CloudVault

Group Members :
1. Harshal Gavali - 2003040
2. Adharva Kumar - 2003042
3. Gourav Powar - 2003044
4. Rohan Chinchkar - 2003046

Contents

Introduction and Motivation

Cloud storage is a popular solution for businesses and individuals as it offers easy and secure storage, access, and management of data.Cloud storage is scalable, cost-effective, and accessible from anywhere with an internet connection.

Storing data remotely poses several security risks that need to be addressed with enhanced security measures.The purpose of this project is to develop a free cloud storage platform that provides robust security measures to safeguard user data.The platform will be developed using Java, Spring Framework, Spring Boot, REST API, Apache Tomcat Server, MySQL, and AWS.

Literature Survey

- Data Security and Privacy Protection for Cloud Storage
- Key Aggregate Cryptosystem for Scalable Data Sharing in Cloud Storage
- Achieving Secure Role based Access Control on Encrypted Data in Cloud Storage
- A Cost effective Dynamic Replication Management Scheme for Cloud Storage Cluster
- Privacy Preserving Public Auditing for Secure Cloud Storage
- Combining Data Owner Side and Cloud-Side Access Control for Encrypted Cloud Storage
- Enabling Cloud Storage Auditing with Key Exposure Resistance
- Dual server public key encryptio n with keyword Search for secure cloud storage

Problem Statement

Develop a high storage cloud platform that provides enhanced security measures to protect user data while maintaining the confidentiality, integrity, and availability of their data.

Objectives

- Develop a high storage cloud architecture.
- Implement effective authentication mechanisms.
- Implement robust data encryption techniques to protect user data both in transit and at rest.
- Ensure the confidentiality,integrity, and availability of user data.

Scope

- The scope of this project includes developing a cloud storage platform using Java, Spring Framework, Spring Boot, REST API, Apache Tomcat Server, MySQL, and AWS.
- The platform will be designed to store data and provide users with easy access to their data.
- The platform will also include enhanced security measures, such as data encryption, access control mechanisms, and authentication mechanisms.

Limitations

- The project will not provide real-time monitoring and analysis of security events, leaving the system vulnerable to cyber-attacks that can go undetected.
- The project will not incorporate advanced threat intelligence capabilities, which are necessary to proactively identify and mitigate potential security threats.
- The project will not include redundancy and failover mechanisms to ensure business continuity in case of hardware or software failures.
- The project will not provide scalability features, which may lead to performance issues and data loss when the system is under heavy loads.

Proposed Methodology

- Define cloud architecture requirements and specifications, storage capacity, expected volume of user data, and scalability of the system.
- Choose a cloud service provider, set up necessary infrastructure components, and deploy using Java, Spring Framework, and Spring Boot for scalability.
- Implement user authentication, access controls, SSL/TLS encryption, two-factor authentication, and AES/RSA encryption for data protection.
- Implement encryption key management, secure protocols, data masking, backup and disaster recovery procedures, automated security testing, and monitoring.
- Establish security policies and procedures for user awareness and best practices for securing data.

Time Frame of Schedule

The development of the cloud storage and cloud security project will take approximately six months. The following is a tentative schedule for the project:

Month 1: Planning phase
Month 2: Designing phase
Month 3-4: Developing phase
Month 5: Testing phase
Month 6: Deployment and maintenance

References & Bibliography

1.Yang, Pan, Naixue Xiong, and Jingli Ren. "Data security and privacy protection for cloud stor age: A survey." IEEE Access 8 (2020): 131723-131740.

2. Chu, Cheng-Kang, et al. "Key-aggregate cryptosystem for scalable data sharing in cloud stor age." IEEE transactions on parallel and distributed systems 25.2 (2013): 468-477.

3. Zhou, Lan, Vijay Varadharajan, and Michael Hitchens. "Achieving secure role-based access control on encrypted data in cloud storage." IEEE transactions on information forensics and se curity 8.12 (2013): 1947-1960.

4. Wei,Qingsong, et al. "CDRM: A cost-effective dynamic replication management scheme for cloud storage cluster." 2010 IEEE international conference on cluster computing. IEEE, 2010.

5. Wang,Cong, et al. "Privacy-preserving public auditing for secure cloud storage." IEEE trans actions on computers 62.2 (2011): 362-375.

“ Thank You ”