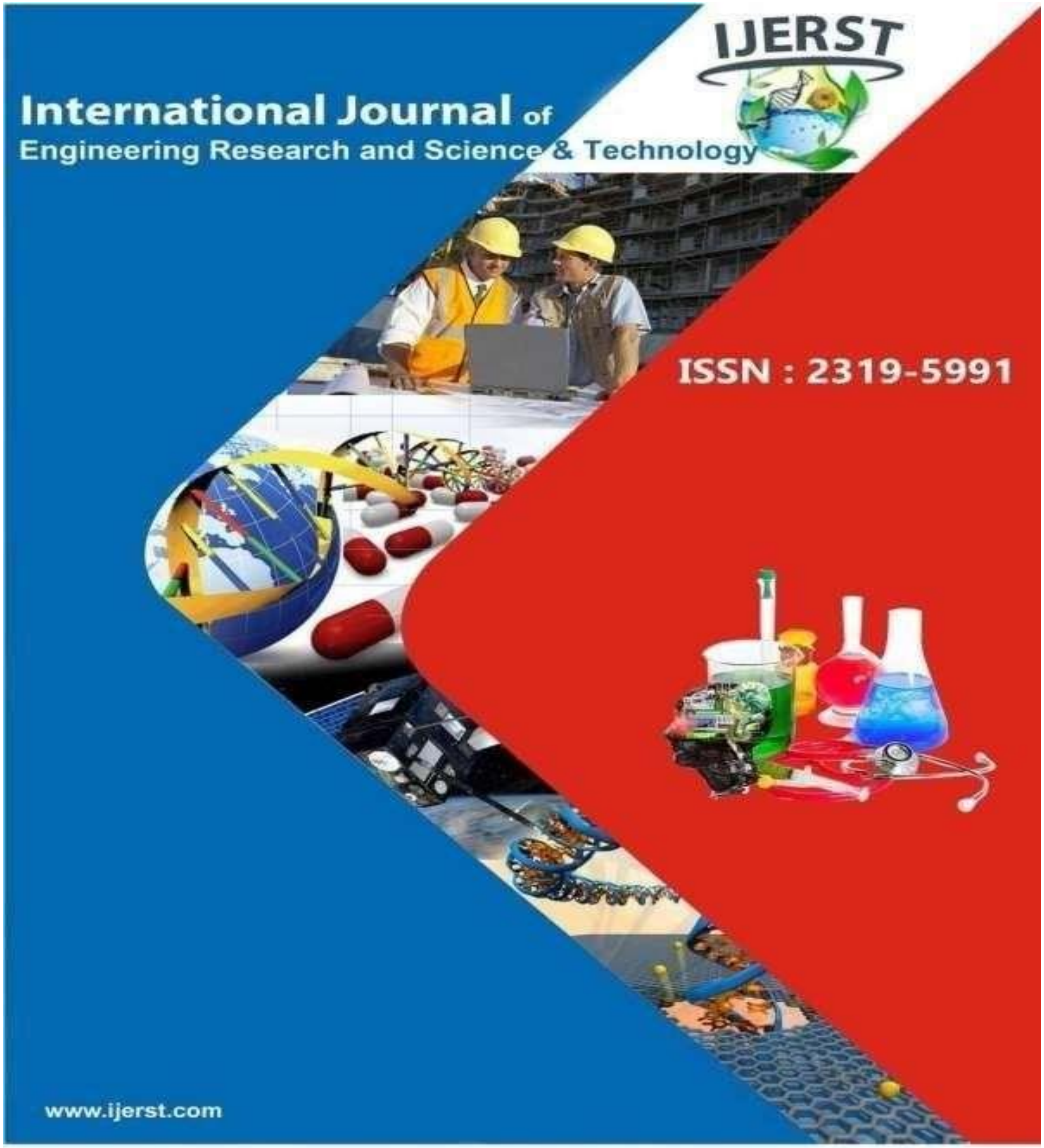

IJERST

International Journal of Engineering Research and Science & Technology

ISSN : 2319-5991

www.ijerst.com

Email: editor@ijerst.com or editor.ijerst@gmail.com

ISSN 2319-5991 www.ijerst.com

https://doi.org/10.62643/ijerst.2022.v18.i4.pp73-86

Vol. 18, Issue 4, 2022

SYMMETRIC KEY-BASED DUPLICABLE STORAGE PROOF FOR ENCRYPTED DATA IN CLOUD STORAGE ENVIRONMENTS: SETTING UP AN INTEGRITY AUDITING HEARING

Poovendran Alagarsundaram,

AWS Solution Architect, Humetis Technologies, New Jersey, United States.

Email ID: poovasg@gmail.com

ABSTRACT

The safe and effective administration of data in cloud storage systems poses major issues in the current digital environment. Deduplicable Proof of Storage (DPOS) is a viable solution that successfully addresses these issues by utilizing sophisticated encryption algorithms and symmetric keys. Symmetric key encryption techniques are used by DPOS to encrypt data prior to storage, guaranteeing secrecy and promoting effective data deduplication. DPOS enhances storage efficiency by optimizing storage resources by detecting and removing redundant data copies. DPOS also makes proof of storage easier, allowing users to confirm data accuracy without laborious decryption processes. The significance of data integrity in contemporary digital contexts is emphasized in this study, which also examines the technical challenges of implementing an integrity auditing protocol within Sec-DPoS. The approach includes critical steps including challenge, reaction, and verification, all of which are necessary to guarantee the auditing process' efficacy. Moreover, assessing Sec-DPoS effectiveness using performance measures offers important information about its scalability and efficacy in comparison to other systems. Athorough architecture diagram provides a visual depiction of the integrity auditing procedure within Sec-DPoS by highlighting the interactions between various components. In summary, thisstudy offers a methodical framework for putting integrity auditing techniques into practice, guaranteeing the dependability and security of data in cloud storage settings.

Keywords: Deduplicable Proof of Storage, DPOS, Symmetric Keys, Encryption, Data Integrity, Cloud Storage, Integrity Auditing, Security, Efficiency, Cryptographic Techniques.

https://doi.org/10.62643/ijerst.2022.v15.i4.pp73-86

Vol. 15 , Issue 4, 2022

1 INTRODUCTION

An intelligent method for safely and effectively managing data in cloud storage systems is Deduplicable Proof of Storage (DPOS). It all comes down to protecting and organizing data while making sure we don't use up more space than is necessary.

First and foremost, these keys serve as the code of secret that locks and unlocks our data. Our data becomes a jumbled mess that only a person with the correct key can decipher when we encrypt it with a symmetric key. In the unlikely event that someone manages to gain access to our data, this guarantees that it will remain confidential and unreadable. Second, symmetric keys assist us in organizing our storage capacity by locating and eliminating redundant data copies. DPOS saves us valuable storage space by using these keys to identify identical data bits and guarantee that we only maintain one copy. This keeps our storage expenses low and our systems operating efficiently.

With its unmatched simplicity and scalability, cloud storage has completely changed how we save and retrieve data. However, it gets harder to guarantee data integrity and secrecy as more and more data is kept on cloud servers. Conventional methods of managing data frequently fail to solve these issues, which results in inefficiencies and security flaws. A comprehensive method for handling encrypted data in cloud storage systems is provided by Deduplicable Proof of Storage (DPOS), which appears to be a promising answer to these problems. DPOS is a useful tool for contemporary cloud storage apps since it maximizes storage efficiency and improves data security by utilizing symmetric keys and cutting-edge encryption techniques.

DPOS Mechanics: The use of symmetric keys to guarantee data integrity and confidentiality is the foundation of DPOS. Data is encrypted before being stored using symmetric key encryption algorithms, such AES, to keep it safe and impenetrable. Furthermore, symmetric keys facilitate effective data deduplication by detecting and removing duplicates. This procedure improves overall storage efficiency by lowering storage overhead and streamlining data management chores. DPOS also makes proof of storage easier, enabling users to confirm the accuracy of their data without requiring laborious decryption procedures. In cloud storage environments, data is kept safe, arranged, and easily accessible thanks to this creative approach to data management.

https://doi.org/10.62643/ijerst.2022.v15.i4.pp73-86

Vol. 15 , Issue 4, 2022

Benefits of DPOS: Companies looking to improve data efficiency and integrity in cloud storage can reap a number of advantages by implementing DPOS. Symmetric keys are utilized by DPOS to optimize storage resources and secure sensitive data through encryption and deduplication. DPOS also simplifies storage management chores, lowering administrative burden and enhancing operational effectiveness. Additionally, DPOS improves data accessibility by allowing users to confirm the accuracy of their data without requiring laborious decryption procedures. All things considered, DPOS proves to be a complete answer to the problems of data security, integrity, and storage optimization in contemporary cloud storage settings.

Deduplicable Proof of Storage (DPOS), which provides an all-inclusive solution for maintaining encrypted data, is a noteworthy development in cloud storage technology. In cloud storage environments, DPOS protects data integrity, confidentiality, and storage effectiveness by utilizing symmetric keys and cutting-edge encryption algorithms. Organizations can increase operational efficiency, simplify storage management responsibilities, and strengthen security by implementing DPOS. With the amount of data being saved in the cloud increasing, DPOS is becoming a useful tool for handling the changing problems with data security and administration.

In the present digital landscape, maintaining data integrity is essential for businesses in a number of industries. Building stakeholder confidence, following regulations, and making well-informed decisions all depend on data. Integrity auditing is a crucial step in preserving data integrity since it ensures that information remains reliable, accurate, and consistent while pointing out any unauthorized changes or manipulations.

Integrity auditing includes a number of crucial elements that are necessary for thorough data validation and verification. These elements consist of audit trails, encryption methods, access controls, logging systems, and data validation processes. Cryptographic techniques provide confidentiality and integrity of data, while data validation processes check data quality and consistency. Sensitive data cannot be accessed by unauthorized parties thanks to access restrictions, which also provide audit trails and logging systems that keep track of all data access and modification activity. Organizations can create a strong framework for preserving data integrity and reliability by incorporating these elements.

https://doi.org/10.62643/ijerst.2022.v15.i4.pp73-86

Vol. 15 , Issue 4, 2022

Establishing an integrity auditing procedure is a process that requires several important steps. Organizations first establish the goals and parameters of auditing, specifying the kinds of data that need to be examined, how often they should be performed, and the expected results. Afterwards, suitable auditing technologies and tools are chosen, like integrity monitoring software andintrusion detection systems, in order to automate the auditing process and quickly identify integrityviolations. Organizations also create auditing policies and procedures that define roles and dutiesand regularly teach staff members on the value of data integrity and audit procedures. Organizations can make the necessary adjustments based on audit results and new threats by continuously monitoring and reviewing the auditing procedure.

With today's digital landscape, it is imperative to ensure the security and dependability of data housed in cloud environments. With an emphasis on its use within the context of Sec-DPoS (Secure Deduplicable Proof of Storage), this paper explores the technical details of an integrity auditing protocol. The novel Sec-DPoS method preserves data integrity and security while managing encrypted data in cloud storage systems.

In order to carry out its integrity auditing procedure, Sec-DPoS randomly challenges indices included in encrypted files. The protocol confirms data integrity using this technique without jeopardizing encryption or requiring unnecessary data transmission. As a result, there is less chance of illegal access or alteration and the data will remain reliable.

Utilizing a variety of software tools and technologies may be necessary to implement the Sec-DPoS integrity auditing protocol. These might include cryptography libraries, encryption techniques, and specially designed auditing software that meets Sec-DPoS's unique needs. Furthermore, the analysis and interpretation of implementation outcomes may be facilitated by data visualization tools.

Software developers that specialize in cloud storage and data security, researchers, and cybersecurity specialists may integrate integrity auditing procedures, particularly inside Sec-DPoS. Interactions between research and business are another factor in putting these methods to use and evaluating them in practical settings.

ISSN 2319-5991 www.ijerst.com

https://doi.org/10.62643/ijerst.2022.v15.i4.pp73-86

Vol. 15 , Issue 4, 2022

Strong integrity auditing procedures are required as cloud storage becomes more and more important for data management. The intricacies and security issues pertaining to the storage of confidential data in cloud environments are frequently beyond the capabilities of conventional techniques. Sec-DPoS is a viable solution that protects data integrity and security by utilizing cutting-edge cryptographic techniques and effective auditing procedures.

Several technological breakthroughs are utilized in the Sec-DPoS integrity auditing techniques. To begin with, sophisticated cryptographic methods and algorithms are essential for protecting data and confirming its accuracy without jeopardizing encryption. Additionally, the accuracy and dependability of integrity audits in cloud environments are improved by the use of effective auditing procedures, automated tools, and advanced software solutions.

Furthermore, academics and practitioners may now better assess and comprehend implementation results because to developments in data visualization tools. These technologies help discover possible security threats or integrity breaches by making audit logs, data validation results, and integrity verification processes easier to visualize.

Technological breakthroughs in integrity auditing procedures are also driven by partnerships between academia and industry. To develop and deploy cutting-edge solutions that solve the changing issues of data security and integrity in cloud storage, researchers collaborate closely with cybersecurity professionals and cloud service providers.

Even with recent advances in cloud storage technology, there is still a need to develop efficient integrity auditing procedures that are specific to the difficulties that arise in cloud systems. Current solutions could be ineffective or neglect to take into account particular needs for data security and integrity in cloud storage systems. To close these loopholes and guarantee the reliability of data in cloud storage, the problem statement centers on creating and putting into practice efficient integrity auditing techniques, such as Sec-DPoS.

Ensuring the security and integrity of encrypted data stored in cloud environments is the main objective of integrating an integrity auditing protocol in Sec-DPoS. This entails ensuring that data is consistently and accurately preserved while reducing the possibility of data breaches or

https://doi.org/10.62643/ijerst.2022.v15.i4.pp73-86

Vol. 15 , Issue 4, 2022

unwanted access. The implementation also attempts to evaluate Sec-DPoS's effectiveness and performance in comparison to other systems.

2 LITERATURESURVEY

EI (2018) With an emphasis on efficiency and integrity, this paper explores cloud storage security for data deduplication. In order to achieve this, integrity audits and symmetric key encryption are used. The technology guarantees effectiveness and privacy by eliminating unnecessary data and safely encrypting it. Through frequent inspections and problem-solving, integrity auditing preserves data integrity. Consolidating audits with proof of storage, automating monitoring, and encrypting data in advance are all steps in the integration process. This method ensures reliable, safe, and effective cloud data storage overall.

Cui (2019) presents SPEED, a novel technique that uses secure deduplication to accelerate enclave applications. Through elimination of unnecessary computations, it maintains high security criteria while optimizing enclave performance. SPEED represents a substantial breakthrough in enclave technology since it increases productivity without sacrificing data integrity or confidentiality. SPEED guarantees data security while increasing overall speed by efficiently minimizing duplicate computations, offering gains for a variety of computing activities in secure contexts.

Kaur (2017) analysis explores data deduplication techniques and highlights how important they are for optimizing storage. It talks about different methods of getting rid of redundant data and how they affect storage performance. For the benefit of scholars and practitioners alike, a full analysis is provided of the advantages and disadvantages of each approach. The paper highlights the importance of deduplication techniques in storage optimization by providing a comprehensive overview of these techniques. It thoroughly examines and assesses methods such as chunking, delta encoding, and content-defined storage in relation to storage efficiency. Through a rigorous evaluation of each approach, the assessment facilitates decision-making and directs future studies and real-world data storage applications.

In Geeta (2020) work, a unique system that combines safe deduplication, dynamic ownership management, and virtual auditing in the cloud is introduced: VASD2OM. Data security and

https://doi.org/10.62643/ijerst.2022.v15.i4.pp73-86

Vol. 15 , Issue 4, 2022

storage efficiency are improved by VASD2OM through data integrity verification, redundant data removal, and customizable access control. In order to ensure effective data management in cloud environments, it provides strong security measures while optimizing storage resources.

The impact of management integrity on audit planning and evidence is examined in Kizirian (2005) research. It explores the risk assessment, planning, and evidence sufficiency of auditors, highlighting the importance of taking management integrity into account in audit engagements. By emphasizing the influence of management integrity on risk assessment and evidence gathering, the research seeks to improve audit methods.

The importance of Supreme Audit Institutions (SAIs) as fundamental pillars of integrity in the battle against corruption is emphasized in Dye (1998) text. It emphasizes how SAIs support good governance, accountability, and openness. The study highlights the importance of SAIs in reducing corrupt practices and increasing integrity within governance systems by discussing their roles in government financial auditing, good governance promotion, and corruption prevention.

The impact of auditing integrity on organizational value is examined in Stojanović (2019) work. It emphasizes how auditing procedures can go above and beyond legal obligations to improve integrity and add value. The article emphasizes how crucial it is to question established auditing practices in order to promote integrity and maximize value generation. It highlights how ethical behavior, accountability, and openness are ensured by auditing integrity, which ultimately maximizes value and assures long-term corporate viability.

The difficulties with audit reporting when financial reporting shifts to an information-centric paradigm are examined in Cohen (2014) write-up. It talks about how it affects integrity and communication and offers solutions to keep things honest and transparent. In this dynamic environment, the study emphasizes the necessity of adjusting to new communication techniques and technological advancements in order to maintain the integrity of audit reports.

Integrity issues arise while reviewing trustworthy database management systems (DBMS), as discussed in Filsinger (1992) work. It draws attention to how important integrity is to maintaining the security and dependability of data in these systems. The paper addresses issues specific to

https://doi.org/10.62643/ijerst.2022.v15.i4.pp73-86
Vol. 15 , Issue 4, 2022

trusted database management systems (DBMSs), like intricate security features, and suggests auditing techniques that work. Dependability and trustworthiness—two essential components for the management of sensitive data—can be preserved by reputable DBMS by resolving integrity issues through customized auditing techniques.

The need of guaranteeing data reliability is emphasized in Svanks (1988) work, which investigates automating integrity analysis-based data quality assurance. It covers techniques such as anomaly detection and data profiling and suggests ways to automate tasks with machine learning and validation tools. The study also demonstrates how automation improves efficiency and preserves consistent data quality in domain-specific applications in e-commerce, banking, and healthcare.

The impact of auditors' judgments of client honesty on risk assessments, audit evidence, and fees is examined in Beaulieu (2001) investigate. It looks at how these rulings affect financial calculations and audit decision-making. Evaluations of a client's integrity have an impact on risk assessments, the validity of audit evidence, and price negotiations, which in turn influence overall audit procedures and client interactions.

Yu (2016)XDedup provides an inventive way to store encrypted data in the cloud and perform effective, safe cross-user deduplication. It functions client-side for improved privacy, optimizes storage capacity by removing unnecessary data across users, and provides security through encryption. Cloud storage becomes more economical and efficient when XDedup ensures data confidentiality and integrity.

3. METHODOLOGY

In order to ensure data integrity, confidentiality, and efficiency in cloud storage environments, a comprehensive strategy must be used while establishing an integrity auditing protocol within Sec-DPoS (Secure Deduplicable Proof of Storage). The challenge, answer, and verification phases are some of the crucial steps in this process. For the integrity auditing process to be effective, each phase is essential.

ISSN 2319-5991 www.ijerst.com

https://doi.org/10.62643/ijerst.2022.v15.i4.pp73-86

Vol. 15 , Issue 4, 2022

3.1 Challenge Phase:

The Sec-DPoS integrity auditing method starts with the challenge phase. In this case, the basis for evaluating the data integrity is the random selection of indices from within an encrypted file for verification.

We take into account the corrupt proportion of the target data, represented by δ, in order to calculate the magnitude of the challenge. We can customize the auditing procedure using this option to reach the required degree of confidence. We can change the challenge size to reach a 99% or 95% confidence level, for instance, if δ is 0.01 and indicates a 1% corruption rate. This reduces computational needs while guaranteeing that the auditing process covers a representative amount of the data.

3.2 Response Phase:

The response phase assumes a central role following the challenge phase. Here, solutions to the problems posed in the preceding phase are produced. This usually entails decrypting the chosen indices and evaluating their integrity based on predetermined standards.

Providing proof of data integrity while protecting the privacy of stored data and the security of encryption algorithms is the main objective of the response phase. This can include verifying the data's compatibility with the original copies and authenticating it using cryptographic methods like digital signatures or hash functions.

3.3 Verification Phase:

The verification phase intervenes after the challenge and response phases to assess the previously generated responses and validate the data's integrity. To ensure data consistency, this step usually involves checking the decrypted data against the original copies or performing checksum validations.

Additionally, at this stage, cryptographic hash algorithms might be used to generate distinct identifiers for the audited data. These IDs are used to confirm that the data being examined is accurate and authentic.

ISSN 2319-5991 www.ijerst.com

https://doi.org/10.62643/ijerst.2022.v15.i4.pp73-86

Vol. 15 , Issue 4, 2022

The verification phase's ultimate goal is to ensure the effectiveness of the auditing process by verifying data integrity with the least amount of computing overhead.

3.3.1 Evaluation of Sec-DPoS Efficiency:

Apart from the approach stated, we may evaluate Sec-DPoS's efficacy for integrity auditing by taking into account other performance measures. These metrics provide important information about Sec-DPoS performance relative to other systems such as Message-locked PoOR and SecCloud.

3.4 Computation Costs:

Computation costs are an important factor to take into account when evaluating the effectiveness of integrity auditing procedures. The time required for the auditing process's challenge, response, and verification phases is included in these expenses.

Reduced computing costs indicate Sec-DPoS's superior scalability and efficiency over competing systems. This is due to the fact that reduced computing overhead results in quicker auditing processes and better resource management.

Computation costs over a range of file sizes and confidence levels must be measured in order to assess Sec-DPoS's effectiveness. With the least amount of computational overhead possible, this examination helps determine the optimal parameters for integrity audits.

3.5 Network Latency:

An further crucial element in assessing how well integrity auditing technologies work is network latency. By maximizing data transfer and response times, Sec-DPoS seeks to reduce communication expenses.

Sec-DPoS's efficacy in cutting overhead and enhancing data access efficiency can be evaluated by contrasting network latency with that of other methods.

For the purpose of preserving data integrity and guaranteeing timely auditing procedures, lower network latency means faster data transmission and better responsiveness.

ISSN 2319-5991 www.ijerst.com

https://doi.org/10.62643/ijerst.2022.v15.i4.pp73-86

Vol. 15 , Issue 4, 2022

The architecture diagram sketch that follows shows the main elements and their interactions in the integrity auditing process inside Sec-DPoS:

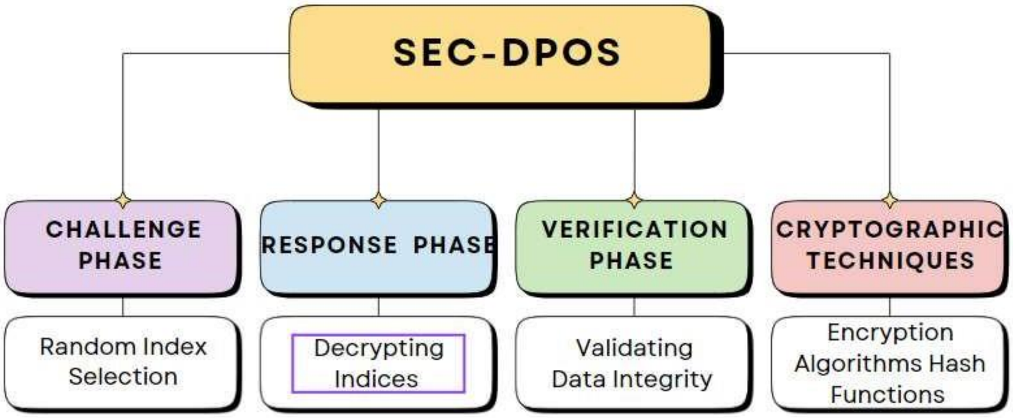

Figure 1: Essential Elements of the Sec-DPoS Integrity Auditing Procedure

The architecture diagram shows the essential elements of the Sec-DPoS integrity auditing procedure. The challenge phase, the response phase, and the verification phase are its three primary phases.

The auditing procedure is started during the challenge phase when random indices inside the encrypted file are chosen for verification.

After the challenge phase, there is a response phase during which solutions to the challenges are developed. This stage responds to the chosen indices while maintaining data confidentiality and integrity.

The responses produced during the challenge phase are then evaluated in the verification step to verify the validity and integrity of the data.

Cryptographic techniques like hash functions and encryption algorithms are used during the auditing process to protect the confidentiality and security of data.

The architectural diagram shows the data flow during the integrity auditing process within Sec-DPoS and clarifies the interconnections between various components.

To sum up, the above-described methodology offers a methodical way to set up an integrity auditing mechanism for cloud-based encrypted data within Sec-DPoS. Sec-DPoS provides a strong solution for maintaining data integrity and improving storage efficiency by combining cutting-edge cryptographic approaches, streamlined auditing procedures, and performance evaluation criteria. Comparing Sec-DPoS's efficacy and scalability to other methods, the evaluation of its efficiency using a variety of performance measures provides insightful information. Furthermore, the architectural diagram clearly illustrates how the approach is implemented by showing the crucial elements and interactions in the integrity auditing process within Sec-DPoS. All things considered, the approach presented in this research provides a workable foundation for implementing integrity auditing methods inside Sec-DPoS, guaranteeing the reliability and security of data in cloud storage settings.

4. RESULTS AND DISCUSSION

Sec-DPoS (Secure Deduplicable Proof of Storage) greatly improves storage efficiency and data integrity when it is integrated into cloud systems. While preserving data secrecy, symmetric keys are used for encryption and deduplication to minimize storage overhead. Data integrity is guaranteed by the protocol's challenge, response, and verification phases without requiring time-consuming decryption. Because of its effective, selective auditing of data samples, Sec-DPoS exhibits reduced computing costs and network delay as compared to systems such as Message-locked PoOR and SecCloud. Hash functions and digital signatures are additional security layers added by this technology that make it more difficult for unwanted access. Furthermore, Sec-DPoS makes audits easier, lessens administrative work, and boosts operational effectiveness, which makes it perfect for handling massive amounts of data in the cloud.

5. CONCLUSION

To summarise, the methodology shown here offers a methodical way to integrate an integrity auditing protocol into Sec-DPoS, guaranteeing the security and dependability of encrypted data stored in cloud storage. Through the use of sophisticated cryptographic methods and effective

https://doi.org/10.62643/ijerst.2022.v15.i4.pp73-86

Vol. 15 , Issue 4, 2022

auditing processes, Sec-DPoS provides a reliable way to preserve data integrity and maximize storage effectiveness. The assessment of Sec-DPoS performance using diverse indicators yields significant insights into its efficacy and expandability, whereas the architectural diagram furnishes a pictorial depiction of the integrity auditing procedure. In summary, this study establishes a strong basis for the integration of integrity auditing techniques into Sec-DPoS, guaranteeing the security and integrity of data in cloud storage settings. Future work may concentrate on improving Sec-DPoS integrity auditing processes' computing efficiency, particularly for bigger datasets and greater confidence levels. Furthermore, enhancing data access efficiency and decreasing network latency will improve Sec-DPoS's overall performance and effectiveness in preserving data security and integrity in cloud storage environments. Prolonged cooperation between experts from academia and business could spur innovation and developments in this area, which would ultimately help consumers and companies that depend on cloud storage solutions.

6. References

[1] EI, M. C. (2018). Secure Multiple Group Data Deduplication in Cloud Data Storage. Doctoral Dissertation, Graduate School of Science and Engineering, Saitama University (Doctoral Program).

[2] Cui, H., Duan, H., Qin, Z., Wang, C., & Zhou, Y. (2019, July). SPEED: Accelerating enclave applications via secure deduplication. In 2019 IEEE 39th International Conference on Distributed Computing Systems (ICDCS) (pp. 1072-1082). IEEE.

[3] Kaur, G., & Devgan, M. S. (2017). Data deduplication methods: a review. International Journal of Information Technology and Computer Science, 10, 29-36.

[4] Geeta, C. M., Nikhil, R. C., Raghavendra, S., & Venugopal, K. R. (2020). VASD2OM: Virtual Auditing and Secure Deduplication with Dynamic Ownership Management in Cloud. International Journal of Recent Technology and Engineering (IJRTE), 8(6), 5504-5514.

[5] Kizirian, T. G., Mayhew, B. W., & Sneathen Jr, L. D. (2005). The impact of management integrity on audit planning and evidence. Auditing: A Journal of Practice & Theory, 24(2), 49-67.

ISSN 2319-5991 www.ijerst.com

https://doi.org/10.62643/ijerst.2022.v15.i4.pp73-86

Vol. 15 , Issue 4, 2022

[6] Dye, K. M., & Stapenhurst, R. (1998). Pillars of integrity: the importance of supreme audit institutions in curbing corruption. Washington, DC: Economic development institute of the World Bank.

[7] Stojanović, T. (2019, March). AUDITING INTEGRITY–THROUGH CHALLENGE TO ADDED VALUE. In Third International Scientific Conference on Economics and Management-EMAN 2019: How to Cope with Disrupted Times-Conference Proceedings, Ljubljana, Slovenia-March 28, 2019 (pp. 171-184). Udruženje ekonomista i menadžera Balkana.

[8] Cohen, E. E., Debreceny, R., Farewell, S., & Roohani, S. (2014). Issues with the communication and integrity of audit reports when financial reporting shifts to an information-centric paradigm. International Journal of Accounting Information Systems, 15(4), 400-422.

[9] Filsinger, J. (1992, July). Integrity and the Audit of Trusted Database Management Systems. In DBSec (pp. 349-366).

[10] Svanks, M. I. (1988). Integrity analysis: Methods for automating data quality assurance. Information and Software Technology, 30(10), 595-605.

[11] Beaulieu, P. R. (2001). The effects of judgments of new clients' integrity upon risk judgments, audit evidence, and fees. Auditing: A Journal of Practice & Theory, 20(2), 85-99.

[12] Yu, C. M. (2016). Xdedup: Efficient provably-secure cross-user chunk-level client-side deduplicated cloud storage of encrypted data. Cryptology ePrint Archive.