ĐẠI HỌC THÁI NGUYÊN
TRƯỜNG ĐẠI HỌC CÔNG NGHỆ THÔNG TIN VÀ TRUYỀN THÔNG

TRỊNH MINH PHÚ

NGHIÊN CỨU GIẢI PHÁP BẢO MẬT, XÁC THỰC CHO ỨNG DỤNG VĂN PHÒNG ĐIỆN TỬ DỰA TRÊN CÔNG NGHỆ MỞ

***Chuyên ngành*: Khoa học máy tính**
***Mã số*: 60 48 01**

LUẬN VĂN THẠC SĨ KHOA HỌC MÁY TÍNH

NGƯỜI HƯỚNG DẪN KHOA HỌC: TS. HỒ VĂN HƯƠNG

Thái Nguyên - 2015

LỜI CẢM ƠN

Trước tiên tôi xin được bày tỏ lòng biết ơn tới các thầy, cô đang công tác tại trường Đại học CNTT & TT – Đại Học Thái Nguyên, những người đã giảng dạy và cung cấp những kiến thức khoa học quý báu trong suốt những năm học vừa qua để tôi có nền tảng kiến thức thực hiện khoá luận này.

Đặc biệt, tôi xin bày tỏ lòng biết ơn sâu sắc tới **TS. Hồ Văn Hương**, người đã tận tình chỉ bảo, giúp đỡ và tạo điều kiện về nhiều mặt để tôi có thể hoàn thành khoá luận này và công ty Ecoit đã tạo điều kiện môi trường nghiên cứu tốt để tôi có thể hoàn thành khoá luận này.

Tôi cũng xin gửi lời cảm ơn tới tập thể lớp CHK11G, trường Đại học CNTT & TT đã giúp đỡ, nhiệt tình chia sẻ đóng góp những kinh nghiệm quý báu cho tôi.

Cuối cùng tôi xin cảm ơn gia đình, bạn bè đã giúp đỡ, tạo điều kiện và đóng góp cho tôi nhiều ý kiến quý báu trong cuộc sống, công việc và học tập nói chung cũng như trong quá trình thực hiện khóa luận này.

Mặc dù, đã có nhiều cố gắng nhưng do hạn hẹp về thời gian, điều kiện và trình độ nên không tránh khỏi khuyết điểm. Tôi chân thành mong nhận được sự góp ý của thầy cô và bạn bè.

Thái Nguyên, tháng năm 2015

Học viên

Trịnh Minh Phú

MỤC LỤC

Trang

ĐỊNH NGHĨA, VIẾT TẮT

Ký hiệu	Tiếng Anh	Tiếng Việt
AES	Advanced Encryption Standard	Tiêu chuẩn mã hóa tiên tiến
PI	Application Programming Interfaces	Giao diện lập trình ứng dụng
CAS	Central Authentication Service	Hệ thống xác thực tập trung
CIFS	Common Internet File System	Hệ thống chia sẻ file phổ biến trện mạng
CMIS	Content Managenment Interoperability Servic s	Dịch vụ tương tác hệ quản trị nội dung
CNTT		Công nghệ thông tin
CSDL		Cơ sở dữ liệu
ECM	Enterprise Content Management	Hệ quản trị nội dung
FTP	File Transfer Protocol	Giao thức truyền tệp tin
GSM	Global System for Mobile Communication	Hệ thống thông tin di động toàn cầu
TTP	Hyper Text Transfer Protocol	Giao thức truyền tải siêu văn bản
ISO	Intrernational Organization for Standardization	Tổ chức chuẩn hóa quốc tế
PMNM		Phần mềm nguồn mở
SHA	Secure Hash Algorithm	Thuật giải băm bảo mật
SMTP	Simple Mail Transfer Protocol	Giao thức truyền tải tệp tin đơn giản
TCP-IP	Internet Protocol Suite	Bộ giao thức liên mạng
UID	User Identification	Mã người dùng
URL	Uniform Resource Locator	Liên kết dẫn địa chỉ web
VPĐT		Văn phòng điện tử
WCM	Web Content Mananement	Hệ thống quản trị nội dung Web
WebDAV	Web-based Distributed Authoring And Versioning	Hệ thống quản lý chứng thực và phiên bản dựa trên môi trường web
SSL	Secure Socket Layer	

DANH MỤC CÁC HÌNH

MỞ ĐẦU

Ngày nay, trong bối cảnh xã hội thông tin đang dần pháp triển, việc quản lý, điều hành và tác nghiệp theo phương thức cũ đã ngày càng lộ nhiều tính bất cập, tính hiệu quả không cao. Mặc dù việc các cơ quan, tổ chức, doanh nghiệp trang bị máy tính cho mỗi nhân viên phục vụ cho công việc không còn xa lạ. Nhưng hầu hết tại các cơ quan, tổ chức, doanh nghiệp việc sử dụng máy tính còn rất hạn chế, chỉ phục vụ cho một cá nhân. Các cơ quan, tổ chức, doanh nghiệp là một khối, là một hệ thống cần có sự quản lý chặn chẽ điều hành tác nghiệp và luôn có sự trao đổi thông tin thường xuyên giữa các nhân viên. Từ những nhu cầu thực tế trên việc tạo ra môi trường làm việc mới, cách thức quản lý mới để việc sử dụng công cụ máy tính trong công việc đạt hiệu quả cao nhất là cấp thiết.

Trước nhu cầu thực tế và chủ chương của Đảng và Nhà nước là đưa công nghệ thông tin (CNTT) vào cuộc sống, giải pháp Văn phòng điện tử (VPĐT) - một văn phòng không giấy tờ, giúp lãnh đạo có thể trao đổi với nhân viên, phòng ban trong cơ quan nhanh chóng, kịp thời. VPĐT ra đời là một giải pháp hữu hiệu.

Nhiều phần mềm VPĐT đã ra đời trên nhu cầu thực tế đó với nhiều tính năng quản lý tài liệu hấp dẫn, giao diện thân thiện, dễ sử dụng. Tuy nhiên, vấn đề bảo mật và xác thực trên các phần mềm VPĐT hiện nay vẫn còn nhiều lỗ hổng, thiếu xót và chưa được quan tâm đúng mức.

Xuất phát từ những nhu cầu trên, học viên quyết định lựa chọn đề tài: "*Nghiên cứu giải pháp bảo mật, xác thực cho ứng dụng Văn phòng điện tử dựa trên công nghệ mở*". Nhiệm vụ chính của đề tài là nghiên cứu, đề xuất ra các giải pháp bảo mật cho VPĐT, cụ thể là áp dụng cho phần mềm VPĐT **Alfresco** dựa trên kiến trúc của công nghệ mở và vận dụng cơ sở lý thuyết mật mã, ứng dụng trong bảo mật xác thực file dữ liệu.

Nội dung luận văn được trình bày trong ba chương

Chương l. Tổng quan về an ninh an toàn văn phòng điện tử trên công nghệ mở. Trong chương này tôi sẽ trình bày về an toàn thông tin, công nghệ mở, đánh giá tổng quan về một số phần mềm VPĐT và đặc biệt là phần mềm VPĐT mã nguồn mở Alfresco. Ngoài ra, tôi còn đề cập đến vấn đề về cách thiết kế văn phòng điện tử an toàn, phân tích lựa chọn các chính sách an toàn, bảo mật trên văn phòng điện tử.

Chương 2. Cơ sở lý thuyết mật mã ứng dụng an toàn bảo mật trong văn phòng điện tử. Trong chương này tôi sẽ trình bày khái quát về cơ sở lý thuyết mật mã ứng dụng an toàn bảo mật trong VPĐT cụ thể là tổng quan về hệ mật mã, vai trò của hệ mật mã trong an toàn bảo mật VPĐT, trình bày về thuật toán AES, thuật toán RSA, vấn đề phân phối khóa công khai, tổng quan về hàm băm, chữ ký số.

Chương 3. Giải pháp bảo mật, xác thực văn phòng điện tử và xây dựng ứng dụng. Trong chương này tôi sẽ trình bày thực trạng an toàn bảo mật VPĐT hiện nay. Từ thực trạng mất an ninh, an toàn trên VPĐT. Tôi sẽ lựa chọn Alfresco là nền tảng để đề xuất giải pháp bảo mật và xác thực văn phòng điện tử. Giải pháp bảo mật và xác thực văn phòng điện tử Alfresco bao gồm những giải pháp sau:

Giải pháp 1: Phân tích, xây dựng giải pháp đăng nhập duy nhất trên Alfresco và triển khai hệ thống đăng nhập duy nhất với giải pháp được lựa chọn.

Giải pháp 2: Phân tích xây dựng ứng dụng mã hóa, giải mã, chữ ký số và xác thực chữ ký tài liệu lưu trữ trên kho dữ liệu Alfresco.

CHƯƠNG 1
TỔNG QUAN VỀ AN NINH AN TOÀN VĂN PHÒNG ĐIỆN TỬ TRÊN CÔNG NGHỆ MỞ

1.1. Vấn đề an toàn thông tin

Trước nhu cầu trao đổi thông tin dữ liệu ngày càng lớn và đa dạng, các tiến bộ về điện tử - viễn thông và CNTT không ngừng được phát triển ứng dụng để nâng cao chất lượng và lưu lượng truyền tin thì các quan niệm ý tưởng và biện pháp bảo vệ thông tin dữ liệu cũng được đổi mới. Bảo vệ an toàn thông tin dữ liệu là một chủ đề rộng, có liên quan đến nhiều lĩnh vực và trong thực tế có thể có rất nhiều phương pháp được thực hiện để bảo vệ an toàn thông tin dữ liệu. Các phương pháp bảo vệ an toàn thông tin dữ liệu có thể được quy tụ vào ba nhóm sau:

- Bảo đảm an toàn thông tin tại máy chủ.
- Bảo đảm an toàn cho phía máy trạm.
- An toàn thông tin trên đường truyền.

Ba nhóm trên có thể được ứng dụng riêng rẽ hoặc phối kết hợp. Môi trường khó bảo vệ an toàn thông tin nhất và cũng là môi trường đối phương dễ xâm nhập nhất đó là môi trường mạng và truyền tin. Biện pháp hiệu quả nhất và kinh tế nhất hiện nay trên mạng truyền tin và mạng máy tính là biện pháp thuật toán.

An toàn thông tin bao gồm các nội dung sau:

- Tính bí mật: tính kín đáo riêng tư của thông tin.
- Tính xác thực của thông tin, bao gồm xác thực đối tác (bài toán nhận danh), xác thực thông tin trao đổi.
- Tính chống chối bỏ: đảm bảo người gửi thông tin không thể thoái thác trách nhiệm về thông tin mà mình đã gửi.

Để đảm bảo an toàn thông tin dữ liệu trên đường truyền tin và trên mạng máy tính có hiệu quả thì điều trước tiên là phải lường trước hoặc dự đoán trước các khả năng không an toàn, khả năng xâm phạm, các sự cố rủi ro có thể xảy ra đối với thông tin dữ liệu được lưu trữ và trao đổi trên đường truyền tin cũng như trên mạng. Xác định càng chính xác các nguy cơ nói trên thì càng quyết định được tốt các giải pháp để giảm thiểu các thiệt hại.

1.2. Công nghệ mở

1.2.1. Tổng quan về công nghệ mở

Hiện nay CNTT đang phát triển như vũ bão tác động đến mọi mặt đời sống của con người. Song song với sự phát triển của CNTT, công nghệ mở đang có những bước phát triển vượt bậc và ngày càng chiếm nhiều thị phần trong lĩnh vực phần mềm so với công nghệ mã nguồn đóng. Đối với những nước đang phát triển như nước ta hay những nước đang phát triển thế giới thì công nghệ mở là giải pháp tối ưu cho nhiều vấn đề và đặc biệt là chính phủ điện tử vấn đề đang được quan tâm hiện nay. Việc xây dựng chính phủ điện tử trên nền tảng công nghệ mở có chi phí rẻ hơn nhiều so với công nghệ nguồn đóng đặc biệt là trong khía cạnh bản quyền phần mềm.

Công nghệ mở có thể cung cấp phần mềm hoàn toàn đáp ứng được nhu cầu sử dụng ở nhiều mức độ khác nhau với các ưu điểm: phần mềm nguồn mở (PMNM) thường miễn phí hoặc chi phí rất thấp; có sự hỗ trợ hậu mãi tuyệt vời có thể sánh ngang với những tính năng công nghệ mà các công ty độc quyền truyền thống giới thiệu; có tính an ninh và độ tin cậy cao. PMNM được tìm ra lỗi và sửa sai bởi hàng nghìn người nên khả năng phát hiện lỗi và các lỗ hổng an ninh cao và nhanh chóng. Ngoài ra, những rủi ro về virus, adware, spyware... được giảm đáng kể vì virut rất ít, làm bất cứ điều gì có thể gây hại đều yêu cầu nhập mật khẩu. Đa dạng trong tính tùy biến nguồn dữ liệu nhưng chất lượng PMNM cũng được đảm bảo do người sử dụng phát triển nên có tính năng thích hợp, ít khi có yếu tố dư thừa và gần gũi với người sử dụng.