XÁC THỰC ĐA YẾU TỐ VÀ THỎA THUẬN KHÓA PHIÊN TRONG MÔ HÌNH MẠNG ĐA MÁY CHỦ

Tạ Việt Hoàng [1,2]

[1] Trường Đại Học Công nghệ thông tin

[2] Đại học Quốc gia Thành phố Hồ Chí Minh

Mục tiêu

- Tìm hiểu về xác thực đa yếu tố dựa trên mật khẩu, TOTP, xác thực và bảo vệ các mẫu sinh trắc học.
- Tìm hiểu về cách xác thực sử dụng sinh trắc của thiết bị (Device Fingerprints) và cách sử dụng module phần cứng (Hardware Assisted) để bảo vệ các thông tin dùng trong xác thực.
- Triển khai thực nghiệm và đánh giá tính hiệu quả trong việc xác thực trong Telecare Medical Information System

Lý do chọn đề tài

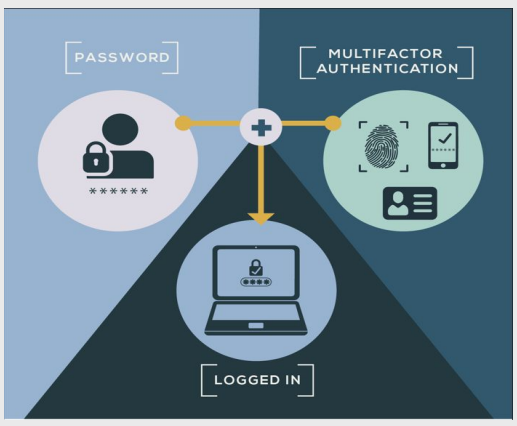
- Đề tài nghiên cứu về xác thực đa yếu tố (MFA) được chọn để nâng cao tính an toàn khi sử dụng dịch vụ trực tuyến. MFA sử dụng nhiều yếu tố xác thực như mật khẩu, mã PIN, thẻ thông minh và dấu vân tay để tăng cường bảo mật.
- Nghiên cứu tập trung vào phân tích và đánh giá hiệu quả cũng như đảm bảo tính bảo mật của các phương pháp MFA. Thông qua thực nghiệm theo kịch bản thực tế, nghiên cứu nhằm xác định những phương pháp tốt nhất để bảo vệ thông tin và tài khoản người dùng.

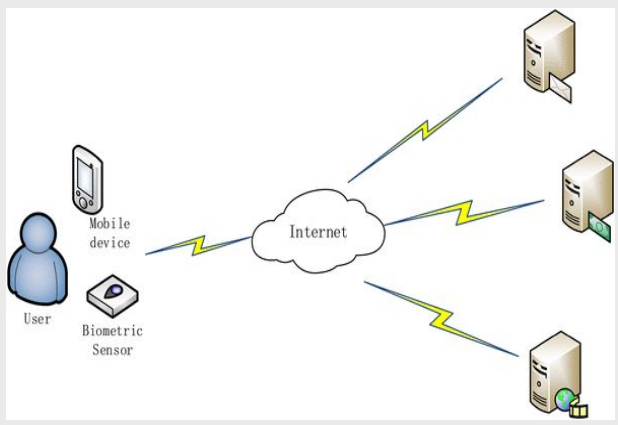
Tổng quan

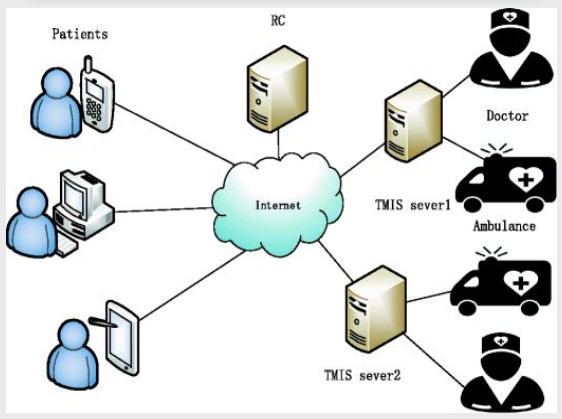
Nghiên cứu, triển khai và đánh giá hiệu quả các phương pháp xác thực đa yếu tố

Ứng dụng xác thực đa yếu tố trong môi trường multi-server

Thực nghiệm: đánh giá hiệu quả và tính bảo mật trong Telecare Medical Information System.







Chi tiết

1. Nội dung

Nghiên cứu các yếu tố sử dụng trong xác thực:

- Mật khẩu sử dụng một lần: Sử dụng mật khẩu dựa trên thời gian (TOTP) để đảm bảo tính duy nhất và tăng cường bảo mật trong quá trình xác thực.
- Sinh trắc học (vân tay): Sử dụng kỹ thuật Biohashing và Fuzzy-extractor để bảo vệ và xác thực các mẫu sinh trắc học như vân tay.
- Sinh trắc thiết bị dựa trên hệ điều hành và phần cứng: Sử dụng thông tin từ hệ điều hành và phần cứng máy tính (GPU, CPU) để xác thực người dùng và tăng cường tính bảo mật.
- Module phần cứng hỗ trợ: Sử dụng TPM (Trusted Platform Module) để đảm bảo tính toàn vẹn và bảo mật thông tin trong quá trình xác thực.

Nghiên cứu các đề án xác thực và tạo khóa phiên cho môi trường ứng dụng đa máy chủ:

- Nghiên cứu và phát triển phương pháp xác thực đa yếu tố trong môi trường multi-server, đảm bảo tính ẩn danh cho người dùng. Điều này đảm bảo rằng các người dùng có thể truy cập vào các máy chủ khác nhau mà không cần tiết lộ danh tính của họ.

2. Phương pháp

- Lựa chọn kịch bản ứng dụng: Triển khai xác thực đa yếu tố trong môi trường multi-server, cụ thể là **Telecare Medical Information System**. Đây là một hệ thống thông tin y tế trực tuyến, nơi xác thực đa yếu tố có thể đảm bảo tính bảo mật và an toàn cho dữ liệu y tế.
- Đánh giá tính hiệu quả và bảo mật và khả năng đáp ứng các yêu cầu của hệ thống trong việc xác thực người dùng: Tiến hành đánh giá hiệu quả của các phương pháp xác thực đa yếu tố đã triển khai trong **Telecare Medical Information System.**

3. Kết quả mong đợi

- Kết quả dự kiến từ nghiên cứu này là tăng cường tính bảo mật và hiệu quả trong xác thực đa yếu tố.
- Sử dụng các phương pháp như mật khẩu một lần (TOTP), sinh trắc học và module phần cứng hỗ trợ, nghiên cứu mong đợi đạt được những kết quả sau: tăng cường tính bảo mật, bảo vệ thông tin và quyền riêng tư của người dùng, đáp ứng yêu cầu bảo mật và độ tin cậy trong hệ thống thông tin y tế trực tuyến.

NII

Tên Tạ Việt Hoàng– Trường Đại học Công nghệ thông tin

TEL : 0828422091 Email : hoangtv.17@grad.uit.edu.vn