**ABSTRACT**

The rapid adoption of cloud storage services necessitates robust mechanisms for ensuring data privacy and security. This project presents a comprehensive three-layer intelligent data privacy protection scheme tailored for cloud storage, implemented using Java for backend processes, and JSP, HTML, CSS, and JavaScript for the frontend interface. The database management is handled using MySQL, ensuring efficient data storage and retrieval.

Our system leverages the DriveHQ Cloud service provider for cloud storage solutions. It introduces a controlled user registration process where new users can only access the system upon administrative approval, enhancing security by preventing unauthorized access. Once registered, users can upload files to the cloud, where the system employs a multi-faceted approach to data protection.

Uploaded files are partitioned into three distinct blocks, each encrypted using the Caesar Cipher algorithm. This classical encryption method, despite its simplicity, provides a foundational layer of security. Additionally, our system incorporates a deduplication feature that identifies and manages redundant data uploads, thereby optimizing storage efficiency.

To ensure secure access and retrieval, a unique Message Authentication Code (MAC) is generated for each of the three blocks of data. This MAC Code is essential for the decryption process, ensuring that only authorized users can reconstruct and access the original files. The combination of data splitting, encryption, and MAC-based authentication forms a robust framework for maintaining data confidentiality and integrity in cloud environments.

This project demonstrates a practical approach to enhancing data privacy in cloud storage systems, offering a scalable and secure solution for both individual users and organizations.