

Voultify: A File Storage Solution

Ayushman Tripathi, Ujjawal Sharma, Ayush Chaudhary

CSE Department of Mahatma Gandhi Mission's College Of Engineering & Technology, Noida

Guide

Mr. Abhishek Chaudhary

Abstract—

Voultify is a secure cloud-based file storage system designed using hybrid cryptography, distributed object storage, and zero-knowledge principles. This paper presents the architecture, methodology, and performance evaluation of Voultify. Experimental results demonstrate efficient encryption overhead, low-latency file operations, and strong access control accuracy. Voultify provides a scalable, privacy-enhanced alternative to centralized cloud storage platforms.

1. Introduction

Rapid digitalization has increased the demand for secure, scalable, and reliable cloud-based storage systems. Existing platforms suffer from privacy concerns, centralized architectures, and provider-controlled encryption keys. Voultify addresses these issues using distributed storage and hybrid cryptography.

2. Related Work

Previous studies on distributed file systems such as GFS and HDFS highlight scalable storage and fault tolerance. Cloud platforms like Google Drive and Dropbox provide convenience but lack complete end-to-end encryption. Hybrid cryptography research suggests combining AES and RSA for optimal security and performance.

3. Problem Identification

Current cloud storage solutions expose metadata, lack user-controlled key management, create redundancy, and suffer from central server dependency. These issues motivate the design of a more secure and privacy-focused system.

4. Proposed System

Voultify is designed as a zero-knowledge, distributed cloud platform. AES-256 encrypts file data while RSA-2048 secures keys. Additional features include version control, activity logs, permission-controlled sharing, and deduplication.

4.1 System Architecture

The system uses microservices including Authentication, File Operations, Encryption Service, Storage Orchestrator, and Audit Logging. Data flows from client to API gateway, encryption layer, storage cluster, and metadata database.

5. Methodology

The system was developed using React.js, Node.js, MongoDB/PostgreSQL, and MinIO. Security relies on TLS, JWT, and OpenSSL. Containerization uses Docker, and deployment uses Kubernetes for scalability.

6. Results

Performance tests show average upload time of 1.4 seconds, download time of 2.1 seconds, encryption overhead less than 0.5 seconds, and 100% decryption accuracy. Access control tests confirmed successful prevention of unauthorized access.

7. Discussion

Results validate that Voultify improves privacy, reliability, and efficiency over traditional cloud platforms. Distributed storage ensures fault tolerance, and hybrid cryptography enforces strong user data confidentiality.

8. Conclusion

Voultify provides a secure, scalable, and user-friendly cloud storage solution. The system meets all major objectives including distributed storage, encryption, version control, and permission-based sharing.

9. Future Work

Potential improvements include blockchain-based integrity proofs, AI-powered file classification, desktop synchronization, real-time collaboration, and multi-cloud redundancy.

References

- [1] J. Dean and S. Ghemawat, 'The Google File System,' ACM SOSP, 2004.
- [2] K. Shvachko et al., 'The Hadoop Distributed File System,' IEEE MSST, 2010.
- [3] R. Rivest et al., 'A Method for Obtaining Digital Signatures and Public-Key Cryptosystems,' Communications of the ACM, 1978.
- [4] J. Daemen and V. Rijmen, 'The Design of Rijndael: AES,' Springer, 2002.
- [5] NIST, 'The NIST Definition of Cloud Computing,' 2011.
- [6] Amazon Web Services, 'Amazon S3 Documentation,' 2023.