TỔNG LIÊN ĐOÀN LAO ĐỘNG VIỆT NAM
TRƯỜNG ĐẠI HỌC TÔN ĐỨC THẮNG
KHOA CÔNG NGHỆ THÔNG TIN

BÁO CÁO CUỐI KỲ MÔN

NHẬP MÔN BẢO MẬT THÔNG TIN

RSA VÀ CHỮ KÝ SỐ

Người hướng dẫn: TS.**HUỲNH NGỌC TÚ**

Người thực hiện: **NGÔ MINH TIẾN – 52100125**

PHẠM ĐĂNG KHOA - 52100971

NGUYỄN MINH TUẤN - 52300079

THÀNH PHỐ HỒ CHÍ MINH, NĂM 2024

TỔNG LIÊN ĐOÀN LAO ĐỘNG VIỆT NAM
TRƯỜNG ĐẠI HỌC TÔN ĐỨC THẮNG
KHOA CÔNG NGHỆ THÔNG TIN

BÁO CÁO CUỐI KỲ MÔN

NHẬP MÔN BẢO MẬT THÔNG TIN

RSA VÀ CHỮ KÝ SỐ

Người hướng dẫn: TS.**HUỲNH NGỌC TÚ**

Người thực hiện: **NGÔ MINH TIẾN – 52100125**

PHẠM ĐĂNG KHOA - 52100971

NGUYỄN MINH TUẤN - 52300079

THÀNH PHỐ HỒ CHÍ MINH, NĂM 2024

LỜI CẢM ƠN

Em xin chân thành cảm ơn sự giúp đỡ và giảng dạy tận tình của quý thầy cô, đặc biệt là giảng viên – Huỳnh Ngọc Tú trong suốt thời gian qua. Mặc dù có những khó khăn trong lúc học tập và nghiên cứu, nhưng nhờ có sự chuyên nghiệp và tâm huyết của cô qua những bài giảng, em đã có thêm nhiều kiến thức về môn Nhập môn Bảo mật thông tin, ngày càng khai thác được thêm nhiều kiến thức chuyên ngành. Báo cáo giữa kỳ này là kết quả cho những ngày học tập và làm việc nhóm đầy hiệu quả, là kiến thức mà em tích luỹ được trong suốt thời gian qua. Tuy nhiên, bài báo cáo còn nhiều thiếu sót cần sửa chữa, kính mong thầy cô góp ý để em hoàn thiện hơn ở tương lai.

BÁO CÁO ĐƯỢC HOÀN THÀNH
TẠI TRƯỜNG ĐẠI HỌC TÔN ĐỨC THẮNG

Chúng tôi xin cam đoan đây là sản phẩm đồ án của riêng chúng tôi và được sự hướng dẫn của giảng viên Huỳnh Ngọc Tú. Các nội dung nghiên cứu, kết quả trong đề tài này là trung thực và chưa công bố dưới bất kỳ hình thức nào trước đây. Những số liệu trong các bảng biểu phục vụ cho việc phân tích, nhận xét, đánh giá được chính tác giả thu thập từ các nguồn khác nhau có ghi rõ trong phần tài liệu tham khảo.

Ngoài ra, trong đồ án còn sử dụng một số nhận xét, đánh giá cũng như số liệu của các tác giả khác, cơ quan tổ chức khác đều có trích dẫn và chú thích nguồn gốc.

Nếu phát hiện có bất kỳ sự gian lận nào tôi xin hoàn toàn chịu trách nhiệm về nội dung đồ án của mình. Trường đại học Tôn Đức Thắng không liên quan đến những vi phạm tác quyền, bản quyền do tôi gây ra trong quá trình thực hiện (nếu có).

TP. Hồ Chí Minh, ngày 9 tháng 12 năm 2024

Tác giả

(ký tên và ghi rõ họ tên)

Ngô Minh Tiến

Phạm Đăng Khoa

Nguyễn Minh Tuấn

PHẦN XÁC NHẬN VÀ ĐÁNH GIÁ CỦA GIẢNG VIÊN

Phần xác nhận của GV hướng dẫn

_____

_____

_____

_____

_____

_____

_____

Tp. Hồ Chí Minh, ngày tháng năm
(kí và ghi họ tên)

Phần đánh giá của GV chấm bài

_____

_____

_____

_____

_____

_____

_____

Tp. Hồ Chí Minh, ngày tháng năm
(kí và ghi họ tên)

MỤC LỤC

DANH MỤC KÍ HIỆU VÀ CHỮ VIẾT TẮT

CÁC KÝ HIỆU

CÁC CHỮ VIẾT TẮT

DANH MỤC CÁC BẢNG BIỂU, HÌNH VẼ, ĐỒ THỊ

DANH MỤC HÌNH

Error! No table of contents entries found.

CHƯƠNG 1 – CHỨC NĂNG CHÍNH

Giới thiệu chung

Hệ thống ký hợp đồng điện tử là một giải pháp giúp số hoá quá trình soạn thảo, ký kết, xác minh và lưu trữ hợp đồng giữa các bên liên quan. Ứng dụng này cho phép quản lý hợp đồng, người dùng, cặp khoá RSA (khoá công khai/riêng tư), chữ ký số và trạng thái hợp đồng một cách an toàn, minh bạch và tuân thủ pháp lý.

1.1. Quản lý người dùng và phân quyền:

1.1.1. Admin:

- Tạo, quản lý hợp đồng.
- Cấu hình, xem và quản lý khóa công khai của người dùng.
- Theo dõi trạng thái hợp đồng và nhật ký hoạt động.

1.1.2. User:

- Xem danh sách hợp đồng được phân công.
- Tải hợp đồng (PDF) để xem nội dung.
- Ký hợp đồng bằng khóa riêng tư của họ.
- Cập nhật cặp khóa (khi cần) và quản lý bảo mật khóa riêng tư.

1.2. Quản lý hợp đồng:

- Tạo hợp đồng mới: Nhập tiêu đề, nội dung, tải lên tệp PDF.
- Chỉ định danh sách người ký (signerIds).
- Hiển thị trạng thái hợp đồng: pending, signed, completed.
- Lưu trữ lịch sử các hành động (tạo, cập nhật, ký).

1.3. Ký và xác minh chữ ký số:

- Người ký dùng khóa riêng tư để ký băm (hash) của tệp PDF hợp đồng.
- Hệ thống sử dụng khóa công khai tương ứng để xác minh chữ ký.
- Cập nhật kết quả xác minh (isValid) và trạng thái hợp đồng khi tất cả các bên đã ký.

1.4. Quản lý cặp khóa RSA:

- Người dùng có thể đổi cặp khóa mới khi cần.
- Hệ thống lưu trữ khóa công khai cũ để xác minh các chữ ký đã ký trước đó.
- Bảo đảm tính toàn vẹn và giá trị pháp lý của chữ ký dù cặp khóa đã thay đổi.

1.5. Gửi thông báo và tương tác người dùng:

- Gửi email hoặc thông báo trong ứng dụng khi người dùng tạo tài khoản, cung cấp link để tải khóa riêng tư, yêu cầu ký lại từ admin, hoặc thông báo cung cấp cặp khóa mới.
- Cung cấp giao diện trực quan để người ký xem và ký hợp đồng thuận tiện.

CHƯƠNG 2 – CÔNG NGHỆ VÀ KIẾN TRÚC SỬ DỤNG

2.1. Nền tảng Backend:

- Node.js: Xây dựng máy chủ backend, xử lý logic nghiệp vụ.
- Express.js: Xây dựng API RESTful, quản lý định tuyến, middleware.

2.2. Mã hóa và ký số:

- Module crypto (Node.js): Tạo, ký và xác minh chữ ký số (RSA, SHA-256).
- OpenSSL (ngoại tuyến): Tạo cặp khóa RSA (nếu cần).

2.3. Cơ sở dữ liệu:

- MongoDB + Mongoose: Lưu trữ thông tin người dùng, hợp đồng, chữ ký, khóa công khai.
- Model tiêu biểu:

  - User: Lưu thông tin người dùng, danh sách khóa công khai.

  - Contract: Lưu thông tin hợp đồng, danh sách người ký, chữ ký.

  - Signature (tuỳ chọn tách riêng): Lưu chữ ký, tham chiếu đến hợp đồng và người ký.

  - PublicKey: Lưu khóa công khai của người dùng

2.4. Xử lý tệp PDF:

- fs (Node.js) để đọc tệp PDF.
- pdf-lib (hoặc thư viện tương tự) để xử lý PDF nếu cần phân tích, xác nhận tính toàn vẹn trước và sau khi ký.

2.5. Giao diện người dùng (tùy chọn):

- Dùng view engine Handlebars để tạo giao diện cho người dùng.

CHƯƠNG 3 – QUY TRÌNH NGHIỆP VỤ

3.1. Khởi tạo người dùng và khóa:

- Người dùng đăng ký tài khoản, hệ thống sẽ tự động tạo cặp khóa RSA.
- Khóa công khai được lưu trên hệ thống, khóa riêng tư do người dùng giữ.

3.2. Tạo hợp đồng (Admin):

- Admin tải lên PDF, nhập thông tin hợp đồng.
- Chọn danh sách người ký.
- Hợp đồng ở trạng thái pending.

3.3. Người ký xem và ký hợp đồng:

- Người ký đăng nhập, xem danh sách hợp đồng cần ký.
- Tải và đọc PDF.
- Sử dụng khóa riêng tư để ký, gửi chữ ký số lên hệ thống.

3.4. Xác minh chữ ký và cập nhật trạng thái:

- Hệ thống xác minh chữ ký bằng khóa công khai đã lưu.
- Nếu chữ ký hợp lệ, cập nhật trạng thái chữ ký và hợp đồng.
- Khi tất cả người ký đã ký hợp lệ, hợp đồng chuyển sang completed.

3.5. Cấp lại cặp khóa mới:

- Người dùng có thể yêu cầu admin cấp lại cặp khóa mới.
- Khóa công khai cũ vẫn được lưu để xác minh chữ ký trong quá khứ.
- Không làm mất tính hợp lệ của các hợp đồng đã ký trước đó.

TÀI LIỆU THAM KHẢO