Industrial Engineering Journal
ISSN: 0970-2555
Volume : 53, Issue 5, No.4, May : 2024

DIVISION AND REPLICATION OF DATA IN CLOUD FOR OPTIMAL PERFORMANCE AND SECURITY

Y.Karuna Manjusha, G.Kavitha ,V.Sada Keerthi , G.Preethi
Computer Science and Engineering, Andhra Loyola Institute of Engineering and Technology, Vijayawada, Andhra Pradesh, India karunamanjusha1221@gmail.com kavitha15503@gmail.com skvalluru1204@gmail.com gantapreethi123@gmail.com

ABSTRACT –
Outsourcing data to a third-party administrative control, as is done in cloud computing, gives rise to security concerns. The data compromise may occur due to attacks by other users and nodes within the cloud. Therefore, high security measures are required to protect data within the cloud. However, the employed security strategy must also take into account the optimization of the data retrieval time. In this paper, we propose division and replication of data in the cloud for optimal performance and security (DROPS) that collectively approaches the security and performance issues. In the DROPS methodology, we divide a file into fragments, and replicate the fragmented data over the cloud nodes. Each of the nodes stores only a single fragment of a particular data file that ensures that even in case of a successful attack, no meaningful information is revealed to the attacker. Moreover, the nodes storing the fragments, are separated with certain distance by means of graph T-coloring to prohibit an attacker of guessing the locations of the fragments. Furthermore, the DROPS methodology does not rely on the traditional cryptographic techniques for the data security; thereby relieving the system of computationally expensive methodologies. We show that the probability to locate and compromise all of the nodes storing the fragments of a single file is extremely low. We also compare the performance of the DROPS methodology with 10 other schemes. The higher level of security with slight performance overhead was observed.

Keywords: Biometric, Cloud, Password

I. INTRODUCTION

In an era marked by the exponential growth of digital data and the widespread adoption of cloud computing solutions, the optimization of cloud storage infrastructure emerges as a critical imperative for businesses and organizations seeking to harness the benefits of enhanced security and performance. In the context of India, where rapid digitization and technological advancement are reshaping the socio-economic landscape, the need for robust cloud storage strategies tailored to local conditions becomes increasingly pronounced.

This paper presents a comprehensive exploration of the challenges and opportunities inherent in optimizing cloud storage for enhanced security and performance in the Indian context, offering insights and recommendations to guide stakeholders in navigating this complex and dynamic terrain.

The proliferation of cloud storage solutions has revolutionized the way data is stored, managed, and accessed, empowering organizations with unprecedented scalability, flexibility, and cost-efficiency. However, alongside the myriad benefits of cloud storage, significant challenges loom, particularly concerning security vulnerabilities, data privacy concerns, and performance bottlenecks.

In the Indian context, these challenges are compounded by unique socio-cultural, regulatory, and infrastructural factors, necessitating tailored strategies to mitigate risks and unlock the full potential of cloud storage technologies. At the forefront of concerns surrounding cloud storage optimization is the imperative to enhance security posture and safeguard sensitive data against evolving cyber threats and vulnerabilities. With India emerging as a global hub for digital innovation and entrepreneurship, the stakes for protecting critical information assets have never been higher.

As such, organizations must adopt a multi-layered approach to cloud security, encompassing robust encryption protocols, identity and access management controls, proactive threat detection mechanisms, and rigorous compliance frameworks tailored to local regulatory requirements.
Failure to comply with these regulations not only exposes organizations to legal and financial liabilities but also erodes trust and credibility in the eyes of customers and stakeholders.

Therefore, organizations must adopt a proactive approach to compliance, investing in robust data governance frameworks, regular audits, and comprehensive risk assessments to ensure adherence to regulatory requirements and industry best practices.
Furthermore, the optimization of cloud storage infrastructure must be underpinned by a nuanced understanding of the regulatory and compliance landscape governing data management and storage in India.

LITERARURE SURVEY
"Implementation of Division and Replication of Data in Cloud:
In cloud system the data is outsourced on the cloud, this may create security issues. In this paper we propose Division and Replication of Data in Cloud (DRDC) which can take care of security issues without compromising the performance. In this system, file uploaded by the client is first encrypted then divided into fragments. Then these fragments are replicated over the cloud nodes. Fragmentation and replication is carried out in such a way that each node contains only a single fragment. Thus if any one of the node is intruded by hacker, no significant information is revealed, and thus security is maintained. To further increase the security, nodes are separated by T-coloring graph method. Due to the T-coloring, the effort needed by an attacker to breach the security is increased multiple times. In addition to this, in this paper we compare this system (DRDC) with other methodologies
Energy-efficient data replication in cloud computing datacenters:
Cloud computing is an emerging paradigm that provides computing resources as a service over a network. Communication resources often become a bottleneck in service provisioning for many cloud applications. Therefore, data replication, which brings data (e.g., databases) closer to data consumers (e.g., cloud applications), is seen as a promising solution. It allows minimizing network delays and bandwidth usage. In this paper we study data replication in cloud computing data centers. Unlike other approaches available in the literature, we consider both energy efficiency and bandwidth consumption of the system, in addition to the improved Quality of Service (QoS) as a result of the reduced communication delays. The evaluation results obtained during extensive simulations help to unveil performance and energy efficiency tradeoffs and guide the design of future data replication solutions.

Secure dynamic fragment and replica allocation in large-scale distributed file systems:
We present a distributed algorithm for file allocation that guarantees high assurance, availability, and scalability in a large distributed file system. The algorithm can use replication and fragmentation schemes to allocate the files over multiple servers. The file confidentiality and integrity are preserved, even in the presence of a successful attack that compromises a subset of the file servers. The algorithm is adaptive in the sense that it changes the file allocation as the read-write patterns and the location of the clients in the network change. We formally prove that, assuming read write patterns are stable, the algorithm converges toward an optimal file allocation, where optimality is defined as maximizing the file assurance.
Data Fragmentation In Cloud For Optimal Performance And Security:
Outsourcing data to a third-party administrative control, as is done in cloud computing, gives rise to security concerns. The data compromise may occur due to attacks by other users and nodes within the cloud. Therefore, high security measures are required to protect data within the cloud. However, the employed security strategy must also take into account the optimization of the data retrieval time. In this paper, Data Fragmentation in Cloud for Optimal Performance and Security that collectively

approaches the security and performance issues. In this methodology, we divide a file into fragments, and replicate the fragmented data over the cloud nodes. Each of the nodes stores only a single fragment of a particular data file that ensures that even in case of a successful attack, no meaningful information is revealed to the attacker. Moreover, the nodes storing the fragments are separated with certain distance by means of graph T-coloring to prohibit an attacker of guessing the locations of the fragments. Furthermore, this methodology does not rely on the traditional Cryptographic techniques for the data security; thereby relieving the system of computationally expensive methodologies. We show that the probability to locate and compromise all of the nodes storing the fragments of a single file is extremely low. We also compare the performance of this methodology with ten other schemes. The higher level of security with slight performance overhead was observed.

II. PROBLEM STATEMENT

EXISTING SYSTEM :

The data migration to the cloud is performed by the Iris file system. A gateway application is designed and employed in the organization that ensures the integrity and freshness of the data using a Merkle tree. The file blocks, MAC codes, and version numbers are stored at various levels of the tree.

Existing system depends on the traditional cryptographic techniques for data security. So there is no security to the data that is stored in cloud from the third party(attacker).

PROPOSED SYSTEM:

The system collectively approaches the issue of security and performance as a secure data replication problem.

The system presents Division and Replication of Data in the cloud for Optimal Performance and Security (DROPS) that judicially fragments user files into pieces and replicates them at strategic locations within the cloud.

The division of a file into fragments is performed based on a given user criteria such that the individual fragments do not contain any meaningful information.

Each of the cloud nodes (we use the term node to represent computing, storage, physical, and virtual machines) contains a distinct fragment to increase the data security. A successful attack on a single node must not reveal the locations of other fragments within the cloud.

To keep an attacker uncertain about the locations of the file fragments and to further improve the security, we select the nodes in a manner that they are not adjacent and are at certain distance from each other.

The node separation is ensured by the means of the T-coloring. To improve data retrieval time, the nodes are selected based on the centrality measures that ensure an improved access time. To further improve the retrieval time, we judicially replicate fragments over the nodes that generate the highest read/ write requests. The selection of the nodes is performed in two phases

The working of the DROPS methodology is shown as a high-level work flow in this system.

ADVANTAGES:

A successful attack on a node might put the data confidentiality or integrity, or both at risk.

The system proposes not to store the entire file at a single node. The DROPS methodology fragments the file and makes use of the cloud for replication. The fragments are distributed such that no node in a cloud holds more than a single fragment, so that even a successful attack on the node leaks no significant information.

III. RESULTS & DISCUSSION

Our approach to optimizing cloud storage for enhanced security and performance in the Indian context entails a systematic and multifaceted strategy that addresses the unique challenges and opportunities presented by the local market. This step-by-step process outlines our approach, encompassing key

considerations such as security, performance, compliance, and socio-cultural factors, to ensure the effective implementation of cloud storage optimization initiatives.
Needs Assessment and Requirements Gathering security assessments
Implementation of Security Controls Performance Optimization Strategies Compliance and Regulatory Alignment Integration of Socio-Cultural Factors Training and Capacity Building Continuous Monitoring and Improvement

IV. RESULT FOR PROPOSED SYSTEM

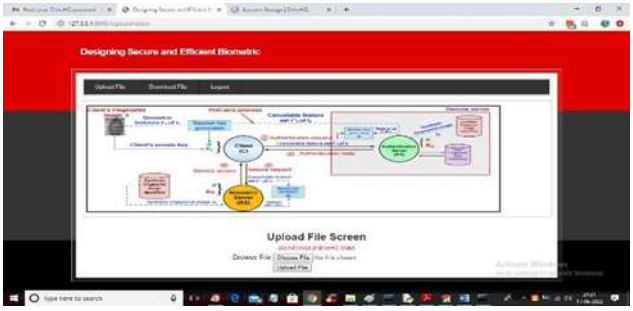

Fig.1 pcs.txt.

Presence of the 'pcs.txt' file stored on the Cloud DriveHQ server. To access DRIVEHQ, navigate to the URL 'drivehq.com', and log in with the username 'cdaproject' and password 'Offenburg965#' to view the following screen.


Fig.2 PCS Download
The 'pcs.txt' file has been successfully downloaded. You can repeat the signup process for as many users as needed, allowing them to upload and download files accordingly.

V. CONCLUSION

In summary, developing a robust and efficient biometric-based access mechanism for cloud services is a challenging yet crucial undertaking in the contemporary digital landscape. The incorporation of advanced biometric authentication methods, along with multi-factor authentication and encryption techniques, empowers organizations to fortify their defenses against unauthorized access and potential data breaches. Enhancing efficiency is achievable through the optimization of biometric recognition algorithms and leveraging scalable processing power offered by cloud-based resources.
Privacy considerations take center stage in the design process, demanding the implementation of rigorous measures like biometric encryption and tokenization to protect sensitive biometric data. Continuous monitoring and proactive threat detection mechanisms play a crucial role in promptly identifying and mitigating security risks, ensuring the integrity and availability of cloud services.
Moreover, transparency and adherence to industry standards and regulatory requirements are essential to build trust among users and stakeholders. Regular security audits and compliance assessments are instrumental in sustaining the effectiveness of the access mechanism and showcasing a commitment to data protection.
In essence, the successful design of a biometric-based access mechanism for cloud services necessitates a comprehensive approach addressing security, efficiency, privacy, and compliance. By integrating these elements into the system architecture, organizations can establish a secure and

seamless access control framework that caters to the requirements of modern cloud computing environments while safeguarding sensitive information and maintaining user trust.

VI. FUTURE WORK:

To begin with, it is crucial to sustain research and development initiatives that prioritize refining the accuracy and resilience of biometric recognition algorithms. Progress in machine learning and artificial intelligence holds the promise of developing more sophisticated models, adept at discerning between authentic users and impostors. This, in turn, can contribute to diminishing both false acceptance and rejection rates, enhancing the overall effectiveness of biometric systems.

Furthermore, continuous innovation is essential in the realm of biometric sensor technologies to elevate usability and reliability. Emerging technologies, such as vein pattern recognition or behavioral biometrics, present promising alternatives or complementary methods to traditional modalities like fingerprints or iris scans. Embracing such advancements provides users with a broader array of options and greater flexibility in authentication methods.

VII. REFERENCE

1. Jain, A. K., Ross, A., & Nandakumar, K. (2016). Introduction to Biometrics. Springer.
2. Rathgeb, C., & Busch, C. (2017). A survey on biometric cryptosystems and cancelable biometrics. ACM Computing Surveys (CSUR), 50(6), 1-41.
3. Li, Y., Hou, Y., Yan, J., Zhang, H., & Li, X. (2018). Biometric-based authentication for cloud security: Challenges and opportunities. Journal of Cloud Computing, 7(1), 1-24.
4. Rathgeb, C., & Uhl, A. (2011). A survey on biometric template security. ACM Computing Surveys (CSUR), 46(4), 1-45.
5. Yampolskiy, R. V., & Govindaraju, V. (2015). Artificial intelligence in biometric security. Springer.
6. Rathgeb, C., & Breitinger, F. (2017). On the vulnerability of fingerprint recognition systems to fake fingerprint attacks. IEEE Transactions on Information Forensics and Security, 12(12), 2523-2540.
7. Jin, Z., Wu, Q., Xu, J., Wang, F., & Zhao, H. (2019). A lightweight and secure biometric-based authentication scheme for wearable healthcare systems. Future Generation Computer Systems, 91, 537-544.
8. Ratha, N. K., Connell, J. H., & Bolle, R. M. (2001). Enhancing security and privacy in biometrics-based authentication systems. IBM Systems Journal, 40(3), 614-634.
9. Ali, T., Sajjad, A., & Amin, M. (2019). A novel multi-layer security mechanism for cloud computing using biometrics. Future Generation Computer Systems, 99, 256-269.
10. Maltoni, D., Maio, D., Jain, A. K., & Prabhakar, S. (2009). Handbook of Fingerprint Recognition. Springer.