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: 7.53
Volume 4, Issue 1, June 2024

Secure Storage on Cloud using Hybrid Cryptography

Debarpita Dutta
Student, School of Computing Science and Engineering
Department of Cloud Computing and Automation
Vellore Institute of Technology, Bhopal, India

Abstract: *The Evolving Landscape of Cloud Storage Security: A Focus on Hybrid Cryptography Techniques*

Data security and privacy have become paramount concerns for small and medium-sized businesses (SMBs) contemplating the migration of their data from on-premises storage to cloud-based solutions. This apprehension stems from the perceived lack of control over data stored with cloud service providers (CSPs). The concern lies in the potential for unfettered access by CSPs to a client's sensitive information. Additionally, there is a prevailing sentiment that current safeguards are inadequate in preventing unauthorized access and data modification within cloud infrastructures. While some CSPs have implemented symmetric and asymmetric cryptographic techniques to bolster security, this paper delves deeper into the realm of emerging hybrid cryptography techniques, specifically in the context of cloud storage security.

Case Study: Secure Storage Web Application

This section details the "Secure Storage" web application, designed to provide users with a secure platform for file management and storage. Developed using Python and the Flask framework, the application prioritizes user privacy by encrypting uploaded files with the Advanced Encryption Standard (AES) algorithm before persisting them on the server. User authentication is meticulously handled, with passwords stored as irreversible hashes within a SQLite database, mitigating the risk of password exposure in the event of a security breach.

Upon registering, users are granted the ability to upload files, which are subsequently encrypted using AES with a pre-defined key. These encrypted files are then stored within a designated directory on the server. Users can download their encrypted files at any time, with on-the-fly decryption occurring during the download process. The application demonstrably prioritizes user privacy and data security by leveraging industry-standard encryption practices and robust user authentication mechanisms. Additionally, it offers an intuitive interface that facilitates the secure storage and retrieval of files.

Keywords: Security Concepts: Cloud Storage Security, Encryption, Cryptography (Hybrid techniques), User Authentication, Data Management: Data Privacy, File Storage & Retrieval, Technical Specifications: AES (Advanced Encryption Standard), SQLite Database, Development Tools: Python (programming language), Flask (web framework), Other: SMBs (Small and Medium-sized Businesses), CSPs (Cloud Service Providers)