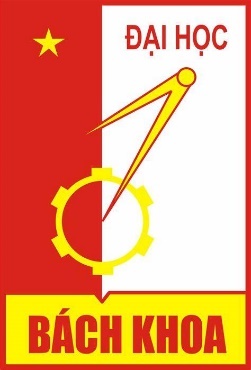
TRƯỜNG ĐẠI HỌC BÁCH KHOA HÀ NỘI

**VIỆN ĐÀO TẠO LIÊN TỤC**

-----🙞🙜🕮🙞🙜-----

**BÁO CÁO PROJECT 2**

**Tìm hiểu, áp dụng Google Authenticator xây dựng website có cơ chế xác thực hai yếu tố**

|  |  |
| --- | --- |
| *Giáo viên hướng dẫn:* | **ThS. Bùi Trọng Tùng** |
| *Sinh viên thực hiện:* | **Phạm Thành Vân** |
|  |  |

**Hà Nội 12/2020**

MỤC LỤC

[DANH MỤC HÌNH ẢNH 2](#_Toc59477756)

[DANH MỤC BẢNG 3](#_Toc59477757)

[LỜI MỞ ĐẦU 4](#_Toc59477758)

[CHƯƠNG 1. Phân tích bài toán 5](#_Toc59477759)

[CHƯƠNG 2. Thiết kế giải pháp 6](#_Toc59477760)

[CHƯƠNG 3. Thử nghiệm, đánh giá 7](#_Toc59477761)

[KẾT LUẬN 8](#_Toc59477762)

# DANH MỤC HÌNH ẢNH

[Hình 1. Cấu trúc 1 trang HTML và hiển thị trên trình duyệt 6](#_Toc57058883)

[Hình 2. Trang HTML có sử dụng CSS 8](#_Toc57058884)

[Hình 3. Virtual DOM 9](#_Toc57058885)

[Hình 4. One-way data binding 10](#_Toc57058886)

[Hình 5. Kiến trúc hệ thống 12](#_Toc57058887)

[Hình 6. Các bảng và quan hệ giữa các bảng trong CSDL 13](#_Toc57058888)

[Hình 7. Màn hình đăng ký tài khoản 15](#_Toc57058889)

[Hình 8. Màn hình đăng nhập 16](#_Toc57058890)

[Hình 9. Giao diện chính của phần mềm 16](#_Toc57058891)

[Hình 10. Tải file lên để thực hiện số hóa 17](#_Toc57058892)

[Hình 11. Các file tải lên được đưa vào danh sách xử lý 17](#_Toc57058893)

[Hình 12. Hệ thống thông báo lỗi khi có file không nhận dạng được 18](#_Toc57058894)

# DANH MỤC BẢNG

[Bảng 1. Bảng User 14](#_Toc56427039)

[Bảng 2. Bảng Job 15](#_Toc56427040)

[Bảng 3. Bảng FileStorage 16](#_Toc56427041)

# LỜI MỞ ĐẦU

Hiện nay, khi internet đã trở nên phổ biến, nhu cầu sử dụng các dịch vụ, trao đổi thông tin, dữ liệu của người dùng qua mạng đang tăng lên ngày một mạnh mẽ. Bên cạnh những lợi ích mà internet mang lại cũng tiềm ẩn những hiểm họa và nguy cơ mất an toàn như tài khoản cá nhân có thể bị đánh cắp và sử dụng mào mục đích bất hợp pháp. Chính vì vậy, có rất nhiều giải pháp nhằm đảm bảo an toàn cho thông tin của người sử dụng được triển khai và thiết lập như quản lý tài khoản người dùng thông qua username và password, xác thực khi truy cập và sử dụng dịch vụ, một số giải pháp bảo vệ hệ thống như sử dụng hệ thống pháp hiện xâm nhập, tường lửa để ngăn chặn và cảnh báo truy cập trái phép vào hệ thống, các công cụ quét và phát hiện mã độc hại, v.v. trong đó thì phương pháp xác thực danh tính người dung khi sử dụng một dịch vụ trên mạng là một điều quan trọng, giup đảm bỏa an toàn cho hệ thống cũng như đảm bảo thông tin riêng cho người dùng.

Xác thực danh tính là tạo ra liên kết giữa định danh và đối tượng, thực thể. Xác thực danh tính được thực hiện qua 2 bước:

* Chủ thể cung cấp một định danh trong hệ thống
* Chủ thể cung cấp thông tin xác thực có thể chứng minh sự liên kết giữa định danh và chủ thể

Các phương pháp xác thực chính:

* Cái chủ thể biết
* Cái chủ thể có
* Chủ thể là gì
* Vị trí của chủ thể

Đối với phương pháp xác thực phổ biến là sử dụng tài khoản đăng nhập của người dùng gồm username và password đã bộ lộ những điểm yếu khi có thể bị đánh cắp trong trường hợp máy tính của người dùng bị cài đặt các phần mềm, chương trình có khả năng đánh cắp dữ liệu, hay trong quá trình trao đổi thông tin qua mạng bị nghe lén trên đường truyền, bị chuyển hướng đến trang web chứa mã độc hại, v.v. Để đảm bảo an toàn hơn cho người dùng, các nhà cung cấp dịch vụ đã áp dụng những phương pháp xác thực mạnh hơn khi kết hợp các yếu tố có được từ người dùng như username, password, mã PIN, đặc điểm sinh trắc học, v.v. Trong đó, phương pháp xác thực hai nhân tố với mật khẩu sử dụng một lần (OTP) kết hợp thông tin về username, password của người dùng hiện đang được áp dụng phổ biến.

Project này sẽ tìm hiểu, áp dụng Google Authenticator để xây dựng một website có cơ chế xác thực hai yếu tố với username, password và OTP khi người dùng đăng nhập vào hệ thống.

Nội dung của project bao gồm:

* Chương 1: Phân tích bài toán.

Phân tích các mối đe dọa với phương pháp xác thực bằng username, password truyền thống. Trình bày về xác thực hai yếu tố.

* Chương 2: Thiết kế giải pháp.

Trình bày use cases, mô tả hoạt động của việc xác thực hai yếu tố trong hệ thống, biểu đồ lớp, thiết kế cơ sở dữ liệu.

* Chương 3: Thử nghiệm, đánh giá.

Mô tả hoạt động của phần mềm thử nghiệm xác thực hai yếu tố.

# CHƯƠNG 1. Phân tích bài toán

## Hệ thống xác thực bằng mật khẩu

Các thành phần của hệ xác thực bao gồm:

**A**: Tập các thông tin đặc trưng mà chủ thể sử dụng để chứng minh định danh của mình.

**C**: Tập các thông tin mà hệ thống lưu trữ và sử dụng để xác minh sự đúng đắn của thông tin trong tập **A**.

**F**: Tập các hàm sinh **C** từ **A**

**L**: Tập các hàm xác thực

**S**: Tập các hàm lựa chọn cho phép các thực thể tạo hoặc thay thế các thông tin trong **A** và **C**.

Hệ xác thực mật khẩu, giả sử mật khẩu lưu dưới dạng rõ:

**A**: tập các chuỗi ký tự được chấp nhận là mật khẩu.

**C = A**

**F**: hàm đồng nhất thức I

**L**: hàm so sánh =

**S**: hàm thiết lập, thay đổi mật khẩu.

## Đe dọa đối với phương thức xác thực bằng mật khẩu

Một số điểm yếu trên hệ thống xác thực bằng mật khẩu:

* Lưu trữ mật khẩu trong CSDL không an toàn.
* Truyền mật khẩu trên kênh không an toàn
* Người dùng không cẩn trọng:
  + Sử dụng mật khẩu yếu
  + Ghi chép mật khẩu vào văn bản
  + Chi sẻ mật khẩu cho người khác (vô tình hoặc cố ý)
  + v.v.

Thông thường, chúng ta thường đổ lỗi cho người dùng khi họ sơ ý bị kẻ tấn công khai thác. Tuy nhiên, chúng ta cần xây dựng hệ thống có khả năng hỗ trợ người dùng không hành động sai.

* **Tấn công vào hệ xác thực bằng mật khẩu**
* Tấn công thụ động: nghe lén, quan sát quá trình nhập mật khẩu
  + Nhìn trộm
  + Sử dụng chương trình key logging
  + Tấn công kênh bên
  + Chặn bắt gói tin
* Tấn công chủ động:
  + Giả mạo chương trình cung cấp dịch vụ (server)
  + Giả mạo chương trình khách (client)
  + Tấn công man-in-the-middle
  + Tấn công vào máy chủ vật lý cung cấp dịch vụ
* **Tấn công dạng online**
* Kẻ tấn công biết tập hàm xác thực **L**
* Mục đích: dò thử lần lượt các mật khẩu dựa trên kết quả xác thực hệ thống trả lại
* Đặc điểm:
  + Tương tác trực tiếp với hệ xác thực
  + Có thể thử trên 1 hoặc đồng thời nhiều tài khoản
* Xác suất tấn công thành công:
  + G: tốc độ kẻ tấn công dò thử
  + T: thời gian kẻ tấn công dò thử
  + N: số mật khẩu hệ thống có thể tạo ra
* Giảm thiểu:
  + Tăng độ dài của mật khẩu
  + Quy định số lần thử xác thực tối đa trong một khoảng thời gian
* **Tấn công dạng off-line**
* Kẻ tấn công biết:
  + Tập thông tin **C** hệ thống dùng để xác thực
  + Các hàm biến đổi **F**
* Mục tiêu: tìm các thông tin
* Đặc điểm: không tương tác với hệ xác thực
* Ví dụ: kẻ tấn công biết có CSDL chứa mã băm của mật khẩu vả hàm băm sử dụng.
* Nguy cơ: người dùng sử dụng các mật khẩu dễ đoán, kẻ tấn công có một bộ từ điển chứa mã băm tương ứng
* Giảm thiểu nguy cơ: băm mật khẩu với “salt”
* **Một số chính sách sử dụng mật khẩu**

Mục đích: tăng cường an toàn cho hệ xác thực dựa trên mật khẩu

* Quy định độ dài tối thiểu
* Quy định các ký tự bắt buộc phải sử dụng
* Thay đổi mật khẩu định kỳ
* Hạn chế sử dụng lại mật khẩu cũ trong một khoảng thời gian nhất định
* Hạn chế số lần thử xác thực
* Tăng thời gian chờ thử xác thực lại
* Yêu cầu đổi mật khẩu sau lần đăng nhập đầu tiên

## Xác thực đa yếu tố

Phương pháp xác thực sử dụng mật khẩu không đủ an toàn, nguyên nhân chủ yếu từ người dùng. Để sử dụng mật khẩu một cách an toàn như sử dụng mật khẩu đủ dài và khó đoán, không dùng chung cho nhiều tài khoản, thay đổi thường xuyên, v.v. thì hầu hết người dùng không thực hiện được. Vì vậy, cần thêm các yếu tố xác thực an toàn hơn, không phụ thuộc vào thói quen của người dùng. Mức độ an toàn, bảo mật càng cao khi số yếu tố xác thực càng nhiều. Tuy nhiên, khi số yếu tố xác thực lớn thì hệ thống càng phức tạp, kéo theo chi phí đầu tư và duy trì vận hành tốn kém, đồng thời lại bất tiện cho người sử dụng. Do vậy, trên thực tế để cân bằng giữa an toan, bảo mật và tính tiện dụng, hiện nay sử dụng phổ biến nhất là xác thực 2 yếu tố:

* Cái người dùng biết: mật khẩu
* Cái người dùng có: thường là thiết bị phần cứng.

Ví dụ như xác thực chủ thẻ trong giao dịch ATM, yếu tố xác thực đầu tiên của khách hàng là thẻ ATM (cái khách hang có), sau khi đưa thẻ vào máy, khách hàng sẽ phải đưa tiếp yếu tố xác thực thứ hai là số PIN (cái khách hàng biết). Một ví dụ khác là xác thực người sử dụng dịch vụ giao dịch Internet Banking: khách hàng đăng nhập với username và password sau đó còn phải cung cấp tiếp OTP (One Time Password) được sinh ra trên token riêng của khách hàng.

* **Mật khẩu sử dụng một lần (One Time Password - OTP)**

Mật khẩu sử dụng một lần là loại mật khẩu chỉ dùng một lần và chỉ có giá trị cho một phiên đăng nhập hoặc cho một giao dịch trong một khoảng thời gian nhất định.

Mục đích của mật khẩu OTP là làm cho mật khẩu lúc nào cũng thay đổi, tránh việc kẻ tấn công dễ dàng đánh cắp tài khoản của người dùng và sử dụng vào mục đích bất hợp pháp. Yêu cầu đối với mật khẩu OTP là có thể chống lại được cách thức tấn công phát lại, có nghĩa là trong trường hợp có được thông tin về OTP trong một phiên làm việc thì cũng không thể sử dụng nó trong phiên làm việc kế tiếp, không thể đoán được mật khẩu tiếp theo để sử dụng.

Phân loại:

* S/Key OTP
* Hased-based OTP (HOTP)
* Time-based OTP (TOTP)

Cách thức phân phối:

* SMS
* Ứng dụng
* Email
* Token

Trong project sẽ sử dụng xác thực 2 yếu tố dựa trên mật khẩu và TOTP sinh bởi ứng dụng Google Authenticator trên điện thoại của người dùng.

# CHƯƠNG 2. Thiết kế giải pháp

# CHƯƠNG 3. Thử nghiệm, đánh giá

# KẾT LUẬN