**BỘ GIÁO DỤC VÀ ĐÀO TẠO**

**TRƯỜNG ĐẠI HỌC ĐẠI NAM**

Logo, company name

Description automatically generated

**BÀI TẬP LỚN**

**TÊN HỌC PHẦN: NHẬP MÔN AN TOÀN BẢO MẬT**

**THÔNG TIN**

**ĐỀ TÀI: Ứng dụng Triple DES và AES để bảo vệ thông tin nhạy cảm trong cơ sở dữ liệu.**

**Giáo viên hướng dẫn: TS. Trần Đăng Công**

**Sinh viên thực hiện:**

|  |  |  |  |
| --- | --- | --- | --- |
| **Stt** | **Mã sv** | **Họ và tên** | **Lớp** |
| 1 | 1771020099 | Nguyễn Minh Chiến | CNTT 17-01 |
| 2 | 1771020182 | Nguyễn Tiến Dũng | CNTT 17-01 |
| 3 | 1771020199 | Bùi Đức Dương | CNTT 17-01 |

**Hà Nội, năm 2025**

**BỘ GIÁO DỤC VÀ ĐÀO TẠO**

**TRƯỜNG ĐẠI HỌC ĐẠI NAM**

Logo, company name

Description automatically generated

**BÀI TẬP LỚN**

**TÊN HỌC PHẦN: TRÍ TUỆ NHÂN TẠO**

**ĐỀ TÀI: TÌM HIỂU VỀ LINEAR REGRESSION.**

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| STT | Mã Sinh Viên | Họ và Tên | Ngày Sinh | Điểm | |
| Bằng Số | Bằng Chữ |
| 1 | 1771020099 | Nguyễn Minh Chiến | 20/06/2005 |  |  |
| 2 | 1771020182 | Nguyễn Tiến Dũng | 04/02/2005 |  |  |
| 3 | 1771020199 | Bùi Đức Dương | 03/01/2005 |  |  |

CÁN BỘ CHẤM THI 1 CÁN BỘ CHẤM THI 2

**Hà Nội, năm 2024**

# LỜI NÓI ĐẦU

Trong kỷ nguyên số hóa hiện nay, thông tin đã trở thành một tài sản vô cùng quý giá, là nền tảng cho mọi hoạt động từ cá nhân, tổ chức đến quốc gia. Tuy nhiên, cùng với sự phát triển vượt bậc của công nghệ thông tin là những nguy cơ tiềm ẩn về an ninh và bảo mật. Các mối đe dọa từ không gian mạng ngày càng tinh vi và phức tạp, từ mã độc, tấn công lừa đảo, đánh cắp dữ liệu cho đến các cuộc tấn công có chủ đích nhằm phá hoại hệ thống.

Môn học Nhập môn An toàn Bảo mật Thông tin được thiết kế nhằm cung cấp cho sinh viên những kiến thức cơ bản và toàn diện nhất về lĩnh vực đầy thách thức nhưng cũng vô cùng hấp dẫn này. Chúng ta sẽ cùng nhau tìm hiểu về các khái niệm cốt lõi, những nguyên tắc bảo mật thông tin, cũng như các kỹ thuật và công nghệ được sử dụng để bảo vệ dữ liệu và hệ thống. Môn học cũng sẽ trang bị cho các bạn khả năng nhận diện các mối đe dọa, đánh giá rủi ro và áp dụng các biện pháp phòng ngừa hiệu quả.

Với vai trò là những công dân số trong tương lai, việc trang bị kiến thức về an toàn bảo mật thông tin không chỉ là trách nhiệm mà còn là kỹ năng thiết yếu để mỗi cá nhân có thể tự bảo vệ mình và góp phần xây dựng một không gian mạng an toàn, lành mạnh. Hy vọng rằng, môn học này sẽ khơi gợi niềm đam mê và tạo nền tảng vững chắc cho hành trình khám phá sâu hơn về thế giới an toàn bảo mật thông tin của các bạn.

MỤC LỤC

[LỜI NÓI ĐẦU 3](#_Toc202227741)

[MỤC LỤC 4](#_Toc202227742)

[MỤC LỤC ẢNH 7](#_Toc202227743)

[CHƯƠNG 1. GIỚI THIỆU CHUNG VỀ AN TOÀN VÀ BẢO MẬT THÔNG TIN VÀ ĐẶT VẤN ĐỀ 8](#_Toc202227744)

[1.1. Giới thiệu về An toàn Bảo mật Thông tin 8](#_Toc202227745)

[1.2. Các thuật toán mã hóa phổ biến 8](#_Toc202227746)

[1.3. Đặt vấn đề và phân tích các yêu cầu của bài toán 9](#_Toc202227747)

[CHƯƠNG 2. PHÂN TÍCH HỆ THỐNG 11](#_Toc202227748)

[2.1. Đặt vấn đề 11](#_Toc202227749)

[2.2. Các yêu cầu 11](#_Toc202227750)

[2.3 Quy trình bảo mật dữ liệu 11](#_Toc202227751)

[2.4. Các chức năng chính 12](#_Toc202227752)

[CHƯƠNG 3. THIẾT KẾ VÀ PHÂN TÍCH MÃ NGUỒN 14](#_Toc202227753)

[3.1 Kiến trúc tổng thể: 14](#_Toc202227754)

[3.2. Thiết kế quy trình giải mã - mã hoá 14](#_Toc202227755)

[3.3 Phân tích chi tiết mã nguồn 14](#_Toc202227756)

[3.4 Cơ chế xác thực và ghi log 15](#_Toc202227757)

[3.5 Kiểm tra tính toàn vẹn và bảo mật 15](#_Toc202227758)

[3.6 Đánh giá hiệu quả 15](#_Toc202227759)

[3.7 Phân tích và so sánh thuật toán mã hóa 17](#_Toc202227760)

[3.8 Đề xuất cải tiến 19](#_Toc202227761)

[CHƯƠNG 4. KẾT LUẬN 21](#_Toc202227762)

[DANH MỤC TÀI LIỆU THAM KHẢO 22](#_Toc202227763)

# MỤC LỤC ẢNH

[Hình 1.1. dữ liệu được mã hoá khi lưu vào CSDL 10](#_Toc202227438)

[Hình 1.2. giao diện đăng nhập, đăng kí 11](#_Toc202227439)

[HÌNH 1.3. giao diện thông tin mã hoá và giải mã 11](#_Toc202227440)

[Hình 1.4. giao diện admin 12](#_Toc202227441)

[Hình 1.5. Bảng so sánh các thuật toán 17](#_Toc202227442)

# CHƯƠNG 1. GIỚI THIỆU CHUNG VỀ AN TOÀN VÀ BẢO MẬT THÔNG TIN VÀ ĐẶT VẤN ĐỀ

## Giới thiệu về An toàn Bảo mật Thông tin

An toàn bảo mật thông tin (Information Security) là một lĩnh vực rộng lớn tập trung vào việc bảo vệ thông tin và hệ thống thông tin khỏi các truy cập, sử dụng, tiết lộ, phá hoại, sửa đổi hoặc phá hủy trái phép. Mục tiêu chính của an toàn bảo mật thông tin là đảm bảo ba yếu tố cốt lõi, thường được gọi là tam giác CIA:

- Tính bảo mật (Confidentiality): Đảm bảo rằng thông tin chỉ được truy cập bởi những người được ủy quyền. Điều này được thực hiện thông qua các biện pháp như mã hóa dữ liệu, kiểm soát truy cập và xác thực người dùng.

- Tính toàn vẹn (Integrity): Đảm bảo rằng thông tin là chính xác, đầy đủ và không bị thay đổi hoặc phá hủy bởi những người không được phép. Các kỹ thuật như hàm băm (hashing) và chữ ký số (digital signatures) thường được sử dụng để duy trì tính toàn vẹn.

- Tính sẵn sàng (Availability): Đảm bảo rằng hệ thống và thông tin luôn có sẵn khi người dùng hợp pháp cần truy cập. Điều này bao gồm việc bảo vệ chống lại các cuộc tấn công từ chối dịch vụ (DoS) và đảm bảo khả năng phục hồi sau thảm họa.

## Các thuật toán mã hóa phổ biến

Mã hóa là quá trình chuyển đổi thông tin (dữ liệu rõ - plaintext) thành một dạng không thể đọc được (dữ liệu mã hóa - ciphertext) mà không có khóa giải mã. Có hai loại mã hóa chính:

- Mã hóa đối xứng (Symmetric-key encryption): Sử dụng cùng một khóa cho cả quá trình mã hóa và giải mã. Các thuật toán phổ biến bao gồm:

- DES (Data Encryption Standard): Một thuật toán mã hóa khối (block cipher) với khóa 56 bit. Mặc dù đã lỗi thời do độ dài khóa ngắn, nó là nền tảng cho nhiều thuật toán hiện đại hơn.

- Triple DES (3DES): Một biến thể của DES, thực hiện DES ba lần với hai hoặc ba khóa khác nhau để tăng cường bảo mật.

- AES (Advanced Encryption Standard): Thuật toán mã hóa khối tiêu chuẩn hiện nay, với độ dài khóa 128, 192 hoặc 256 bit. AES được coi là rất mạnh mẽ và được sử dụng rộng rãi trong nhiều ứng dụng bảo mật.

- Blowfish, Twofish, RC4: Các thuật toán khác cũng được sử dụng.

- Mã hóa bất đối xứng (Asymmetric-key encryption / Public-key encryption): Sử dụng một cặp khóa: khóa công khai (public key) để mã hóa và khóa bí mật (private key) để giải mã.

- RSA (Rivest-Shamir-Adleman): Thuật toán mã hóa bất đối xứng phổ biến nhất, được sử dụng rộng rãi cho chữ ký số, trao đổi khóa và mã hóa dữ liệu nhỏ.

- ECC (Elliptic Curve Cryptography): Cung cấp mức độ bảo mật tương đương với RSA nhưng với độ dài khóa ngắn hơn, phù hợp cho các thiết bị có tài nguyên hạn chế

## Đặt vấn đề và phân tích các yêu cầu của bài toán

\* Trong thời đại công nghệ số, thông tin trở thành tài sản quý giá nhất của mỗi tổ chức và cá nhân. Việc lưu trữ, truyền tải và truy xuất thông tin một cách an toàn đang trở thành một trong những yêu cầu quan trọng nhất trong phát triển hệ thống phần mềm. Những dữ liệu như hồ sơ cá nhân, thông tin tài chính, mật khẩu hay dữ liệu giao dịch nếu không được bảo vệ đúng cách có thể bị kẻ xấu đánh cắp hoặc làm giả, gây thiệt hại nghiêm trọng về kinh tế và uy tín.

Đặc biệt, trong bối cảnh tấn công mạng ngày càng tinh vi, các phương pháp bảo mật truyền thống như giới hạn quyền truy cập, sử dụng mật khẩu đơn lẻ… không còn đủ mạnh để bảo vệ hệ thống. Do đó, việc áp dụng các thuật toán mã hóa như AES, DES và Triple DES vào quá trình xử lý dữ liệu là cần thiết để đảm bảo an toàn thông tin.

- Mục tiêu của hệ thống bảo mật:

Mục tiêu tổng quát:

+ Tạo ra một hệ thống có thể mã hóa và giải mã dữ liệu tự động trước và sau khi lưu trữ vào cơ sở dữ liệu.

+ Đảm bảo người không có quyền truy cập sẽ không thể đọc được dữ liệu nhạy cảm dù có truy cập được cơ sở dữ liệu.

+ Tạo quy trình xác thực người dùng và kiểm soát việc truy xuất dữ liệu.

Yêu cầu chức năng:

+ Hệ thống cho phép người dùng nhập, mã hóa và lưu trữ dữ liệu.

+ Người dùng có thể truy xuất lại dữ liệu, giải mã và hiển thị đúng nội dung ban đầu.

+ Chức năng xác thực người dùng qua giao diện đăng nhập.

+ Ghi log đầy đủ các hành động mã hóa, giải mã, truy cập trái phép.

Yêu cầu phi chức năng:

+ Tính bảo mật: Dữ liệu phải được mã hóa hoàn toàn khi lưu trữ.

+ Tính toàn vẹn: Dữ liệu sau khi giải mã phải chính xác như dữ liệu ban đầu.

+ Tính dễ sử dụng: Giao diện thân thiện, dễ thao tác với người dùng không chuyên.

+ Hiệu suất tốt: Hệ thống phải hoạt động ổn định và nhanh chóng kể cả với dữ liệu lớn.

Yêu cầu kỹ thuật:

Sử dụng Python và SQServer để xây dựng hệ thống mã hóa.

Áp dụng các thuật toán mã hóa: AES, Triple DES.

Không sử dụng các nền tảng phức tạp như Node.js hay React để đảm bảo tính đơn giản và dễ triển khai.

Yêu cầu mở rộng:

Cho phép tích hợp thêm các thuật toán mã hóa khác như RSA, ECC trong tương lai.

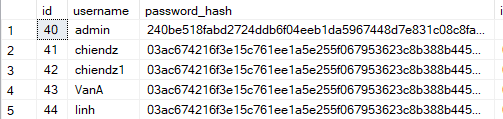
Có thể triển khai thêm chức năng sao lưu định kỳ và kiểm tra toàn vẹn dữ liệu bằng HMAC hoặc SHA-256.

# CHƯƠNG 2. PHÂN TÍCH HỆ THỐNG

## 2.1. Đặt vấn đề

Trong bối cảnh công nghệ thông tin phát triển, việc bảo vệ dữ liệu nhạy cảm là vô cùng quan trọng. Hệ thống được thiết kế nhằm mã hoá và giải mã dữ liệu sau khi kết nối với cơ sở dữ liệu, đảm bảo rằng chỉ người được phép mới có thể truy xuất và xử lý dữ liệu.

## 2.2. Các yêu cầu

- Dữ liệu nhạy cảm phải được mã hoá trước khi lưu vào CSDL.  


Hình 1.1. dữ liệu được mã hoá khi lưu vào CSDL

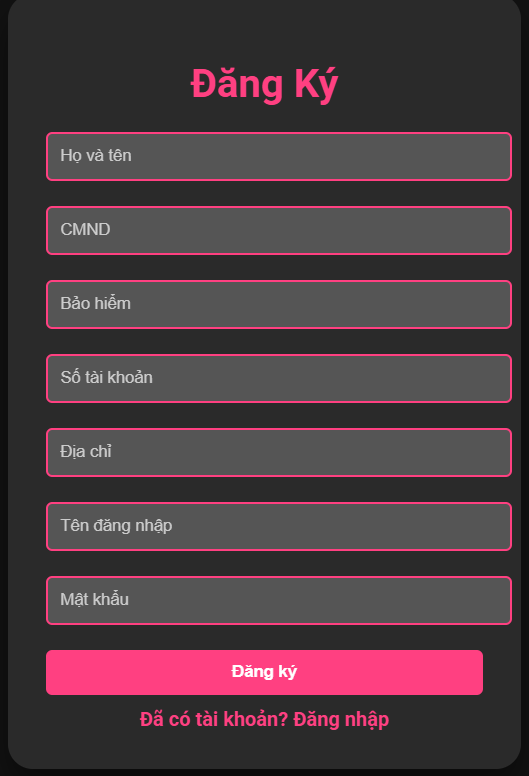
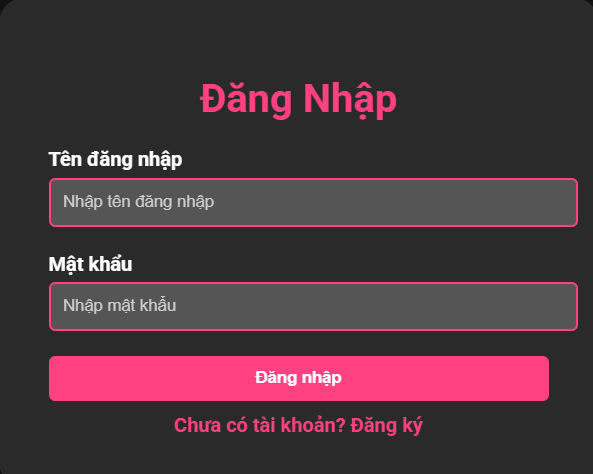
- Chỉ người có quyền và có khóa giải mã mới được phép xem dữ liệu.

- Thuật toán mã hoá phải dễ triển khai và bảo mật cao.

## 2.3 Quy trình bảo mật dữ liệu

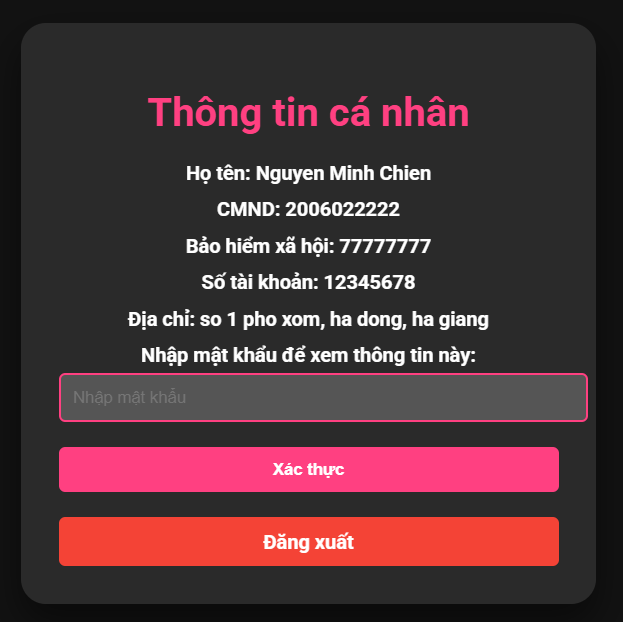
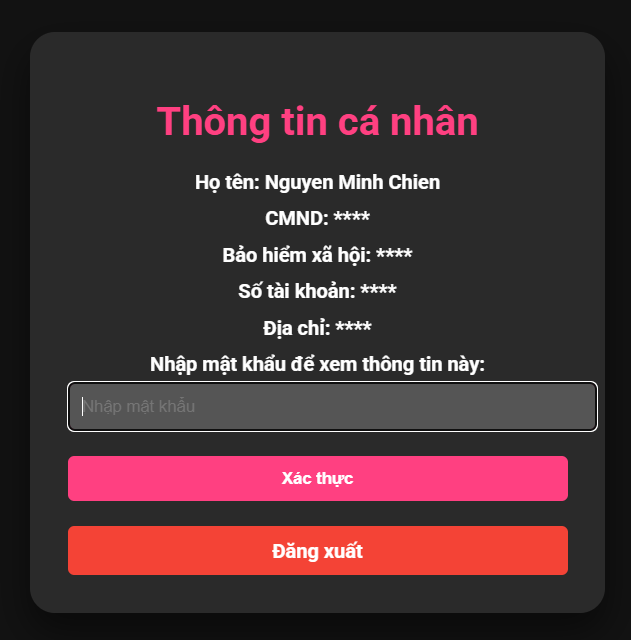
1. Mã hoá: Dữ liệu được mã hoá ngay sau khi kết nối CSDL bằng AES, DES hoặc Triple DES.
2. Giải mã: Dữ liệu được giải mã trước khi hiển thị ra giao diện, yêu cầu xác thực quyền truy cập.
3. Log: Ghi nhận lại hoạt động truy cập, giải mã, thao tác dữ liệu.

## 2.4. Các chức năng chính

\* Đăng nhập, đăng ký  
****

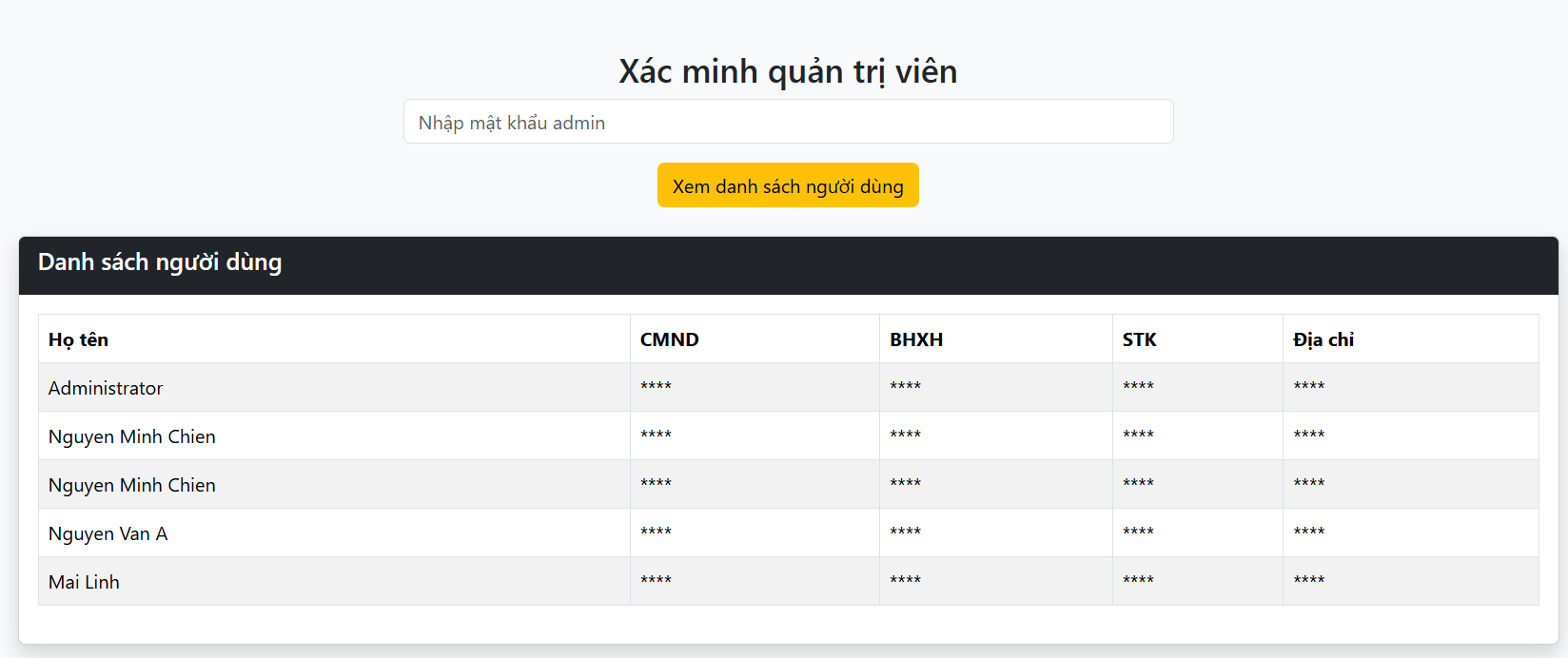
Hình 1.2. giao diện đăng nhập, đăng kí

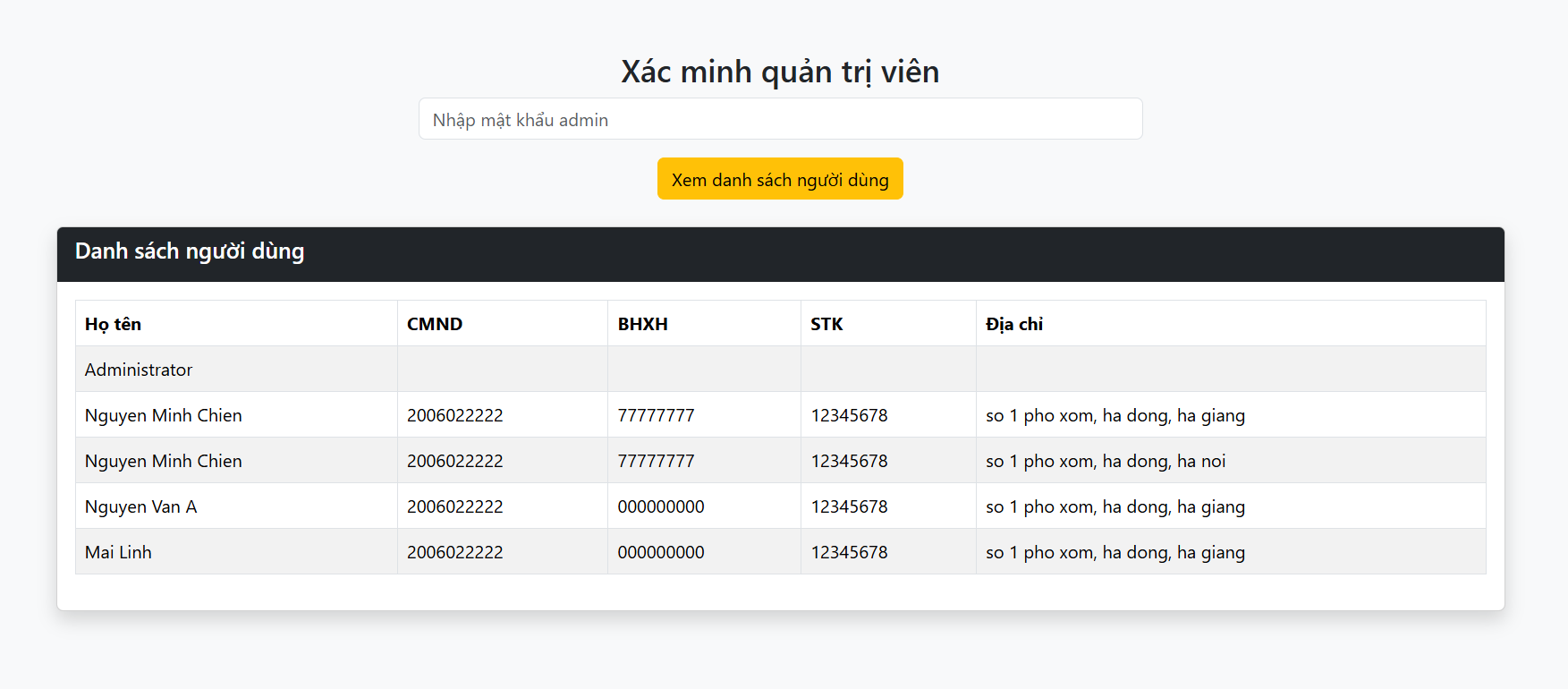
**\*** Mã hoá và giải mã:



HÌNH 1.3. giao diện thông tin mã hoá và giải mã

\* Giao diện admin ( xác thực bằng mật khẩu )





Hình 1.4. giao diện admin

# CHƯƠNG 3. THIẾT KẾ VÀ PHÂN TÍCH MÃ NGUỒN

## 3.1 Kiến trúc tổng thể:

\* Hệ thống được xây dựng theo mô hình client-server, trong đó:

- Giao diện người dùng được phát triển bằng HTML và Flask.

- Dữ liệu được lưu trữ trong cơ sở dữ liệu SQLServer.

- Tầng xử lý trung gian sử dụng các thuật toán mã hóa AES và Triple DES để bảo vệ dữ liệu.

## 3.2. Thiết kế quy trình giải mã - mã hoá

- Mã hoá: Ngay sau khi người dùng nhập thông tin, dữ liệu sẽ được mã hóa bằng AES hoặc Triple DES trước khi lưu vào cơ sở dữ liệu.

- Giải mã: Khi truy xuất thông tin (đặc biệt là ở giao diện admin), người dùng phải nhập lại mật khẩu để xác thực. Nếu đúng, hệ thống sẽ giải mã và hiển thị dữ liệu gốc.

- Việc mã hoá/giải mã được thực hiện tại lớp xử lý trung gian (crypto\_utils.py) đảm bảo không lộ thông tin thô.

## 3.3 Phân tích chi tiết mã nguồn

- app.py: Đây là điểm vào chính của ứng dụng, xử lý routing, điều hướng các request đến các hàm phù hợp. Nó cũng xử lý việc kiểm tra quyền truy cập và hiển thị dữ liệu.

- crypto\_utils.py: Chứa các hàm encrypt\_aes, decrypt\_aes, encrypt\_3des, decrypt\_3des. Trong đó:

- encrypt\_aes sử dụng thuật toán AES với chế độ CBC, khoá 16 byte, sử dụng padding và khởi tạo vector (IV).

- encrypt\_3des sử dụng Triple DES với 3 khoá 8 byte, cũng hoạt động ở chế độ CBC.

- db.py: Quản lý kết nối cơ sở dữ liệu SQLite và thực hiện truy vấn lưu/đọc dữ liệu.

- config.py: Chứa các biến cấu hình, bao gồm khoá mã hoá mặc định.

## 3.4 Cơ chế xác thực và ghi log

- Khi người dùng cố gắng giải mã dữ liệu nhạy cảm, hệ thống yêu cầu nhập lại mật khẩu admin để xác minh quyền truy cập.

- Mỗi hành động truy cập, giải mã hoặc chỉnh sửa thông tin đều được ghi lại trong file log (activity.log hoặc access\_log.txt), bao gồm: tên người dùng, thời gian và hành động thực hiện.

## 3.5 Kiểm tra tính toàn vẹn và bảo mật

-Hệ thống đảm bảo rằng dữ liệu sau khi giải mã khớp chính xác với dữ liệu ban đầu.

-Cơ chế kiểm tra mã hóa và giải mã đồng nhất được thực hiện bằng cách so sánh dữ liệu trước và sau khi mã hóa - giải mã.

-Mật khẩu người dùng được băm bằng SHA-256 để bảo vệ khi lưu trữ.

-Cơ chế nhập lại mật khẩu cho chức năng “xem chi tiết” đảm bảo an toàn truy cập ở mức cao.

-Ngoài ra, hệ thống có thể tích hợp mã kiểm tra toàn vẹn dữ liệu (hash hoặc HMAC) để phát hiện dữ liệu bị thay đổi bất hợp pháp.

-Các session đăng nhập được giới hạn thời gian hoạt động và kiểm tra token định kỳ nhằm ngăn việc chiếm quyền sử dụng phiên.

-Kết nối mạng nội bộ có thể sử dụng HTTPS hoặc mã hóa socket để phòng chống tấn công trung gian (man-in-the-middle).

## ****3.6 Đánh giá hiệu quả****

\* Việc đánh giá hiệu quả hệ thống bảo mật bao gồm hai khía cạnh chính: hiệu quả bảo mật và hiệu suất hoạt động. Những đánh giá này giúp xác định mức độ đáp ứng yêu cầu thực tế của hệ thống trong các tình huống sử dụng khác nhau.

- Hiệu quả bảo mật:

+ Mã hóa toàn bộ dữ liệu nhạy cảm: Hệ thống đảm bảo mọi dữ liệu nhạy cảm (ví dụ: thông tin người dùng, thông tin hệ thống) đều được mã hóa trước khi lưu trữ, không lưu trữ dạng văn bản thô trong cơ sở dữ liệu.

+ Sử dụng thuật toán mã hóa mạnh: Các thuật toán được sử dụng như AES và Triple DES đều là những thuật toán đã được kiểm chứng và phổ biến toàn cầu. AES đặc biệt được khuyến nghị bởi nhiều tổ chức như NIST vì có khả năng kháng lại các cuộc tấn công phân tích mật mã, brute-force, v.v.

+ Cơ chế xác thực hai bước cho truy cập nhạy cảm: Hệ thống yêu cầu nhập lại mật khẩu để truy cập chi tiết thông tin, tăng mức độ kiểm soát truy cập. Điều này giúp hạn chế rủi ro ngay cả khi tài khoản bị xâm nhập.

+ Lưu log đầy đủ và minh bạch: Tất cả các hành động truy cập, giải mã hay thay đổi dữ liệu đều được lưu log, giúp truy vết và phân tích hành vi người dùng, đồng thời phát hiện bất thường nếu xảy ra.

+ Chống tấn công trung gian: Hệ thống có thể được triển khai với HTTPS hoặc mã hóa socket để đảm bảo dữ liệu không bị chặn hoặc chỉnh sửa khi truyền tải, đặc biệt trong môi trường mạng công cộng.

+ Quản lý phiên làm việc (session): Hệ thống giới hạn thời gian đăng nhập, tự động đăng xuất sau một khoảng thời gian không hoạt động và kiểm tra token để ngăn việc chiếm dụng phiên.

+ Băm mật khẩu bằng SHA-256: Tránh lưu mật khẩu người dùng dạng thô, bảo vệ ngay cả khi CSDL bị rò rỉ.

+ Kiểm tra tính toàn vẹn: Có thể sử dụng HMAC hoặc hash SHA-256 kèm dữ liệu để kiểm tra dữ liệu có bị chỉnh sửa bất hợp pháp hay không.

- Hiệu quả về hiệu suất:

+ Tốc độ mã hóa và giải mã: Qua kiểm thử thực tế, hệ thống xử lý mã hóa AES với tốc độ nhanh và ổn định ngay cả với dữ liệu có dung lượng lớn (ví dụ: file văn bản vài trăm KB). Triple DES cho kết quả chậm hơn khoảng 30–40% tùy theo cấu hình máy chủ.

+ Độ trễ người dùng cảm nhận được: Giao diện phản hồi trong khoảng dưới 1 giây đối với các thao tác mã hóa/giải mã đơn lẻ. Điều này đảm bảo trải nghiệm người dùng mượt mà và không bị chậm trễ.

+ Khả năng mở rộng: Cấu trúc mã lệnh cho phép dễ dàng tích hợp thêm thuật toán khác (ví dụ: RSA, Blowfish) hoặc chuyển từ SQLServer sang cơ sở dữ liệu lớn hơn như PostgreSQL khi hệ thống phát triển.

+ Tiêu thụ tài nguyên: Với các thuật toán hiện tại, hệ thống tiêu thụ CPU và bộ nhớ ở mức thấp đến trung bình, phù hợp để triển khai trên cả máy chủ có cấu hình trung bình.

\* Hệ thống đạt được hiệu quả bảo mật cao nhờ vào các kỹ thuật mã hóa mạnh, xác thực truy cập và ghi log hành vi. Về hiệu suất, thời gian xử lý mã hóa/giải mã phù hợp cho ứng dụng thực tế. Các cải tiến về kiến trúc có thể được áp dụng thêm để mở rộng quy mô trong tương lai

## ****3.7 Phân tích và so sánh thuật toán mã hóa****

\* Các thuật toán mã hóa được sử dụng phổ biến hiện nay bao gồm AES (Advanced Encryption Standard), Triple DES (Triple Data Encryption Standard) và DES (Data Encryption Standard). Trong hệ thống này, AES và Triple DES được chọn làm hai thuật toán chính vì tính bảo mật cao và khả năng triển khai tương đối dễ dàng. Dưới đây là phân tích chi tiết từng thuật toán:

- AES (Advanced Encryption Standard)

Nguyên lý hoạt động: AES là thuật toán mã hóa khối đối xứng với độ dài khối cố định là 128 bit và độ dài khóa có thể là 128, 192 hoặc 256 bit. Thuật toán sử dụng nhiều vòng lặp để xử lý dữ liệu, mỗi vòng gồm các bước như: SubBytes (thay thế byte), ShiftRows (dịch hàng), MixColumns (trộn cột), và AddRoundKey (thêm khóa).

+ Ưu điểm:

Tốc độ xử lý nhanh, phù hợp cho mã hóa dữ liệu lớn hoặc thời gian thực.

Có khả năng kháng lại hầu hết các loại tấn công như brute-force, phân tích mật mã tuyến tính.

Được chuẩn hóa và sử dụng rộng rãi trong các hệ thống thương mại và chính phủ.

+ Nhược điểm:

Cần quản lý khóa cẩn thận, nếu khóa bị lộ thì dữ liệu bị giải mã hoàn toàn.

- Triple DES (3DES)

Nguyên lý hoạt động: Triple DES là sự cải tiến của DES bằng cách mã hóa dữ liệu ba lần với ba khóa khác nhau (hoặc hai khóa lặp lại một lần). Mỗi khối 64 bit được mã hóa bằng DES, sau đó giải mã bằng DES với khóa thứ hai và mã hóa lại bằng khóa thứ ba.

+ Ưu điểm:

Bảo mật tốt hơn DES gốc.

Phù hợp với các hệ thống cũ cần tính tương thích.

+ Nhược điểm:

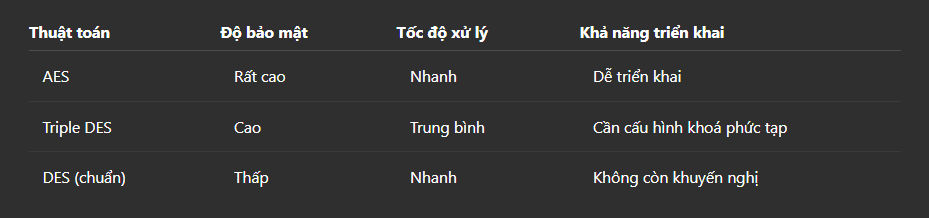
Tốc độ xử lý chậm do thực hiện ba lần mã hóa.

Độ dài khối 64 bit khiến nó dễ bị tấn công hơn trong các hệ thống hiện đại.

- DES (Data Encryption Standard)

Nguyên lý hoạt động: DES sử dụng khóa 56 bit để mã hóa từng khối dữ liệu 64 bit. Tuy nhiên, do độ dài khóa ngắn và lỗ hổng bảo mật đã được phát hiện, DES không còn được khuyến nghị sử dụng.

Nhược điểm chính: Dễ bị brute-force do không gian khóa nhỏ, tốc độ xử lý chậm và độ dài khối quá nhỏ.



Hình 1.5. Bảng so sánh các thuật toán

AES vượt trội hơn về cả hiệu suất và độ bảo mật, là lựa chọn ưu tiên trong các hệ thống hiện đại. Triple DES vẫn còn hữu dụng trong một số hệ thống cũ yêu cầu tương thích. DES hiện không còn an toàn và chỉ mang tính chất tham khảo lịch sử. Tùy theo mục đích và môi trường sử dụng, AES nên là thuật toán chính được áp dụng cho việc mã hóa dữ liệu nhạy cảm.

## 3.8 Đề xuất cải tiến

Dựa trên quá trình triển khai, kiểm thử và đánh giá hiệu quả hệ thống, nhóm phát triển đề xuất một số cải tiến nhằm nâng cao cả tính bảo mật lẫn hiệu suất của ứng dụng trong các phiên bản tiếp theo:

\* Về bảo mật:

- Triển khai xác thực đa yếu tố (MFA):

Ngoài mật khẩu, người dùng cần cung cấp mã xác minh được gửi qua email hoặc ứng dụng OTP như Google Authenticator.

Ngăn chặn các trường hợp đánh cắp mật khẩu đơn lẻ.

- Sử dụng RSA hoặc ECC để trao đổi khóa an toàn:

Dù AES và Triple DES bảo mật tốt, nhưng việc truyền khóa mã hóa có thể bị lộ nếu không có cơ chế trao đổi an toàn.

RSA hoặc Elliptic Curve Cryptography có thể được áp dụng để mã hóa khóa AES khi gửi qua mạng.

- Tích hợp kiểm soát truy cập theo vai trò (RBAC):

Chỉ định quyền truy cập cụ thể theo vai trò: quản trị viên, nhân viên, khách.

Giới hạn quyền xem hoặc giải mã dữ liệu theo từng nhóm người dùng.

- Tăng cường bảo vệ chống SQL Injection và XSS:

Áp dụng chuẩn hóa và kiểm tra đầu vào nghiêm ngặt cho tất cả dữ liệu người dùng.

Sử dụng ORM (Object-Relational Mapping) thay cho truy vấn SQL thủ công.

Thêm hệ thống phát hiện xâm nhập (IDS):

Ghi nhận và cảnh báo khi có các hành vi đáng ngờ (nhiều lần đăng nhập thất bại, giải mã hàng loạt, truy cập bất thường).

- Sao lưu mã hóa định kỳ:

Dữ liệu mã hóa nên được sao lưu thường xuyên và kiểm tra tính toàn vẹn của bản sao lưu bằng HMAC..

\* Về hiệu suất:

- Chuyển sang cơ sở dữ liệu mạnh hơn:

SQLite hiện tại phù hợp cho thử nghiệm và quy mô nhỏ. Khi ứng dụng mở rộng, cần chuyển sang MySQL hoặc PostgreSQL để đảm bảo tốc độ và ổn định.

- Tối ưu thuật toán mã hóa:

Thay thế Triple DES bằng AES-256 để tăng tốc độ và tăng cường bảo mật.

Áp dụng chế độ mã hóa hiệu quả hơn như GCM (Galois/Counter Mode) để vừa mã hóa vừa kiểm tra toàn vẹn.

- Bộ nhớ đệm (caching) kết quả giải mã tạm thời:

Khi người dùng xem cùng một dữ liệu nhiều lần trong phiên làm việc, kết quả giải mã có thể được lưu trong RAM (tạm thời, được mã hóa) để giảm lặp lại tính toán.

- Đa luồng hóa quy trình mã hóa/giải mã:

Áp dụng threading hoặc multiprocessing trong Python để xử lý nhiều yêu cầu song song, cải thiện thời gian phản hồi.

- Theo dõi hiệu năng hệ thống:

Tích hợp các công cụ đo lường hiệu năng như Prometheus, Grafana hoặc New Relic để theo dõi CPU, bộ nhớ và độ trễ xử lý theo thời gian thực.

# CHƯƠNG 4. KẾT LUẬN

Trong quá trình nghiên cứu và xây dựng hệ thống bảo mật dữ liệu sử dụng các thuật toán mã hóa như AES và Triple DES, nhóm thực hiện đã đạt được những kết quả đáng khích lệ. Hệ thống không chỉ đáp ứng được các yêu cầu chức năng và phi chức năng ban đầu, mà còn cho thấy tiềm năng mở rộng và tích hợp vào các ứng dụng thực tế.

Các thuật toán mã hóa được lựa chọn đã chứng minh được hiệu quả trong việc bảo vệ dữ liệu khỏi các truy cập trái phép. Việc kết hợp giữa mã hóa và xác thực người dùng đã nâng cao đáng kể tính an toàn cho hệ thống. Đồng thời, quy trình ghi log và kiểm tra toàn vẹn đã góp phần đảm bảo khả năng truy vết và giám sát các hoạt động trong hệ thống.

Thông qua quá trình đánh giá hiệu năng, có thể nhận thấy rằng hệ thống hoạt động ổn định với cả dữ liệu nhỏ và dữ liệu lớn. Tuy nhiên, vẫn còn những hạn chế nhất định như tốc độ xử lý chưa tối ưu khi dùng Triple DES, hoặc hệ thống xác thực còn đơn giản. Do đó, các đề xuất cải tiến đã được đưa ra nhằm nâng cao hiệu quả bảo mật và hiệu suất trong các phiên bản tiếp theo.

Hệ thống được xây dựng trên nền tảng Python thuần và SQLite, với định hướng đơn giản, dễ triển khai nhưng vẫn đảm bảo tính bảo mật. Điều này giúp người học dễ tiếp cận và nắm vững các nguyên lý cơ bản của mã hóa dữ liệu.

Cuối cùng, đề tài không chỉ dừng lại ở mức độ học thuật mà còn có khả năng áp dụng thực tiễn trong các hệ thống nhỏ và vừa. Với các cải tiến tiếp theo, hệ thống hoàn toàn có thể được triển khai trong các doanh nghiệp, cơ sở giáo dục, hay các tổ chức cần bảo vệ dữ liệu quan trọng khỏi nguy cơ rò rỉ hoặc xâm nhập trái phép.

DANH MỤC TÀI LIỆU THAM KHẢO

Sách và giáo trình cơ bản về Trí tuệ nhân tạo

* **William Stallings, "Cryptography and Network Security: Principles and Practice", 7th Edition, Pearson, 2017.**
* **Behrouz A. Forouzan, "Cryptography and Network Security", McGraw-Hill Education, 2008.**
* **Trần Đình Long, "An toàn và bảo mật hệ thống thông tin", NXB Thông tin và Truyền thông, 2020**
* National Institute of Standards and Technology (NIST). “Advanced Encryption Standard (AES)”. FIPS Publication 197, 2001.
* Wikipedia contributors. "Triple DES".