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

PHAYU KHOUNVITHONG

NGHIÊN CỨU MỘT SỐ GIẢI PHÁP ĐẢM BẢO AN NINH HỆ THỐNG ĐIỆN TOÁN ĐÁM MÂY RIÊNG

LUẬN VĂN THẠC SĨ KHOA HỌC MÁY TÍNH

THÁI NGUYÊN - 2020

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

PHAYU KHOUNVITHONG

NGHIÊN CỨU MỘT SỐ GIẢI PHÁP ĐẢM BẢO AN NINH HỆ THỐNG ĐIỆN TOÁN ĐÁM MÂY RIÊNG

CHUYÊN NGÀNH: KHOA HỌC MÁY TÍNH
Mã số: 8 480101

LUẬN VĂN THẠC SĨ KHOA HỌC MÁY TÍNH

Hướng dẫn khoa học: TS. Nguyễn Đức Bình

THÁI NGUYÊN - 2020

LỜI CẢM ƠN

Để hoàn thành luận văn tốt nghiệp này, lời đầu tiên em xin gửi lời biết ơn chân thành và sâu sắc nhất đến thầy giáo **TS. Nguyễn Đức Bình** đã tận tình hướng dẫn, truyền đạt những kinh nghiệm quý giá cho em trong suốt quá trình nghiên cứu và thực hiện đề tài.

Em xin gửi lời cảm ơn đến các thầy cô giáo trong khoa Công nghệ thông tin cùng toàn thể các thầy cô giáo đã truyền đạt vốn kiến thức quý báu cho chúng em trong suốt quá trình học tập vừa qua. Em đã được quý thầy cô cung cấp và truyền đạt những kiến thức chuyên môn cần thiết và quý giá nhất. Ngoài ra em còn được rèn luyện một tinh thần học tập và làm việc độc lập và sáng tạo. Đây là nền tảng hết sức cần thiết để có thể thành công như hôm nay.

Luận văn là cơ hội để em có thể áp dụng, tổng kết lại những kiến thức mà mình đã học. Đồng thời, rút ra được những kinh nghiệm thực tế và quý giá trong suốt quá trình thực hiện đề tài. Sau một thời gian em tập trung công sức cho đề tài và làm việc tích cực, đặc biệt là nhờ sự chỉ đạo và hướng dẫn tận tình của thầy giáo **TS. Nguyễn Đức Bình** cùng với các thầy cô trong trường Đại học Công nghệ thông tin và Truyền thông - Đại học Thái Nguyên, đã giúp cho em hoàn thành đề tài một cách thuận lợi và gặt hái được những kết quả mong muốn.

Bên cạnh những kết quả khiêm tốn mà em đạt được, chắc chắn không tránh khỏi những thiếu sót khi thực hiện báo cáo của mình, kính mong thầy cô thông cảm. Sự phê bình, góp ý của quý thầy cô sẽ là những bài học kinh nghiệm rất quý báu cho công việc của em sau này. Là học viên ngành khoa học máy tính, em rất tự hào về khoa mà mình theo học, tự hào về tất cả các thầy cô của mình.

Kính chúc quý thầy cô mạnh khoẻ, hạnh phúc, tiếp tục đạt được nhiều thắng lợi trong việc giảng dạy, nghiên cứu khoa học và sự nghiệp trồng người.

Em xin chân thành cảm ơn

MỤC LỤC

LỜI CẢM ƠN i
MỤC LỤC iv
BẢNG CHỮ VIẾT TẮT, TỪ CHUYÊN MÔN BẰNG TIẾNG ANH vii
DANH MỤC CÁC BẢNG viii
DANH MỤC CÁC HÌNH VẼ ix
LỜI MỞ ĐẦU 1
CHƯƠNG 1 TỔNG QUAN VỀ MÔI TRƯỜNG ẢO HÓA VÀ ĐIỆN TOÁN ĐÁM MÂY 3
1.1 Khái niệm và đặc trưng ảo hóa 3
1.1.1 Định nghĩa ảo hóa 3
1.1.2 Phân loại nền tảng Ảo hóa 4
1.1.3 Ảo hóa kiến trúc vi xử lý x86 5
1.2 Khái niệm điện toán đám mây 6
1.3 Đặc trưng điện toán đám mây 7
1.4 Mô hình lớp dịch vụ của điện toán đám mây 7
1.4.1 Hạ tầng hướng dịch vụ (IaaS) 7
1.4.2 Dịch vụ nền tảng (PaaS) 8
1.4.3 Dịch vụ phần mềm (SaaS) 8
1.5 Mô hình triển khai điện toán đám mây 8
1.5.1 Đám mây công cộng (Public Cloud) 8
1.5.2 Đám mây riêng (Private Cloud) 8
1.5.3 Đám mây cộng đồng (Community Cloud) 9
1.5.4 Đám mây lai (Hybrid Cloud) 9
CHƯƠNG 2 CÁC NGUY CƠ, THÁCH THỨC AN NINH THÔNG TIN TRONG MÔI TRƯỜNG ẢO HÓA VÀ ĐIỆN TOÁN ĐÁM MÂY 10
2.1 Mối đe dọa, rủi ro an ninh thông tin môi trường ảo hóa 10
2.1.1 Tồn tại lỗ hổng bảo mật trong phần mềm lõi của nền tảng Ảo hóa (hypervisor) 10
2.1.2 Tấn công chéo giữa các máy ảo 11
2.1.3 Hệ điều hành máy ảo 11

2.1.4 Thất thoát dữ liệu giữa các thành phần Ảo hóa 12
2.1.5 Sự phức tạp trong công tác quản lý kiểm soát truy cập 12
2.1.6 Lây nhiễm mã độc hại 12
2.1.7 Tranh chấp tài nguyên 12
2.2 Mối đe dọa an ninh thông tin trong môi trường điện toán đám mây 13
2.2.1 Các mối đe dọa an ninh thông tin đối với điện toán đám mây 14
2.2.2 Các rủi ro an ninh thông tin đối với điện toán đám mây 17
CHƯƠNG 3 GIẢI PHÁP ĐẢM BẢO AN NINH THÔNG TIN HỆ THỐNG ĐIỆN TOÁN ĐÁM MÂY RIÊNG 19
3.1 Giải pháp bảo vệ dữ liệu trong môi trường ảo hóa 19
3.1.1 Xây dựng kiến trúc ảo hóa an toàn 19
3.1.2 Công nghệ phòng chống mã độc chuyên biệt cho môi trường ảo hóa 19
3.1.3 Thực hiện cấu hình an toàn lớp phần mềm lõi Hypervisor 22
3.1.4 Cấu hình an toàn máy chủ ảo hóa 22
3.1.5 Thiết kế mạng ảo đảm bảo an toàn thông tin 22
3.1.6 Giới hạn truy cập vật lý các máy chủ ảo hóa (Host) 23
3.1.7 Mã hóa dữ liệu máy ảo 23
3.1.8 Tách biệt truy cập, cô lập dữ liệu giữa các máy ảo 23
3.1.9 Duy trì sao lưu 24
3.1.10 Tăng cường tính tuân thủ 24
3.2 Giải pháp bảo vệ dữ liệu trong điện toán đám mây 24
3.2.1 Lớp phòng thủ thứ nhất kiểm soát truy cập 25
3.2.2 Lớp phòng thủ thứ hai mã hóa 27
3.2.3 Lớp phòng thủ thứ ba khôi phục nhanh chóng 34
3.2.4 Một số biện pháp phòng thủ bổ sung nhằm bảo vệ dữ liệu trong môi trường điện toán đám mây 35
3.3 Triển khai giải pháp bảo vệ nền tảng ảo hóa 36
3.3.1 Thiết kế giải pháp 36
3.4 Triển khai giải pháp 40
3.4.1 Mô hình Triển khai giải pháp mã hóa SecureCloud 40
3.4.2 Mô hình triển khai Deep Security 41

3.4.3 Thành phần giải pháp.....41
3.4.4 Các tính năng chính triển khai.....42
3.4.5 Cấu hình thiết lập chính sách bảo vệ.....43
3.4.6 Kết quả triển khai giải pháp.....48
KẾT LUẬN VÀ ĐỀ NGHỊ.....49
TÀI LIỆU THAM KHẢO.....51

BẢNG CHỮ VIẾT TẮT, TỪ CHUYÊN MÔN BẰNG TIẾNG ANH

Viết tắt	Tên tiếng Anh	Tên tiếng Việt
PI	Programming Interface.	Giao diện lập trình.
AWS	Amazon Web Services.	Dịch vụ web của Amazon.
CIA	Confidentiality Integrity Availability	Tính bí mật Tính toàn vẹn thông tin. Tính sẵn sàng
CC	Cloud computing.	Điện toán đám mây.
DOS	Denial-of-service attack.	Tấn công từ chối dịch vụ
FHE	Fully Homomorphic Encryption.	Mã hóa hoàn toàn đồng nhất.
EC2	Elastic Compute Cloud.	Đám mây điện toán đàn hồi.
HSM	Hardware Security Modules.	Mô-đun bảo mật phần cứng.
MAC	Media access control address.	Địa chỉ kiểm soát truy cập phương tiện.
IaaS	Infrastructure as a Service.	Cơ sở hạ tầng như một dịch vụ.
I/O	Input/output.	Đầu ra/đầu vào.
NIST	The national institute of technology.	Viện công nghệ quốc gia.
PaaS	Platform as a service.	Nền tảng như một dịch vụ.
SaaS	Software as a service.	Phần mềm như là một dịch vụ.
TLS	Transport Layer Security.	Bảo mật tầng vận tải.
PKI	Public Key Infrastructure.	Cơ sở hạ tầng nơi công cộng.
VM	Virtual Machine.	Máy ảo VM.
VPNs	Virtual Private Network Security.	Bảo mật mạng riêng ảo.

DANH MỤC CÁC BẢNG

Bảng 1: Các lỗ hổng bảo mật được phát hiện và công bố năm 2012 11
Bảng 2: Vấn đề an toàn thông tin của môi trường ảo hóa chiếu theo mô hình CIA 13
Bảng 3: Các mối đe dọa đối với điện toán đám mây.....14
Bảng 4: Các rủi ro an ninh thông tin đối với điện toán đám mây [5].....17
Bảng 5: So sánh giải pháp Deep Security Trendmicro và một số giải pháp an ninh khác dựa trên tổng hợp, đánh giá và quan điểm cá nhân của tác giả.....39

DANH MỤC CÁC HÌNH VẼ

Hình 1.1: Mô hình Ảo hóa.....3
Hình 1.2: Hypervisor kiểu 1- Hệ thống Xen 4
Hình 1.3: Hypervisor kiểu 2 - Hệ thống KVM.....4
Hình 1.4: Các mức đặc quyền vi xử lý x86 5
Hình 1.5: Tổng quan điện toán đám mây 6
Hình 1.6: Mô hình ba lớp của điện toán đám mây 7
Hình 1.7: Mô hình đám mây lai.....9
Hình 2.1: Các hướng khai thác tấn công môi trường ảo 10
Hình 3.1: Kiến trúc An ninh ảo hóa 19
Hình 3.2: Phát hiện mã độc hại 20
Hình 3.3: Luồng xử lý mã độc hại.....21
Hình 3.4: Kiến trúc sử dụng bộ đệm 21
Hình 3.5: Mô hình bảo vệ dữ liệu.....25
Hình 3.6: Mô hình sử dụng mã hóa đồng cấu mã hóa dữ liệu điện toán đám mây.....28
Hình 3.7: Mô hình mã hóa dữ liệu điện toán đám mây sử dụng mã hóa đồng cấu.....29
Hình 3.8: Thiết kế chương trình 30
Hình 3.9: Kiến trúc chương trình 30
Hình 3.10: Thuật toán chương trình 32
Hình 3.11: Dữ liệu dạng bản rõ trước khi mã hóa.....33
Hình 3.12: Dữ liệu sau khi mã hóa.....33
Hình 3.13: Dữ liệu sau khi giải mã.....34
Hình 3.14: Giải pháp bảo vệ điện toán đám mâyTrendmicro 37
Hình 3.15: Giải pháp bảo vệ Ảo hóa và Điện toán đám mây Trendmicro.....39
Hình 3.16: Mô hình triển khai giải pháp mã hóa dữ liệu trên điện toán đám mây.....41
Hình 3.17: Cấu hình thiết bị mã hóa.....40
Hình 3.18: Cấu hình thư mục cần mã hóa 41
Hình 3.19: Mô hình triển khai hệ thống Deep Security 41
Hình 3.120: Giao diện thành phần Deep Security Manager**Error! Bookmark not defined.**

Hình 3.21: thiết lập tính năng phòng chống mã độc 44
Hình 3.22: cấu hình chính sách tường lửa.....44
Hình 3.23: cấu hình chính sách tường lửa ứng dụng.....45
Hình 3.24: cấu hình tính năng Deep Packet Inspection 45
Hình 3.25: cấu hình tính năng Deep Packet Inspection 46
Hình 3.26: cấu hình giám sát thay đổi cấu hình 46
Hình 3.27: cấu hình giám sát thay đổi cấu hình 47
Hình 3.28: Cấu hình tính năng Log Inspection 47
Hình 3.29: Kết quả hoạt động tính năng Anti-Malware.....48
Hình 3.30: Kết quả hoạt động tính năng Deep Packet Inspection.....49
Hình 3.31: Kết quả hoạt động tính năng tường lửa.....50
Hình 3.32: Tính năng giám sát phát hiện thay đổi file cấu hình trái phép 50