Cloud-Based Storage System Security Measures

Overview

This document provides a comprehensive overview of the security measures implemented in the cloud-based storage system. The system is designed to ensure robust protection for data at rest, during transmission, and in terms of user authentication and access controls.

File Encryption Techniques

Data at Rest

Data at rest is secured using industry-standard AES-256 encryption. AWS S3, the chosen storage service, automatically encrypts each object before persisting it. This encryption mechanism guarantees the confidentiality and integrity of stored data, preventing unauthorized access.

Data in Transit

Secure data transmission is achieved through the use of HTTPS (Hypertext Transfer Protocol Secure) facilitated by the TLS (Transport Layer Security) protocol. All communication between clients and the server, as well as any communication between internal components, is encrypted to safeguard against eavesdropping and data tampering.

User Authentication Mechanisms

User authentication is a critical aspect of the security architecture. The system utilizes JSON Web Tokens (JWT) for secure user authentication. Here's an overview of the authentication process:

1. **User Requests Access:** When a user initiates an action that requires authentication, such as uploading or downloading a file, they include a JWT in the Authorization header.
2. **JWT Verification:** The server validates the JWT using a secure, secret key. This process ensures that the token is genuine and has not been tampered with.
3. **Authorization:** Once the user is successfully authenticated, the system performs authorization checks to determine whether the user has the necessary permissions for the requested action.

Access Controls

Access controls are implemented to govern user permissions and restrict unauthorized access to sensitive resources.

AWS Identity and Access Management (IAM)

AWS IAM is utilized for fine-grained access control to AWS resources. This includes controlling access to the S3 buckets where files are stored. IAM policies are configured to grant users the minimum necessary permissions based on their roles and responsibilities.

Custom Authorization Checks

While IAM handles the low-level access control to AWS resources, custom authorization checks are implemented at the application level. These checks provide an additional layer of control to ensure that users can only access files for which they have explicit permission.

Conclusion

The implemented security measures form a multi-layered defense strategy, encompassing encryption at rest and in transit, robust user authentication, and access controls. This approach ensures that the cloud-based storage system adheres to industry best practices and regulatory standards, providing a secure environment for storing and managing sensitive data.