App Chat áp dụng mã hóa E2E, xác thực JWT và lưu trữ thông tin bản mã:

Mô tả: App cho phép hai client thực hiện nhắn tin realtime sau khi đăng nhập

* Chức năng: Đăng ký, Đăng nhập và Chat. Cả 3 chức năng này đều có thể áp dụng các thuật toán mã hóa khác nhau để tăng tính bảo mật.

1. Đăng ký: Sử dụng username và password để tạo tài khoản mới -> Implement thuật toán SHA-256 để băm mật khẩu trước khi lưu vào Database
2. Đăng nhập: So trùng username và password client gửi lên với thông tin trong Database. Nếu trùng khớp thì thực hiện sinh AccessToken và trả về cho client, để client dùng Token này xác thực trong những request tiếp theo. AccessToken được sinh bằng thuật toán HMAC-SHA256
3. Chat: Sử dụng socket.io và NodeJS.
   1. Alice soạn tin nhắn trên máy mình, nhấn nút gửi cho Bob.
   2. Tin nhắn được truyền đến server.
   3. Server kiểm tra AccessToken, nếu token hợp lệ (đúng là request của Alice) thì lưu tin nhắn vào Database
   4. Server sử dụng socket để “bắn” event tin nhắn mới sang cho Bob
   5. Bob nhận tin nhắn

* Có thể áp dụng mã hóa tin nhắn khi ấn nút gửi, để bản tin được truyền đi và lưu trữ trong Database là bản mã. Chỉ có người nhận mới giải mã được để đọc.
* Implement thuật toán RSA cho tác vụ mã hóa/giải mã
* Mỗi khi tạo một cuộc trò chuyện mới (hai người nhắn tin lần đầu), server sẽ sinh hai cặp khóa cho hai người (một người có n cuộc trò chuyện sẽ có n cặp khóa public/private key với n người khác). Private key được lưu dưới trên máy client dưới dạng các cặp key-value (key là tên người nhận, value là giá trị khóa), public key được lưu trên server. Khi mở cuộc trò chuyện (cũ) với một người, server sẽ gửi khóa công khai của người đó về cho client, client dùng khóa này để mã hóa tin nhắn và gửi đi. Khi nhận được tin nhắn từ người bên kia, client dùng private key lưu trong máy mình để giải mã và đọc.

Graphical user interface, diagram, application, Teams

Description automatically generated