TRƯỜNG ĐẠI HỌC QUỐC GIA TP – HỒ CHÍ MINH
ĐẠI HỌC KHOA HỌC TỰ NHIÊN

BÁO CÁO: THIẾT KẾ HỆ THỐNG

ĐỒ ÁN: ỨNG DỤNG WEB TRAO ĐỔI DỮ LIỆU ĐA PHƯƠNG TIỆN BẢO MẬT

GIẢNG VIÊN:	Nguyễn Đình Thúc	
	Nguyễn Văn Quang Huy	
	Ngô Đình Hy	
LỚP:	20CNTThuc	
SINH VIÊN:	Trần Quang Duy	20127015
	Hoàng Hữu Minh An	20127102
	Lê Nguyễn Minh Quang	20127295
	Trần Hoàng Minh Quang	20127299

Ho Chi Minh, 28-02-2024

Contents

I. Thông tin nhóm:

Họ và tên	Mã số sinh viên
Trần Quang Duy	20127015
Hoàng Hữu Minh An	20127102
Lê Nguyễn Minh Quang	20127295
Trần Hoàng Minh Quang	20127299

II. Mục tiêu:

Mục tiêu của đồ án là xây dựng website trao đổi tin nhắn có thực hiện chức năng đính kèm các thư mục (bao gồm yêu cầu bảo mật) như sau:

- Dựa trên ý tưởng gửi và nhận tin nhắn như các ứng dụng Messenger, Skype, Viber,... có yêu cầu bảo mật. Lịch sử tin nhắn trong Chatroom được lưu trữ tạm thời, và sau thời gian nhất định, dữ liệu sẽ tự động bị xóa và không thể khôi phục được (trừ trường hợp back-up).
- Cho phép người dùng trao đổi thông tin an toàn và riêng tư với người dùng khác thông qua một Chatroom cho cá nhân. Trong đó, thư mục sẽ được mã hóa và sử dụng chữ ký điện tử để xác thực người dùng.
- Public key được lưu trữ toàn cục trong khi Private key được lưu trữ cục bộ và các thư mục mã hóa và chữ kí điện tử được lưu trữ trên cloud. Tức nghĩa, với Private key chỉ người dùng nắm giữ, hệ thống không thể can thiệp hay khôi phục Private key nếu người dùng quên hoặc làm mất. Webiste sẽ chỉ quản lý thông tin cá nhân như Public key, username, password của các người dùng khi đã đăng ký thành công.

III. Yêu cầu:

Thực hiện được việc trao đổi thông tin (tin nhắn, file,…) trên website có bảo mật:

- Sau khi đăng ký thành công tài khoản, người dùng sẽ được cấp một cặp khóa Public key và Private key. Đối với Private key, người dùng phải tự lưu trữ và bảo vệ khóa cá nhân của mình. Hệ thống không thể can thiệp, hay khôi phục.
- Trong ứng dụng này, người dùng đóng hai vai trò gửi và nhận thông điệp có kèm chức năng mã hóa và giải mã, tùy thuộc vào mục đích sử dụng.
- Người gửi và người nhận tham gia Chatroom thực hiện trao đổi thông tin như sau:
  + Người gửi (Mã hóa): Người dùng upload file trên cloud (Google Drive, One Drive,…) để được cấp link đường dẫn. Ban đầu, hệ thống thực hiện

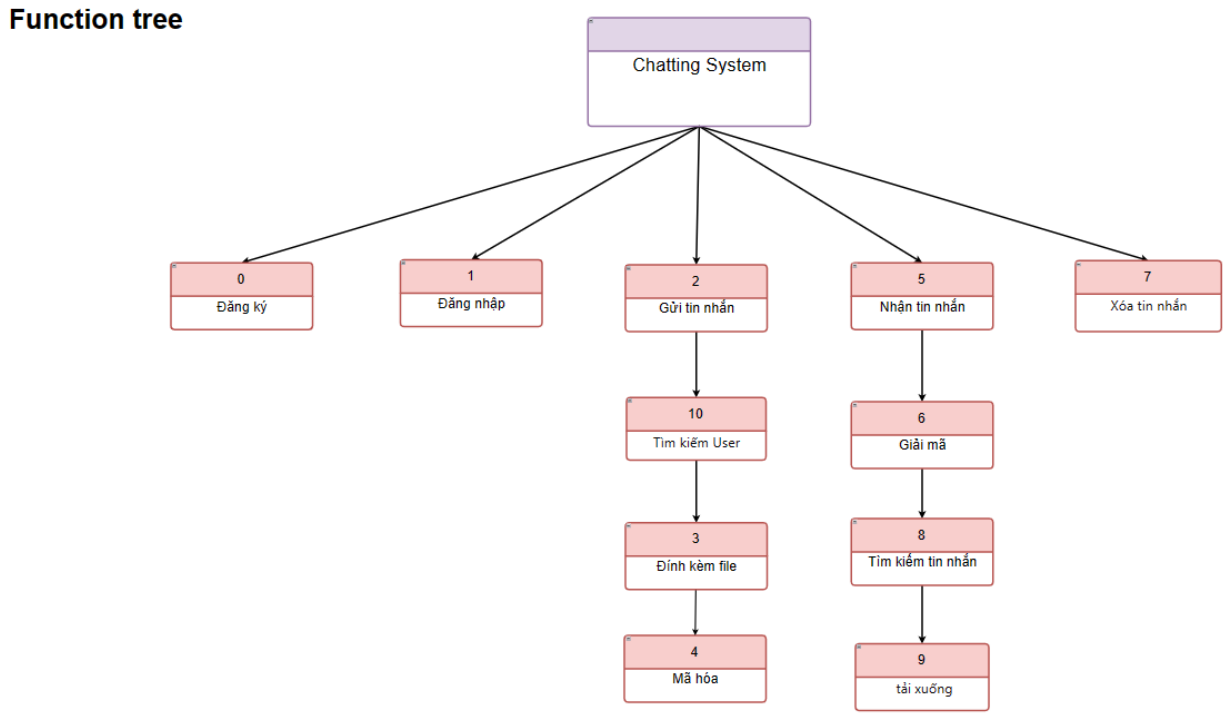
việc sinh khóa và mã hóa file dựa trên thuật toán AES (khóa sẽ gửi về phía người dùng để thực hiện việc giải mã). Song song đó, link sẽ được băm và sử dụng Private key của người gửi để thực hiện chữ kí điện tử. Link đã mã hóa và chữ kí điện tử sẽ được gửi cho người nhận.

+ Người nhận (Giải mã): Người dùng tiến hành nhập Public key của người gửi để xác thực thông qua chữ kí điện tử. Sau khi xác thực thành công, sử dụng key AES mà người gửi đã gửi trước đó để tiến hành việc giải mã file. **Lưu ý:** chỉ tiến hành mã hóa file, không mã hóa tin nhắn.

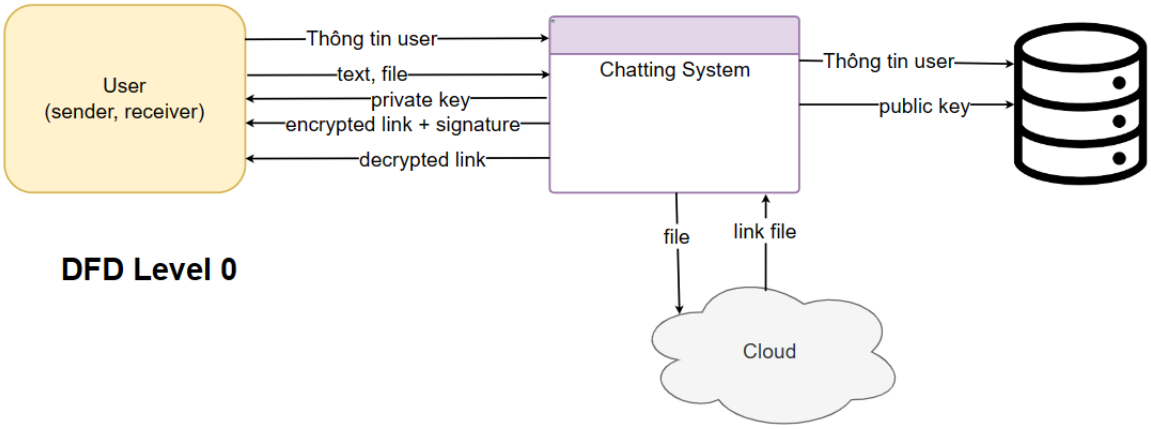
- Chỉ người dùng mới có thể truy xuất việc trao đổi tin nhắn; xóa tin nhắn và file thông qua các room_id.
- Chat room sẽ được lưu tạm thời từ 14-30 ngày kể từ ngày tạo, và sẽ tự động xóa sau đó, không thể khôi phục trừ trường hợp back-up.

IV. Data Flow Diagram:

1. Function tree:



2. Level 0:



DFD Level 0

Ký hiệu:

: Người dùng

: Hệ thống

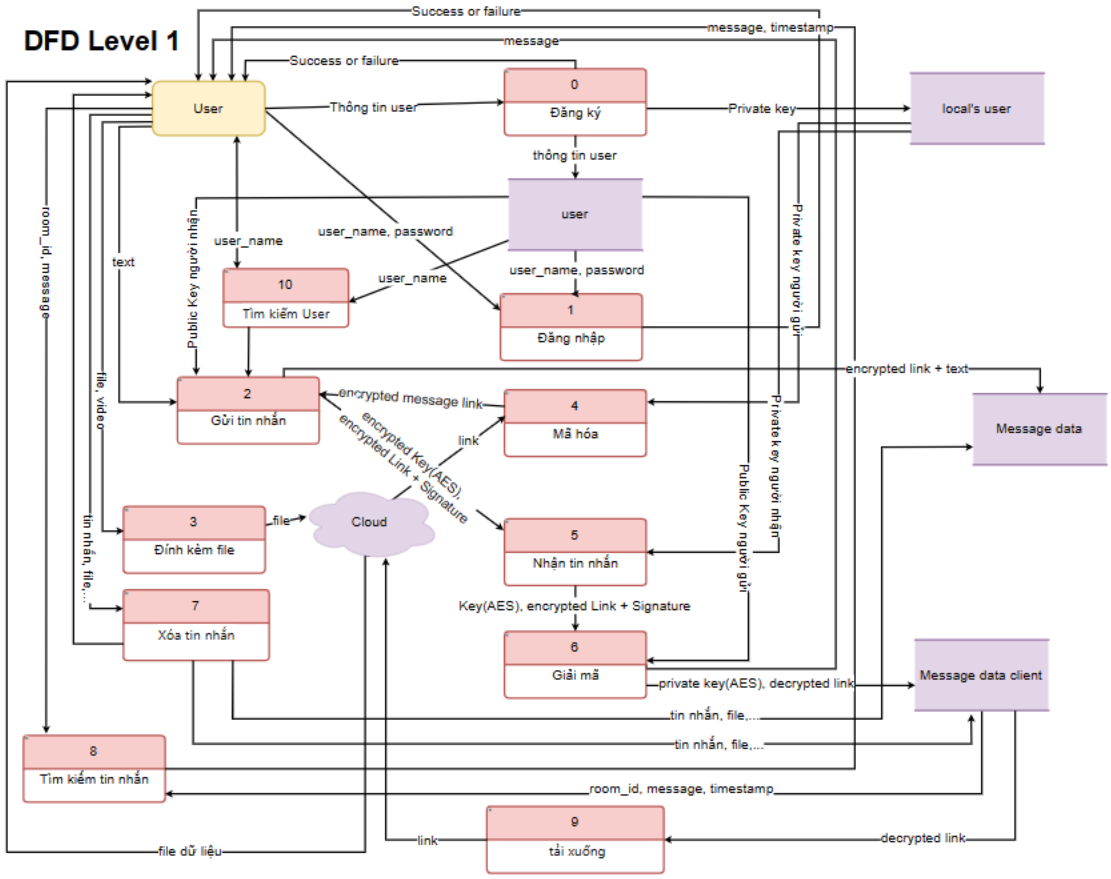
3. Level 1:

Ký hiệu:

: Chức năng

: Database ở dạng bảng

: người dùng



Thực thể : User

Tiến trình:

- Đăng kí
- Đăng nhập
- Tìm kiếm User
- Gửi tin nhắn
- Đính kèm file
- Nhận tin nhắn
- Mã hóa
- Giải mã
- Tìm kiếm tin nhắn
- Xóa tin nhắn
- Tải xuống
- Tạo nhóm chat mới

- Add thành viên vào nhóm chat

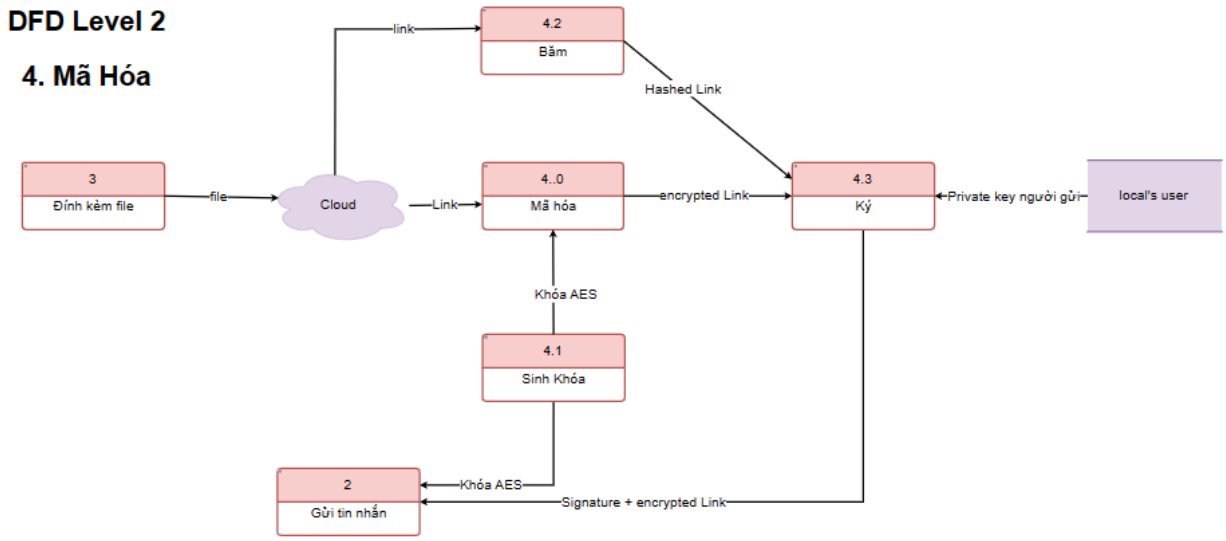
Kho dữ liệu: User, Local's user, Message Data, Message Data Client, ChatroomID

Các chức năng nổi bật:

- Mã hóa:
  - Input : Private Key của người gửi ở Local's User, Link file
  - Output: Link file đã được mã hóa và gửi tin nhắn mã hóa này cho người nhận
- Giải mã:
  - Input: Encrypted Key(AES), Encrypted Link + Signature, Private Key Người nhận
  - Output: Private Key (AES), Decrypted Link và lưu trữ ở Message Data Client

4. Level 2:

4.1. Mã hóa:



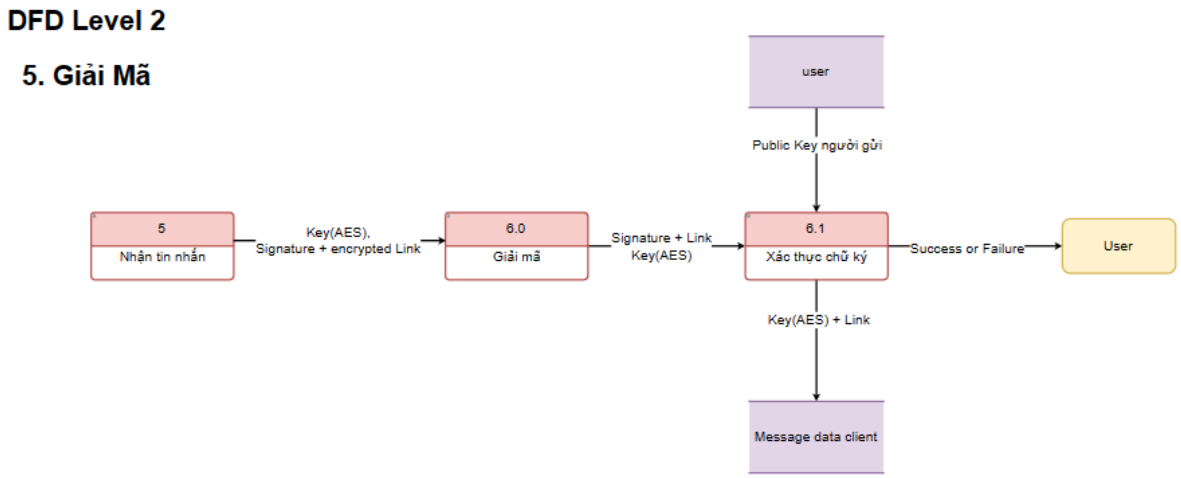
Chức năng Mã hóa sẽ liên kết với 2 chức năng khác là Gửi tin nhắn và Đính kèm file

Chi tiết:

1. Sau khi chức năng Đính kèm file được thực hiện file đầu vào sẽ được upload lên cloud
2. Khi chức năng mã hóa bắt đầu sẽ sinh khóa AES bất kì
3. Cloud sẽ tạo ra link file ngẫu nhiên và được mã hóa lại bằng khóa AES ở bước 2 và băm lại phục vụ cho việc tạo chữ kí
4. Hashed Link sử dụng Private Key người gửi từ Local' User để Ký lại tạo ra Signature xác thực

5. Key AES được mã hóa bởi Public Key của người nhận
6. Key AES đã được mã hóa , Signature+Encrypted Link sẽ được gửi đi

4.2. Giải mã:



Chức năng Giải mã sẽ liên kết với chức năng khác là Nhận tin nhắn.

Chi tiết:

1. Sau khi nhận tin nhắn (Key AES , Signature + Encrypted Link) , Key AES sẽ được giải mã bởi Private Key người nhận
2. Encrypted Link sẽ được giải mã bởi Key AES ở bước 1
3. Link sẽ được băm lại tạo ra chữ kí mới để so sánh với chữ kí từ người gửi
4. Dùng Public Key người gửi để giải mã Signature từ đó sẽ có được chữ kí gốc.
5. So sánh chữ kí mới và chữ kí gốc
6. Kết quả ở bước 5 nếu 2 chữ kí giống nhau sẽ trả về link cho người nhận và lưu về Message Data Client, ngược lại sẽ báo lỗi.

V. Chi phí triển khai:

Chi phí triển khai:

-Frontend: sử dụng HTML,CSS (HTML được sử dụng để cấu trúc nội dung và xác định ngữ nghĩa của nó, trong khi CSS được sử dụng để tạo kiểu và tăng cường trực quan các thành phần HTML.) → Miễn phí

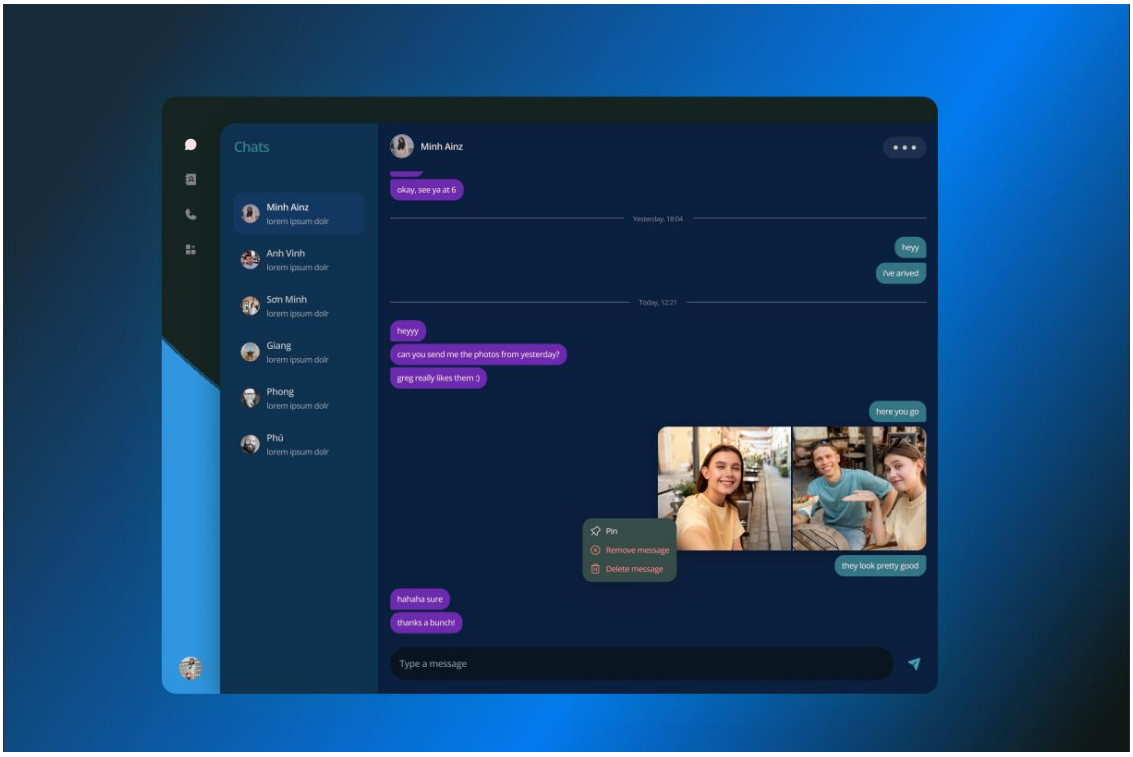
-Backend: sử dụng Nodejs (NodeJS có thể mở rộng, Thời gian thực thi code nhanh, Khả năng tương thích trên nhiều nền tảng, Truyền dữ liệu nhanh, Tiết kiệm thời gian, công sức và chi phí) → Miễn phí

-Cơ sở dữ liệu sử dụng NoSQL database – MongoDB → **Miễn phí** .Các dữ liệu được lưu trữ trong document kiểu JSON nên truy vấn sẽ rất nhanh, Dữ liệu lưu trữ phi cấu trúc, không có tính ràng buộc, toàn vẹn nên tính sẵn sàng cao, hiệu suất lớn và dễ dàng mở rộng lưu trữ.

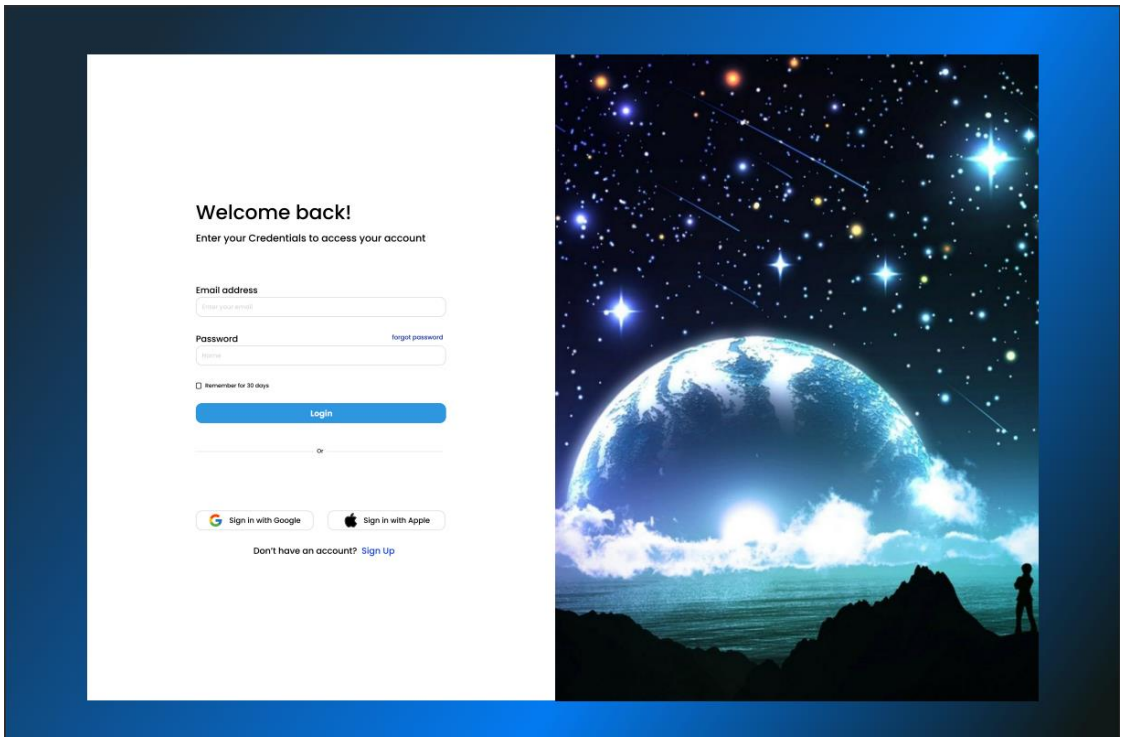
-API Cloud sẽ sử dụng Google Drive, hỗ trợ API → **Miễn phí :**

- Download và Upload file lên Google Drive
- Tìm kiếm file, thư mục trên Google Drive.
- User có thể chia sẻ file, thư mục hợp tác về nội dung trên Google Drive.
- Kết hợp với API Google Picker để tìm kiếm tất cả các tệp trong Google Drive, sau đó trả lại tên tệp, URL, ngày sửa đổi cuối cùng và người dùng.
- Tạo các phím tắt là các liên kết bên ngoài đến dữ liệu được lưu trữ bên ngoài Drive, trong một kho lưu trữ dữ liệu hoặc hệ thống lưu trữ đám mây khác.
- Tạo thư mục Drive chuyên dụng để lưu trữ dữ liệu của ứng dụng để ứng dụng không thể truy cập tất cả nội dung của người dùng được lưu trữ trong Google Drive. Xem Lưu trữ dữ liệu dành riêng cho ứng dụng.
- Tích hợp với Giao diện người dùng Google Drive, là giao diện người dùng web tiêu chuẩn của Google mà bạn có thể sử dụng để tương tác với các tệp Drive

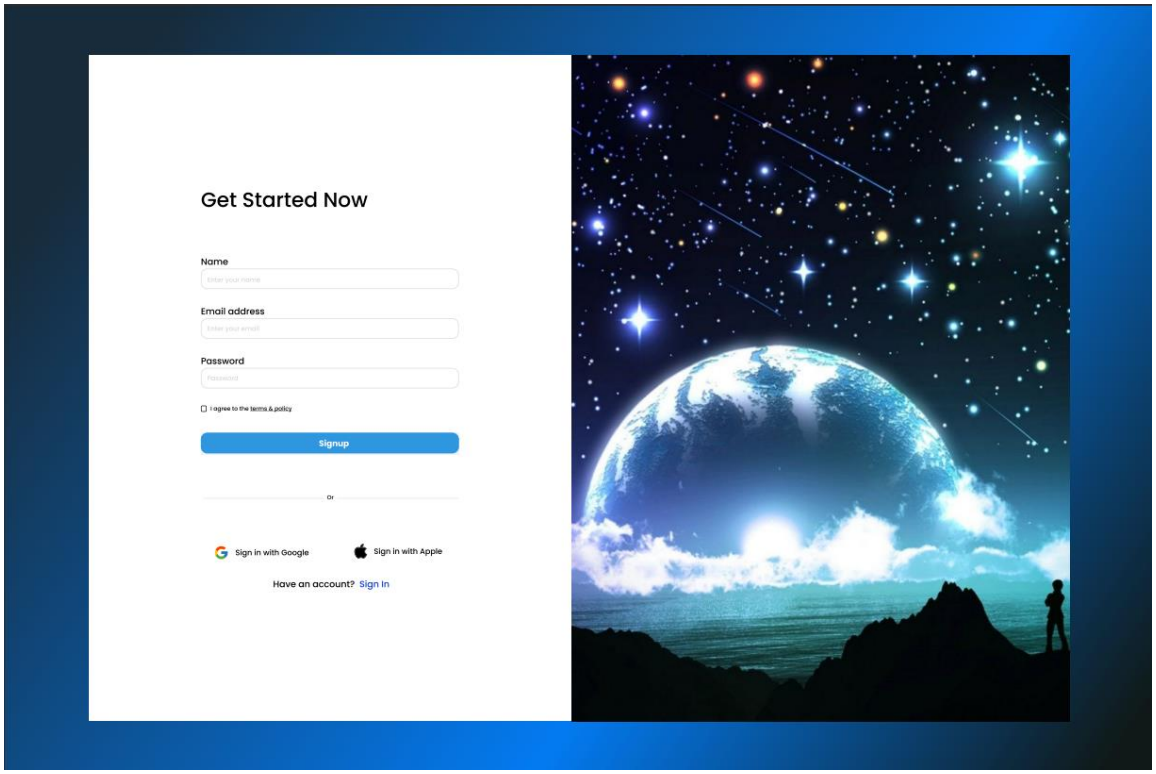
VI. UX/UI:



Màn hình tin nhắn



Màn hình đăng nhập



Màn hình đăng ký

VII. Tham khảo:

[1]: What is Data Flow Diagram? (visual-paradigm.com)

[2]: What is Entity Relationship Diagram (ERD)? (visual-paradigm.com)

Cảm ơn thầy/cô và các bạn đã xem