CLOUD SECURITY

Log-in Authentication, File Encryption and Hiearchy

Alex Xiao Cai and Tien Dinh
axiaocai@uoregon.edu and tvd@uoregon.edu

UNIVERSITY OF OREGON

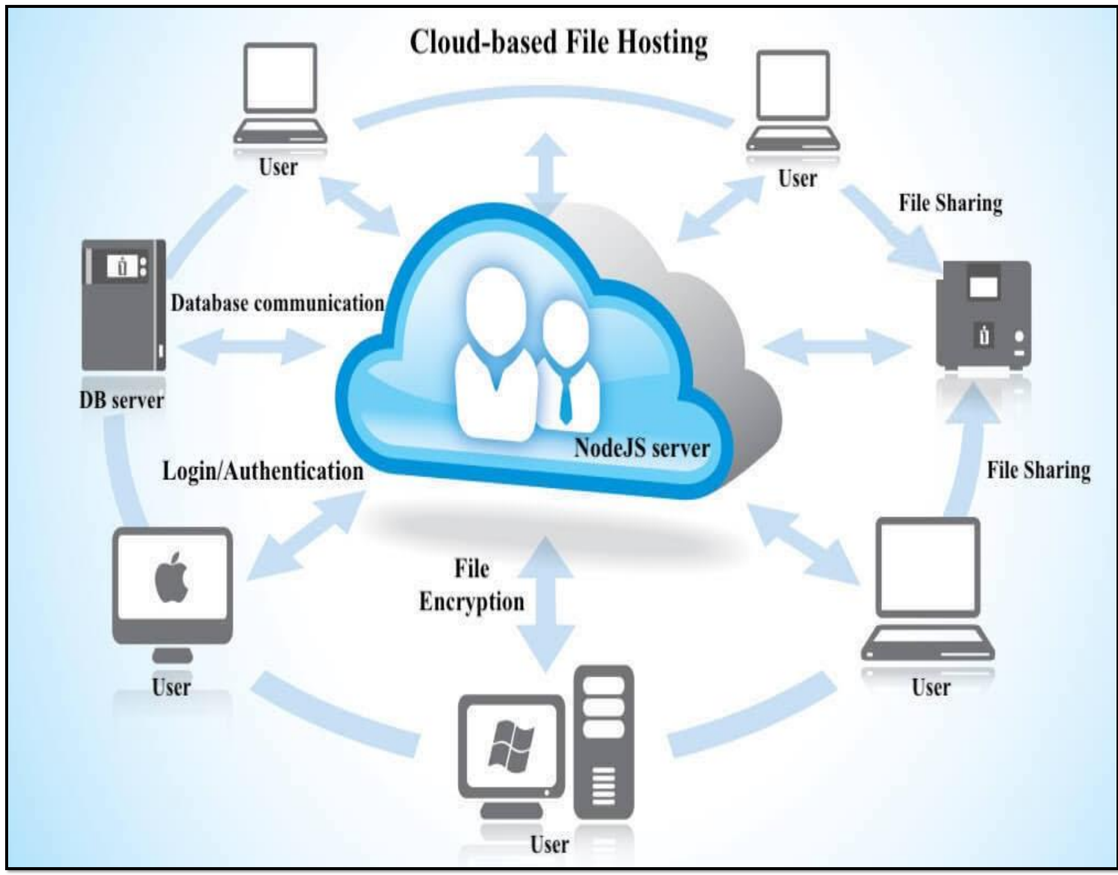
Problem

- **Problem**: Many companies and individuals opt to store applications and valuable information into a cloud as it provides several advantages such as cost savings, virtually unlimited storage capacity, accessibility, availability, etc. Cloud computing security is becoming one of the major concerns.
- **Solution**: A cloud-based file storage web application that authenticates users, allows encrypted file sharing/hosting and hierarchy-based access control

Approach

Objectives: Building a flexible and secure cloud-based file storage platform by:

- A log-in (Authentication) system is required to verify legitimate user.
- File (Encryption) using server and client's public and private key to ensure the confidentiality of the data.
- A file system hierarchy (Access Control) is implemented to ensure the availability to access the right content.



Implementation

- A file-hosting server using NodeJS back-end and React/EJS front-end.
- MongoDB that supports user's login authentication, data storage and encryption
- Implement "bcrypt" encryption package to protect user's password using hash function and salt value
- Implement "crypto" encryption package to protect user's data using public/private key pair
- File sharing is divided into public sharing (for anyone) and private sharing (group-based sharing and link-based sharing)