Secure File Upload System with Policy Enforcement

A secure file upload and processing system that enforces security and compliance policies using Open Policy Agent (OPA). This project demonstrates secure backend design, policy-as-code, and full-stack integration.

Key Features

1. Secure file upload API
2. Metadata extraction (filename, size, hash)
3. Policy enforcement using OPA
4. Accepted and rejected file separation
5. Admin visibility into file status
6. React-based dashboard

Architecture Overview

Files uploaded from the React frontend are processed by a FastAPI backend. Metadata is extracted and evaluated by OPA policies before files are stored in accepted or rejected directories. Admins can review file status via the UI.

Installation & Execution

1. Clone the repository and install backend dependencies using Python virtual environments.
2. Run the FastAPI backend using Uvicorn on port 8000.
3. Start Open Policy Agent (OPA) as a server on port 8181 with Rego policies loaded.
4. Install frontend dependencies and start the React development server on port 3000.

OPA Policy Example

Policies are written in Rego. Example rules restrict file size and disallow executable uploads. OPA evaluates metadata sent from the backend and returns allow or deny decisions.

Trade-offs & Design Decisions

1. OPA used as external service for centralized policy management
2. Local filesystem storage chosen for simplicity
3. Backend-enforced security prevents frontend bypass
4. In-memory metadata storage simplifies demo but limits persistence

License