Abstract

With the increasing reliance on cloud computing for data storage and processing, ensuring the security and privacy of sensitive data has become a critical concern. Traditional cloud storage models pose significant risks, such as unauthorized access, data breaches, and data loss. To address these issues, this paper proposes a novel cloud secure storage mechanism that combines **data dispersion** and **encryption** techniques.

Data dispersion involves splitting the data into multiple fragments and distributing them across different storage locations or cloud servers. This technique reduces the risk of data loss or unauthorized access, as even if one server is compromised, the complete data remains unrecoverable. Each fragment is then encrypted using advanced cryptographic algorithms to further protect it from unauthorized access during transmission and storage. By leveraging both data dispersion and encryption, the proposed mechanism ensures high levels of confidentiality, availability, and resilience.

This approach not only enhances data security but also improves data redundancy and fault tolerance, making it an ideal solution for storing sensitive data in multi-cloud environments. The paper also explores the trade-offs between storage efficiency, encryption overhead, and data retrieval performance, providing a comprehensive analysis of the proposed mechanism's effectiveness and scalability. Through extensive simulations and case studies, we demonstrate the practical viability of the proposed solution in real-world cloud infrastructures.

The findings highlight the potential of this hybrid approach to significantly reduce the risks associated with cloud storage while maintaining data accessibility and integrity, ultimately advancing the state of secure cloud storage mechanisms.