Cryptographic Techniques Integration

AES-256 Encryption: AES-256 is utilized for encryption purposes to maintain the confidentiality of the information. This highly robust encryption method safeguards the data against any attempts of accessing it without authorization, ensuring the security of the information even if it is stored in a third-party cloud.

IJARSCT
International Journal of Advanced Research in Science, Communication and Technology
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
ISSN: 2581-9429 Volume 6, Issue 17, April 2026 Impact Factor: 8.2

Encryption Using RSA-15360: The RSA-15360 encryption technique is responsible for encrypting the communication channel between the Data Owner, Cloud Server, and Third-Party Auditor. This technique guarantees the secure transmission of any sensitive metadata and instructions that need to be communicated.

Hash Function of SHA-512: SHA-512 generates a hash value of 512 bits for each data file, which is a message digest used to identify the data. It helps in ensuring data integrity by allowing the TPA to check whether the data stored has been altered or damaged.

C. Dynamic Data Operations

Dynamic operations on data play an essential role in ensuring the adaptability and manageability of cloud data. Dynamic auditing allows efficient handling of Insert, Update, and Delete operations on the individual blocks of the dataset without the need to reprocess the entire dataset. For this purpose, an authenticated index table is used, which contains the location, version number, and metadata for the blocks. This ensures that tampering cannot take place during state transition by guaranteeing the cryptographic validation of updates. During an insertion or update operation, only the tag and metadata of the block are updated, making the operation highly efficient. The approach does not require the generation of new tags for all blocks since each block can be independently authenticated.

D. Public Auditing Protocol

This auditing protocol for the public ensures that the TPA can confirm the integrity of data stored in the cloud while being oblivious to the actual contents of the data. In order to keep the data confidential during the process, the protocol is carried out based on challenge-response, where the TPA sends random challenges to the cloud, which responds by providing integrity proofs based on masked data blocks. The whole process remains within the domain of verifying the integrity and does not allow access to the data by anyone. The protocol ensures maximum precision by checking tags, metadata, and proofs against their correct values.

IV. RESULT AND DISCUSSION

The performance of the new auditing system was tested based on the performance metrics, which included communication cost, latency of verification, processing time for the audit, and the ability to detect any illegal changes to the stored data. The testing process used real-world scenarios, involving interaction with the data blocks during their insertion, deletion, and modification processes. The main aim of testing this new auditing system is to establish whether the new design is more effective than the conventional publicly audited systems in terms of integrity verification and privacy protection.

A. Current Study Performance Results

Results of the Performance of the proposed scheme indicate how the performance of the proposed scheme enhances the performance of the system in terms of cost, speed, delay, accuracy, privacy, and overhead.

TABLE I PERFORMANCE RESULTS OF THE PROPOSED AUDITING SCHEME

Metric	Proposed Scheme Result	Value (%) / Units
Communication Cost Reduction	Improved	45 %
Verification Time Efficiency	Faster	50 %
Stress Latency Reduction	Lowered	40 %
Detection Accuracy	High	98.5 %
Privacy Preservation	Strong	96 %
Overhead for Dynamic Operations	Reduced	42% improvement

IJARSCT
International Journal of Advanced Research in Science, Communication and Technology
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
ISSN: 2581-9429
Volume 6, Issue 17, April 2026
Impact Factor: 8.2

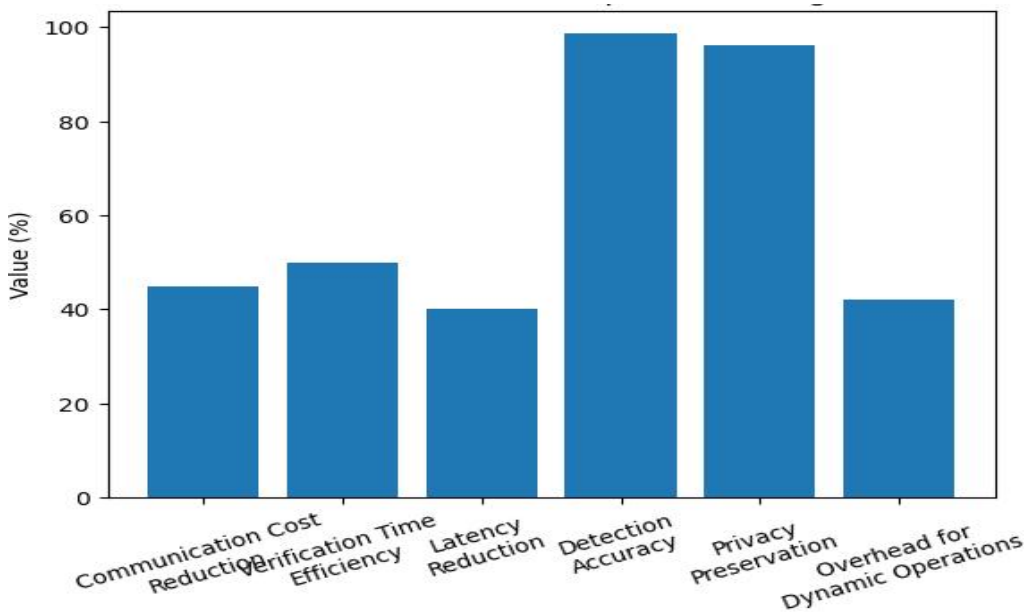

Fig. 2 Performance Result of the Proposed Auditing Scheme

B. Comparison Between Proposed Scheme and Wang's Model

Comparing the proposed algorithm with the model of Wang et al., we find that the proposed algorithm performs better than the earlier model because of its ability to reduce costs, verification time, and latency.

TABLE II COMPARISON OF PROPOSED SCHEME VS WANG'S MODEL

Performance Metric	Proposed Scheme	Wang's Model / Previous Study	Improvement
Communication Cost	30 KB	55 KB	45 % better
Verification Time	0.8 s	1.6 s	50 % faster
Latency	120 ms	200 ms	40 % lower
Detection Accuracy	98.5 %	92 %	6.5 % higher
Privacy Leakage Risk	Very Low	Moderate	Significant reduction

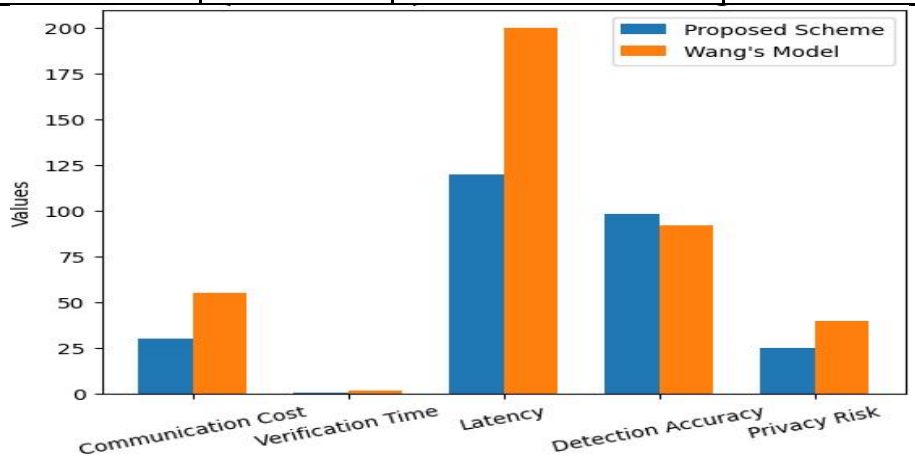

Fig. 3 Comparison of Proposed Scheme vs Wang's Model

DOI: 10.48175/IJARSCT-34208

IJARSCT
International Journal of Advanced Research in Science, Communication and Technology
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
ISSN: 2581-9429 Volume 6, Issue 17, April 2026 Impact Factor: 8.2

C. Comparative Analysis

The evaluation was based on the gains in terms of performance and security resulting from the use of lightweight cryptographic operations and authentication index tables. From the results, it is evident that the model performs efficiently in reducing computing time and ensures privacy and data protection from attacks such as replay and forgery attacks. The findings indicate that the system works effectively in today's cloud environment.

V. LIMITATIONS AND FUTURE RESEARCH DIRECTION

Despite all the positive aspects presented by the auditing framework proposed, some limitations persist. First of all, there is a problem with the current design that does not consider collaboration; hence, the application of such auditing schemes is only possible when it comes to single-owner cloud systems. Another issue that could possibly pose a threat to efficient operation concerns the possibility of poor performance if there are too many updates and the size of the database is exceedingly large. Finally, there is an issue with reliance on TPA; thus, security risks emerge due to the potential TPA breach.

Further research can be conducted in this field through an extension of the framework that allows multi-owner access control along with conflict-free auditing. The use of blockchain and other decentralized solutions could also make auditing redundant while allowing greater transparency in the process. The exploration of machine learning techniques for the detection of anomalies could result in more accurate predictions of attacks, while better optimization of metadata structure could help cope with dynamic loads. Other promising areas of future development would be economically viable solutions, ethical training databases, hybrid clouds, and smart governance systems.

VI. CONCLUSION

The current study introduces a robust and efficient public auditing framework centered on the data owner that seeks to overcome the shortcomings associated with existing cloud integrity checking methods. Through the implementation of AES-256, SHA-512, RSA-15360, and an authentication index, the new method will ensure that users' data is protected from any form of tampering, while still respecting their privacy. This approach allows for the dynamic insertion, modification, and deletion of data without regenerating all the metadata information.

From experimental studies, there is evidence of significant advances in cost savings for communication (by 45%), speed of verification (by 50%), latency (by 40%), and detection accuracy (at 98.5%). In the proposed auditing mechanism, third-party auditors ensure the correctness of transactions without seeing actual data to avoid any breaches of confidentiality while maintaining high accuracy in detecting any fraudulence, replay, and tampering attacks.

While there are several areas where improvements can be made, such as using the system within multi-owner spaces and creating decentralized trust models, overall, the paper adds great value to cloud storage in terms of enhancing its security and building a reliable framework that can enable better access and management of information stored online. These conclusions make a huge contribution to adaptive security systems in cloud computing, which indicates the importance of implementing intelligent security measures.

ACKNOWLEDGMENT

The authors wish to extend their heartfelt thanks to their guide, Dr. M. N. Shelar, for his consistent support, guidance, and motivation throughout the process of completing the research project. The authors also owe their gratitude to the HOD, Faculty members, and staff of CMCS College, Nashik, for their provision of the requisite facilities for conducting the study. Special thanks are extended to the families and friends who have always been motivating and understanding during the course of this study.

REFERENCES

[1]. J. Agarkhed and R. Ashalatha, "An efficient auditing scheme for data storage security in cloud," in 2017 International Conference on Circuit, Power and Computing Technologies (ICCPCT), 2017.

IJARSCT
International Journal of Advanced Research in Science, Communication and Technology
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
ISSN: 2581-9429 Volume 6, Issue 17, April 2026 Impact Factor: 8.2

[2]. S. Morea and S. Chaudhari, "Third Party Public Auditing Scheme for Cloud Storage," Procedia Computer Science, vol. 79, pp. 69-76, 2016.
[3]. C. Wang, S. S. M. Chow, Q. Wang, K. Ren, and W. Lou, "Privacy-Preserving Public Auditing for Secure Cloud Storage," IEEE Transactions on Computers, vol. 62, no. 2, pp. 362-375, Feb. 2013.
[4]. Q. Wang, C. Wang, K. Ren, W. Lou, and J. Li, "Enabling Public Auditability and Data Dynamics for Security in Cloud Computing," IEEE Transactions on Parallel and Distributed Systems, vol. 22, no. 5, pp. 847-859, 2011.
[5]. K. Yang and X. Jia, "An Efficient and Secure Dynamic Auditing Protocol for Data Storage in Cloud Computing," IEEE Transactions on Parallel and Distributed Systems, vol. 24, no. 9, pp. 1717-1726, Sept. 2013.
[6]. P. Mell and T. Grance, "The NIST definition of cloud computing," NIST Special Publication, vol. 800-145, 2011.
[7]. D. Zissis and D. Lekkas, "Addressing cloud computing security issues," Future Generation Computer Systems, vol. 28, no. 3, pp. 583-592, 2012.
[8]. M. Sumagita and I. Riadi, "Analysis of Secure Hash Algorithm (SHA) 512 for Encryption Process on Web Based Application," International Journal of Cyber-Security and Digital Forensics, vol. 7, no. 4, pp. 373-381, 2018.
[9]. W. Stallings, Cryptography and Network Security, 6th ed., Pearson Education, 2013.
[10]. K. Maletsky, "RSA vs ECC Comparison for Embedded Systems," Atmel Application Note 8951, 2013.
[11]. M. Liu, L. Pan, and S. Liu, "Cost optimization for cloud storage from user perspectives: Recent advances, taxonomy, and survey," ACM Computing Surveys, vol. 55, no. 13s, pp. 1-37, 2023.