BỘ KHOA HỌC VÀ CÔNG NGHỆ

HỌC VIỆN CÔNG NGHỆ BƯU CHÍNH VIỄN THÔNG

ĐỀ CƯƠNG BÁO CÁO GIỮA KỲ

Thiết kế và xây dựng ứng dụng quản lý mật khẩu bảo mật dựa trên cơ chế mã hóa phía máy khách và xác thực blockchain

Giảng viên hướng dẫn:	TS. Kim Ngọc Bách
Họ và tên sinh viên:	Hoàng Tiến Đạt
Mã sinh viên:	B23DCCE015
Lớp:	D23CQCE06-B
Nhóm:	01

HÀ NỘI - 2026

Mục lục

Chương 1

Giới thiệu Dự án

1.1 Lý do chọn đề tài

Trong bối cảnh chuyển đổi số và gia tăng các cuộc tấn công mạng, thông tin đăng nhập đã trở thành mục tiêu khai thác phổ biến, chiếm tỷ lệ lớn trong các vụ vi phạm dữ liệu quy mô lớn [10]. Mô hình lưu trữ tập trung truyền thống luôn tiềm ẩn rủi ro về "điểm yếu tập trung" (Single Point of Failure), nơi một sự cố bảo mật đơn lẻ có thể dẫn đến rò rỉ dữ liệu trên diện rộng [13]. Đặc biệt, đánh cắp thông tin đăng nhập (credential theft) vẫn là một trong những nguyên nhân hàng đầu gây ra các vụ xâm phạm an toàn thông tin hiện nay.

Các hệ thống quản lý mật khẩu truyền thống, dù được mã hóa, vẫn yêu cầu người dùng đặt niềm tin vào một bên trung gian quản lý dữ liệu. Điều này đặt ra yêu cầu cấp thiết về một kiến trúc bảo mật giảm thiểu sự phụ thuộc vào bên trung gian và tăng cường quyền kiểm soát dữ liệu cá nhân cho người dùng [13].

Xuất phát từ những hạn chế của mô hình quản lý mật khẩu tập trung, đề tài hướng tới nghiên cứu và xây dựng một ứng dụng quản lý mật khẩu an toàn theo hướng giảm thiểu sự phụ thuộc vào bên trung gian, tăng cường quyền kiểm soát dữ liệu cho người dùng và tích hợp cơ chế hỗ trợ đánh giá bảo mật hiện đại.

1.2 Mục tiêu nghiên cứu

- **Mục tiêu tổng quát:** Nghiên cứu và xây dựng một ứng dụng quản lý mật khẩu theo định hướng tăng cường bảo mật và quyền riêng tư, giúp người dùng chủ động kiểm soát và bảo vệ thông tin đăng nhập trong môi trường số.
- **Mục tiêu cụ thể:** Đề tài tập trung đề xuất và hiện thực hóa mô hình quản lý mật khẩu dựa trên cơ chế mã hóa phía client và xác thực dữ liệu bằng blockchain, với các nội dung

chính sau:

- *Về kỹ thuật:* Triển khai cơ chế mã hóa phía máy khách (Client-side encryption), đảm bảo nhà cung cấp dịch vụ không thể tiếp cận dữ liệu gốc của người dùng.
- *Về lưu trữ:* Lưu trữ dữ liệu đã mã hóa cục bộ phía trình duyệt, đồng thời sử dụng blockchain để lưu trữ giá trị băm (hash) của vault nhằm đảm bảo tính toàn vẹn và khả năng phát hiện thay đổi trái phép.
- *Về tính năng hỗ trợ:* Tích hợp công cụ ước lượng entropy thực nghiệm để đánh giá độ mạnh của mật khẩu, đưa ra các cảnh báo trực quan cho người dùng.
- *Về trải nghiệm:* Xây dựng giao diện thân thiện với hai phương thức xác thực: kết nối ví blockchain (MetaMask) và đăng nhập qua tài khoản xã hội (Google), phù hợp với đa dạng đối tượng người dùng.

1.3 Ý nghĩa

1.3.1 Giá trị học thuật (Ý nghĩa khoa học)

- **Mô hình bảo mật hướng người dùng:** Đề tài nghiên cứu và áp dụng mô hình mã hóa phía client kết hợp với cơ chế xác thực dữ liệu trên blockchain nhằm giảm thiểu sự phụ thuộc vào máy chủ trung tâm và hạn chế rủi ro rò rỉ dữ liệu.
- **Sự kết hợp công nghệ:** Đề tài góp phần phân tích tính khả thi của việc tích hợp công nghệ blockchain vào hệ thống ứng dụng Web truyền thống, trong đó blockchain đóng vai trò đảm bảo tính toàn vẹn dữ liệu thay vì lưu trữ dữ liệu nhạy cảm [2, 13].

1.3.2 Tính ứng dụng (Ý nghĩa thực tiễn)

- **Giải pháp bảo mật cá nhân:** Ứng dụng cung cấp một công cụ hỗ trợ người dùng quản lý mật khẩu an toàn hơn, góp phần giảm thiểu rủi ro từ các kịch bản rò rỉ dữ liệu và tấn công phổ biến [10].
- **Công cụ hỗ trợ nâng cao nhận thức bảo mật:** Thông qua việc tích hợp thư viện đánh giá độ mạnh mật khẩu dựa trên mô hình entropy thực nghiệm [12], hệ thống không chỉ lưu trữ mật khẩu mà còn hỗ trợ người dùng cải thiện thói quen bảo mật.
- **Khả năng mở rộng:** Mô hình được đề xuất có thể mở rộng cho các ứng dụng lưu trữ thông tin nhạy cảm khác như ghi chú bảo mật, quản lý tài liệu cá nhân hoặc các hệ thống xác thực số trong tương lai.

Chương 2

Cơ sở lý thuyết và công nghệ sử dụng

Chương này trình bày các nền tảng lý thuyết phục vụ việc xây dựng ứng dụng quản lý mật khẩu theo định hướng tăng cường bảo mật và quyền riêng tư. Trọng tâm nghiên cứu bao gồm:

- Cơ chế mã hóa phía máy khách.
- Phương pháp dẫn xuất và quản lý khóa an toàn.
- Cơ chế đảm bảo tính toàn vẹn dữ liệu bằng blockchain.

Blockchain và công cụ đánh giá mật khẩu đóng vai trò hỗ trợ trong việc hiện thực hóa kiến trúc bảo mật này.

2.1 Cơ sở lý thuyết

2.1.1 Mật mã học ứng dụng trong bảo vệ mật khẩu

Mật mã học đóng vai trò nền tảng trong các hệ thống bảo mật hiện đại [5]. Trong ứng dụng quản lý mật khẩu, dữ liệu cần được bảo vệ thông qua cơ chế mã hóa đối xứng mạnh nhằm đảm bảo tính bí mật (confidentiality).Thuật toán AES-256-GCM (Advanced Encryption Standard, 256-bit key, Galois/Counter Mode) được sử dụng nhờ tính an toàn, hiệu suất cao và khả năng xác thực toàn vẹn dữ liệu tích hợp [8]. Để tăng cường khả năng chống tấn công brute-force, khóa mã hóa được sinh từ mật khẩu chính thông qua hàm dẫn xuất khóa PBKDF2 (Password-Based Key Derivation Function 2).

- Hệ thống sẽ triển khai PBKDF2 theo khuyến nghị của tiêu chuẩn NIST SP 800-132 [9]. Cơ chế này áp dụng một hàm giả ngẫu nhiên (PRF) như HMAC-SHA256 kết hợp với một chuỗi muối (salt) ngẫu nhiên, thực hiện lặp lại nhiều lần để tạo ra khóa dẫn xuất an toàn.

- Công thức dẫn xuất khóa được thực thi dựa trên đặc tả kỹ thuật của RFC 8018 [6]:

$$DK = \text{PBKDF2}(PRF, Password, Salt, c, dkLen) \tag{2.1}$$

Trong đó:

- *DK*: Khóa dẫn xuất (Derived Key).
- *PRF*: Hàm giả ngẫu nhiên (Pseudorandom Function).
- *Password*: Mật khẩu gốc của người dùng.
- *Salt*: Chuỗi dữ liệu ngẫu nhiên chống tấn công Rainbow Table.
- *c*: Số lần lặp (Iteration count).
- *dkLen*: Độ dài khóa dẫn xuất mong muốn.

2.1.2 Kiến trúc mã hóa phía máy khách (Client-side Encryption)

Kiến trúc mã hóa phía máy khách là mô hình thiết kế hệ thống trong đó toàn bộ quá trình mã hóa và giải mã được thực hiện tại thiết bị người dùng đảm bảo nhà cung cấp dịch vụ không có khả năng truy cập dữ liệu gốc. Mô hình này được xây dựng trên ba nguyên tắc cốt lõi [1] :

- Dữ liệu được mã hóa tại thiết bị người dùng trước khi truyền đi.
- Khóa giải mã không bao giờ rời khỏi thiết bị người dùng.
- Nền tảng lưu trữ chỉ tiếp nhận bản mã và không có công cụ để giải mã chúng .

Kiến trúc này loại bỏ rủi ro "điểm yếu tập trung" — ngay cả khi hạ tầng lưu trữ bị xâm phạm, dữ liệu gốc vẫn được bảo vệ nhờ tính chất toán học của thuật toán mã hóa. Dữ liệu được cache cục bộ phía trình duyệt luôn ở dạng ciphertext, trong khi khóa mã hóa chỉ tồn tại trong bộ nhớ tạm của phiên làm việc hiện tại.

2.1.3 Cơ chế xác thực liên kết danh tính (Social Login)

Federated Authentication là mô hình xác thực trong đó ứng dụng ủy quyền việc xác minh danh tính cho một nhà cung cấp danh tính (Identity Provider – IdP) bên thứ ba thay vì tự quản lý thông tin đăng nhập. Chuẩn OAuth 2.0 (RFC 6749) [4] cung cấp nền tảng giao thức cho mô hình này.

Hệ thống triển khai thông qua Firebase Authentication [3] với Google là IdP. Sau khi xác thực thành công, hệ thống nhận được một mã định danh duy nhất (UID) dùng để định danh vault trong bộ nhớ cục bộ. Cơ chế này chỉ đảm nhiệm việc xác thực danh tính, không tham gia

vào quá trình mã hóa dữ liệu, toàn bộ bảo mật vẫn phụ thuộc vào Master Password phía máy khách.

2.1.4 Cơ chế xác thực toàn vẹn dữ liệu bằng Blockchain

Blockchain là hệ thống sổ cái phân tán với đặc tính bất biến và minh bạch, trong đó dữ liệu được lưu trữ trên nhiều nút mạng thay vì một máy chủ trung tâm [7]. Trong đề tài này, blockchain không đóng vai trò lưu trữ dữ liệu chính mà được sử dụng như một lớp xác thực tính toàn vẹn. Cụ thể, hash SHA-256 của vault đã mã hóa cùng timestamp được ghi lên smart contract trên Sepolia Testnet, cho phép người dùng tự xác minh dữ liệu cục bộ không bị can thiệp trái phép [2].

2.1.5 Công cụ phân tích dựa trên mô hình ước lượng entropy thực nghiệm

Việc người dùng sử dụng mật khẩu yếu là nguyên nhân phổ biến dẫn đến tấn công mạng [10]. Công cụ đánh giá độ mạnh mật khẩu dựa trên các thuật toán phân tích mẫu và ước lượng entropy (zxcvbn) giúp xác định mức độ an toàn của mật khẩu theo thời gian bẻ khóa ước tính [12].

2.2 Công nghệ sử dụng

2.2.1 Nền tảng Blockchain

Hệ thống sử dụng hạ tầng mạng lưới Ethereum [2] nhằm đảm bảo tính toàn vẹn dữ liệu thông qua hợp đồng thông minh:

- **Ngôn ngữ:** Solidity - ngôn ngữ lập trình hướng đối tượng chuyên dụng cho việc xây dựng hợp đồng thông minh.
- **Mạng thử nghiệm:** Sepolia Testnet - môi trường mô phỏng mạng chính thức để kiểm thử hiệu năng và bảo mật.
- **Công cụ phát triển:** Hardhat hoặc Remix IDE giúp quản lý vòng đời phát triển của mã nguồn.
- **Ví kết nối:** MetaMask đóng vai trò định danh và ký xác nhận các giao dịch trên mạng lưới.

Smart contract được thiết kế để lưu trữ hash SHA-256 của vault đã mã hóa kèm timestamp, phục vụ mục đích xác thực tính toàn vẹn dữ liệu thay vì lưu trữ ciphertext trực tiếp.

2.2.2 Frontend

Để đáp ứng yêu cầu xử lý phía máy khách (Client-side), hệ thống sử dụng bộ công cụ:

- **React.js:** Thư viện JavaScript hỗ trợ xây dựng giao diện người dùng theo kiến trúc thành phần.
- **Tailwind CSS:** Framework CSS tối ưu hóa quy trình thiết kế giao diện linh hoạt.
- **Ethers.js:** Thư viện trung gian kết nối ứng dụng với các nút mạng (nodes) của Blockchain. item Firebase Authentication SDK: Thư viện xác thực danh tính qua Google Sign-In, cung cấp UID dùng làm định danh người dùng [3].
- **Web Crypto API [11]:** API tích hợp sẵn trong trình duyệt, dùng để thực thi AES-256-GCM và PBKDF2 phía máy khách.

2.2.3 Công cụ đánh giá mật khẩu

Hệ thống sẽ tích hợp thư viện **zxcvbn-ts** dựa trên nghiên cứu về ước lượng entropy thực tế của mật khẩu [12]. Công cụ này cho phép phân tích độ mạnh mật khẩu dựa trên các mẫu (patterns) phổ biến mà không cần gửi dữ liệu về máy chủ, đảm bảo tính riêng tư tuyệt đối cho người dùng.

Chương 3

Phân tích yêu cầu dự án

Chương này trình bày toàn bộ phân tích yêu cầu cho hệ thống ứng dụng quản lý mật khẩu. Nội dung chương bao gồm: Đặc tả yêu cầu chức năng và phi chức năng.

3.1 Tổng quan dự án

Dự án tập trung vào việc cung cấp một nền tảng quản lý mật khẩu an toàn với các đặc điểm chính:

- Cung cấp giao diện để người dùng tạo, lưu trữ, cập nhật và truy xuất mật khẩu.
- Thực hiện mã hóa và giải mã dữ liệu hoàn toàn phía máy khách (client-side encryption).
- Lưu trữ vault đã mã hóa cục bộ phía trình duyệt; blockchain chỉ lưu giá trị băm (hash) của vault nhằm đảm bảo tính toàn vẹn dữ liệu.
- Hỗ trợ hai nhóm người dùng: người dùng quen thuộc với ví blockchain và người dùng phổ thông.
- Tích hợp công cụ đánh giá độ mạnh mật khẩu nhằm nâng cao nhận thức bảo mật.

Dự án không bao gồm: xây dựng hệ sinh thái ví blockchain hoàn chỉnh, triển khai Account Abstraction, phát triển mô hình AI, hay đồng bộ dữ liệu đa thiết bị. Blockchain chỉ đóng vai trò lưu trữ hash của vault nhằm xác thực tính toàn vẹn dữ liệu; công cụ đánh giá mật khẩu chỉ mang tính hỗ trợ. Người dùng có thể sao lưu thủ công bằng cách xuất vault đã mã hóa (export).

3.2 Yêu cầu dự án

3.2.1 Mô tả yêu cầu chức năng

Xác thực và định danh:

Người dùng:

+ Đăng nhập qua MetaMask hoặc Google Sign-In.
+ Nhập Master Password để mở vault sau khi xác thực.
+ Đăng xuất khi kết thúc phiên làm việc.

Hệ thống:

+ Xác thực chữ ký số với MetaMask hoặc xác minh token với Google.
+ Dẫn xuất khóa mã hóa từ Master Password qua PBKDF2.
+ Xóa khóa khỏi bộ nhớ tạm khi đăng xuất.

Quản lý mật khẩu:

Người dùng:

+ Xem danh sách, xem chi tiết, thêm, chỉnh sửa, xóa mục mật khẩu và tìm kiếm và lọc theo từ khóa
+ Xuất và nhập vault dưới dạng file mã hóa.

Hệ thống:

+ Mã hóa dữ liệu bằng AES-256-GCM trước khi lưu vào bộ nhớ cục bộ.
+ Tự động đánh giá độ mạnh mật khẩu khi thêm hoặc chỉnh sửa và đưa ra thông báo.
+ Cập nhật hash vault lên blockchain sau mỗi thay đổi.

Xác thực toàn vẹn dữ liệu:

Người dùng:

+ Đối chiếu hash cục bộ với giá trị trên blockchain khi cần kiểm tra.

Hệ thống:

+ Ghi hash SHA-256 của vault kèm timestamp lên smart contract.

+ Phát hiện và cảnh báo nếu dữ liệu cục bộ không khớp với hash trên blockchain.

3.2.2 Yêu cầu phi chức năng

Bảo mật:

+ Toàn bộ dữ liệu phải được mã hóa phía máy khách trước khi lưu trữ.
+ Master Password và khóa mã hóa không được lưu trữ dưới bất kỳ hình thức nào.
+ Dữ liệu trên blockchain chỉ chứa hash, không có thông tin nhạy cảm.

Khả dụng:

+ Giao diện thân thiện với cả người dùng Web3 lẫn người dùng phổ thông.
+ Thời gian phản hồi các thao tác của người dùng phải đảm bảo mượt mà trong điều kiện mạng ổn định.
+ Hoạt động ổn định trên các trình duyệt hiện đại hỗ trợ Web Crypto API.

Chương 4

Kế hoạch thực hiện dự án

- **Tuần 1–2: Nghiên cứu và thiết kế kiến trúc & UI/UX**
  - Nghiên cứu chuẩn mã hóa AES-256-GCM và hàm dẫn xuất khóa PBKDF2.
  - Tìm hiểu cơ chế Social Login, IndexedDB và nền tảng Ethereum.
  - Thiết kế sơ đồ luồng dữ liệu phía Client.
  - Xây dựng mô hình Actor và Use Case; thiết kế giao diện UI/UX.
- **Tuần 3–4: Phát triển Smart Contract**
  - Xây dựng Smart Contract bằng Solidity và triển khai lên Sepolia Testnet.
  - Tích hợp cơ chế Social Login phía frontend
- **Tuần 5–6: Phát triển Frontend**
  - Xây dựng ứng dụng React.js và tích hợp cơ chế mã hóa phía Client.
  - Tích hợp công cụ đánh giá entropy mật khẩu (zxcvbn-ts).
- **Tuần 7: Kiểm thử**
  - Kiểm thử toàn bộ Use Case và đánh giá tính bảo mật của dữ liệu đã mã hóa.
  - Tối ưu hiệu năng xử lý và trải nghiệm người dùng.
- **Tuần 8: Tổng kết**
  - Đánh giá kết quả đạt được, phân tích hạn chế và đề xuất hướng phát triển.
  - Hoàn thiện báo cáo và chuẩn bị nội dung thuyết trình.

Chương 5

Kết luận

Đề cương đã trình bày tổng quan về vấn đề bảo mật mật khẩu trong bối cảnh gia tăng các rủi ro an toàn thông tin, từ đó đề xuất hướng tiếp cận xây dựng một ứng dụng Web tăng cường bảo mật với cơ chế xác thực tính toàn vẹn bằng blockchain.

Hệ thống tập trung vào cơ chế mã hóa phía máy khách, xác thực linh hoạt cho người dùng phổ thông và lưu trữ vault đã mã hóa cục bộ tại trình duyệt và sử dụng Blockchain Ethereum để xác thực tính toàn vẹn dữ liệu thông qua hash. Bên cạnh đó, việc tích hợp công cụ đánh giá độ mạnh mật khẩu giúp nâng cao nhận thức bảo mật cho người dùng.

Trong giai đoạn tiếp theo, đề tài sẽ tiến hành nghiên cứu sâu, thiết kế, phát triển, kiểm thử và đánh giá hiệu năng – mức độ an toàn của hệ thống, từ đó hoàn thiện sản phẩm và báo cáo thực tập cơ sở.

Tài liệu tham khảo

[1] Bitwarden. Bitwarden security whitepaper. Bitwarden Documentation, 2024.

[2] Vitalik Buterin. A next-generation smart contract and decentralized application platform, 2014.

[3] Google Firebase. Firebase authentication. Firebase Documentation, 2024.

[4] D. Hardt. The OAuth 2.0 authorization framework. RFC 6749, IETF, 2012.

[5] Jonathan Katz and Yehuda Lindell. *Introduction to Modern Cryptography*. CRC Press, 3 edition, 2020.

[6] K. Moriarty, B. Kaliski, and A. Rusch. PKCS #5: Password-based cryptography specification version 2.1. RFC 8018, RFC Editor, 2017.

[7] Satoshi Nakamoto. Bitcoin: A peer-to-peer electronic cash system, 2008.

[8] National Institute of Standards and Technology. Advanced encryption standard (AES). FIPS Publication 197, National Institute of Standards and Technology, 2001.

[9] Meltem Sönmez Turan, Elaine Barker, William Burr, and Lily Chen. Recommendation for password-based key derivation: Part 1: Storage applications. NIST Special Publication 800-132, National Institute of Standards and Technology, 2010.

[10] Verizon. 2024 data breach investigations report. Technical report, Verizon Business, 2024.

[11] W3C. Web cryptography API. W3C Recommendation, 2017.

[12] Daniel Lowe Wheeler. zxcvbn: Low-budget password strength estimation. In *25th USENIX Security Symposium (USENIX Security 16)*, 2016.

[13] Guy Zyskind, Oz Nathan, and Alex Pentland. Decentralizing privacy: Using blockchain to protect personal data. In *2015 IEEE Security and Privacy Workshops*, pages 180–184. IEEE, 2015.