

**Hệ thống xác thực dựa vào mặt người
Tài liệu đặc tả trường hợp sử dụng**

Revision History

Date	Version	Description	Author

Nội dung

1. Giới thiệu.....	4
2. Bối cảnh	4
3. Phạm vi.....	4
3.1. <i>Use-case diagram</i>	4
3.2. <i>Hệ thống xác thực bằng khuôn mặt sẽ bao gồm các “Actor”</i>	5
3.3. <i>Danh sách Use-case:</i>	5
4. Mô tả danh sách Use-case	5
4.1. <i>Đăng nhập bằng email và mật khẩu</i>	5
4.2. <i>Đăng kí tài khoản cho người dùng mới</i>	6
4.3. <i>Đăng nhập bằng khuôn mặt</i>	6
4.4. <i>Bật tính năng xác thực bằng khuôn mặt</i>	7
4.5. <i>Tắt tính năng xác thực bằng khuôn mặt</i>	7
4.6. <i>Đăng xuất</i>	8

Tài liệu đặc tả trường hợp sử dụng

1. Giới thiệu

Hệ thống xác thực khuôn mặt là một giải pháp bảo mật hiện đại, được phát triển nhằm tăng cường tính an toàn và tiện lợi cho người dùng khi đăng nhập vào hệ thống. Thông qua việc sử dụng công nghệ nhận diện khuôn mặt, hệ thống cho phép người dùng dễ dàng và nhanh chóng xác thực danh tính của mình mà không cần phải nhớ mật khẩu phức tạp.

Hệ thống được thiết kế để tích hợp trên các nền tảng web và di động, giúp các doanh nghiệp nâng cao khả năng bảo mật và giảm rủi ro về tấn công bảo mật như ăn cắp mật khẩu. Các nhóm người dùng chính bao gồm nhân viên, quản trị viên hệ thống và khách hàng doanh nghiệp.

2. Bối cảnh

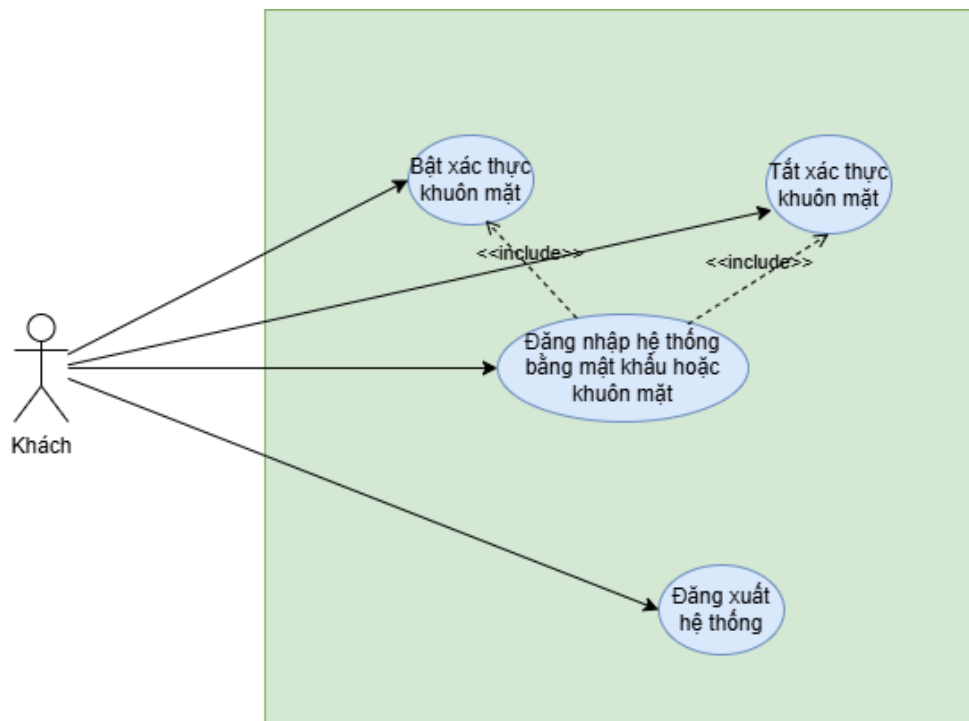
Với sự phát triển của công nghệ nhận diện khuôn mặt, nhiều tổ chức và doanh nghiệp đang dần chuyển sang các giải pháp xác thực phi truyền thống nhằm nâng cao bảo mật. Hệ thống xác thực khuôn mặt sẽ được tích hợp vào nền tảng ứng dụng quản lý doanh nghiệp, giúp nhân viên đăng nhập và bảo mật dữ liệu dễ dàng hơn mà không cần phải sử dụng mật khẩu.

Trong môi trường doanh nghiệp, việc bảo vệ dữ liệu khách hàng và thông tin nội bộ là rất quan trọng. Hệ thống này cung cấp một cách tiếp cận nhanh chóng và an toàn, đồng thời giảm thiểu sự phụ thuộc vào các yếu tố bảo mật dễ bị tổn thương như mật khẩu. Hệ thống cũng tích hợp với các giải pháp bảo mật hiện có như quản lý truy cập dựa trên vai trò và mã hóa dữ liệu đầu cuối.

Các bên liên quan chính bao gồm quản trị viên hệ thống, người dùng doanh nghiệp, và đội ngũ IT chịu trách nhiệm duy trì và quản lý hệ thống.

3. Phạm vi

3.1. Use-case diagram



3.2. Hệ thống xác thực bằng khuôn mặt sẽ bao gồm các “Actor”

Actor ID	Actor
A01	Khách

3.3. Danh sách Use-case:

Use-case ID	Description
UC01	Đăng nhập bằng email và mật khẩu
UC02	Đăng kí tài khoản cho người dùng mới
UC03	Đăng nhập bằng khuôn mặt
UC04	Bật tính năng xác thực bằng khuôn mặt
UC05	Tắt tính xác thực bằng khuôn mặt (Chỉ sử dụng xác thực truyền thống)
UC06	Đăng xuất

4. Mô tả danh sách Use-case

4.1. Đăng nhập bằng email và mật khẩu

Use-case ID	UC01
Use-case name	Đăng nhập bằng email và mật khẩu
Brief description	Người dùng đăng nhập vào hệ thống bằng tài khoản và mật khẩu
Actor(s)	Khách
Precondition(s)	Người dùng truy cập vào trang web chọn đăng nhập
Postcondition(s)	Người dùng truy cập được vào trang chính (dashboard) của hệ thống
<i>Basic flow</i>	1. Người dùng truy cập vào trang web 2. Người dùng nhập thông tin vào các ô nhập email 3. Chờ hệ thống xác thực xem email đã được đăng kí chưa 4. Người dùng nhập thông tin vào ô mật khẩu 5. Người dùng nhấn nút “Sign In” để đăng nhập vào hệ thống
<i>Alternative flow(s)</i>	1. Ở bước 2, nếu người dùng không nhập đúng định dạng của email, hiển thị phải nhập đúng định dạng email 2. Ở bước 3, nếu người dùng nhập 1 email chưa được đăng kí, hiển thị rằng email đó chưa được đăng kí 2. Ở bước 5, nếu người dùng nhập thông tin đăng nhập chưa được đăng kí trên hệ thống, hiển thị sai thông tin tài khoản hoặc mật khẩu

Non-functional requirement(s)	Giao diện phải gần gũi và thân thiện với người dùng
-------------------------------	---

4.2. Đăng kí tài khoản cho người dùng mới

Use-case ID	UC02
Use-case name	Đăng kí tài khoản cho người dùng mới
Brief description	Người dùng đăng kí tài khoản mới khi người dùng là lần đầu truy cập vào hệ thống
Actor(s)	Khách
Precondition(s)	Email người dùng dùng để đăng kí chưa tồn tại trên hệ thống
Postcondition(s)	Người dùng có thể đăng nhập vào hệ thống
<i>Basic flow</i>	<ol style="list-style-type: none"> 1. Người dùng bấm vào “Don’t have an account” 2. Người dùng điền tên, thông tin email, mật khẩu 3. Người dùng bấm nút “Sign Up”
<i>Alternative flow(s)</i>	<ol style="list-style-type: none"> 1. Ở bước 3, nếu email đã được đăng kí trước đó thì hiển thị email đã được sử dụng trước đó
Non-functional requirement(s)	Giao diện thân thiện và dễ sử dụng

4.3. Đăng nhập bằng khuôn mặt

Use-case ID	UC03
Use-case name	Đăng nhập bằng khuôn mặt
Brief description	Người dùng có thể đăng nhập vào hệ thống bằng khuôn mặt đã được đăng kí trên hệ thống
Actor(s)	Khách
Precondition(s)	Người dùng đã có thông tin đăng nhập bằng phương thức truyền thống và đã bật tính năng xác thực bằng khuôn mặt
Postcondition(s)	Người dùng truy cập được vào trang chính (dashboard) của hệ thống
<i>Basic flow</i>	<ol style="list-style-type: none"> 1. Người dùng truy cập vào trang web 2. Người dùng nhập thông tin vào các ô nhập email 3. Chờ hệ thống xác thực xem email đã được đăng kí chưa 4. Người dùng nhấn vào biểu tượng camera để chờ xác thực
<i>Alternative flow(s)</i>	<ol style="list-style-type: none"> 1. Ở bước 2, nếu người dùng không nhập đúng định dạng của email, hiển thị phải nhập đúng định dạng email 2. Ở bước 3, nếu người dùng nhập 1 email chưa được đăng kí, hiển thị rằng

	email đó chưa được đăng kí 3. Ở bước 3, nếu người dùng chưa đăng kí xác thực bằng khuôn mặt, người dùng hãy đăng nhập bằng mật khẩu 1. Ở bước 4, nếu người dùng không cho phép truy cập vào camera, hệ thống xác thực khuôn mặt không thể thực hiện, người dùng đăng nhập bằng mật khẩu
Non-functional requirement(s)	Thời gian tối đa để truy cập vào hệ thống là 10 giây

4.4. Bất tính năng xác thực bằng khuôn mặt

Use-case ID	UC04
Use-case name	Bất tính năng xác thực bằng khuôn mặt
Brief description	Người dùng đăng kí khuôn mặt cho hệ thống để có thể đăng nhập hệ thống bằng khuôn mặt
Actor(s)	Khách
Precondition(s)	Người dùng đã tồn tại trên hệ thống và chưa bất tính năng xác thực khuôn mặt
Postcondition(s)	Người dùng có thể sử dụng khuôn mặt đã đăng kí để đăng nhập vào hệ thống
<i>Basic flow</i>	<ol style="list-style-type: none"> 1. Người dùng đăng nhập vào hệ thống 2. Người dùng nhấn vào biểu tượng avatar, chọn tag “account setting” 3. Tại thẻ FaceID setting, người dùng nhấn bật 4. Người dùng nhấn vào biểu tượng camera xuất hiện để có thể quay được khuôn mặt được đăng kí 5. Xuất hiện alert “Đăng kí khuôn mặt thành công” người dùng nhấn OK để hoàn tất quá trình
<i>Alternative flow(s)</i>	<ol style="list-style-type: none"> 1. Ở bước 4, nếu không bật quyền truy cập vào camera thì không thể bất tính năng, người dùng tải lại trang web để thoát quá trình
Non-functional requirement(s)	Mỗi người dùng chỉ có thể đăng kí 1 khuôn mặt

4.5. Tắt tính năng xác thực bằng khuôn mặt

Use-case ID	UC05
Use-case name	Tắt tính năng xác thực bằng khuôn mặt
Brief description	Người dùng xóa khuôn mặt đã đăng kí trước đó, người dùng chỉ còn có thể đăng nhập bằng phương thức truyền thống (email và mật khẩu)
Actor(s)	Khách
Precondition(s)	Người dùng đã tồn tại trên hệ thống và đã bất tính năng xác thực khuôn mặt
Postcondition(s)	Người dùng không thể dùng khuôn mặt để đăng nhập vào hệ thống

<i>Basic flow</i>	<ol style="list-style-type: none"> 1. Người dùng đăng nhập vào hệ thống 2. Người dùng nhấn vào biểu tượng avatar, chọn tag “account setting” 3. Tại thẻ FaceID setting, người dùng nhấn tắt
<i>Alternative flow(s)</i>	
Non-functional requirement(s)	Thời gian xử lý không quá 3 giây

4.6. Đăng xuất

Use-case ID	UC18
Use-case name	Đăng xuất
Brief description	Người dùng đăng xuất khỏi tài khoản hiện tại
Actor(s)	Khách
Precondition(s)	Người dùng có tồn tại trong hệ thống và đang được đăng nhập vào hệ thống
Postcondition(s)	Người dùng đăng xuất thành công
<i>Basic flow</i>	<ol style="list-style-type: none"> 1. Từ góc bên phải trên cùng của trang hiện tại, người dùng chọn vào biểu tượng avatar 2. Người dùng bấm vào tag “Log out”
<i>Alternative flow(s)</i>	
Non-functional requirement(s)	Giao diện thân thiện và dễ sử dụng cho người dùng