BỘ KHOA HỌC VÀ CÔNG NGHỆ

HỌC VIỆN CÔNG NGHỆ BƯU CHÍNH VIỄN THÔNG

ĐỀ CƯƠNG BÁO CÁO GIỮA KỲ

Thiết kế và triển khai DApp quản lý mật khẩu phi tập trung tích hợp cơ chế đánh giá độ mạnh mật khẩu

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 [9]. 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 [12]. 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 niềm tin (trustless) và tăng cường quyền kiểm soát dữ liệu cá nhân cho người dùng [12].

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 ứng dụng quản lý mật khẩu an toàn, sử dụng kiến trúc phi tập trung nhằm bảo vệ tối ưu thông tin đăng nhập của người dùng trong môi trường số.
- **Mục tiêu cụ thể:** Đề tài hướng đến đề xuất và hiện thực hóa một mô hình quản lý mật khẩu theo kiến trúc bảo mật hiện đại, đặt trọng tâm vào bảo mật quyền riêng tư, tính phi

tập trung và kiểm soát dữ liệu từ phía người dùng.

- *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:* Áp dụng công nghệ Blockchain để lưu trữ dữ liệu dưới dạng phi tập trung, giúp loại bỏ rủi ro mất mát thông tin khi máy chủ trung tâm gặp sự cố (SPOF).
- *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 ứng dụng theo hai cách để phù hợp cho cả người dùng quen thuộc với ví blockchain và người dùng phổ thông.

1.3 Ý nghĩa

1.3.1 Giá trị học thuật (Ý nghĩa khoa học)

- **Mô hình bảo mật phi tập trung:** Đề tài hệ thống hóa lý thuyết về việc áp dụng kiến trúc Trustless vào quản lý danh tính số. Cơ chế mã hóa phía máy khách đảm bảo hệ thống không có khả năng truy cập dữ liệu gốc của người dùng ngay cả khi hạ tầng bị xâm phạm.
- **Sự kết hợp công nghệ:** Giá trị học thuật nằm ở việc nghiên cứu tính tương thích giữa tốc độ xử lý phía Client và tính toàn vẹn của dữ liệu trên mạng lưới Blockchain [4, 12].

1.3.2 Tính ứng dụng (Ý nghĩa thực tiễn)

- **Giải pháp bảo mật cá nhân:** Ứng dụng cung cấp một công cụ thực tế giúp người dùng bảo vệ tài sản số trước các kịch bản tấn công phổ biến. [9].
- **Công cụ đánh giá bảo mật:** Bằng cách tích hợp thư viện zxcvbn-ts dựa trên mô hình ước lượng entropy thực nghiệm [11], ứng dụng không chỉ là nơi lưu trữ mà còn là công cụ giúp người dùng nhận biết và hạn chế rủi ro từ việc sử dụng mật khẩu yếu.
- **Định hướng người dùng:** Ứng dụng hướng tới việc phục vụ đa dạng đối tượng người dùng:
  - Người dùng quen thuộc với ví blockchain: Những người đã quen thuộc với ví điện tử như MetaMask có thể sử dụng ứng dụng như một lớp bảo mật bổ sung cho các tài khoản Web2 của họ.
  - Người dùng phổ thông (Mainstream): Để tối ưu hóa trải nghiệm người dùng mà vẫn đảm bảo tính phi tập trung, hệ thống tích hợp giải pháp Web3Auth. Đây là một cơ sở

hạ tầng quản lý khóa phân tán dựa trên kỹ thuật mật mã ngưỡng (Threshold Cryptography) và tính toán đa bên (Multi-Party Computation - MPC) [10]. Web3Auth cho phép người dùng đăng nhập bằng các định danh quen thuộc (như Google, Facebook).

- **Khả năng mở rộng:** Mô hình này có thể ứng dụng rộng rãi cho các hệ thống quản lý ghi chú bảo mật, ví tiền mã hóa hoặc lưu trữ tài liệu nhạy cảm của doanh nghiệp.

Chương 2

Cơ sở lý thuyết và công nghệ sử dụng

Chương này tập trung làm rõ các nền tảng lý thuyết cốt lõi phục vụ mục tiêu chính của đề tài, đó là xây dựng kiến trúc mã hóa phía máy khách cho ứng dụng quản lý mật khẩu phi tập trung. Trong đó, trọng tâm nghiên cứu bao gồm:

- Cơ chế mã hóa phía client.
- Phương pháp dẫn xuất và quản lý khóa an toàn.
- Mô hình lưu trữ phi tập trung nhằm giảm thiểu rủi ro điểm lỗi đơn.

Các công nghệ như Blockchain và công cụ đánh giá mật khẩu chỉ 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 [2]. 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 [5]. 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 [8]. 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.

- Nhằm đối phó với sức mạnh tính toán từ các phần cứng hiện đại như NVIDIA RTX 4090, số lần lặp (c) được thiết lập tuân thủ theo khuyến cáo mới nhất của OWASP (2023) [6], với mức tối thiểu là 600.000 vòng lặp cho biến thể PBKDF2-HMAC-SHA256. Điều này giúp gia tăng đáng kể chi phí tính toán cho các cuộc tấn công vét cạn (brute-force).
- Công thức dẫn xuất khóa được thực thi dựa trên đặc tả kỹ thuật của RFC 8018 [3]:

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

  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 :

- 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" vì ngay cả khi hạ tầng lưu trữ bị xâm phạm, dữ liệu gốc vẫn được bảo vệ nhờ tính chất toán học của các thuật toán mã hóa.

2.1.3 Hạ tầng quản lý khóa phân tán (DKMS)

Hệ thống quản lý khóa phân tán dựa trên kỹ thuật Tính toán đa bên (Multi-Party Computation - MPC) cho phép bảo mật khóa bí mật mà không cần lưu trữ tập trung [10]. Nguyên lý này thường dựa trên giao thức chia sẻ bí mật của Shamir (Shamir's Secret Sharing), trong đó một bí mật được chia thành n phần riêng biệt và chỉ có thể khôi phục khi tập hợp đủ số lượng ngưỡng t phần ($t \leq n$) [7]. Cơ chế này đảm bảo tính không lưu ký (Non-custodial), giúp người dùng duy

trì quyền kiểm soát khóa cá nhân thông qua các định danh xã hội mà không cần trực tiếp quản lý cụm từ hạt giống (seed phrase).

2.1.4 Mô hình lưu trữ phi tập trung trên Blockchain

Blockchain là hệ thống sổ cái phân tán, trong đó dữ liệu được lưu trữ trên nhiều nút mạng thay vì một máy chủ trung tâm [4]. Đặc tính phi tập trung và bất biến của blockchain giúp giảm thiểu rủi ro "Single Point of Failure" và đảm bảo tính toàn vẹn dữ liệu [12]. Trong đề tài này, blockchain đóng vai trò là lớp lưu trữ các bản ghi đã được mã hóa thông qua nền tảng hợp đồng thông minh [1].

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 [9]. 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 [11].

2.2 Công nghệ sử dụng

2.2.1 Nền tảng Blockchain

Hệ thống sử dụng hạ tầng mạng lưới **Ethereum** [1] để triển khai các logic nghiệp vụ phi tập trung:

- **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 sẽ được thiết kế để lưu trữ dữ liệu đã mã hóa (ciphertext), tuân thủ nghiêm ngặt nguyên tắc không lưu trữ khóa giải mã hay dữ liệu nhạy cảm dưới dạng bản rõ.

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.

2.2.3 Cơ chế mã hóa

Tính bảo mật của dữ liệu dựa trên các tiêu chuẩn mã hóa quốc tế:

- **AES-256-GCM:** Thuật toán mã hóa đối xứng đạt chuẩn FIPS 197 [5], được triển khai thông qua Web Crypto API. Chế độ GCM (Galois/Counter Mode) cung cấp đồng thời tính bảo mật (confidentiality) và xác thực toàn vẹn dữ liệu (authenticated encryption), đảm bảo phát hiện mọi can thiệp trái phép vào bản mã.
- **PBKDF2:** Hàm dẫn xuất khóa đạt chuẩn NIST SP 800-132 [8] được sử dụng để tạo khóa mã hóa từ mật khẩu chính (Master Password), giúp chống lại các cuộc tấn công brute-force và dictionary.

Toàn bộ quy trình mã hóa AES-256-GCM [5] và dẫn xuất khóa PBKDF2 [8] được thực thi tại máy khách, đảm bảo nhà cung cấp dịch vụ không có khả năng truy cập dữ liệu gốc.

2.2.4 Hạ tầng quản lý khóa và định danh

Để hiện thực hóa kiến trúc quản lý khóa phân tán và tối ưu hóa quy trình Onboarding, dự án sử dụng các bộ giải pháp sau:

- **Web3Auth SDK:** Sử dụng làm lớp cơ sở hạ tầng để quản lý khóa thông qua MPC. SDK này cho phép tích hợp các phương thức đăng nhập xã hội (Social Login) và tạo khóa riêng tư dưới dạng không lưu ký (non-custodial).
- **Khởi tạo khóa (Key Reconstruction):** Quá trình tập hợp các mảnh khóa (shares) được thực hiện hoàn toàn trong bộ nhớ tạm của trình duyệt, đảm bảo khóa đầy đủ không bao giờ được gửi lên máy chủ.

2.2.5 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 [11]. 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 phi tập trung. Nội dung chương bao gồm: xác định các tác nhân (actor), đặc tả yêu cầu chức năng và phi chức năng, sơ đồ usecase tổng quát.

3.1 Tổng quan dự án

3.1.1 Phạm vi 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 dữ liệu dưới dạng đã mã hóa trên một hạ tầng lưu trữ phi tập trung (Blockchain Ethereum).
- 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 triển khai cơ chế quản trị viên (admin) và không cho phép bất kỳ bên trung gian nào truy cập dữ liệu gốc của người dùng.

Dự án không hướng tới xây dựng một hệ sinh thái ví Blockchain hoàn chỉnh, không triển khai cơ chế tài khoản trừu tượng (Account Abstraction), và không phát triển mô hình AI phức tạp. Blockchain được sử dụng thuần túy như một lớp lưu trữ phi tập trung cho dữ liệu đã mã

hóa, trong khi công cụ đánh giá mật khẩu chỉ đóng vai trò hỗ trợ nâng cao nhận thức bảo mật.

3.2 Actor (Tác nhân)

3.2.1 Actor chính

Bảng 3.1: Các tác nhân (Actors) tham gia hệ thống

Actor	**Vai trò**	**Mô tả**	**Phương thức xác thực**
Người dùng Web3-native	Người dùng chính	Người dùng đã quen thuộc với ví blockchain (ví dụ: MetaMask), tự quản lý private key và ký giao dịch trực tiếp trên mạng Ethereum.	MetaMask + chữ ký số
Người dùng phổ thông	Người dùng chính	Người dùng không có kiến thức chuyên sâu về blockchain; đăng nhập thông qua tài khoản xã hội (Google, Facebook, v.v.) nhờ cơ chế MPC của Web3Auth.	Social Login
Mạng Ethereum	Actor bên ngoài	Hệ thống blockchain thực hiện lưu trữ dữ liệu đã mã hóa và xác thực giao dịch; không thể truy cập nội dung plaintext của mật khẩu.	Cơ chế đồng thuận Blockchain

3.2.2 Giả định về actor

- Người dùng quen thuộc với ví blockchain tự chịu trách nhiệm bảo vệ private key và seed phrase của MetaMask; hệ thống không có khả năng khôi phục nếu người dùng làm mất khóa.
- Người dùng phổ thông ủy quyền quản lý khóa cho Web3Auth; khóa được tái tạo thông qua cơ chế MPC và không bao giờ tồn tại đầy đủ tại một thực thể đơn lẻ.
- Người dùng không chia sẻ Master Password cho bên thứ ba và hiểu rằng hệ thống không lưu trữ Master Password dưới bất kỳ hình thức nào.

- Giả định môi trường thực thi phía client (trình duyệt) là đáng tin cậy tại thời điểm sử dụng, và không bị can thiệp bởi mã độc.
- Người dùng có trách nhiệm bảo mật thiết bị cá nhân (máy tính, điện thoại) khỏi malware, keylogger hoặc truy cập trái phép.
- Hệ thống Ethereum hoạt động đúng theo cơ chế đồng thuận (consensus), đảm bảo tính toàn vẹn dữ liệu và không bị kiểm soát bởi một thực thể đơn lẻ.
- Không có actor admin hay superuser — hệ thống vận hành theo kiến trúc phi tập trung và không tồn tại thực thể có quyền truy cập hoặc can thiệp vào dữ liệu người dùng.

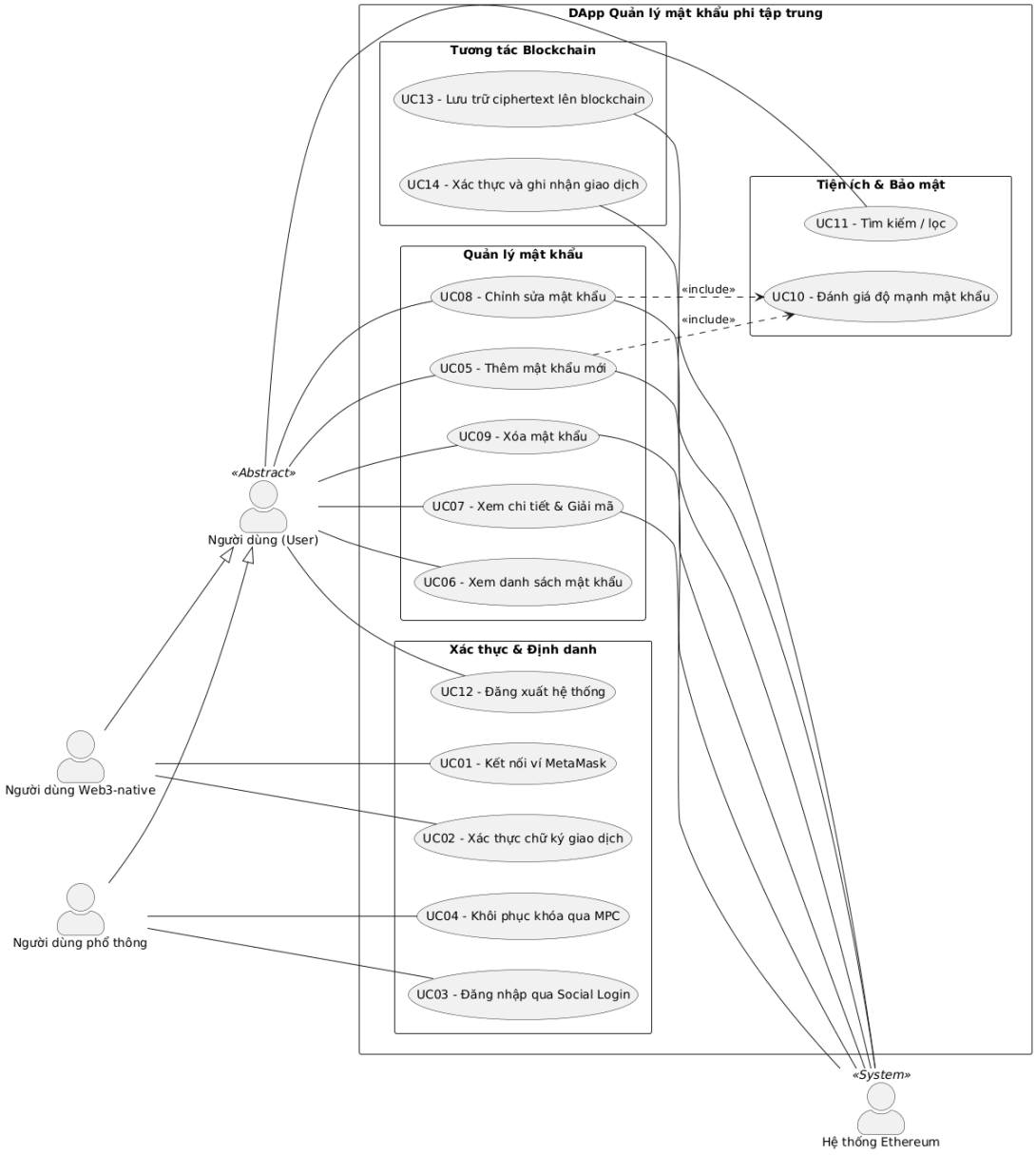
3.3 Sơ đồ usercase

3.3.1 Danh sách Use Case

- **Người dùng quen thuộc với ví blockchain**
  - UC01 – Kết nối ví MetaMask
  - UC02 – Xác thực chữ ký giao dịch
- **Người dùng phổ thông**
  - UC03 – Đăng nhập qua Social Login (Google/Facebook)
  - UC04 – Khôi phục khóa thông qua cơ chế MPC
- **Cả hai loại người dùng**
  - UC05 – Thêm mật khẩu mới
  - UC06 – Xem danh sách mật khẩu
  - UC07 – Xem chi tiết và giải mã mật khẩu
  - UC08 – Chỉnh sửa mật khẩu
  - UC09 – Xóa mật khẩu
  - UC10 – Đánh giá độ mạnh mật khẩu
  - UC11 – Tìm kiếm / lọc mật khẩu
  - UC12 – Đăng xuất hệ thống
- **Hệ thống Ethereum (Actor bên ngoài)**

- UC13 – Lưu trữ dữ liệu đã mã hóa (ciphertext) lên blockchain
- UC14 – Xác thực và ghi nhận giao dịch

3.3.2 Sơ đồ tổng quát



Hình 3.1: Sơ đồ Use Case tổng quát của hệ thống

3.4 Yêu cầu dự án

3.4.1 Yêu cầu chức năng (Functional Requirements)

Các yêu cầu chức năng được phân loại theo nhóm nghiệp vụ chính của hệ thống. Mức độ ưu tiên được đánh giá theo thang MoSCoW: M (Must have), S (Should have), C (Could have).

Nhóm chức năng Xác thực và Định danh

- **FR-01 (M)**: Hệ thống phải cho phép người dùng xác thực thông qua ví blockchain.
- **FR-02 (M)**: Hệ thống phải hỗ trợ đăng nhập thông qua tài khoản mạng xã hội.
- **FR-03 (M)**: Sau khi xác thực, hệ thống yêu cầu người dùng nhập Master Password để truy cập dữ liệu đã mã hóa.
- **FR-04 (M)**: Hệ thống phải cho phép người dùng đăng xuất và kết thúc phiên làm việc.

Nhóm chức năng Quản lý mật khẩu

- **FR-05 (M)**: Người dùng có thể thêm mục mật khẩu mới.
- **FR-06 (M)**: Hệ thống hiển thị danh sách các mục mật khẩu thuộc người dùng hiện tại.
- **FR-07 (M)**: Người dùng có thể xem chi tiết một mục mật khẩu.
- **FR-08 (M)**: Người dùng có thể chỉnh sửa thông tin mật khẩu.
- **FR-09 (M)**: Người dùng có thể xóa một mục mật khẩu.
- **FR-10 (S)**: Hệ thống hỗ trợ tìm kiếm và lọc mật khẩu theo từ khóa.
- **FR-11 (S)**: Hệ thống cho phép sao chép mật khẩu tạm thời vào clipboard.

Nhóm chức năng Đánh giá bảo mật mật khẩu

- **FR-12 (M)**: Hệ thống phải phân tích và đánh giá độ mạnh mật khẩu khi người dùng nhập.
- **FR-13 (M)**: Hệ thống hiển thị cảnh báo trực quan đối với mật khẩu yếu.
- **FR-14 (C)**: Hệ thống cung cấp thống kê tổng quan về tình trạng mật khẩu của người dùng.

3.4.2 Yêu cầu phi chức năng (Non-Functional Requirements)

Yêu cầu bảo mật

- **NFR-01**: Dữ liệu nhạy cảm phải được mã hóa trước khi rời khỏi thiết bị người dùng.
- **NFR-02**: Hệ thống không lưu trữ Master Password dưới bất kỳ hình thức nào.
- **NFR-03**: Dữ liệu lưu trữ trên hạ tầng phi tập trung phải ở dạng đã mã hóa.
- **NFR-04**: Khóa mã hóa chỉ tồn tại trong bộ nhớ tạm của phiên làm việc.

Yêu cầu hiệu năng

- **NFR-05**: Thời gian phản hồi cho các thao tác thêm, sửa, xem mật khẩu phải đảm bảo trải nghiệm người dùng mượt mà trong điều kiện mạng ổn định.

Yêu cầu khả dụng

- **NFR-06**: Giao diện phải thân thiện với cả người dùng quen thuộc Web3 và người dùng phổ thông.
- **NFR-07**: Hệ thống phải hoạt động trên các trình duyệt hiện đại.

Chương 4

Kế hoạch thực hiện dự án

4.1 Lộ trình triển khai chi tiết

- **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 kiến trúc MPC của Web3Auth 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 quản lý khóa phân tán (DKMS) thông qua Web3Auth.
- **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 DApp quản lý mật khẩu theo kiến trúc phi tập trung.

Hệ thống tập trung vào cơ chế mã hóa phía máy khách, quản lý khóa phân tán thông qua Web3Auth và lưu trữ dữ liệu đã mã hóa trên Blockchain Ethereum nhằm giảm thiểu rủi ro điểm lỗi đơn (Single Point of Failure). 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 triển khai, 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] Vitalik Buterin. A next-generation smart contract and decentralized application platform, 2014.

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

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

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

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

[6] OWASP Foundation. Password storage cheat sheet, 2023.

[7] Adi Shamir. How to share a secret. *Communications of the ACM*, 22(11):612–613, 1979.

[8] 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.

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

[10] Web3Auth. Understanding Web3Auth: Multi-party computation (MPC) architecture, 2024.

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

[12] 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.