EduLock – Secure Educational Content Distribution Platform

Technical Workflow and System Documentation

1. System Overview

EduLock is a secure educational content distribution platform designed to prevent unauthorized access, sharing, and piracy of digital academic materials. The system ensures that educational files are encrypted, access-controlled, and viewable only within a secure environment.

The platform uses strong encryption, role-based access control, secure authentication, and device binding to protect intellectual property and maintain controlled distribution of educational content.

2. System Architecture

EduLock follows a **three-tier architecture**:

2.1 Presentation Layer (Frontend)

- Built using React.js or similar frameworks.
- Provides teacher and student dashboards.
- Handles secure file viewing.
- Sends requests to backend APIs.
- Prevents unauthorized actions (copy, download, screen capture attempts).

Components:

- Login Interface
- Teacher Dashboard
- Student Dashboard
- Secure Content Viewer

2.2 Application Layer (Backend Server)

- Handles authentication and authorization.
- Processes file encryption and decryption.
- Manages classrooms and user roles.
- Verifies device binding and session validity.
- Communicates with database and cloud storage.

Modules:

- Authentication Service (JWT)
- File Encryption Service
- Access Control Manager
- Key Management Service (KMS)
- Activity Monitoring System

2.3 Data Layer (Storage & Database)

- Stores encrypted files.
- Maintains user data and classroom information.
- Stores access logs and activity records.

Storage Components:

- Cloud Storage (AWS S3 / Firebase)
- Database (MySQL / MongoDB)

3. Secure Content Distribution Workflow

The EduLock system follows a secure multi-step workflow to protect educational content.

3.1 Teacher Content Upload Process

1. Teacher logs into system using secure authentication.
2. Teacher uploads educational files (PDF, PPT, Video).
3. Backend validates file and user permissions.
4. File is encrypted using AES-256 encryption.
5. File is converted into proprietary .edulock format.
6. Encrypted file is stored in cloud storage.
7. File is mapped to classroom access permissions.

Outcome:

Only encrypted content exists in storage.

3.2 Student Content Access Process

1. Student logs in using institutional credentials.
2. System verifies identity using JWT authentication.
3. Student requests file access through secure viewer.
4. Server checks:
    - Classroom membership
    - Device registration
    - Active session
5. If authorized, system grants temporary access.

Outcome:

Only authorized users proceed to file viewing.

3.3 Secure File Viewing Process

1. Secure viewer fetches encrypted .edulock file.
2. Viewer requests temporary decryption key from KMS.
3. Server verifies access rights.
4. Server sends short-lived decryption key.
5. File is decrypted in memory (RAM only).
6. Content is rendered using secure viewer.
7. No decrypted file is stored on device.

Outcome:

Content remains protected even after access.

4. Security Mechanisms

EduLock integrates multiple security layers:

4.1 Encryption

- AES-256 encryption for file protection.
- RSA encryption for key exchange.

4.2 Authentication

- JWT-based secure login.
- Role-based access control (Teacher, Student).

4.3 Device Binding

- Content accessible only on registered devices.
- Prevents forwarding across systems.

4.4 Secure File Format

- Proprietary .edulock format.
- Prevents external file usage.

4.5 Secure Viewing Environment

- Right-click disable.
- Copy-paste restriction.
- Tab-switch detection.
- Screen capture protection.

4.6 Dynamic Watermarking

- Displays user identity on content.
- Prevents misuse.

4.7 Activity Logging

- Tracks suspicious actions.
- Records user behavior.

5. Key Management System (KMS)

The Key Management System controls encryption keys.

Functions:

- Generates encryption keys.
- Issues temporary decryption keys.
- Verifies user authorization.
- Revokes access when permissions change.

Features:

- Short-lived keys.
- Secure storage.
- Automatic key expiration.

6. Access Control Model

EduLock uses hierarchical access control.

Teacher → Classroom → Students

- Teachers manage classroom membership.
- Students access only assigned content.
- Permissions dynamically updated.

7. System Components

7.1 User Management System

- User registration and authentication.
- Role assignment.

7.2 Classroom Management

- Create classroom groups.
- Assign students.

7.3 File Processing Module

- File encryption.
- Format conversion.

7.4 Secure Viewer

- Displays protected content.
- Prevents external storage.

7.5 Monitoring System

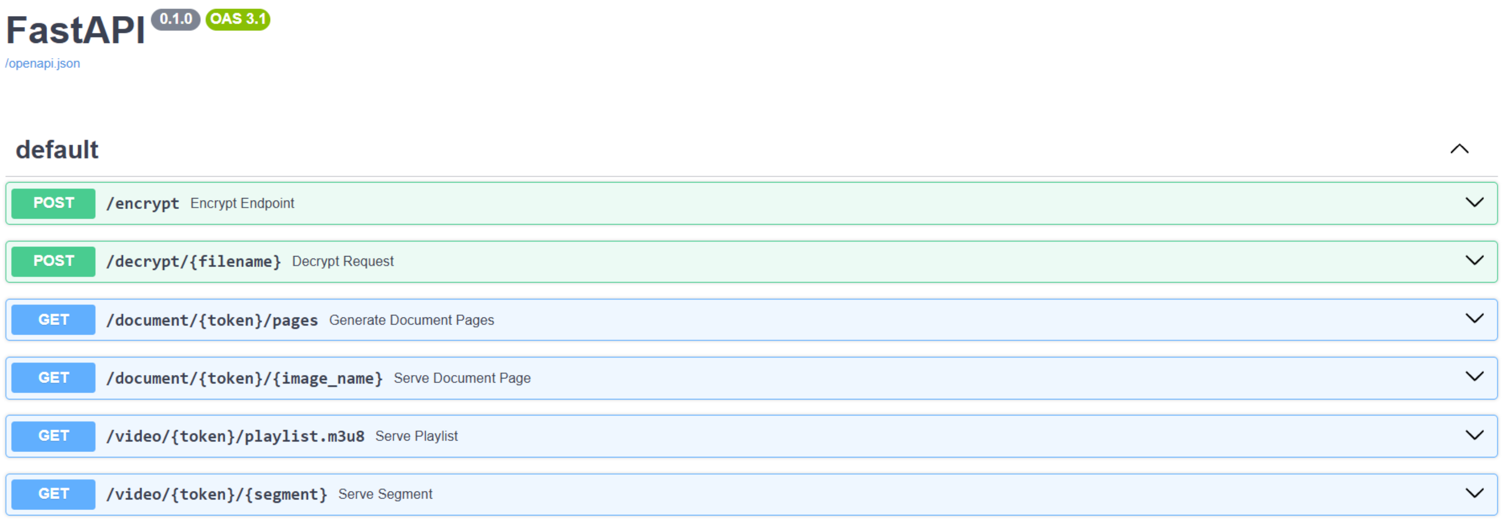
- Tracks usage and security violations.

8. Conclusion

EduLock provides a comprehensive solution for secure educational content distribution by integrating encryption, access control, and secure viewing technologies. The platform ensures content protection, controlled access, and improved digital learning security, making it highly suitable for modern educational institutions.

Screenshot of the prototype:

- **POST /encrypt**: An endpoint to upload or send data to be encrypted.
- **POST /decrypt/{filename}**: An endpoint to decrypt a specific file, likely identified by the filename parameter.
- **GET /document/{token}/pages**: This suggests a feature that processes a document (like a PDF) and splits it into pages, likely returning metadata or a list of page images. It uses a {token} for access or session identification.
- **GET /document/{token}/{image_name}**: This endpoint serves the actual image of a specific page from the document.
- **GET /video/{token}/playlist.m3u8**: This indicates the API supports **HLS (HTTP Live Streaming)**. The .m3u8 file is a playlist file used by video players to stream content.
- **GET /video/{token}/{segment}**: This serves the actual video data chunks (segments) referenced in the playlist file.



FastAPI 0.1.0 OAS 3.1

/openapi.json

default

POST `/encrypt` Encrypt Endpoint

POST `/decrypt/{filename}` Decrypt Request

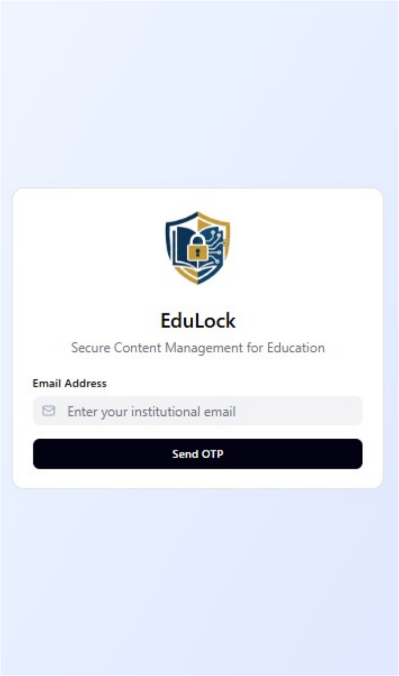
GET `/document/{token}/pages` Generate Document Pages

GET `/document/{token}/{image_name}` Serve Document Page

GET `/video/{token}/playlist.m3u8` Serve Playlist

GET `/video/{token}/{segment}` Serve Segment

EduLock – Secure Educational Content Distribution Platform



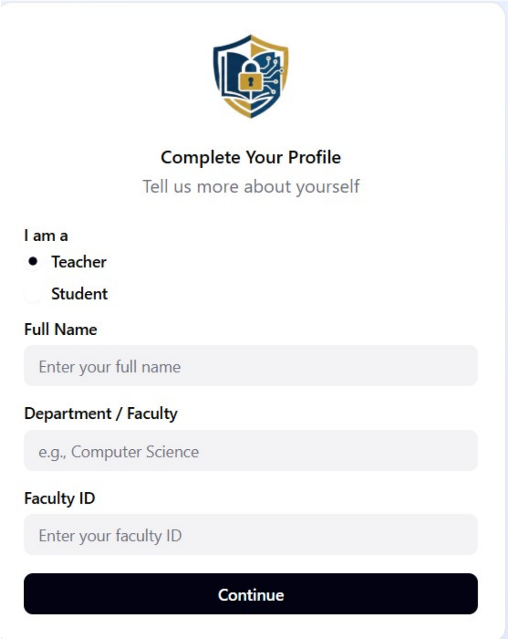
EduLock

Secure Content Management for Education

Email Address

Enter your institutional email

Send OTP



Complete Your Profile

Tell us more about yourself

I am a

● Teacher

○ Student

Full Name

Enter your full name

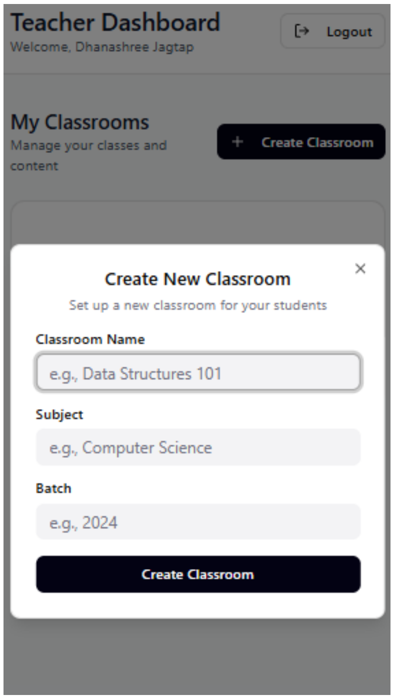
Department / Faculty

e.g., Computer Science

Faculty ID

Enter your faculty ID

Continue



Teacher Dashboard

Welcome, Dhanashree Jagtap

Logout

My Classrooms

Manage your classes and content

+ Create Classroom

Create New Classroom

Set up a new classroom for your students

Classroom Name

e.g., Data Structures 101

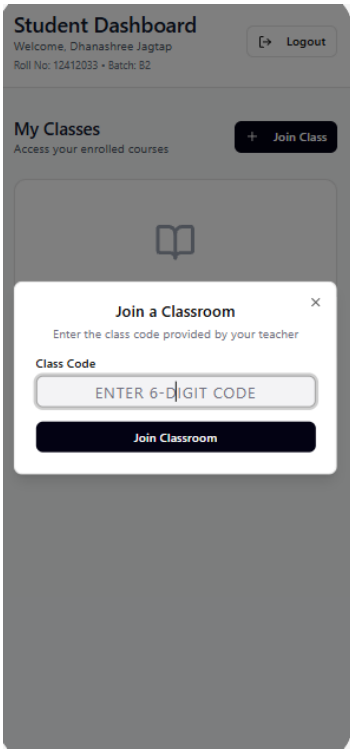
Subject

e.g., Computer Science

Batch

e.g., 2024

Create Classroom



Student Dashboard

Welcome, Dhanashree Jagtap

Roll No: 12412033 • Batch: B2

Logout

My Classes

Access your enrolled courses

+ Join Class

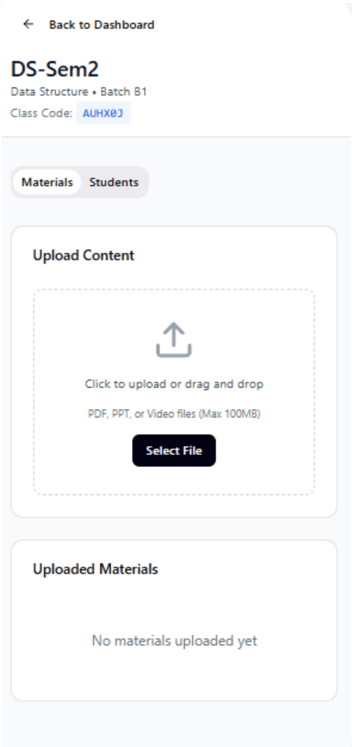
Join a Classroom

Enter the class code provided by your teacher

Class Code

ENTER 6-DIGIT CODE

Join Classroom



Back to Dashboard

DS-Sem2

Data Structure • Batch B1

Class Code: AUHX0J

Materials Students

Upload Content

Click to upload or drag and drop

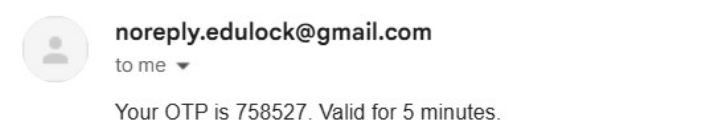
PDF, PPT, or Video files (Max 100MB)

Select File

Uploaded Materials

No materials uploaded yet

Verification Mail:



noreply.edulock@gmail.com

to me

Your OTP is 758527. Valid for 5 minutes.