IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
Impact Factor: 7.301
Volume 3, Issue 1, November 2023

An Application to Improve the Performance and Security in Cloud by File Division Technique

Mr. Vikas Singh, Tarun Bommawar, Tejas Kalaskar, Parthav Yengantiwar, Sameer Ghatbandhe, Manish Goabde, Sanket Ghuge
Department of Computer Science & Engineering
GH Raisoni Institute of Engineering & Technology, Nagpur, Maharashtra, India

Abstract: *Cloud computing has transformed the modern business landscape by providing scalable, flexible, and cost-effective solutions for data storage and processing. However, relying on external cloud providers to manage and protect sensitive data has raised significant security concerns, namely the risk of data breaches. To address these issues and optimize system performance concurrently, this research project introduces a novel approach that combines data fragmentation and replication in the cloud environment.*
Data fragmentation involves breaking down large files into smaller fragments or pieces, each of which contains only a portion of the original data. The fragments are then dispersed across multiple cloud nodes to ensure that no single node stores an entire file. This fragmentation and replication strategy reduces the potential risk of data exposure during a security breach.
Data replication across multiple nodes improves system performance in addition to providing security benefits. Replicating data fragments facilitates more efficient data distribution and retrieval, thereby reducing response times and enhancing overall system performance.
This paper provides a comprehensive overview of the methodology employed in this approach, highlighting its fundamental concepts, potential benefits, and key security considerations, such as the importance of data isolation and encryption. By combining data fragmentation and replication, organizations can strengthen their cloud data security while improving system performance, providing a comprehensive answer to the challenges posed by cloud computing.

Keywords: Cloud computing, data processing, scalability, flexibility, cost-effective solutions, security concerns, data breaches, data fragmentation, data replication, system performance, response times, encryption, benefits, cloud data security.

I. INTRODUCTION

Cloud computing has transformed data storage, access, and management. Internet-based remote servers and services give people, businesses, and organizations unprecedented scalability and accessibility. However, this technological paradigm change has created significant data security and system performance issues. As more data is stored in the cloud, security and privacy issues have grown. At the same time, cloud services must perform well to give users efficient and dependable data access.

This research report examines how to improve data security and cloud system performance. The File Division Technique, which securely distributes data into smaller, non-meaningful fragments among several cloud nodes, is the main strategy. Authorization rules and Proxy Re-Encryption control access to these AES-encrypted fragments. This technique rethinks the security-performance trade-off to improve data security and cloud system operation.

We'll discuss this project's core components in the following sections:

File Fragmentation and Replication: Breaking data into fragments prevents attackers from accessing meaningful information after a breach.

Advanced Encryption Standard (AES): A fragment-level encryption algorithm that protects data.

Access Control and Authorization: A granular system that lets data owners control who can access their data and how.

PRE: Proxy Re-Encryption A data-sharing method that protects encryption keys from intermediaries.

IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
Impact Factor: 7.301
Volume 3, Issue 1, November 2023

Optimizing Data Security without Performance Loss: Critical analysis shows that better security and cloud system performance are not mutually exclusive.

We will discover the importance of each component in improving cloud security and performance as we examine them.

The Cloud Computing Era

Cloud computing is essential to current technology and information management. The cloud symbolizes the abstraction of complex infrastructure into internet-based, scalable, and adaptable resources. Cloud service providers provide data storage, processing, applications, and platforms remotely.

This paradigm shift transformed industries, businesses, and individuals. The cloud lets companies focus on their core capabilities while outsourcing infrastructure maintenance due to its cost-effectiveness, scalability, and flexibility. Small startups, huge organizations, and government agencies are using the cloud to streamline operations and decrease IT costs.

Consumers have also benefited from cloud computing. From email and file storage to video streaming and social networking, it's everywhere. Cloud-based services and applications enable data access from anywhere with an internet connection, creating a mobile and connected world.

II. METHODOLOGY

This project strengthens cloud security and system performance with a holistic approach. File Division—a multi-step data fragmentation and replication process—is the main method. This method is strengthened by fragment-level AES encryption, granular access control and authorization, and Proxy Re-Encryption (PRE) for safe data transfer. The technique optimises performance, scalability, and usability. Mobile OTP verification, various encryption techniques, machine learning anomaly detection, point-in-time recovery, and data analytics and insights are continuous improvement areas.

Fractionation and Replication of Files

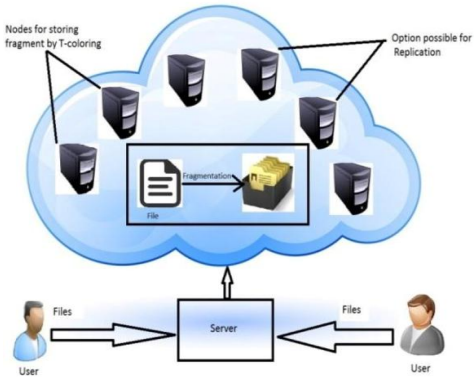
This project relies on the File Division Technique to improve security and resilience. Initial data fragmentation breaks files into useless pieces. Data redundancy and equitable distribution are achieved by replicating these fragments and their information across various cloud nodes. Load balancing prevents node overloads to improve system performance.

Fragment-Level AES Encryption

AES encryption, a safe method, protects data fragments after fragmentation and duplication. This dual-layered protection assures that attackers cannot decipher fragmented data without the encryption key. Protecting encryption keys and managing access requires a secure key management system.

Controller and Authorization Model

Access management and authorization are crucial to data security. A user management interface lets data owners manage accounts and determine rights. Data owners can control their data by specifying who can access, read, and alter data components using authorization rules.



IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
Impact Factor: 7.301
Volume 3, Issue 1, November 2023

PRE Secure Data Sharing: Proxy Re-Encryption

Proxy Re-Encryption (PRE) allows secure data sharing without providing encryption keys. If a user's authorization is removed, PRE can revoke keys to prevent unauthorized access. Authorized users decrypt re-encrypted data with their private keys to restrict access.

Performance and Scalability Optimization

Performance optimization and security are prioritized. Parallelism fetches pieces from numerous nodes simultaneously, speeding up data retrieval. Since strong encryption and access controls do not slow data access, latency is low. Scalability is achieved by optimizing resource allocation and load balancing for growing data and users. Data backup and redundancy provide data availability even if hardware fails or unexpected events occur. User-friendly interfaces improve user experience.

Audit and compliance

The system includes regulatory compliance and audit logs for data access and change transparency and accountability. This ensures system compliance and records system actions.

III. FUTURE SCOPE

The approach takes into account the fact that technological advances are always being made, yet it still allows for the possibility of further development. Potential areas for improvement include the implementation of Mobile One-Time Password (OTP) verification for stronger user authentication, the incorporation of diverse encryption algorithms to provide users with more security options, machine learning for anomaly detection to identify and mitigate unusual access patterns or threats, point-in-time recovery, and granular data restoration to offer users greater control in the event of data loss or inadvertent changes. Data analytics and insights can also be exploited to give users with a better understanding of data usage, access patterns, and security issues, which contributes to the continual improvement of the system.

IV. RESULT

In the swiftly evolving landscape of cloud computing, ensuring the security and performance of data stored in the cloud has become an absolute necessity. The transition to cloud-based solutions has ushered in a new era of accessibility and scalability, but with it comes a greater risk of data breaches and unauthorized access. This project was tasked with developing a comprehensive system that incorporates the File Division Technique, encryption, and access control mechanisms to improve data security and system performance. The project's outcomes demonstrate a productive strategy for attaining these objectives.

Improving Security for Data

The primary objective of our project was to substantially enhance the security of cloud-based data storage. To achieve this, we implemented a multifaceted strategy that included file fragmentation, advanced encryption, access control, and Proxy Re-Encryption (PRE). These measures collectively strengthened the data's security, rendering it immune to unauthorized access and data intrusions.

File Replication and Fragmentation:

Our security strategy relies heavily on file fragmentation. We have effectively implemented a technique that divides files into smaller, nonsensical fragments and distributes them across multiple nodes in the cloud infrastructure. This fragmentation strategy ensures that even in the event of a successful attack, the perpetrator can only access a subset of the data, rendering it practically useless. This approach profoundly redefines the security landscape by reducing the risk associated with data breaches. Due to the effective compartmentalization of the data, a successful breach does not yield any useful information.

IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
Impact Factor: 7.301
Volume 3, Issue 1, November 2023

Standard for Enhanced Security (AES):
The Advanced Encryption Standard (AES) was incorporated into our endeavor to improve data security. AES is a widely-recognized and highly-respected encryption algorithm with a reputation for its robust security features. By encrypting the data at the fragment level using AES, we ensure that even if an attacker obtains access to a fragment, the data contained within it will remain unreadable without the decryption key. This dual-layer strategy of data fragmentation and encryption bolsters data security to a remarkable degree.

Authorization and Access Control:
In addition to encryption and fragmentation, our initiative included an extensive access control model. This model permits data owners to define specific authorization criteria that determine who has access to their data. This granular control ensures that only authorized users can decrypt the data and access it. Owners of data retain complete control over their data, designating who has access rights and under what conditions. This access control model not only improves security, but also provides data proprietors with a sense of ownership and control over their data.

Re-Encryption by a proxy (PRE):
Proxy Re-Encryption (PRE) is an integral part of our approach to data security. PRE allows for the secure sharing of data without divulging encryption keys. Using PRE, the data proprietor retains control over the data, while authorized users receive re-encrypted data that can be decrypted using their own private keys. This mechanism eliminates the danger of encryption keys being exposed to potential attackers. It ensures that data remains secure and only accessible to the intended recipients, without any intermediaries compromising security.

Optimizing Data Security Without Affecting Performance
The potential impact on system performance is a prevalent concern when enhancing data security in cloud computing. It is feared that robust security measures may induce latency or other performance issues. The results of our initiative demonstrate, however, that this is not the case. By strategically implementing security measures and optimizing our system, we have achieved the delicate equilibrium between improved system security and performance.

Evaluating Performance:
Throughout the duration of the project, rigorous evaluations were conducted to assess the system's performance and security. Our approach to security enhancements did not compromise system performance, as demonstrated by the results, which were very encouraging. The principal conclusions from our performance evaluation are as follows:
The data retrieval procedure was not hindered by the fragmentation of the data. In fact, parallelism allowed fragments to be retrieved simultaneously from multiple nodes, resulting in a reduction in data retrieval time and a consequent increase in data access speed.

- Low Latency: Our data security strategy did not introduce a significant amount of latency. Encryption and access control mechanisms were in existence, but they did not significantly slow down data access.
- Scalability: The system demonstrated scalability by being able to accommodate a growing volume of data and users without experiencing a significant performance decrease. This scalability was accomplished through optimization of resource allocation and load balancing strategies.
- Redundancy and Backup: The implementation of redundancy and backup strategies by the system ensured data availability even in the event of hardware failures or unanticipated disruptions. This redundancy improved the robustness and dependability of data.
- User-Friendly Interface: An improved user interface not only enhanced the user experience, but also facilitated a seamless interaction with the security and performance-enhancing features of the system.
- Compliance and Audit: The system was created to meet compliance requirements and audit standards. It included features for compliance monitoring and audit traces, ensuring transparency and accountability for data access and modifications.

IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
Impact Factor: 7.301
Volume 3, Issue 1, November 2023

V. CONCLUSION

In conclusion, the results of our research plainly demonstrate that by combining the File Division Technique, advanced encryption, access control, and Proxy Re-Encryption, cloud security can be significantly improved without sacrificing system performance. Along with a user-friendly interface, compliance measures, and the potential for future enhancements, the successful implementation of these strategies provides a solid foundation for addressing the security and performance challenges of cloud computing in today's dynamic technological environment

REFERENCES

[1]. K. Bilal, S. U. Khan, L. Zhang, H. Li, K. Hayat, S. A. Madani,N. Min-Allah, L. Wang, D. Chen, M. Iqbal, C. Z. Xu, and A. Y.Zomaya, "Quantitative comparisons of the state of the art datacentre architectures," Concurrency and Computation: Practice and Experience, Vol. 25, No. 12, 2013, pp.1771-1783.

[2]. K. Bilal, M. Manzano, S. U. Khan, E. Calle, K. Li, and A.Zomaya, "On the characterization of the structural robustness of data center networks," IEEE Transactions on Cloud Computing,Vol.1, No. 1, 2013, pp.64-77.

[3]. D. Boru, D. Kliazovich, F. Granelli, P. Bouvry, and A. Y. Zomaya,"Energy-efficient data replication in cloud computing datacenters," In IEEE Globecom Workshops, 2013, pp.446-451.

[4]. Y. Deswarte, L. Blain, and J-C. Fabre, "Intrusion tolerance in distributed computing systems," In Proceedings of IEEE Computer Society Symposium on Research in Security and Privacy, Oakland CA, pp. 110-121,1991.

[5]. B. Grobauer, T.Walloschek, and E. Stocker, "Understanding cloud computing vulnerabilities," IEEE Security and Privacy, Vol.9, No. 2, 2011, pp.50-57.

[6]. W. K. Hale, "Frequency assignment: Theory and applications, "Proceedings of the IEEE, Vol. 68, No. 12, 1980, pp.1497-1514.

[7]. K. Hashizume, D. G. Rosado, E. Fernndez-Medina, and E. B.Fernandez, "An analysis of security issues for cloud computing," Journal of Internet Services and Applications, Vol. 4, No. 1,2013, pp.1-13.

[8]. K.Bilal,M.Manzano,S.U.Khan,E.Calle,K.Li,andA.Zomaya"OnDROPSmethodology" ," IEEE Transactions on Cloud Computing,