|  |  |
| --- | --- |
| KHOA CÔNG NGHỆ THÔNG TIN  **BỘ MÔN CÔNG NGHỆ PHẦN MỀM**  ­­­­ | **CỘNG HÒA XÃ HỘI CHỦ NGHĨA VIỆT NAM**  **Độc lập - Tự do - Hạnh phúc** |

**ĐỀ CƯƠNG ĐỒ ÁN TỐT NGHIỆP ĐẠI HỌC**

Sinh viên thực hiện:

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| TT | Mã SV | Họ và tên | Lớp | Điện thoại | E-mail |
| 1 | 2121052523 | Lưu Đình Dũng | DCCTCT66\_05C | 0966526728 | Luudinhdung2402  @gmail.com |

Cán bộ hướng dẫn:

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| TT | Mã cán bộ | Họ và tên | Đơn vị | Điện thoại | E-mail |
| 1 | 0802-02 | GVC.Ths. Đặng Hữu Nghị | CNPM | 0989640319 | danghuunghi@humg.edu.vn |

## Tên đề tài

Tiếng Việt: Xây dựng Web chat mã hoá

Tiếng Anh: Building Encrypted Web Chat

## Lý do chọn đề tài

* Trong thời đại công nghệ số phát triển mạnh mẽ, nhu cầu giao tiếp trực tuyến ngày càng trở nên phổ biến và thiết yếu. Các ứng dụng chat trực tuyến như Messenger, Zalo, Telegram, WhatsApp… đã trở thành công cụ liên lạc không thể thiếu trong học tập, công việc và đời sống. Tuy nhiên, song song với sự tiện lợi đó là những vấn đề đáng lo ngại về **an toàn và bảo mật thông tin.**
* Thực tế cho thấy, nhiều vụ rò rỉ dữ liệu, nghe lén hoặc đánh cắp thông tin cá nhân đã xảy ra do tin nhắn không được mã hoá hoặc hệ thống bảo mật kém. Điều này đặt ra yêu cầu cấp thiết phải xây dựng các ứng dụng chat có **tích hợp cơ chế mã hoá dữ liệu** nhằm đảm bảo tính riêng tư và toàn vẹn cho người dùng.
* Xuất phát từ thực trạng trên, em chọn đề tài: **“Xây dựng ứng dụng Web Chat có tích hợp mã hoá dữ liệu”.**

## Mục tiêu của đề tài

## Mục tiêu chính:

## Xây dựng một ứng dụng Web chat thời gian thực có tích hợp cơ chế mã hoá dữ liệu, nhằm đảm bảo tin nhắn được bảo mật trong quá trình truyền tải, chỉ có thể được giải mã và đọc bởi người nhận hợp lệ.

* **Các kết quả mong đợi khi hoàn thành:**

Hoàn thiện một hệ thống chat trực tuyến trên nền tảng Web với đầy đủ các chức năng cơ bản: đăng nhập, gửi/nhận tin nhắn, tạo phòng chat, trò chuyện nhóm.

Tích hợp thành công cơ chế mã hoá/giải mã tin nhắn bằng AES-GCM, đảm bảo an toàn và riêng tư cho dữ liệu trao đổi.

Xây dựng cơ chế trao đổi khóa an toàn (RSA hoặc kết hợp mã hoá bất đối xứng – đối xứng).

Giao diện người dùng thân thiện, dễ sử dụng, hỗ trợ trên nhiều trình duyệt.

Báo cáo mô tả chi tiết kiến trúc hệ thống, thiết kế, quá trình triển khai và kết quả kiểm thử.

* **Đóng góp của đề tài:**

Góp phần nâng cao tính an toàn và bảo mật trong các ứng dụng chat trực tuyến.

Đưa ra một mô hình tham khảo cho việc xây dựng hệ thống chat bảo mật sử dụng mã hoá dữ liệu.

Vận dụng và kết hợp các kiến thức đã học về lập trình Web, cơ sở dữ liệu, giao tiếp thời gian thực và mật mã học vào một sản phẩm thực tiễn.

## Phạm vi nghiên cứu

## Giới hạn về mặt kỹ thuật, công nghệ:

## Ứng dụng được xây dựng trên nền tảng Web:

## FE sử dụng NextJS, Be sử dụng NestJS, cơ sở dữ liệu dùng Postgresql

## Giao tiếp thời gian thực dùng WebSocket(Socket.io)

## Cơ chế mã hoá sử dụng AES-GCM cho mã hoá nội dung tin nhắn và RSA cho trao đổi khóa.

## Giới hạn về đối tượng và dữ liệu nghiên cứu:

## Chỉ tập trung nghiên cứu và triển khai chức năng nhắn tin văn bản trong phạm vi mạng LAN và môi trường thử nghiệm Internet.

## Dữ liệu thử nghiệm là các tin nhắn do người dùng tạo ra trong quá trình sử dụng hệ thống.

## Các yếu tố không nằm trong phạm vi đề tài:

## Chưa triển khai chức năng gửi/nhận âm thanh, video.

## Chưa tích hợp chatbot AI, gọi thoại hoặc gọi video.

## Chưa tối ưu hoá cho hệ thống phân tán với số lượng người dùng cực lớn.

## Các vấn đề về chính sách pháp lý, thương mại hóa, tích hợp với hệ thống bên ngoài không nằm trong phạm vi nghiên cứu của đề tài.

## Nội dung nghiên cứu

## 5.1. Nghiên cứu cơ sở lý thuyết:

* Tìm hiểu về các mô hình mã hoá dữ liệu trong truyền thông trực tuyến.

## Nghiên cứu nguyên lý hoạt động của các thuật toán mã hoá phổ biến: AES-GCM, RSA, PBKDF2 (dùng để tạo và quản lý khóa).

## Tìm hiểu mô hình End-to-End Encryption (E2EE) và ứng dụng trong các hệ thống chat.

## Nghiên cứu cơ chế truyền thông real-time sử dụng WebSocket/Socket.IO.

## 5.2. Phân tích hệ thống:

* Phân tích yêu cầu chức năng: đăng ký, đăng nhập, gửi và nhận tin nhắn.
* Thiết kế sơ đồ use case, sequence diagram, và class diagram.
* Thiết kế cơ sở dữ liệu quan hệ (PostgreSQL) phục vụ lưu trữ tài khoản và tin nhắn.
* Xây dựng mô hình quản lý khóa mã hoá và luồng trao đổi dữ liệu an toàn.
* Xây dựng mô hình quản lý khóa mã hoá và luồng trao đổi dữ liệu an toàn giữa client – server – client.

**5.3. Xây dựng hệ thống:**

* Phát triển backend với NestJS để xử lý đăng ký, đăng nhập, mã hoá/giải mã tin nhắn và quản lý kết nối real-time.
* Phát triển frontend với Next.js để hiển thị giao diện chat, nhập và nhận tin nhắn.
* Tích hợp Socket.IO để đồng bộ tin nhắn thời gian thực giữa người dùng.
* Cài đặt cơ chế mã hoá đầu cuối (E2EE): mã hoá tin nhắn tại client trước khi gửi, giải mã tại client.
* Thực hiện unit test và integration test cho các thành phần chính (mã hoá/giải mã, API, socket).
* Thực hiện thử nghiệm trên nhiều trình duyệt và nhiều người dùng đồng thời.

**5.4. Viết báo cáo và đề xuất hướng phát triển:**

* Hoàn thiện báo cáo chi tiết về cơ sở lý thuyết, phân tích thiết kế, cài đặt và kết quả thực nghiệm.
* Đề xuất các hướng phát triển mở rộng như: mã hoá file, hỗ trợ đa phương tiện (ảnh, video, voice), tối ưu hiệu suất cho hệ thống quy mô lớn, tích hợp 2FA (xác thực hai lớp) để nâng cao bảo mật.

## Kế hoạch thực hiện

|  |  |  |
| --- | --- | --- |
| Tuần | Thời gian | Nội dung công việc |
| 1 | 01/10 - 7/10 | Tìm hiểu, khảo sát nghiệp vụ |
| 2 | 8/10 – 15/10 | Phân tích bài toán và thiết kết mockup |
| 3 | 16/10 – 23/10 | Thiết kế cơ sở dữ liệu; xây dựng class diagram; hoàn thiện mô hình tổng thể hệ thống |
| 4 | 24/10 – 31/10 | Cài đặt môi trường phát triển (NestJs/Next.js, DB); xây dựng khung backend và frontend cơ bản |
| 5 | 1/11- 8/11 | Phát triển chức năng Đăng ký, Đăng nhập, quản lý tài khoản và xác thực người dùng |
| 6 | 9/11 – 16/11 | Tích hợp Socket.IO cho chức năng chat real-time; xây dựng giao diện chat cơ bản |
| 7 | 17/11 – 24/11 | Áp dụng mã hoá đầu cuối (E2EE) cho tin nhắn: tích hợp AES-GCM, RSA và quản lý khoá |
| 8 | 25/11 – 1/12 | Hoàn thiện luồng gửi/nhận tin nhắn mã hoá; xử lý lưu trữ tin nhắn trong cơ sở dữ liệu |
| 9 | 1/12 – 8/12 | Tìm hiểu về cloud (aws) và đưa lên production |
| 10 | 8/12 -15/12 | Viết báo cáo, hoàn thiện tài liệu; đề xuất hướng phát triển mở rộng và chuẩn bị bảo vệ |

*Hà Nội, ngày 03 tháng 10 năm 2025*

|  |  |
| --- | --- |
| **Cán bộ hướng dẫn**  (ký, họ tên) | **Sinh viên thực hiện**  (ký, họ tên) |