ĐẠI HỌC QUỐC GIA HÀ NỘI

TRƯỜNG ĐẠI HỌC CÔNG NGHỆ

NGUYỄN VIỆT DŨNG

BẢO VỆ THÔNG TIN TRONG MÔI TRƯỜNG ẢO HÓA

LUẬN VĂN THẠC SĨ

Hà Nội – 2016

ĐẠI HỌC QUỐC GIA HÀ NỘI

TRƯỜNG ĐẠI HỌC CÔNG NGHỆ

NGUYỄN VIỆT DŨNG

BẢO VỆ THÔNG TIN TRONG MÔI TRƯỜNG ẢO HÓA

Ngành: Hệ thống thông tin

Chuyên ngành: Hệ thống thông tin

Mã số: 60480104

LUẬN VĂN THẠC SĨ

NGƯỜI HƯỚNG DẪN KHOA HỌC: PGS. TS TRỊNH NHẬT TIẾN

Hà Nội – 2016

LỜI CẢM ƠN

Với lòng kính trọng và biết ơn sâu sắc, tôi xin chân thành cảm ơn Thầy PGS.TS Trịnh Nhật Tiến, người đã tận tình giúp đỡ và hướng dẫn tôi trong suốt quá trình làm luận văn.

Xin chân thành cảm ơn gia đình, các bạn bè, đồng nghiệp đã có sự động viên, hỗ trợ và đóng góp ý kiến để tôi có thể hoàn thành công trình nghiên cứu này. Dù đã rất cố gắng nhưng với trình độ hiểu biết và thời gian nghiên cứu thực tế có hạn nên không tránh khỏi những thiếu sót.

Trân trọng cảm ơn!

LỜI CAM ĐOAN

Tôi xin cam đoan luận văn thạc sĩ với đề tài: "BẢO VỆ THÔNG TIN TRONG MÔI TRƯỜNG ẢO HÓA" là công trình nghiên cứu của riêng tôi. Các kết quả nghiên cứu trong luận văn là trung thực và chưa từng được công bố trong bất kỳ một công trình nào khác.

Nguyễn Việt Dũng

MỤC LỤC

BẢNG CHỮ VIẾT TẮT, TỪ CHUYÊN MÔN BẰNG TIẾNG ANH

Viết tắt	Diễn giải
API	Giao diện lập trình
AMS	Amazon Web Services
CIA	Confidentiality-Tính bí mật Integrity-tính toàn vẹn Availability- tính sẵn sàng
ĐTĐM	Điện toán đám mây
DOS	Denial-of-service attack
FHE	Fully Homomorphic Encryption
EC2	Elastic Compute Cloud
HSM	Hardware Security Modules
MAC	Media access control address
IaaS	Infrastructure as a Service
I/O	Input/output
NIST	The national institute of technology
PaaS	Platform as a service
SaaS	Software as a service
TLS	Transport Layer Security
PKI	Public Key Infrastructure
VM	Virtual Machine
VPNs	Virtual Private Network Security

DANH MỤC CÁC BẢNG

DANH MỤC CÁC HÌNH VẼ

LỜI MỞ ĐẦU

Tính cấp thiết của đề tài

Trong những năm gần đây nền tảng Ảo hóa và Điện toán đám mây đã có sự phát triển một cách nhanh chóng. Ảo hóa và Điện toán đám mây giúp cho tổ chức, doanh nghiệp đạt được sự tiết kiệm đáng kể về chi phí phần cứng, chi phí hoạt động, đạt được sự cải thiện về sức mạnh tính toán, chất lượng dịch vụ, và sự thuận lợi trong kinh doanh. Ảo hóa và Điện toán đám mây có quan hệ mật thiết với nhau. Ảo hóa là một công nghệ quan trọng cho sự phát triển của Điện toán đám mây đặc biệt Ảo hóa phần cứng cho phép các nhà cung cấp dịch vụ hạ tầng Điện toán đám mây sử dụng hiệu quả các nguồn tài nguyên phần cứng có sẵn để cung cấp dịch vụ điện toán cho các khách hàng của họ. Cùng với sự tăng trưởng ngày càng nhanh của Ảo hóa và Điện toán đám mây thì vấn đề đặt ra là đảm bảo an toàn dữ liệu trước nguy cơ tính bí mật, toàn vẹn và tính sẵn sàng bị vi phạm càng trở nên cấp thiết hơn. Nền tảng Ảo hóa và Điện toán đám mây có những đặc trưng riêng của chúng vì vậy khi áp dụng các biện pháp an ninh thông tin vật lý truyền thống như tường lửa, phòng chống xâm nhập cho môi trường Ảo hóa và Điện toán đám mây sẽ làm hạn chế khả năng sức mạnh tính toán của nền tảng Ảo hóa và Điện toán đám mây. Thậm chí tệ hơn nó còn tạo ra các lỗ hổng bảo mật nghiêm trọng có thể bị khai thác, mất quyền kiểm soát hệ thống. Với mong muốn tìm ra và hiểu rõ những nguy cơ, mối đe dọa, vấn đề thách thức, rủi ro an ninh thông tin đối với dữ liệu trong môi trường Ảo hóa và Điện toán đám mây, từ đó đề xuất một số giải pháp phù hợp để bảo vệ thông tin trong môi trường Ảo hóa và Điện toán đám mây. Vì thế tôi chọn đề tài nghiên cứu: Bảo vệ thông tin trong môi trường Ảo hóa**.**

Các mục tiêu nghiên cứu của đề tài:

Hiểu rõ các nguy cơ, thách thức và mối đe dọa an ninh thông tin trong môi trường Ảo hóa và Điện toán đám mây hiện tại và tương lai.

Trên cơ sở đó đề xuất một số giải pháp bảo vệ dữ liệu, thông tin trong môi trường Ảo hóa và điện toán đám mây.

Triển khai giải pháp bảo vệ dữ liệu trong môi trường Ảo hóa cho một tổ chức, doanh nghiệp dựa trên giải pháp đề xuất.

Nội dung nghiên cứu

Nghiên cứu tổng quan về môi trường Ảo hóa và Điện toán đám mây: khái niệm, đặc trưng, kiến trúc, mô hình triển khai Ảo hóa và Điện toán đám mây

Tìm hiểu các nguy cơ, mối đe dọa và rủi ro an ninh thông tin trong môi trường Ảo hóa và Điện toán đám mây

Các giải pháp bảo vệ dữ liệu thông tin trong môi trường Ảo hóa và Điện toán đám mây

Ứng dụng, triển khai giải pháp đề xuất cho một tổ chức, doanh nghiệp tại Việt Nam để đảm bảo an ninh an toàn môi trường Ảo hóa.

Đối tượng và phạm vi nghiên cứu

Đặc trưng và kiến trúc của Môi trường Ảo hóa và Điện toán đám mây là đối tượng nghiên cứu của đề tài nhằm tìm hiểu các nguy cơ và rủi ro an toàn thông tin và đề xuất các giải pháp bảo vệ thông tin trong môi trường Ảo hóa và Điện toán đám mây

Phạm vi nghiên cứu: Luận văn nghiên cứu giải pháp bảo vệ thông tin trong môi trường Ảo hóa và Điện toán đám mây đang sử dụng tại một số tổ chức và doanh nghiệp

Phương pháp nghiên cứu

Tổng hợp và phân tích các tài liệu về ảo hóa, an ninh thông tin để từ đó đưa ra được cái nhìn tổng quan nhất cũng như phương pháp hỗ trợ bảo vệ thông tin cho môi trường ảo hóa và điện toán đám mây được an toàn hơn.

Tìm hiểu thuật toán mã hóa đồng cấu. Từ đó đưa ra giải pháp xây dựng ứng dụng đảm bảo tính bí mật dữ liệu. Tìm hiểu các sản phẩm ứng dụng thuật toán mã hóa đồng cấu hiện đang được sử dụng. Tham khảo, vận dụng và kế thừa các thuật toán, mã nguồn mở, v.v…

Cơ sở lý thuyết của đề tài dựa trên ba thành phần cơ bản, cốt lõi của an toàn thông tin là: tính bí mật, tính toàn vẹn, tính sẵn sàng [1]. Đây là cơ sở lý thuyết xuyên suốt đề tài nhằm đánh giá và giải quyết các nguy cơ và thách thức an toàn thông tin môi trường ảo hóa và điện toán đám mây.

Đảm bảo tính bí mật là đảm bảo thông tin, dữ liệu chỉ được phép truy cập bởi những cá nhân, tổ chức và các bên liên quan được cấp phép. Nhiều cuộc tấn công tập trung vào vi phạm tính bí mật: nghe lén dữ liệu trên đường truyền, lừa đảo đánh cắp tài khoản, mật khẩu hoặc lây nhiễm virus, mã độc hại.

Tính toàn vẹn dữ liệu là đảm bảo tính toàn vẹn dữ liệu là đảm bảo chắc chắn dữ liệu không bị sửa đổi hoặc phá hủy bởi những cá nhân, đối tượng không được phép trong quá trình dữ liệu truyền trên mạng, lưu trữ trong các tài liệu hoặc trong cơ sở dữ liệu hoặc trong các thiết bị lưu trữ. Bảo vệ tính toàn vẹn dữ liệu xem xét ba khía cạnh sau: ngăn chặn các cá nhân, đối tượng không được cấp phép sửa đổi dữ liệu trái phép. Ngăn chặn các đối tượng được cấp quyền sửa đổi dữ liệu, ví dụ như dữ liệu bị sửa đổi do thao tác sai. Duy trì tính nhất quán giữa nội bộ và bên ngoài để các dữ liệu chính xác và phản ánh đúng thế giới thực và có thể kiểm chứng.

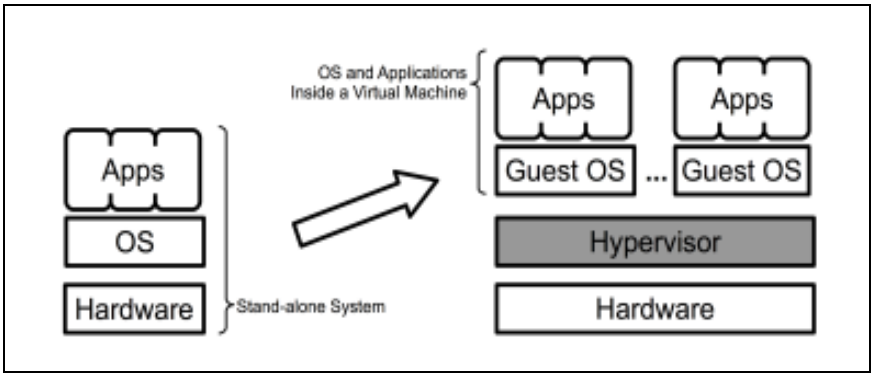
Tính sẵn sàng là đảm bảo sự kịp thời, không bị gián đoạn khi cần truy cập dữ liệu, hệ thống thông tin. Các hệ thống có tính sẵn sàng cao là các hệ thống có đầy đủ các biện pháp dự phòng, duy trì các bản sao lưu đáng tin cậy, có đầy đủ quy trình và thường xuyên diễn tập phản ứng sự cố. Một số nguy cơ đối với tính sẵn sàng dữ liệu như lỗi phần cứng, lỗi phần mềm, môi trường gặp vấn đề (lũ lụt, mất điện, cháy nổ và vv), nó bao gồm một số loại tấn công tập trung vào tính sẵn sàng của hệ thống nhưtấn công từ chối dịch vụ, đối tượng phá hoại và gián đoạn kết nối mạng.

Chương 1 - TỔNG QUAN VỀ MÔI TRƯỜNG ẢO HÓA VÀ ĐIỆN TOÁN ĐÁM MÂY

1.1. KHÁI NIỆM VÀ ĐẶC TRƯNG ẢO HÓA

1.1.1. Định nghĩa Ảo hóa

Định nghĩa Ảo hóa: Ảo hóa là công nghệ được thiết kế tạo ra tầng trung gian giữa hệ thống phần cứng máy tính và phần mềm chạy trên nó. Từ một máy vật lý có thể tạo ra nhiều máy ảo độc lập. Mỗi máy ảo đều được thiết lập một hệ thống riêng rẽ với hệ điều hành, ảo hóa mạng, ảo hóa hóa lưu trữ và các ứng dụng riêng. Ảo hóa có liên quan tới việc tạo ra các máy ảo (Virtual Machine) độc lập về hệ điều hành và các ứng dụng. Hơn nữa, Ảo hóa cho phép nhiều hệ điều hành và các ứng dụng khác nhau chia sẻ cùng một phần cứng. Hình 01 cho thấy ban đầu hệ điều hành và các ứng dụng được chạy trên phần cứng chuyên dụng, có thể được đặt trong một máy ảo và chia sẻ cùng một tài nguyên vật lý với các máy ảo khác.

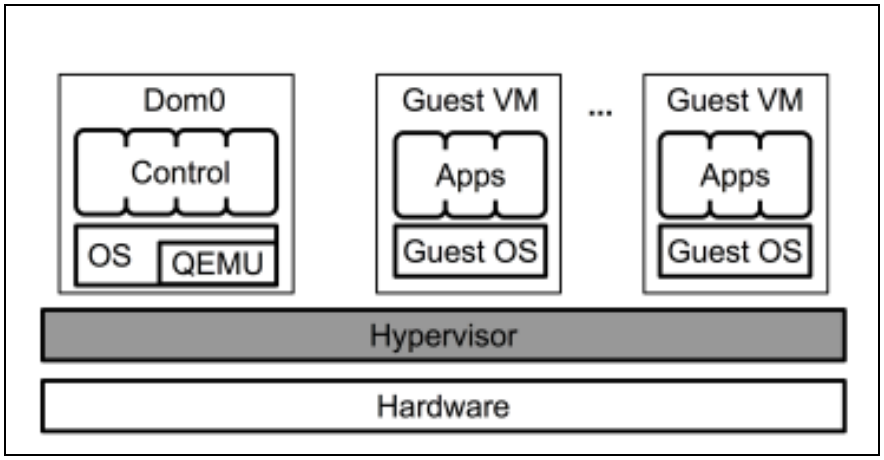


Hình 01: Mô hình Ảo hóa

Điểm khác biệt cốt lõi giữa bên trái và bên phải trong hình 4 chính là tầng Hypervisor. Hypervisor là phần mềm lõi của nền tảng ảo hóa, là tầng phần mềm thấp nhất có trách nhiệm tạo mới và duy trì các máy ảo. Hypervisor là một phần mềm nằm ngay trên phần cứng và bên dưới một hoặc nhiều hệ điều hành nó có nhiệm vụ quản lý các tiến trình, bộ nhớ, thiết bị vào ra (I/O), mạng và vv.

1.1.2. Phân loại nền tảng Ảo hóa

1.1.2.1. Kiểu 1: Bare Metal Hypervisor

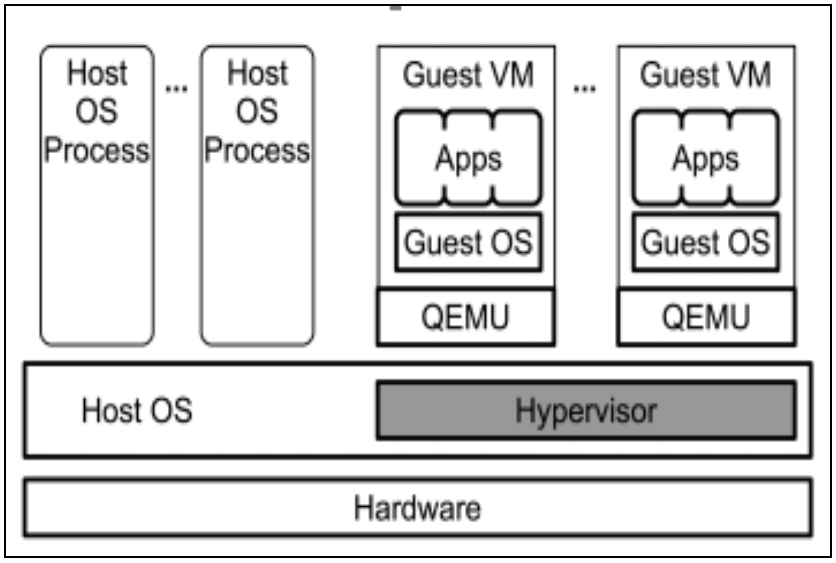


Hình 02: hypervisor kiểu 1-Hệ thống Xen

Kiểu 1: Lớp phần mềm lõi Hypervisor tương tác trực tiếp với phần cứng của máy chủ để quản lý, phân phối và cấp phát tài nguyên. Mục đích chính của nó là cung cấp các môi trường thực thi tách biệt được gọi là các partition (phân vùng) trong đó các máy ảo chứa các hệ điều hành (OS guest) có thể chạy. Mỗi phân vùng được cung cấp tập hợp các tài nguyên phần cứng riêng của nó chẳng hạn như bộ nhớ, các bộ vi xử lý CPU và thiết bị mạng. Hypervisor có trách nhiệm điều khiển và phân kênh truy cập đến các nền tảng phần cứng. Những hypervisor thuộc kiểu 1 là: VMware vSphere, Microsoft Hyper-V, Citrix Xen Server…v.v.

Quá trình máy ảo thuộc kiểu 1 liên lạc với tài nguyên phần cứng: Hypervisor mô phỏng phần cứng, điều này làm cho máy ảo tưởng rằng nó đang truy cập vào phần cứng thật. Hypervisor liên lạc với trình điều khiển thiết bị phần cứng (hay còn gọi là Drivers). Trình điều khiển thiết bị phần cứng liên lạc trực tiếp đến phần cứng vật lý.

1.1.2.2. Kiểu 2: Hosted Hypervisor



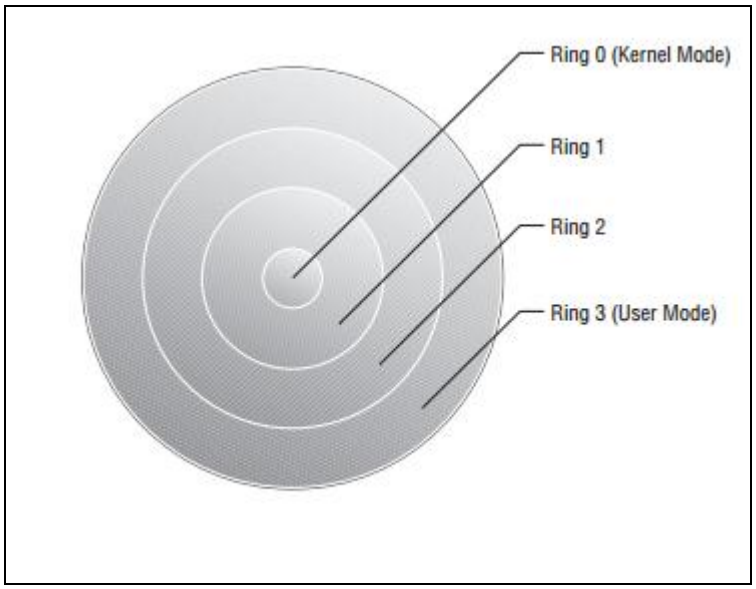
Hình 03: hypervisor kiểu 2-Hệ thống KVM

Loại nền tảng Ảo hóa số hai này chạy trên hệ điều hành như một ứng dụng được cài đặt trên máy chủ. Trên môi trường hypervisor kiểu 2, các máy ảo khách (những máy ảo được cài đặt trên máy thật thì gọi là máy ảo khách-guest virtual machine) chạy trên lớp Hypervisor. Điển hình của Hypervisor loại 2 là: Microsoft Virtual PC, Vmware Workstation, VMware Server.

Quá trình máy ảo liên lạc với tài nguyên phần cứng như sau: mô phỏng phần cứng Hypervisor sẽ tạo ra một phân vùng trên ổ đĩa cho các máy ảo. Hypervisor xây dựng mối liên lạc giữa hệ điều hành máy chủ Host và lớp ảo hóa bên trên. Khi một máy ảo truy xuất tài nguyên thì Hypervisor sẽ thay thế máy ảo đó gửi yêu cầu tới Hệ điều hành Host để thực hiện yêu cầu. Hệ điều hành liên lạc với trình điều khiển thiết bị phần cứng. Các trình điều khiển thiết bị phần cứng liên lạc đến các phần cứng trên

máy thực. Quá trình này sẽ xảy ra ngược lại khi có trả lời từ phần cứng vật lý đến hệ điều hành máy chủ Host.

1.1.3. Ảo hóa kiến trúc vi xử lý x86



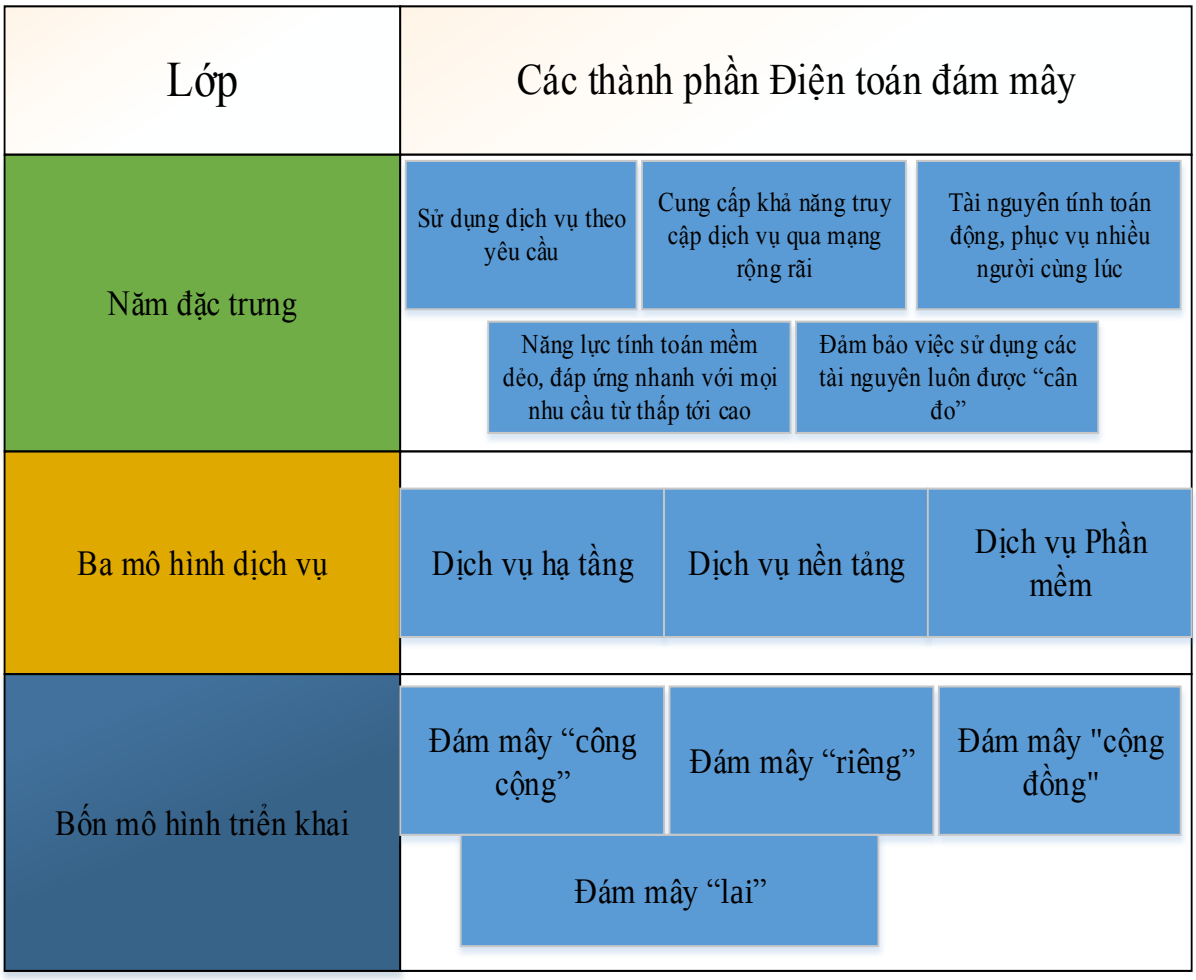
Hình 04: mức đặc quyền vi xử lý x86

Chìa khóa để hiểu biết rõ lớp hypervisor và các vấn đề an ninh thông tin chính là hiểu rõ mức đặc quyền trong kiến trúc vi xử lý x86. Để cung cấp một môi trường hoạt động an toàn, kiến trúc vi xử lý x86 cung cấp một cơ chế đặc biệt để cách ly ứng dụng người dùng và hệ điều hành bằng cách sử dụng các mức đặc quyền khác nhau. Mức đặc quyền trong hình *04* được mô tả bởi các vòng tròn đồng tâm nơi bắt đầu từ 0 đến 3. Mức 0 là là mức đặc quyền nhất, phần mềm chạy ở cấp độ này có toàn quyền kiểm soát các phần cứng cơ bản của máy chủ. Mức 3 là vòng có quyền ít nhất dùng cho phần mềm và phần ứng dụng hay thường gọi là chế độ người dùng. Mức 1 và 2 có thêm một số quyền sử dụng cho middleware. Để hiểu Hypervisor hoạt động như thế nào đầu tiên chúng ta cần hiểu thêm mô hình làm việc của hệ điều hành. Hầu hết mô hình hoạt động của hệ điều hành đều làm việc với 2 chế độ: chế độ người dùng: chỉ cho phép những lệnh cần thiết để tính toán và xử lý dữ liệu. Các ứng dụng chạy ở mode này và chỉ sử dụng phần cứng bằng cách thông qua kernel bằng lời gọi hệ thống. Chế độ nhân: cho phép chạy đầy đủ tập lệnh CPU, bao gồm cả các lệnh đặc quyền. Chế độ này chỉ dành cho hệ điều hành chạy. Hypervisor loại 1 được đề cập trong phần 1.1.2.1 được tích hợp với nền tảng hệ điều hành do vậy nó chạy ở mức 0, 1 hoặc/và 2. Còn hệ điều hành máy ảo chạy mức 3 [2]. Hypervisor loại 2 được đề cập trong phần 1.1.2.2 cả lớp hypervisor và hệ điều hành máy ảo khách đều hoạt động ở mức 3 như các ứng dụng riêng biệt, mục tiêu của mô hình là để an toàn cho phép máy ảo khách chạy mà không ảnh hưởng đến mức đặc quyền 0, mức mà có thể ảnh hưởng đến các nền tảng máy chủ cơ bản và các máy chủ khách khác, để thực hiện điều này các nền tảng Ảo hóa tạo ra một lớp đệm giữa mức 0 và hệ điều hành. Nó gọi là mức đặc quyền 0 ảo. Lớp Ảo hóa này cho phép nhiều máy ảo chạy nhiều hệ điều hành khác nhau trên

một máy chủ vật lý, cho phép thực hiện các cuộc gọi chuẩn đến phần cứng khi có yêu cầu bộ nhớ, đĩa và mạng hoặc các tài nguyên khác.

1.2. KHÁI NIỆM ĐIỆN TOÁN ĐÁM MÂY

Trong đề tài xem xét định nghĩa được đưa ra bởi Viện nghiên cứu tiêu chuẩn và công nghệ quốc gia Hoa Kỳ (NIST) [3]: Điện toán đám mây là mô hình điện toán sử dụng tài nguyên tính toán có khả năng thay đổi theo nhu cầu để lựa chọn và chia sẻ các tài nguyên tính toán (ví dụ: mạng, máy chủ, lưu trữ, ứng dụng và dịch vụ) cung cấp dịch vụ một cách nhanh chóng, thuận tiện. Có thể truy cập đến bất kỳ tài nguyên nào tồn tại trong "điện toán đám mây" tại bất kỳ thời điểm nào và từ bất kỳ đâu thông qua hệ thống Internet. Đồng thời cho phép kết thúc sử dụng dịch vụ, giải phóng tài nguyên dễ dàng, quản trị đơn giản, giảm thiểu các giao tiếp với nhà cung cấp".



Hình 05: Tổng quan điện toán đám mây

Một số nhà cung cấp dịch vụ điện toán đám mây tiên phong, dẫn đầu về công nghệ và mức độ phổ biến cũng như số lượng người dùng đông đảo như: Amazon Web Services bao gồm Elastic Compute Cloud (EC2), Amazon Simple Storage Service (S3). Dịch vụ EC2 giúp cho việc tạo ra, khởi động và dự phòng các ứng dụng ảo cho cá nhân hay doanh nghiệp một cách đơn giản và bất cứ khi nào. Dịch vụ Google App Engine hỗ trợ các giao diện lập trình ứng dụng cho khách hàng, xử lý ảnh, các tài khoản Google và các dịch vụ e-mail. Nhà cung cấp Microsoft cung cấp nền tảng

Windows Azure. Nền tảng Windows Azure là một nhóm các công nghệ đám mây cung cấp một tập hợp cụ thể của các dịch vụ cho các nhà phát triển ứng dụng.

1.3. ĐẶC TRƯNG ĐIỆN TOÁN ĐÁM MÂY

Điện toán đám mây có các đặc trưng chính như sau: đặc trưng thứ nhất là cho phép sử dụng dịch vụ theo yêu cầu. Đặc trưng thứ hai là cung cấp khả năng truy cập dịch vụ qua mạng rộng rãi từ máy tính để bàn, máy tính xách tay tới thiết bị di động. Đặc trưng thứ ba là tài nguyên tính toán động, phục vụ nhiều người cùng lúc. Đặc trưng tiếp theo là năng lực tính toán mềm dẻo, đáp ứng nhanh với mọi nhu cầu từ thấp tới cao. Đặc trưng thứ năm là đảm bảo việc sử dụng các tài nguyên luôn được "cân đo" để nhà cung cấp dịch vụ quản trị và tối ưu hóa được tài nguyên, đồng thời người dùng chỉ phải trả chi phí cho phần tài nguyên sử dụng thực sự.

1.4. MÔ HÌNH LỚP DỊCH VỤ CỦA ĐIỆN TOÁN ĐÁM MÂY

Mô hình dịch vụ điện toán đám mây được chia thành ba dịch vụ chính:

Hình 06: Mô hình ba dịch vụ điện toán đám mây

1.4.1. Hạ tầng hướng dịch vụ

Mô hình hạ tầng hướng dịch vụ là dịch vụ cung cấp cơ sở hạ tầng cơ bản cho một hệ thống Thông tin bao gồm: tài nguyên máy chủ ảo, máy tính ảo hóa, hệ thống lưu trữ, thiết bị mạng, thiết bị an ninh thông tin. Khách hàng sử dụng dịch vụ không phải đầu tư mua sắm thiết bị hạ tầng vật lý và không phải bỏ thêm chi phí bảo trì và sao lưu hệ thống. Khách hàng sử dụng dịch vụ tự cài đặt và triển khai các phần mềm, ứng dụng của mình trên cơ sở hạ tầng đám mây. Một số nhà cung cấp dịch vụ trên thế giới như Amazon với dịch vụ EC2, Microsoft với dịch vụ hạ tầng Azure và nhà cung cấp Google Compute Engine, HP Coud, Rackspace Cloud...Một số nhà cung cấp dịch vụ hạ tầng tại Việt Nam: Viettel IDC, Viễn Thông FPT, VNPT IDC. Tại Viêt Nam mô hình hạ tầng hướng dịch vụ là loại dịch phổ biến nhất vì dịch vụ hạ tầng hướng dịch vụ là dịch vụ cơ bản nhất, dễ triển khai và cung cấp cho khách hàng.

1.4.2. Dịch vụ nền tảng

Cung cấp nền tảng cho phép khách hàng tự phát triển và chạy thử các phần mềm, ứng dụng phục vụ nhu cầu tính toán. Dịch vụ nền tảng được cung cấp dưới một số dạng phổ biến như: công cụ lập trình, ngôn ngữ lập trình, cơ sở dữ liệu. Dịch vụ nền tảng còn có thể được xây dựng riêng và cung cấp cho khách hàng thông qua một giao diện lập trình riêng được gọi là các API. Khách hàng xây dựng ứng dụng và tương tác với hạ tầng Điện toán đám mây thông qua API. Ở mức dịch vụ nền tảng, khách hàng không quản lý nền tảng Điện toán đám mây hay các tài nguyên như hệ điều hành, thiết bị mạng. Một số nhà cung cấp dịch vụ nền tảng như: Amazon AWS, Foundy, Saleforce Force.com và OrangeScape.

1.4.3. Dịch vụ Phần mềm

Cung cấp các ứng dụng hoàn chỉnh như một dịch vụ theo yêu cầu cho nhiều khách hàng. Khách hàng không cần quan tâm tới hay bỏ công sức triển khai phần mềm, quản lý tài nguyên tính toán. Khách hàng có thể sử dụng phần mềm từ xa, mọi lúc mọi nơi bằng trình duyệt web hoặc các thiết bị di động. Mô hình dịch vụ phần mềm ngày càng trở nên phổ biến bởi tính thuận tiện và hiệu quả chi phí cao. Dịch vụ phần mềm phát triển mạnh ở các ứng dụng như: thư điện tử, quản lý nguồn lực, quản lý nhân sự, quản lý Khách hàng.

1.5. MÔ HÌNH TRIỂN KHAI ĐIỆN TOÁN ĐÁM MÂY

1.5.1. Đám mây công cộng

Mô hình đám mây công cộng là mô hình Điện toán đám mây (dịch vụ hạ tầng, dịch vụ nền tảng, phần mềm hoặc hạ tầng ứng dụng) được một tổ chức cung cấp dưới dạng dịch vụ rộng rãi cho tất cả các khách hàng thông qua hạ tầng mạng Internet. Nhà cung cấp điện toán đám mây công cộng có trách nhiệm cài đặt, quản lý, cung cấp và bảo trì. Khách hàng chỉ phải trả chi phí cho các tài nguyên mà họ sử dụng. Các ứng dụng khác nhau chia sẻ chung tài nguyên tính toán, mạng và lưu trữ. Do vậy, hạ tầng Điện toán đám mây công cộng được thiết kế để đảm bảo cô lập về dữ liệu giữa các khách hàng và tách biệt về truy cập. Các dịch vụ đám mây công cộng hướng tới số lượng khách hàng lớn nên có năng lực về hạ tầng cao, đáp ứng nhu cầu tính toán linh hoạt, chi phí thấp. Khách hàng sử dụng dịch vụ trên đám mây công cộng chủ yếu là khách hàng cá nhân và doanh nghiệp nhỏ, họ có được lợi ích trong việc dễ dàng tiếp cận các ứng dụng công nghệ cao, chất lượng mà không phải đầu tư ban đầu, chi phí sử dụng thấp, linh hoạt.

1.5.2. Đám mây riêng

Đám mây riêng là mô hình trong đó hạ tầng đám mây được sở hữu bởi một tổ chức, doanh nghiệp và chỉ phục vụ cho người dùng của tổ chức, doanh nghiệp đó. Tổ chức, doanh nghiệp có trách nhiệm tự thiết lập và bảo trì đám mây riêng của mình hoặc có thể thuê vận hành bởi một bên thứ ba. Hạ tầng đám mây có thể được đặt bên trong hoặc bên ngoài tổ chức ví dụ có thể đặt tại một bên thứ ba như các trung tâm dữ

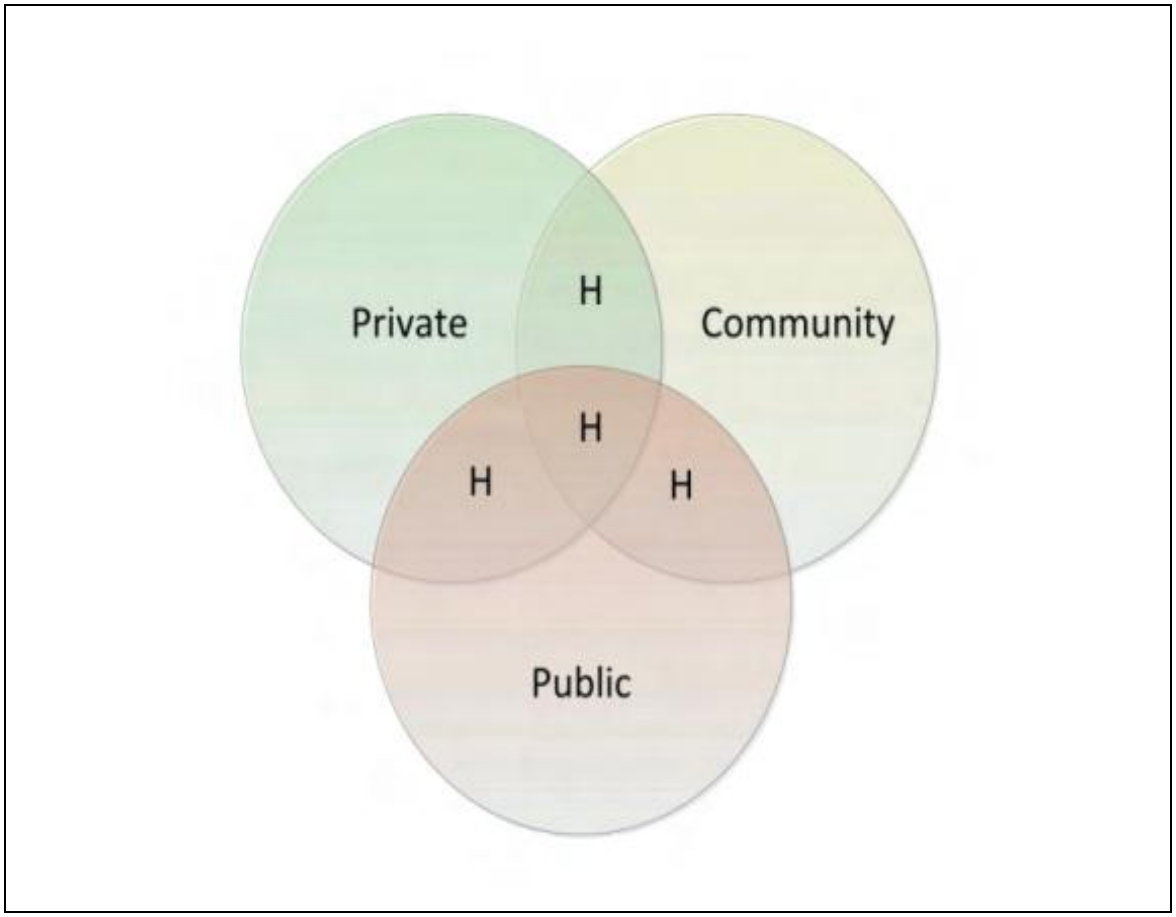
liệu. Đám mây riêng được các tổ chức, doanh nghiệp lớn xây dựng cho mình nhằm khai thác ưu điểm về công nghệ và khả năng quản trị của điện toán đám mây mà vẫn giữ được sự an tâm về vấn đề an ninh dữ liệu và chủ động trong công tác quản lý.

1.5.3. Đám mây cộng đồng

Đám mây cộng đồng là mô hình trong đó hạ tầng đám mây được chia sẻ bởi một số tổ chức cho cộng đồng người dùng trong các tổ chức đó. Các tổ chức này do đặc thù không tiếp cận tới các dịch vụ đám mây công cộng và chia sẻ chung một hạ tầng công cộng để nâng cao hiệu quả đầu tư và sử dụng.

1.5.4. Đám mây lai

Mô hình đám mây lai là mô hình kết hợp của các đám mây công cộng và đám mây riêng. Đám mây này thường do các doanh nghiệp tạo ra và trách nhiệm quản lý bảo trì sẽ được phân chia rõ giữa doanh nghiệp và nhà cung cấp đám mây công cộng.



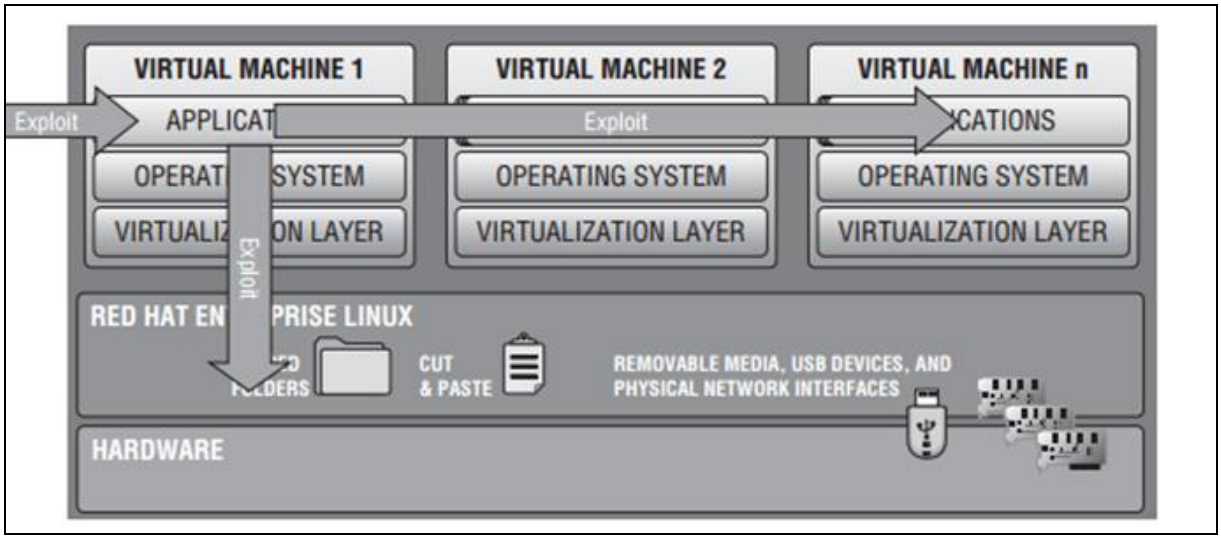
Hình 07: Mô hình đám mây lai

Chương 2 - CÁC NGUY CƠ, THÁCH THỨC AN NINH THÔNG TIN TRONG MÔI TRƯỜNG ẢO HÓA VÀ ĐIỆN TOÁN ĐÁM MÂY

Môi trường Ảo hóa và Điện toán đám mây gặp phải nguy cơ và thách thức an ninh thông tin tương tự như môi trường vật lý tuy nhiên trong môi trường Ảo hóa và điện toán Đám mây có một số nguy cơ và thách thức nghiêm trọng hơn. Trong nội dung đề tài sẽ tập trung đi sâu tìm hiểu các các mối đe dọa và rủi ro an ninh thông tin nghiêm trọng và khác biệt của Ảo hóa và Điện toán đám mây so với môi trường vật lý hiện tại.

2.1. MỐI ĐE DỌA, RỦI RO AN NINH THÔNG TIN MÔI TRƯỜNG ẢO HÓA

Trong hình 08 phía dưới chỉ ra các con đường mà kẻ tấn công có thể tấn công vào môi trường Ảo hóa. Tấn công giữa các máy ảo nhờ khai thác lỗ hổng trên ứng dụng, hệ điều hành của các máy ảo. Cũng có thể là tấn công từ máy ảo xuống các máy chủ Host hoặc tấn công vật lý hoặc tấn công trực tiếp vào lớp phần mềm lõi Hypervisor.



Hình 08: Các hướng khai thác tấn công môi trường ảo

2.1.1. Tồn tại lỗ hổng bảo mật trong phần mềm lõi của nền tảng Ảo hóa (hypervisor)

Phần mềm Ảo hóa lõi là nền tảng cơ bản của môi trường Ảo hóa. Tất cả các máy chủ ảo đều phụ thuộc vào nó và khi một ai đó truy cập được vào giao diện quản lý, toàn bộ cơ sở hạ tầng đều có thể sẽ bị chiếm quyền kiểm soát. Nền tảng Ảo hóa phát triển dựa trên phần mềm vì vậy chính chúng cũng tồn tại các lỗ hổng bảo mật. Các nhà nghiên cứu đã tìm thấy một số lỗ hổng bảo mật trên nền tảng Ảo hóa. Tháng 5 năm 2009 thế giới an ninh thông tin đã xôn xao về một công cụ được phát hành bởi tổ chức Immunity Inc, công cụ này khai thác lỗ hổng trên nền tảng Ảo hóa VMware, công cụ này khai thác lỗi tràn bộ đệm trình điều khiển màn hình máy ảo. Lỗ hổng cho phép mã độc hại thực thi được trên máy chủ Host từ bên trong máy chủ ảo Khách. Tháng ba năm 2010 hãng Ảo hóa VMware thông báo về một loạt các lỗ hổng bảo mật

nghiêm trọng ảnh hưởng trên nền tảng Ảo hóa ESX và ESXi. Nhân điều khiển dịch vụ điều khiển trong gói mã nguồn mở được cài đặt trong Service Console OS có nhiều vấn đề sai sót. Những vấn đề này có thể dẫn đến tấn công từ chối dịch vụ từ xa, thực thi mã độc hại, nâng quyền và nhiều vấn đề an ninh thông tin khác. Hơn 40 lỗ hổng đã được phát hiện và công bố (CVE Common Vulnerabilities and Exposures). Các lỗ hổng còn được tìm thấy trên các nền tảng Ảo hóa khác như Xen, Hyper-V tuy nhiên họ không công bố rộng rãi do thị phần so với hãng VMware trong lĩnh vực Ảo hóa.

Dựa trên thông tin từ các cơ sở dữ liệu về lỗ hổng bảo mật của các tổ chức sau: NIST's National Vulnerability Database, SecurityFocus, Red Hat's Bugzilla, and CVE Details cho thấy đến năm 2012 có 115 lỗ hổng được tìm thấy trên Xen và 79 lỗ hổng bảo mật được tìm thấy trên KVM.

Bảng 1: Các lỗ hổng bảo mật được phát hiện và công bố năm 2012

Ảnh hưởng	**Lỗ hổng hệ thống Ảo hóa XEN**	**Lỗ hổng hệ thống Ảo hóa KVM**
Tính bí mật	30	23
Tính toàn vẹn	31	21
Tính sẵn sàng	54	35

2.1.1. Tấn công chéo giữa các máy ảo

Các thách thức an ninh hiện nay chính là việc tấn công giữa các máy ảo và điểm mù trong việc phát hiện các tấn công khi chỉ dựa vào các hệ thống biện pháp an ninh truyền thống. Tùy thuộc vào thiết lập, nhiều máy ảo có thể được kết nối mạng qua một thiết bị chuyển mạch ảo để cung cấp mạng ảo. Khi một mối đe dọa xâm nhập vào một máy ảo, các mối đe dọa có thể lan sang các máy ảo khác trên cùng một máy chủ vật lý và các biện pháp an ninh truyền thống như tường lửa, thiết bị phát hiện xâm nhập, hệ thống phòng chống thất thoát dữ liệu dựa trên phần cứng có thể bảo vệ máy chủ vật lý, nhưng không thể bảo vệ các máy chủ Ảo hóa vì dữ liệu không đi qua mạng vật lý. Bên cạnh đó khi hệ thống ảo hóa lõi (hypervisor) tồn tại lỗ hổng và bị tấn công dẫn tới mất quyền kiểm soát các máy chủ ảo hóa đang hoạt động trên hệ thống lõi.

2.1.2. Hệ điều hành máy ảo cô lập.

Một máy ảo có thể được tạo ra trong vài giây, nó có thể không được cập nhật bản vá lỗ hổng bảo mật trong một thời gian dài hoặc cấu hình không đúng từ người quản trị hệ thống. Đặc biệt lợi thế của hệ thống ảo hóa là các máy chủ ảo có khả năng nhân bản từ bản ban đầu một cách nhanh chóng. Rủi ro chính từ đây khi các máy chủ gốc không được cập nhật kịp thời các bản vá lỗ hổng bảo mật. Nghiêm trọng hơn máy ảo gốc bị nhiễm mã độc được nhân bản sẽ làm cho mã độc lây lan trên phạm vi rộng hơn. Không giống như các máy chủ vật lý truyền thống, khi một máy chủ ảo hóa ở chế độ ẩn, nó vẫn còn có thể truy cập lưu trữ máy ảo trên mạng, và do đó dễ bị lây nhiễm phần mềm độc hại. Tuy nhiên, khi máy ảo không hoạt động hoặc ở dưới chế độ ẩn các phần mềm diệt Virus không có khả năng quét và phát hiện mã độc hại và Virus.

2.1.3. Thất thoát dữ liệu giữa các thành phần Ảo hóa

Đã ghi nhận trường hợp phần mềm quản lý tập trung vCenter của hãng VMware bị xâm nhập, từ đó những kẻ tấn công có thể sao chép một máy ảo và sử dụng máy ảo này để xâm nhập dữ liệu. Khi rất nhiều máy ảo được chạy trên cùng một hạ tầng vật lý, vấn đề về tuân thủ có thể phát sinh. Nếu một máy ảo có chứa các thông tin nhạy cảm được đặt cùng với các máy ảo không nhạy cảm trên cùng máy chủ vật lý, sẽ khó khăn hơn để quản lý và bảo vệ dữ liệu. Các máy ảo được lưu dưới dạng file có thể dễ dàng chuyển sang một máy chủ ảo hóa khác để chạy, một số rủi ro bảo mật xảy ra khi dữ liệu không truyền không được mã hóa, lỗ hổng bảo mật trong lớp hypervisor cho phép kẻ tấn công có thể kiểm soát dữ liệu trong quá trình di chuyển.

2.1.4. Sự phức tạp trong công tác quản lý kiểm soát truy cập

Tất cả các hệ thống Công nghệ Thông tin đều phải đối mặt với các mối đe dọa đến từ: thao tác sai của nhân viên quản trị tuy nhiên đối với hệ thống ảo hóa nó nghiêm trọng hơn nhiều. Ảo hóa là một hệ thống động, sự kết hợp nhiều máy ảo trên cùng một máy chủ vật lý Host, việc dễ dàng bật, tắt, khởi động, tạo bản sao lưu và di chuyển máy ảo giữa các máy chủ vật lý dẫn tới lỗ hổng bảo mật hoặc lỗi cấu hình có thể bị nhân bản một cách nhanh chóng. Rất khó để duy trì trạng thái an ninh phù hợp của một máy ảo ở thời điểm vì tính động và khả năng mở rộng nhanh chóng của máy ảo. Ảo hóa phá vỡ phân quyền truyền thống, quản trị viên chỉ cần ấn một nút là có thể di chuyển và tắt một máy ảo mà không cần có sự chấp thuận từ bộ phận quản lý tài sản hay sự đồng ý của nhóm bảo mật công nghệ thông tin. Ví dụ các quản trị viên có thể vô tình sử dụng công cụ quản trị máy ảo tập trung để chuyển một máy chủ sang một phần cứng khác vì lý do bảo trì kỹ thuật và không hề nhận thấy đường dẫn mới đang nằm trên một phân hệ mạng không an toàn.

2.1.5. Lây nhiễm mã độc hại.

Năm 2006-2008 một vụ tấn công môi trường ảo hóa nghiêm trọng đã xảy ra. Kẻ tấn công chiếm quyền điều khiển hệ thống máy chủ ảo hóa Vmware ESX. Sau khi chiếm được quyền truy cập kẻ tấn công đã cài đặt Rootkit vào máy chủ ảo hóa ESX để đánh cắp thông tin tài khoản thẻ tín dụng, thông qua kỹ thuật nghe lén dữ liệu truyền đến máy chủ cơ sở dữ liệu, hậu quả là từ 140 đến 180 triệu thẻ tín dụng đã bị đánh cắp. Có hai kịch bản chính phần mềm mã độc hại tấn công hệ thống ảo hóa. Hoặc là máy ảo tồn tại trên máy chủ Host và tấn công các máy ảo hoặc mối đe dọa trên máy ảo tấn công máy chủ Host. Mối nguy cơ còn tiềm ẩn trên chính công nghệ Virtualization Technology của Intel hoặc AMD Virtualization một công nghệ phần cứng được phát triển đảm bảo sự tích hợp của các cơ sở hạ tầng với nền tảng ảo hóa. Có thể xảy ra việc kẻ tấn công sử dụng các rookit dạng Blue Pill nhúng kèm phần cứng để xâm nhập các máy chủ ảo.

2.1.6. Tranh chấp tài nguyên.

Hệ thống bảo mật truyền thống như hệ thống phòng chống mã độc không được thiết kế cho môi trường ảo hóa. Ví dụ việc quét virus đồng thời và cập nhật mẫu nhận dạng Virus mới có thể dẫn tới việc quá tải đối với hệ thống ảo hóa. Vấn đề quá tải hệ thống ảo hóa không chỉ gặp phải khi hệ thống phòng chống mã độc quét hoặc cập nhật đồng thời mà nó còn gặp phải khi các hệ thống bảo mật truyền thống khác hoạt động trên hệ thống ảo hóa. Bởi vì các máy ảo bản chất là chia sẻ tài nguyên máy chủ chẳng hạn như bộ nhớ, vi xử lý, đĩa cứng, thiết bị vào/ra vì vậy nguy cơ tăng lên nhiều, các máy ảo có nhiều tầng phức tạp hơn một hệ thống truyền thống vì vậy các biện pháp phòng chống tấn công từ chối dịch vụ truyền thống có thể không hiệu quả. Hay đơn giản hơn chỉ là hoạt động đĩa đồng thời, chẳng hạn như cập nhật phần mềm hoặc khởi động lại nhiều máy ảo sau khi vá lỗ hổng bảo mật có thể tạo ra một lượng truy cập I/O tăng vọt trên máy chủ vật lý, nó có khả năng làm giảm hiệu suất của máy chủ. Việc quét toàn bộ các ổ đĩa máy ảo làm hiệu suất và hệ thống của máy chủ ảo hóa giảm đáng kể trong khi chúng ta đang cố gắng tối ưu bộ nhớ, bộ vi xử lý

Bảng 2: Vấn đề an toàn thông tin của môi trường ảo hóa chiếu theo mô hình CIA

STT	Vấn đề bảo mật của môi trường ảo hóa	Tính bí mật	Tính toàn vẹn	Tính sẵn sàng
1	Tồn tại lỗ hổng bảo mật trong phần mềm lõi nền tảng ảo hóa	x		
2	Lây nhiễm mã độc hại	x		
3	Tranh chấp tài nguyên			x
4	Các tấn công giữa các máy ảo	x	x	x
5	Sự phức tạp trong công tác quản lý, vận hành			x
6	Thất thoát dữ liệu giữa các thành phần ảo hóa	x	x	

2.2. MỐI ĐE DỌA AN NINH THÔNG TIN TRONG MÔI TRƯỜNG ĐIỆN TOÁN ĐÁM MÂY

Trong một vài năm gần đây ghi nhận nhiều cuộc tấn công nhằm vào dịch vụ điện toán đám mây: Tháng 9/2014 - dịch vụ lưu trữ online Apple's iCloud bị tấn công. Tháng 3/2013 – Dịch vụ ghi chú nổi tiếng Evernote’s Cloud bị tấn công dẫn tới lộ thông tin hơn 50 triệu tài khoản Khách hàng. Tháng 6/2014 – Dịch vụ Code Spaces Amazon Web Services cloud service EC2 bị tấn công. Một số mã nguồn bị kẻ tấn công xóa bỏ hoặc chèn nội dung độc hại.

2.2.1. Các mối đe dọa an ninh thông tin đối với Điện toán đám mây

Bảng 3: các mối đe dọa đối với điện toán đám mây

Mối đe dọa	Mô tả
Tính bí mật	
Mối đe dọa từ nhân viên của các nhà cung cấp dịch vụ điện toán đám mây. [4]	Người dùng sử dụng dịch vụ Điện toán đám mây rất quan tâm đến những cam kết của nhà cung cấp dịch vụ điện toán đám mây như: cơ chế giám sát hoạt động nhân viên của mình trên hệ thống, có tách biệt nhiệm vụ, vai trò giữa người thực hiện, người phê duyệt và kiểm soát thay đổi hay không, thủ tục quy trình vận hành của nhà cung cấp Điện toán đám mây như thế nào trước khi tin tưởng giao dữ liệu, thông tin cho nhà cung cấp dịch vụ Điện toán đám mây. Khách hàng lo ngại mối đe dọa đến từ nhân viên của đơn vị cung cấp dịch vụ điện toán đám mây. Ví dụ: do hành động vô tình hoặc cố ý của nhân viên quản trị có thể làm lộ tính bí mật dữ liệu của Khách hàng do cán bộ quản trị có thể tiếp xúc và tương tác trực tiếp với dữ liệu Khách hàng. Các mối đe dọa còn đến từ các cựu nhân viên, người quản trị hệ thống, đối tác kinh doanh, cộng tác viên. Mục đích cũng khác nhau, đơn giản chỉ như lấy dữ liệu, hay trầm trọng là muốn phá hoại. Trong bối cảnh điện toán đám mây, nguy cơ này tỏ ra nguy hiểm hơn rất nhiều vì người bên trong có thể phá huỷ toàn bộ hệ thống hoặc thay đổi dữ liệu. Một ví dụ khác là cán bộ quản trị có thể vô tình sao chép dữ liệu nhạy cảm của khách hàng A lên một máy chủ khách hàng B nào đó.
Cung cấp ảnh máy ảo và ứng dụng sẵn có	Một trong những lợi ích lớn của điện toán đám mây là số lượng các máy ảo được tạo chuẩn bị sẵn, các ứng dụng tạo sẵn để sẵn sàng sử dụng khi cần đến. Ví dụ như Amazon Machine Images (AMIs). Các máy ảo được tạo sẵn cho mục đích máy chủ website, máy chủ cơ sở dữ liệu. Một số chuyên gia an ninh thông tin đã tìm thấy vấn đề có thể tạo ra các cửa sau vào các ảnh máy ảo được tạo sẵn, khi một Khách hàng mới sử dụng chúng vô tình máy chủ bị điều khiển từ xa. Một lí do nữa là các máy ảo tạo sẵn thường bật sẵn các giao thức cho phép kết nối từ xa như SSH có đi kèm các khóa truy cập.
Tấn công từ bên ngoài hệ thống: 1/. Tấn công khai thác lỗ hổng trong phần	Các tấn công từ bên ngoài là các vấn đề mà điện toán đám mây trên Internet công cộng gặp phải, toàn bộ các mô hình cung cấp điện toán đám mây bị ảnh hưởng bởi tấn công bên ngoài. Các nhà cung cấp điện toán đám mây lưu trữ dữ liệu

mềm, ứng dụng 2/. Xâm nhập trái phép. 3/. Sử dụng kỹ thuật lừa đảo để đánh cắp tài khoản và mật khẩu truy cập hệ thống. 4/. Tấn công vào phiên làm việc hợp lệ trên máy tính. 5/. Lây nhiễm mã độc, virus	thẻ tín dụng, thông tin cá nhân và thông tin nhạy cảm của chính phủ và thông tin sở hữu trí tuệ sẽ phải chịu các cuộc tấn công từ các nhóm tin tặc chuyên nghiệp, có quy mô và nguồn lực rất lớn cố gắng đánh cắp dữ liệu. Chúng tấn công tấn công liên tục các mục tiêu. Ví dụ: tin tặc khai thác các lỗ hổng bảo mật trên hệ thống Điện toán đám mây để xâm nhập trái phép hệ thống, thiết lập và mở các cổng sau trái phép, cài đặt virus. Tin tặc còn sử dụng chính những phiên đăng làm hợp lệ do người dùng không thoát hệ thống đúng cách khi không còn làm việc. Ví dụ năm 2011 hệ thống Sony Play Station Network bị tấn công, hàng triệu tài khoản bị lộ thông tin, dẫn tới nhà cung cấp dịch vụ Sony phải đóng hoàn toàn dịch vụ nhằm điều tra nguyên nhân sự cố. Trong sự cố này Sony thiệt hại tới 170 triệu đô la.
Sự can thiệp chính phủ	Điện toán đám mây phổ biến toàn cầu, dịch vụ điện toán đám mây được cung cấp bởi các nhà cung cấp dịch vụ khác nhau đặt tại các nước khác nhau. Chính phủ các nước sở tại có thẩm quyền nắm rõ dữ liệu đặt tại các trung tâm dữ liệu đặt trong lãnh thổ nước họ. Một số chính phủ ban hành luật nhằm trao cho họ quyền truy cập dữ liệu khách hàng nhằm mục đích chống khủng bố, điều tra tội phạm, hay ngăn chặn khiêu dâm trẻ em, tuy nhiên một số chính phủ còn sử dụng chính lợi thế chính trị của mình để truy cập dữ liệu của người dùng đặt tại các trung tâm dữ liệu trong lãnh thổ nước họ mà không biện minh rõ lí do. Thông thường một số nhà cung cấp dịch vụ điện toán đám mây sẽ thông báo cho Khách hàng của mình và chỉ cho phép chính phủ tiếp xúc với dữ liệu bản sao. Tuy nhiên không phải lúc nào cũng như vậy. Ví dụ: Chính phủ Mỹ buộc tổ chức SWIFT cung cấp thông tin dữ liệu thanh toán, chuyển tiền giữa các chính phủ, tổ chức, liên ngân hàng.
Thất thoát dữ liệu	Thất thoát dữ liệu có thể xảy ra do nhiều nguyên nhân: do các đối thủ cạnh tranh, sử dụng chung một nhà cung cấp dịch vụ điện toán đám mây, do lỗi phần cứng, do thao tác sai của con người. Môi trường đám mây cũng có cùng những rủi ro bảo mật với các hệ thống mạng doanh nghiệp thông thường, nhưng vì có rất nhiều dữ liệu chứa trên các máy chủ đám mây nên nhà cung cấp trở thành đích ngắm hấp dẫn cho kẻ xấu. Mức rủi ro còn tuỳ thuộc vào độ nhạy cảm của dữ liệu. Có

	thể những thông tin về tài chính cá nhân có mức độ nhạy cảm cao nhất, nhưng có thể đó cũng là những thông tin về sức khoẻ, bí mật thương mại, sở hữu trí tuệ… và chúng có sức tàn phá ghê gớm nếu bị rò rỉ.
Tính toàn vẹn	
Dữ liệu bị tách rời:	Môi trường điện toán đám mây phức hợp như mô hình SaaS-chia sẻ tài nguyên tính toán có thể tạo nên nguy cơ chống lại sự toàn vẹn của dữ liệu nếu tài nguyên hệ thống không được tách biệt một cách hiệu quả.
Truy cập tài khoản:	Thủ tục kiểm soát truy cập yếu tạo ra nhiều nguy hiểm cho hệ thống điện toán đám mây, ví dụ vì lí do bất mãn với tổ chức, nhân viên đã nghỉ việc của đơn vị cung cấp dịch vụ điện toán đám mây sử dụng truy cập từ xa được thiết lập từ khi còn làm việc để quản lý dịch vụ đám mây của Khách hàng và có thể gây hại, phá hủy dữ liệu của khách hàng.
Chất lượng dữ liệu:	Các mối đe dọa đối với chất lượng dữ liệu tăng lên đối với nhà cung cấp dịch vụ điện toán đám mây chứa nhiều dữ liệu Khách hàng.
Tính sẵn sàng.	
Quản lý thay đổi:	Nhà cung cấp điện toán đám mây có trách nhiệm lớn hơn trong việc quản lý thay đổi trong tất cả các mô hình cung cấp điện toán đám mây, nó là mối đe dọa rất lớn vì thay đổi có thể gây ra các ảnh hưởng tiêu cực. Ảnh hưởng tiêu cực do việc thay đổi phần mềm và phần cứng của các dịch vụ Điện toán đám mây hiện tại. Ví dụ Khách hàng thực hiện kiểm thử xâm nhập hệ thống, thử tải gây ảnh hưởng đến Khách hàng sử dụng điện toán đám mây khác. Thay đổi cơ sở hạ tầng Điện toán đám mây theo yêu của khách hàng hoặc theo yêu cầu bên thứ ba làm ảnh hưởng đến Khách hàng khác
Tấn công từ chối dịch vụ:	Kiểu tấn công từ chối dịch vụ DoS (denial of service) có đã lâu, nhưng nhờ vào điện toán đám mây phát triển mà kiểu tấn công này càng mạnh hơn, chính vì tính sẵn sàng và nguồn tài nguyên tính toán sẵn có của điện toán đám mây. Có nhiều hình thức tấn công từ chối dịch vụ khác nhau, phổ biến: tấn công truy vấn phân giải tên miền liên tục các máy chủ phân giải tên miền (DNS) hoặc tấn công chiếm dụng một lượng lớn tài nguyên mạng như băng thông, bộ nhớ bằng cách gửi các email, truy vấn, files có dung lượng lớn. Tấn công từ chối dịch vụ bằng cách tạo ra các truy cập ứng dụng với số lượng

	và tần suất rất lớn từ nhiều máy tính khác nhau, hoặc khai thác các điểm yếu bảo mật tồn tại trên ứng dụng. Khi bị tấn công, hệ thống điện toán đám mây hoạt động chậm chạp, thậm chí một số dịch vụ còn bị ngừng hoặc gián đoạn hoạt động. những người dùng hợp pháp không thể truy cập và sử dụng vào dịch vụ. Tấn công từ chối dịch vụ tiêu tốn rất nhiều năng lượng, tài nguyên, thời gian và tiền bạc. Mục tiêu chính của tấn công từ chối dịch vụ là các dịch vụ Điện toán đám mây công cộng.
Gián đoạn vật lý	Sự gián đoạn của dịch vụ Công nghệ thông tin cung cấp dịch vụ điện toán đám mây có thể đến từ gián đoạn vật lý:hỏng hóc phần cứng, mất điện hoặc thảm họa về môi trường như lũ lụt, hỏa hoạn hoặc có thể đến từ sự gián đoạn kết nối với bên cung cấp dịch thứ 3
Mối đe dọa do quy trình khôi phục hệ thống, duy trì kinh doanh khi xảy ra thảm họa có nhiều yếu kém và bất cập	Dữ liệu lưu trữ trong Điện toán đám mây không sẵn sàng và đầy đủ trong và sau khi xảy thảm họa do các nguyên nhân sau: bản sao lưu không đảm bảo, không thường xuyên diễn tập khôi phục hệ thống, không có trung tâm dữ liệu dự phòng hoặc trong khi xảy ra sự cố việc phân tích sự cố không chính xác dẫn tới giải pháp không hiệu quả và làm trầm trọng thêm vấn đề.

2.2.2. Các rủi ro an ninh thông tin đối với điện toán đám mây

Bảng 4: Các rủi ro an ninh thông tin đối với điện toán đám mây [5]

Rủi ro	Mô tả
Tài khoản đặc quyền	Nhà cung cấp dịch vụ điện toán đám mây có quyền truy cập không giới hạn vào dữ liệu người dùng.
Ví trí lưu trữ dữ liệu	Khách hàng có thể không biết nơi lưu trữ dữ liệu của họ trên đám mây, có thể có nguy cơ dữ liệu bí mật được lưu trữ cùng với thông tin của Khách hàng khác.
Xử lý dữ liệu	Xử lý và xóa, tiêu hủy vĩnh viễn dữ liệu là một rủi ro với điện toán đám mây, đặc biệt là nơi tài nguyên lưu trữ được tự động cấp cho Khách hàng dựa trên nhu cầu của họ. Các nguy cơ dữ liệu không bị xóa trong trong máy ảo, nơi lưu trữ, sao lưu và các thiết bị vật lý càng tăng cao.
Giám sát bảo vệ dữ liệu	Khả năng cho Khách hàng sử dụng dịch vụ điện toán đám mây tham gia và thực hiện điều tra số trong điện toán mây có thể bị giới hạn bởi các mô hình cung cấp, kiến trúc phức tạp của điện toán đám mây. Khách hàng không thể triển khai hệ thống giám sát trên cơ sở hạ tầng mà họ không sở hữu, họ phải dựa vào hệ thống được sử dụng bởi các nhà cung cấp dịch vụ điện toán đám mây để hỗ trợ điều tra số. Vấn đề tiếp theo cần quan tâm, đó là kiểm toán các thao tác được thực hiện bởi cả người dùng lẫn quản trị. Khi doanh nghiệp sử dụng nhiều dịch vụ thì có thể sẽ có sự nhầm lẫn trong việc phân quyền. Về nguyên tắc, admin có quyền "làm tất cả" nên sẽ có khả năng hủy hoại hệ thống, dù cho hệ thống chạy trên mạng cục bộ hay chạy trên đám mây. Chỉ cần một vài lệnh của admin là toàn bộ dữ liệu có thể bị xóa, các bản sao lưu cũng có thể bị tiêu hủy. Nhưng trong trường hợp điện toán đám mây, sự hủy hoại này đơn giản và gây hậu quả nghiêm trọng hơn nhiều. ComputerWorld đã dẫn ví dụ về trường hợp admin của một doanh nghiệp, do bức xúc với lãnh đạo, nên đã "phẩy tay" xóa sổ gần một trăm máy chủ làm việc trên VMware vSphere. Nếu sử dụng SaaS thì tình hình có khác đôi chút. Admin của nhà cung cấp dịch vụ có thể xóa cả chục máy tính (ảo) chứa dữ liệu của khách hàng, còn admin của doanh

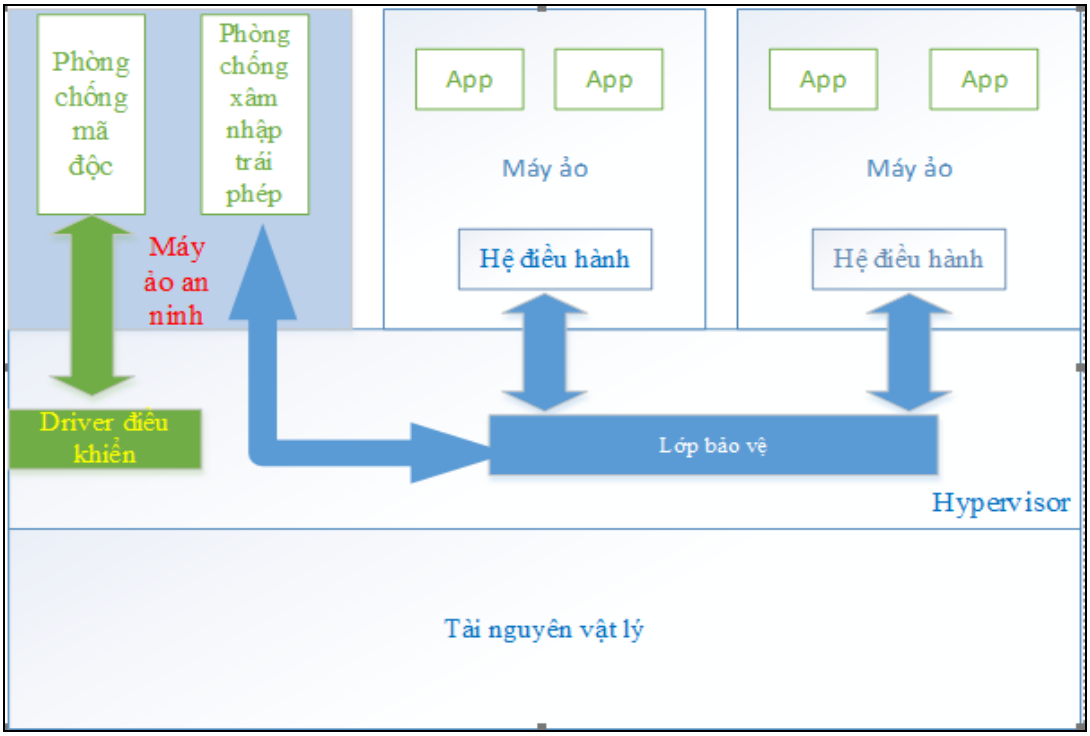
	nghiệp thì chỉ có thể xóa dữ liệu của doanh nghiệp mình. Trong trường hợp thứ hai, mọi trách nhiệm vẫn có thể đổ lên đầu nhà cung cấp, nếu họ không chứng minh được là chính admin của doanh nghiệp đã xóa dữ liệu.
Tuân thủ các quy định	Khách hàng phải chịu trách nhiệm cho sự an toàn dữ liệu của họ vì vậy họ có thể lựa chọn giữa các nhà cung cấp được kiểm toán bởi một bên thứ ba uy tín kiểm tra mức độ an ninh.
Khả năng khôi phục	Mọi nhà cung cấp dịch vụ đám mây đều có phương thức khôi phục thảm họa để bảo vệ dữ liệu Khách hàng. Tuy nhiên không phải nhà cung cấp nào cũng có khả năng khôi phục đầy đủ và kịp thời hệ thống.
Khả năng tồn tại lâu dài.	Đề cập đến khả năng rút lại lại hợp đồng và dữ liệu nếu nhà cung cấp hiện tại được mua lại bởi một công ty khác.
Chia sẻ nhiều người cùng sử dụng dịch vụ	Các dịch vụ điện toán đám mây cung cấp dịch vụ cho hàng triệu người dùng khác nhau, việc phân tách logic dữ liệu được thực hiện ở mức độ khác nhau của ứng dụng, do đó kẻ tấn công có thể lợi dụng các lỗi để truy cập trái phép vào dữ liệu của cá nhân, tổ chức khác.

Chương 3 - GIẢI PHÁP BẢO VỆ THÔNG TIN TRONG MÔI TRƯỜNG ẢO HÓA VÀ ĐIỆN TOÁN ĐÁM MÂY

3.1. GIẢI PHÁP BẢO VỆ DỮ LIỆU TRONG MÔI TRƯỜNG ẢO HÓA

3.1.1. Xây dựng kiến trúc ảo hóa an toàn

Môi trường ảo hóa cần được bảo vệ bởi một kiến trúc đơn giản nhưng hiệu quả và mạnh mẽ. Trong đề tài đề xuất một kiến trúc an toàn cho môi trường ảo hóa sử dụng giải pháp Agentless. Giải pháp Agentless không cần cài đặt bất kì phần mềm bảo mật nào trên máy ảo. Giải pháp sử dụng một máy ảo an ninh tích hợp với tầng phần mềm lõi của nền tảng Ảo hóa và các driver điều khiển để bảo vệ máy ảo. Kiến trúc ảo hóa Agentless tích hợp dễ dàng với nền tảng ảo hóa phổ biến là Vmware và Xen. Kiến trúc Agentless giải quyết được các nguy cơ tấn công chéo giữa các máy ảo, kiểm soát dữ liệu ra vào máy ảo, phát hiện mã độc hại và đặc biệt là giải quyết được bài toán tranh chấp tài nguyên do không phải cài từng phần mềm bảo mật trên từng máy ảo. Trong hình 10 nhiệm vụ quản lý và bảo vệ các máy ảo được trao cho một máy ảo chuyên dụng có tên là máy ảo an ninh. Các dữ liệu vào ra máy ảo sẽ được kiểm tra trước khi đến máy ảo. Sử dụng kiến trúc Agentless giúp cho việc quản trị tập trung, đơn giản giúp giảm chi phí, tiết kiệm thời gian và nguồn lực.

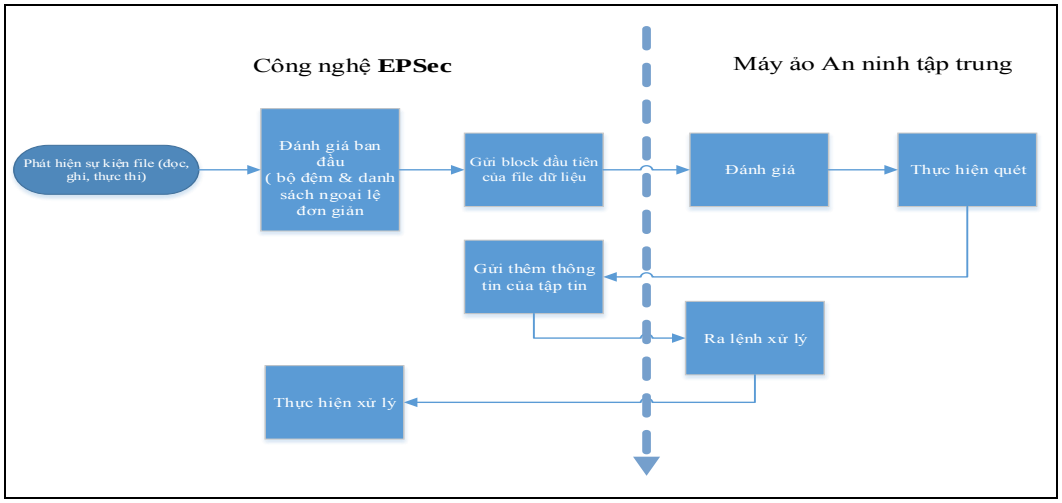


Hình 09: Kiến trúc An ninh ảo hóa

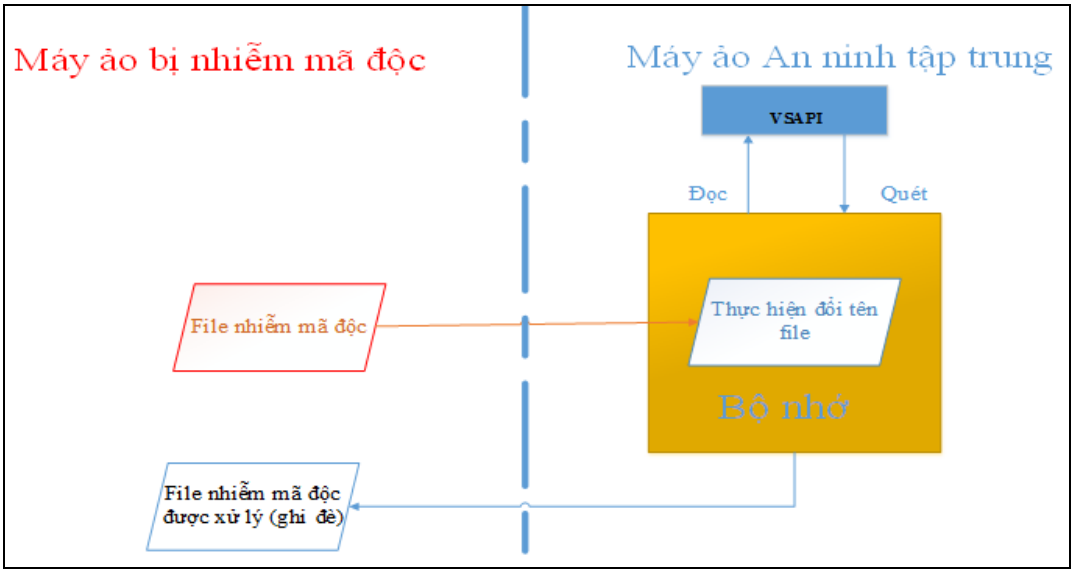
3.1.2. Công nghệ phòng chống mã độc chuyên biệt cho môi trường ảo hóa

Công nghệ phòng chống mã độc nâng cao cho môi trường ảo hóa được đề xuất trong đề tài sử dụng kiến trúc an toàn ảo hóa được đề cập trong phần 3.1.1 có khả năng phát hiện và xử lý mã độc hại trên các máy chủ ảo theo thời gian thực và tiêu tốn hiệu năng nhỏ nhất nhằm giải quyết bài toán xung đột và tranh chấp tài nguyên được đề cập

trong phần 2.1.6 Chương 2. Công nghệ phòng chống mã độc chuyên biệt cho môi trường ảo hóa không sử dụng phương án cài đặt phần mềm diệt virus trên từng máy chủ, máy trạm ảo như phương pháp truyền thống. Công nghệ EPSec lấy các tập tin hoặc phát hiện tập tin vào/ra các sự kiện trên máy ảo và chuyển chúng sang các thành phần quét mã độc tập trung trong máy ảo an ninh. Công nghệ trên quét Virus tập trung trong máy ảo an ninh sẽ kiểm tra và phân tích giúp phát hiện phần mềm độc hại trong các tập tin hoặc vào/ra các sự kiện và hướng dẫn EPSec có những hành động thích hợp khi các tập tin hoặc sự kiện. Giúp tiết kiệm đáng kể hiệu năng và giảm thiểu xung đột tài nguyên. Luồng phát hiện mã độc hại trong máy ảo



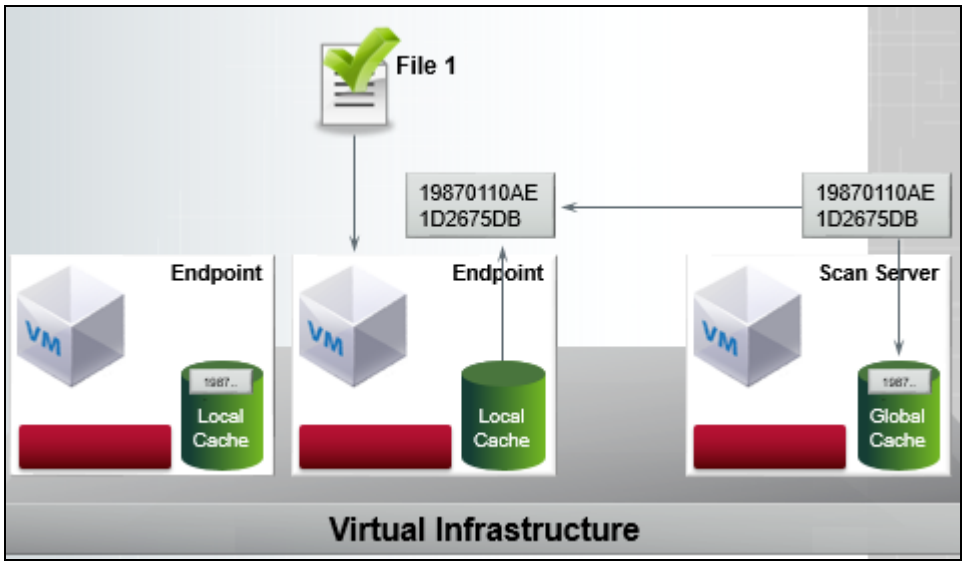
Hình 10: Phát hiện mã độc hại



Hình 11: Luồng xử lý mã độc hại

Công nghệ quét thông minh sử dụng bộ đệm và công nghệ theo dõi sự thay đổi khối (change block tracking - CBT) giúp tập tin đã quét và xác định an toàn không bị quét lại. Khi ứng dụng hoặc mã độc truy cập hoặc thực thi các file trên máy ảo ngay lập tức sẽ được kiểm tra có nằm trong danh sách an toàn hoặc đã được quét trước đó hay không bằng cách so sánh giá trị hàm băm. Nếu file đó không nằm trong danh sách nó sẽ lập tức được đưa lên máy chủ quét tập trung để phân tích. Phân tích file sử dụng

hai công nghệ chính là mẫu nhận dạng và tận dụng lợi thế công nghệ đám mây. Nếu file có nhiễm mã độc ngay lập tức sẽ bị xóa hoặc cô lập. Nếu file đó an toàn sẽ được dán nhãn và ghi vào bộ nhớ đệm tương tự như vậy các file tiếp theo



Hình 12: Kiến trúc sử dụng bộ đệm

3.1.3. Thực hiện cấu hình an toàn lớp phần mềm lõi Hypervisor

1/. Thường xuyên, kịp thời vá các lỗ hổng bảo mật phần mềm lõi Hypervisor và các phần mềm của hệ thống ảo hóa

2/. Kết nối bằng giao thức an toàn Secure Socket Layer (SSL)

3/. Thay đổi cấu hình mặc định của nhà cung cấp

4/. Bật các an ninh vận hành: SNMP, Network Time Protocol (NTP).

5/. Bảo vệ và giám sát các thư mục file cấu hình quan trọng

6/. Bảo vệ tài khoản người dùng và nhóm tài khoản quản trị hệ thống máy chủ ảo hóa

7/. Giới hạn truy cập các truy cập nền tảng nhân ảo hóa. Bảo vệ toàn bộ kênh kết nối quản trị sử dụng mạng quản trị riêng hoặc mạng quản trị có xác thực mạnh và được mã hóa kênh truyền

8/ . Khóa các dịch vụ không sử dụng như sao chép clipboard hoặc chia sẻ file giữa các máy ảo khách.

9/. Tháo/rút các thiết bị vật lý không còn sử dụng ra khỏi máy chủ ảo hóa. Ví dụ tháo ổ đĩa cứng sử dụng cho mục đích sao lưu và dự phòng. Rút các card mạng không sử dụng.

10/. Tắt các máy ảo khi không sử dụng đến nó.

11/. Bảo đảm rằng các driver điều khiển của máy chủ Ảo hóa host được nâng cấp và cập nhật đầy đủ bản vá lỗi mới.

3.1.4. Cấu hình an toàn máy chủ Ảo hóa

1/. Sử dụng mật khẩu mạnh

2/. Đóng các dịch vụ và các chương trình không cần thiết

3/. Yêu cầu xác thực đầy đủ để kiểm soát truy cập.

4/. Thiết lập tường lửa cá nhân trên máy chủ giới hạn truy cập.
5/. Cập nhật kịp thời bản vá lỗi lỗ hổng bảo mật nghiêm trọng

3.1.5. Thiết kế mạng ảo đảm bảo an toàn thông tin

Thực hiện các biện pháp sau nhằm thiết kế mạng ảo đảm bảo an toàn thông tin:
1/. Thiết lập tường lửa ảo giữa các lớp mạng ảo và các máy ảo với nhau. Tường lửa ảo có thể chặn được các gói tin trước khi chúng vào máy ảo.
2/. Triển khai hệ thống phát hiện và chống xâm nhập trên mạng giúp phát hiện và ngăn chặn các tấn công mạng. Nếu có điều gì bất thường trong môi trường ảo, hệ thống phát hiện và chống xâm nhập dựa trên chữ ký số sẽ ngay lập tức cảnh báo về các hoạt động này và tìm cách giải quyết chúng
3/. Tiến hành cô lập mạng quản trị
4/. Phân lập mạng ảo đối với các mạng ảo và mạng vật lý khác
5/. Cô lập Switch ảo sử dụng thiết lập chính sách tường lửa ở tầng 2 và tầng 3 và thiết lập chính sách trên các cổng mạng ảo.
6/. Giám sát hiệu năng hoạt động của các thiết bị mạng ảo nhằm phát hiện và xử lý kịp thời sự cố quá tải, do tấn công hoặc hỏng hóc.
7/. Thiết lập chính sách lọc địa chỉ MAC, kiểm soát cấp phát địa chỉ động DHCP, thiết lập hệ thống kiểm soát truy cập NAC cho các tổ chức lớn
8/. Kiểm soát quản trị và truy cập thiết bị mạng ảo.

3.1.6. Giới hạn truy cập vật lý các máy chủ Ảo hóa (Host)

Thiết lập các biện pháp sau nhằm giới hạn truy cập vật lý các máy chủ Ảo hóa:
1/. Đặt password BiOS
2/. Giới hạn chỉ cho phép khởi động từ ổ cứng máy chủ không cho phép khởi động từ đĩa CD, đĩa quang và đĩa mềm, USB.
3/. Sử dụng khóa để tủ RACK đựng máy chủ nhằm chống lại việc cắm thiết bị ngoại vi.
4./ Sử dụng khóa riêng cho ổ đĩa cứng nhằm đánh cắp ổ đĩa cứng
5/. Đóng các cổng không cần thiết trên thiết bị

3.1.7. Mã hóa dữ liệu máy ảo

Cần mã hóa các ảnh máy ảo khi không sử dụng, mã hóa các file cấu hình máy ảo quan trọng (.vmx), mã hóa ổ đĩa máy ảo (.vmdk). Đề xuất sử dụng giải pháp VMware ACE để mã hóa máy ảo. Bên cạnh đó cần sử dụng giao thức mã hóa an toàn như mạng riêng ảo (VPNs), bảo mật tầng truyền tải (TLS), sử dụng kết nối an toàn SSL giữa các liên kết truyền thông giữa máy chủ host và máy ảo khách, hoặc từ máy chủ đến các hệ thống quản lý tập trung. Tiến hành mã hóa các dữ liệu quan trọng lưu trữ trong máy ảo.

3.1.8. Tách biệt truy cập, cô lập dữ liệu giữa các máy ảo

Tất cả các máy ảo cần được cô lập và có biện pháp kiểm soát cô lập giữa các máy ảo với máy chủ Host và giữa các máy ảo với nhau. Biện pháp cô lập cho phép

nhiều máy ảo chạy một cách an toàn trong khi chia sẻ phần cứng và đảm khả năng truy cập vào phần cứng với hiệu suất cao một cách liên tục, ngay cả một người dùng với quyền quản trị viên hệ thống trên hệ điều hành của máy ảo khách không thể chọc thủng lớp cô lập để truy cập vào một máy ảo khác. Nếu hệ điều hành trên một máy ảo đang chạy trong một máy ảo bị lỗi, các máy ảo khác trên cùng một máy chủ sẽ vẫn hoạt động bình thường.

3.1.9. Duy trì sao lưu

Tổ chức cần thực hiện duy trì sao lưu theo các yêu cầu sau đảm bảo dữ liệu sẵn sàng khi cần sử dụng:

1/. Thực hiện đầy đủ sao lưu ảnh chụp trạng thái máy ảo có đầy đủ cấu hình bao gồm ổ đĩa cứng ảo để khách hàng có có thể dễ dàng khôi phục các dữ liệu và máy ảo ban đầu.

2/. Sử dụng mã hóa bảo vệ luồng dữ liệu khi sao lưu ngăn chặn tin tặc chặn bắt gói tin.

3/. Thiết lập mật khẩu bảo vệ các file sao lưu.

4/. Đề xuất sử dụng công nghệ sao lưu an toàn của hãng Ảo hóa Vmware Consolidated Backed của Vmware vStoreage giúp quản trị viên dễ dàng lập lịch sao lưu, kiểm tra sao lưu

3.1.10. Tăng cường tính tuân thủ

Tổ chức cần định kỳ kiểm toán và đánh giá tuân thủ hệ thống Ảo hóa, quản lý đầy đủ thông tin truy cập dữ liệu. Giám sát tính toàn vẹn của dữ liệu, kiểm tra tính toàn vẹn của máy ảo. Cảnh báo kịp thời khi dữ liệu quan trọng bị thay đổi trái phép. Đào tạo nâng cao nhận thức và tính tuân thủ cho cán bộ quản trị. Thiết lập biện pháp kiểm soát tính tuân thủ của cán bộ quản trị như triển khai quy trình quản lý thay đổi.

3.2. GIẢI PHÁP BẢO VỆ DỮ LIỆU TRONG ĐIỆN TOÁN ĐÁM MÂY

Các biện pháp bảo vệ dữ liệu trong môi trường Điện toán đám mây đề xuất trong đề tài đều được xây dựng trên cơ sở ba nguyên tắc cơ bản của an toàn thông tin: tính bí mật, tính toàn vẹn và sẵn sàng. Mô hình bảo vệ dữ liệu trong môi trường điện toán đám mây hình 13 sử dụng cấu trúc phòng thủ ba lớp, trong đó mỗi lớp thực hiện một nhiệm vụ riêng của mình để bảo vệ dữ liệu trong môi trường ảo hóa [7]. Với cấu trúc ba lớp phòng thủ theo chiều sâu: lớp xác thực người dùng sử dụng nhằm đảm bảo dữ liệu không bị giả mạo. Chỉ những tài khoản được xác thực mới có khả năng quản lý, thao tác dữ liệu như tạo mới, chỉnh sửa hay xóa dữ liệu. Nếu như lớp xác thực người dùng bị đánh bại, hệ thống bị tin tặc xâm nhập, mã hóa dữ liệu và bảo vệ tính riêng tư có thể cung cấp lớp bảo vệ tiếp theo. Trong lớp bảo vệ này dữ liệu được mã hóa chỉ khi cung cấp khóa giải mã hợp lệ thì mới có thể truy cập dữ liệu, nó là một biện pháp bảo vệ dữ liệu rất quan trọng. Cuối cùng, việc phục hồi nhanh chóng dữ liệu nhờ tuân thủ các yêu cầu nghiêm ngặt về sao lưu và phục hồi giúp tổ chức, doanh nghiệp có thể khôi phục tối đa và nhanh chóng dữ liệu trong các trường hợp xảy ra hỏng hóc hoặc hư hại dữ liệu.

Hình 13: Mô hình bảo vệ dữ liệu

3.2.1. Lớp phòng thủ thứ nhất kiểm soát truy cập

Chịu trách nhiệm xác thực tài khoản người dùng sử dụng dịch vụ Điện toán đám mây, cán bộ quản trị hệ thống. Lớp phòng thủ thứ nhất sử dụng các biện pháp xác thực mạnh như: xác thực hai yếu tố, sử dụng chứng thư số được cấp phát riêng cho mục đích xác thực, quản lý quyền của tài khoản, xác định rõ các hành động nào được phép đối với mỗi tài khoản khác nhau. Cụ thể cần tuân theo các nguyên tắc cơ bản sau:

Nguyên tắc cấp cấp quyền: quyền chỉ cấp tối thiểu, đáp ứng đúng đủ nhu cầu công việc. Phân tách rõ ràng vai trò nhiệm vụ của từng cá nhân, tổ chức ví dụ: người thay đổi hệ thống điện toán đám mây, người phê duyệt việc thay đổi và người giám sát quá trình thay đổi là ba người độc lập khác nhau. Định kỳ rà soát đảm bảo các quyền được cấp đúng và đủ theo yêu cầu công việc. Thông báo cho quản lý tài khoản khi:

1/. Tài khoản không còn cần thiết

2/. Người dùng chấm dứt hoặc được chuyển công việc

Giám sát tài khoản thông tin tài khoản hệ thống, thực hiện cảnh báo khi có rủi ro cao liên quan tài khoản xuất hiện.

1/. Khi tài khoản có quyền đăng nhập sai mật khẩu nhiều lần

2/. Khi tài khoản có quyền đăng nhập hệ thống sau giờ làm việc

3/. Khi tài khoản có quyền thay đổi mật khẩu, thông tin số điện thoại.

Phân quyền rõ ràng, thiết lập điều kiện, quyền cho các nhóm và thành viên trong các nhóm khác nhau

1/. Bỏ các tài khoản tạm thời dùng cho việc khẩn cấp

2/. Đóng các tài khoản sau một thời gian không tương tác hệ thống. ví dụ sau 3 tháng không tương tác hệ thống, tài khoản sẽ bị khóa.

Kiểm toán tạo tài khoản, sửa đổi, cho phép, vô hiệu hóa và loại bỏ các hành động, và thông báo liên quan tài khoản

Yêu cầu tự động đăng xuất phiên đăng nhập tài khoản sau thời gian không tương tác hệ thống. Ví dụ: tự động đăng xuất phiên làm việc nếu sau 5 phút tài khoản không có tương tác hệ thống. Không sử dụng chung tài khoản.

Thiết lập các biện pháp ngăn chặn các nỗ lực đăng nhập rò mật khẩu, tài khoản nhiều lần:

1/. Thiết lập số lần sai mật khẩu liên tiếp tối đa 5 lần.

2/. Tự động khóa tài khoản trong vòng 60 phút hoặc chờ đến khi quản trị viên kích hoạt nếu gõ sai mật khẩu liên tiếp 5 lần

3/. Trì hoãn lần đăng nhập tiếp theo phải tiến hành sau một khoảng thời gian nhất định, tối thiểu 15 phút

4/. Yêu cầu nhập captcha đối với các giao diện đăng nhập để đảm bảo người dùng thật đăng nhập hệ thống.

Cần hiển thị thông báo cho người dùng khi người dùng đăng nhập và thoát khỏi hệ thống. Cần lưu đầy đủ thông tin đăng nhập được ghi lại nhằm mục đích kiểm toán.

Kiểm soát phiên đăng nhập: Hệ thống ứng dụng trên điện toán đám mây cần giới hạn số lượng phiên đăng nhập đồng thời cho mỗi tài khoản. Ngăn chặn truy cập trái phép hệ thống bằng cách sử dụng lại khóa phiên đăng nhập đã không còn hoạt động.

Sử dụng phương thức xác thực mạnh kết hợp đa yếu: mật khẩu và sinh trắc học, thẻ thông minh và thiết bị phần cứng sinh mật khẩu động và mật khẩu dùng một lần đối với tài khoản có đặc quyền và không có đặc quyền truy cập từ xa vào hệ thống. Các yếu tố kiểm tra xác thực khác phải được cung cấp bởi thiết bị độc lập.

3.2.2. Lớp phòng thủ thứ hai mã hóa

Lớp phòng thủ thứ hai sử dụng giải pháp mã hóa dữ liệu nhằm đảm bảo tính bí mật dữ liệu. Ngăn chặn những người không được cấp quyền hiểu rõ nội dung dữ liệu. Mã hóa dữ liệu trong khi truyền và lưu trữ trong điện toán đám mây có các lợi ích rõ ràng sau:

Ngăn chặn mối đe dọa truy cập trái phép dữ liệu Khách hàng của nhân viên quản trị của đơn vị cung cấp điện toán đám mây

Ngăn chặn mối đe dọa truy cập trái phép dữ liệu từ bên ngoài của hacker, đối thủ cạnh tranh

Trong nội dung đề tài sẽ tập trung vào sử dụng thuật toán mã hóa đồng cấu để mã hóa dữ liệu trên Điện toán đám mây.

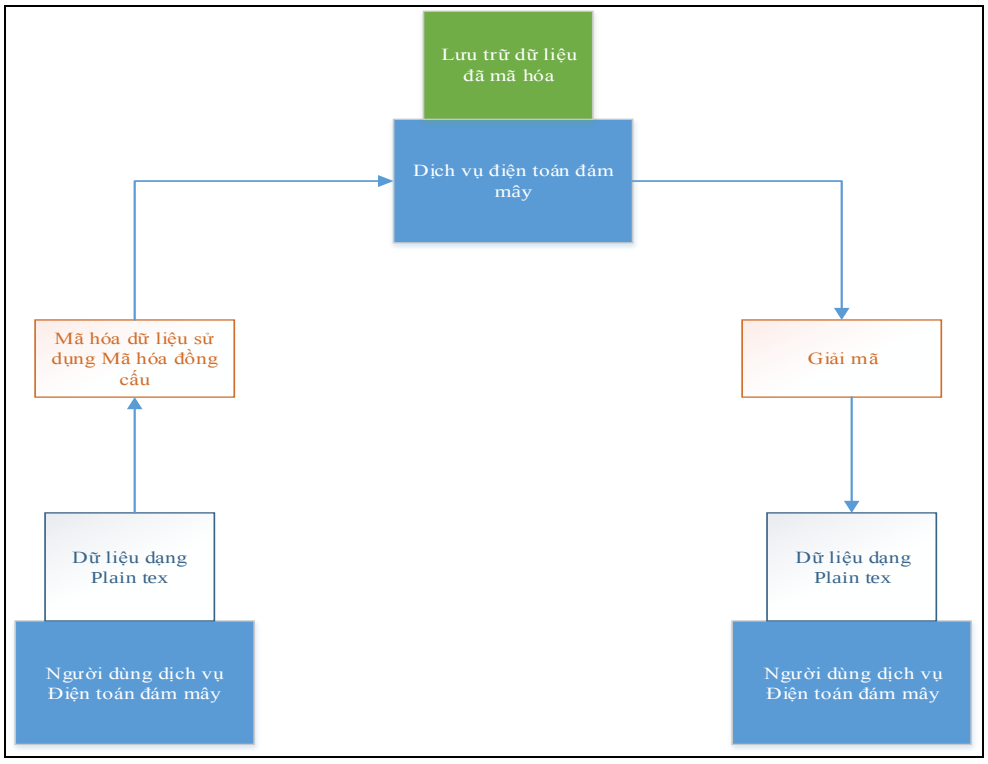
3.2.2.1. Khái niệm, tính chất mã hóa đồng cấu

Thuật toán mã hóa đồng cấu được đề xuất lần đầu tiên bởi ba nhà khoa học Rivest, Adleman và Dertouzos năm 1978. Một số thuật toán mã hóa hỗ trợ nhân như RSA (Rivest, Shamir, và Adleman) và Elgamal (1985). Mã hóa đồng cấu cộng như Paillier (1999).

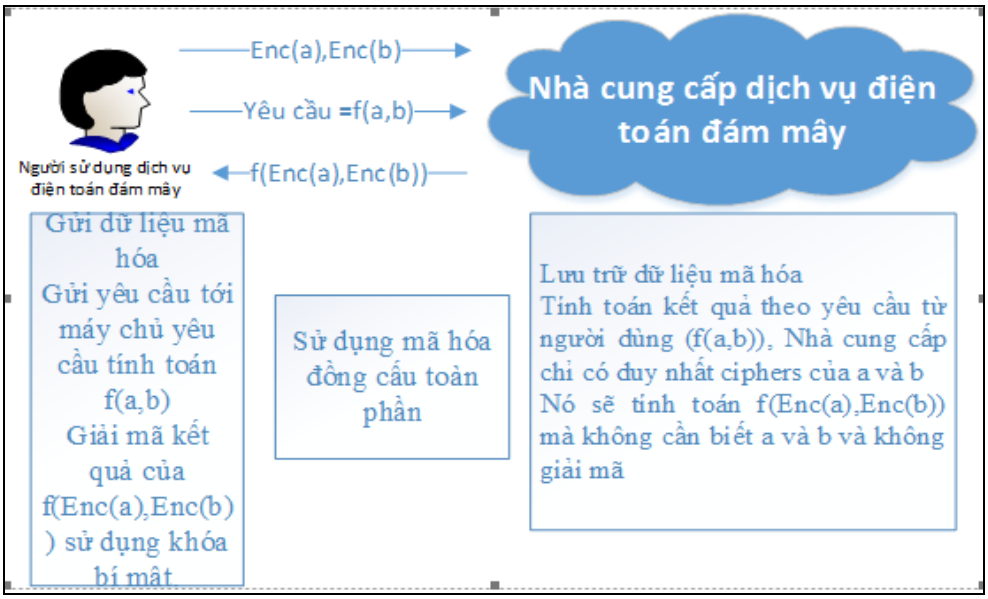
Mã hóa đồng cấu có tính chất đặc biệt: tích của các "bản tin" (messenge) được mã hóa bằng tổng các "bản tin" được mã hóa. Mã hóa đồng cấu có tính chất đặc biệt: gộp các bản mã lại với nhau (⊕ ⊗) cho ta bản mã có nội dung là tổng các bản rõ tương ứng [8]. Năm 2009 nhà khoa học máy tính Craig Gentry của hãng IBM đã đề xuất mã hóa theo cả phép nhân và phép cộng (fully homomorphic encryption). Đây là một ứng dụng quan trọng trong an ninh điện toán đám mây. Hệ mã này cho phép từ hai bản mã của hai bản rõ a và b, ta có thể tính được bản mã nhân của ab và bản mã cộng của a+b. Mã hóa đồng cầu đầy đủ cho phép tính toán có thể được thực hiện trên các dữ liệu được mã hóa mà không biết khóa bí mật.

Nhiều nghiên cứu đề xuất các biến thể của mô hình Craig Gentry với một số cải tiến. Năm 2011 trong công bố trên tạp chí Những nền tảng của Máy tính- FOCS, 2011, pp. 97–106 thuật toán được hai nhà khoa học máy tính Zvika Brakerski và Vinod Vaikuntanatha giúp đầy đủ, đơn giản và hiệu quả hơn so với đề xuất ban đầu nhờ sở dụng kỹ thuật LWE. [09] Năm 2012 ba nhà khoa học máy tính Gentry, Vinod Vaikuntanathan và Zvika Brakerski trong công bố trên tạp chí ITCS, 2012, pp. 97–106 đã đưa ra một cải tiến mã hóa đồng cấu đầy đủ Fully homomorphic encryption không kèm bootstrapping. Dự đoán tiếp tục sẽ có nhiều nghiên cứu về đề tài này đặc biệt là sự phổ biến và thống trị của điện toán đám mây. Thuật toán mã hóa đồng cấu đầy đủ còn gặp phải một số vấn đề tính linh hoạt, tốc độ mã hóa và giải mã, kích thước bản mã lớn

3.2.2.2. Sử dụng mã hóa đồng cấu mã hóa dữ liệu trong điện toán đám mây



Hình 14: Mô hình sử dụng mã hóa đồng cấu mã hóa dữ liệu điện toán đám mây



Hình 15: Mô hình mã hóa dữ liệu điện toán đám mây sử dụng mã hóa đồng cấu

3.2.2.3. Tính toán mã hóa đồng cấu đầy đủ

Mã hóa thông điệp b:

Chọn một cách ngẫu nhiên số "lớn" bội của p: $q \cdot p$ ($q \sim n^5$ bits)

Chọn ngẫu nhiên số "bé" $2 \cdot r$

Bản mã hóa thông điệp b là $c = q \cdot p + 2 \cdot r + b$

Giải mã bản mã c: $c \pmod p = 2 \cdot r + b \pmod p$

Tính toán cộng và nhân

$c_1 = q_1 \cdot p + (2 \cdot r_1 + b_1)$, $c_2 = q_2 \cdot p + (2 \cdot r_2 + b_2)$

$c_1 + c_2 = p \cdot (q_1 + q_2) + \underbrace{2 \cdot (r_1 + r_2) + (b_1 + b_2)}_{\text{LSB} = b1 \text{ XOR } b2}$

$c_1 c_2 = p \cdot (c_2 \cdot q_1 + c_1 \cdot q_2 - q_1 \cdot q_2) + \underbrace{2 \cdot (r_1 r_2 + r_1 b_2 + r_2 b_1) + b_1 b_2}_{\text{LSB} = b1 \text{ XOR } b2}$

Khóa công khai:

$[q_0 p + 2r_0, q_1 p + 2r_1, \ldots, q_t p + 2r_t] = (x_0, x_1, \ldots, x_t)$

Mã hóa thông điệp b: chọn ngẫu nhiên $S \subseteq [1 \ldots t]$

$$c = \sum_{i \in S} x_i + 2r + b \pmod{x_0}$$

Giải mã bản mã c: $c \pmod p = 2 \cdot r + b \pmod p = 2 \cdot r + b$

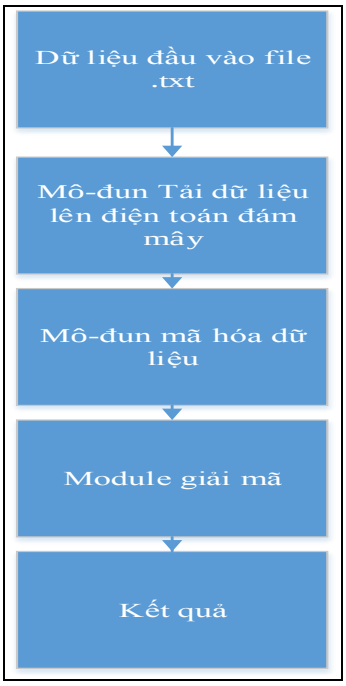
Thuật toán mã hóa đồng cấu đầy đủ gặp phải 2 vấn đề

1/. Bản mã có kích thước lớn

2/. Độ nhiễu cao mỗi lần tính toán.

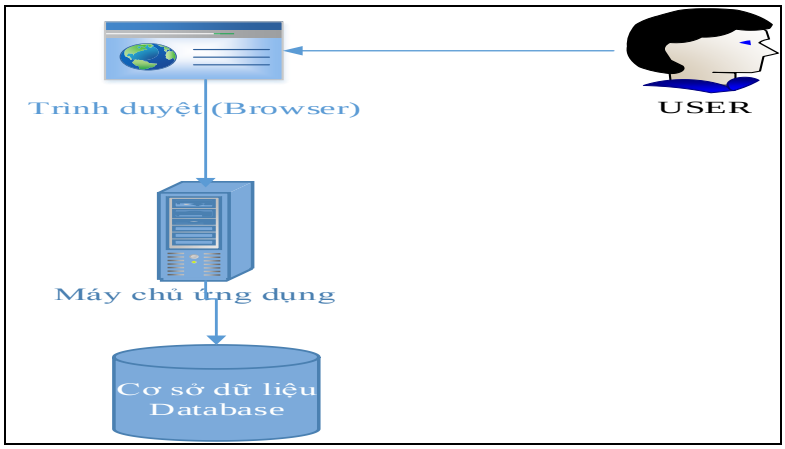
3.2.2.4. Thử nghiệm mã hóa dữ liệu điện toán đám mây sử dụng thuật toán mã hóa đồng cấu

Thiết kế chương trình



Hình 16: Thiết kế chương trình

Kiến trúc chương trình



Hình 17: Kiến trúc chương trình

Thuật toán chương trình

Bước 1: Lựa chọn J (64bit), K (16bit) D and F (256-bit) ngẫu nhiên

Bước 2: Lựa chọn 4 bit ngẫu nhiên K’ tính P0 = JD and P1 = JF + KK’

Bước 3: Chấp nhận Số N từ người dùng

Bước 4: P2 = [T1 P1] mod P0

Bước 5: Perform Encryption Cipher Text C = [N + T2 P2] mod P0 (T1 , T2 are a 4-bit random integer)

Bước 6: Giải mã N = (C mod J) mod K

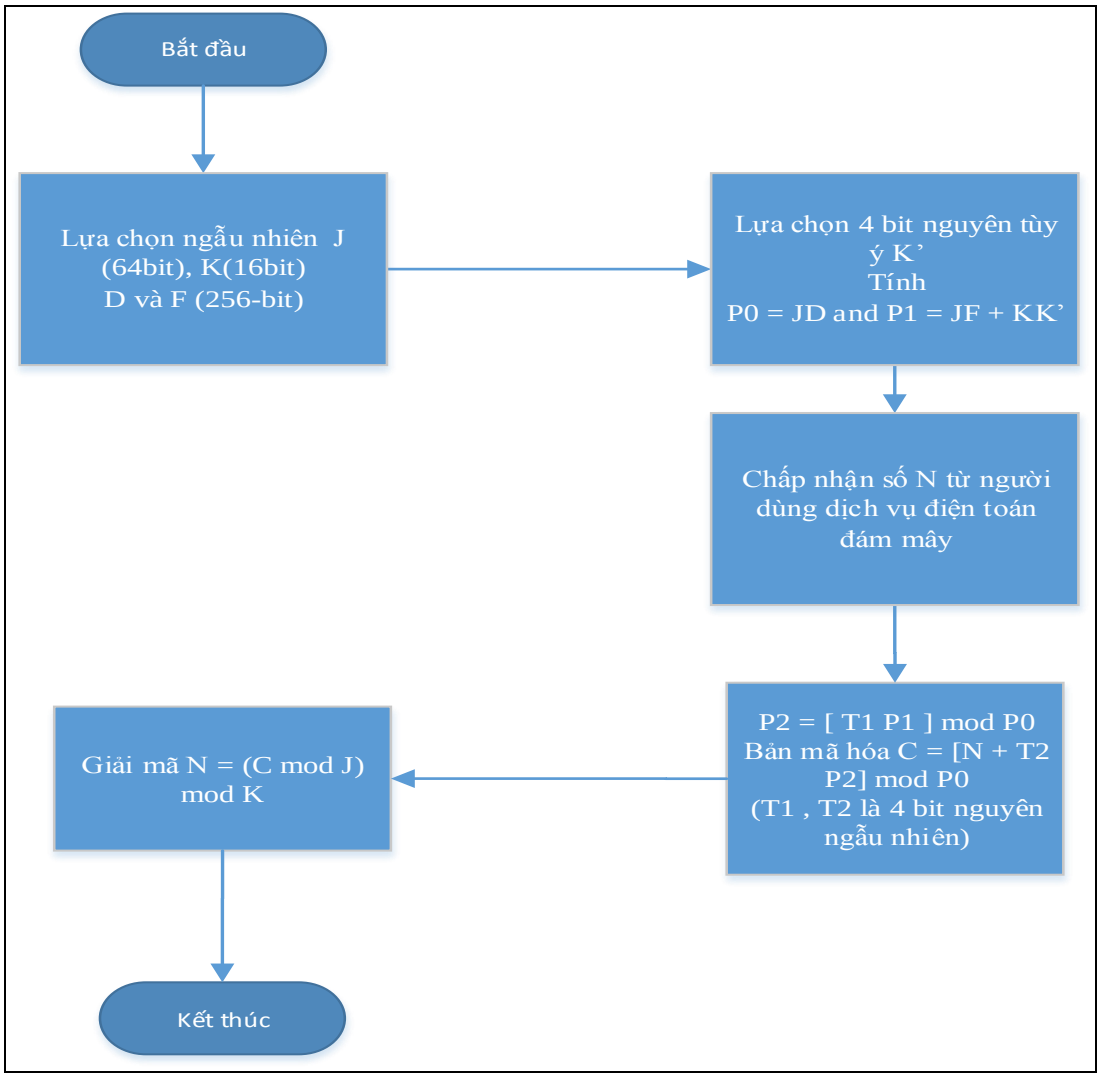
Ví dụ

Bước1: chọn

J= 14883982794894487223,

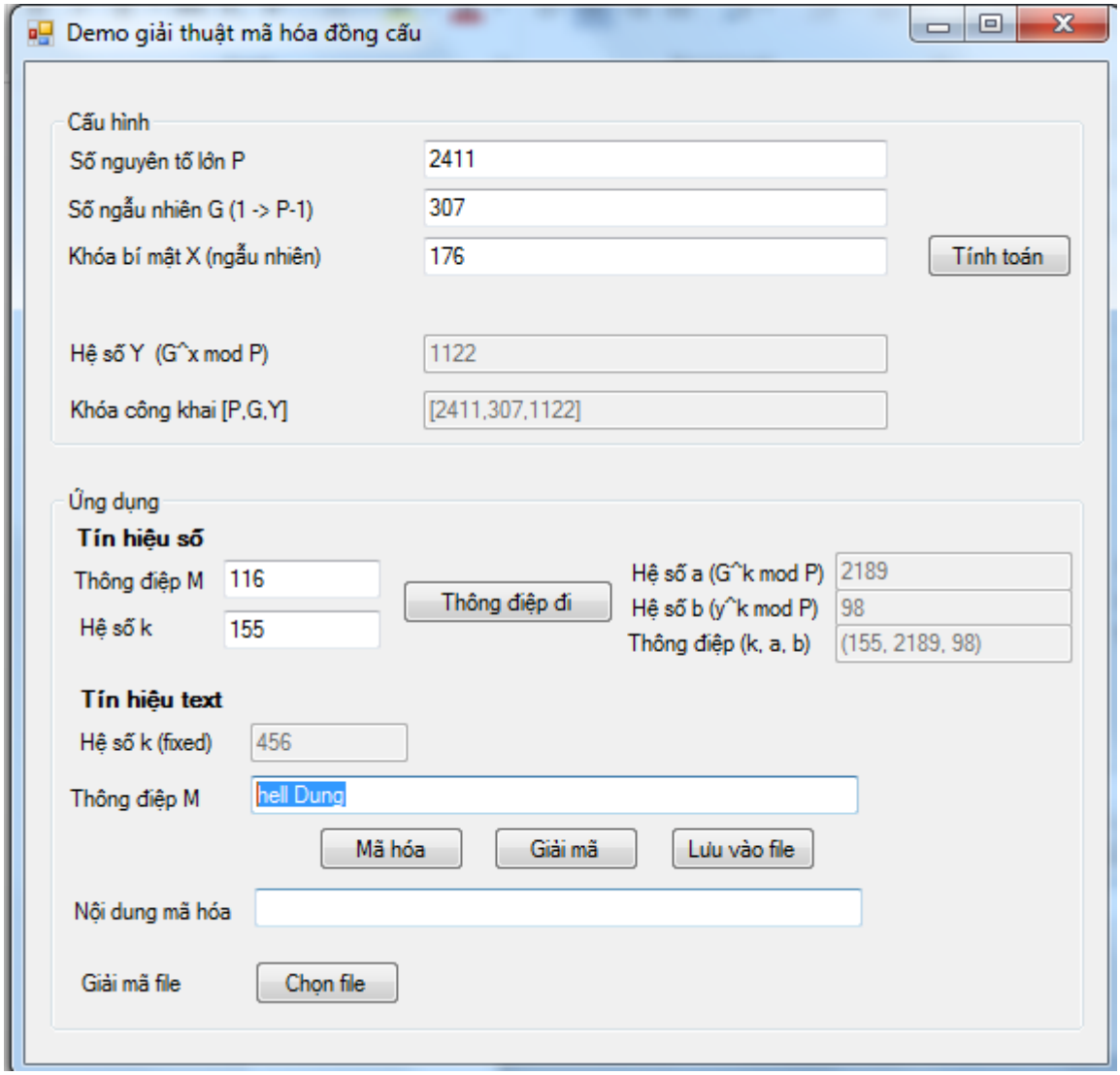
K=43321,

D=706771865439661476141958620420656807042178113071709388236808179724600787707 47
F=730390473299616118774746223206442922044393268447477830706768069042875782436 39
Bước 2: lựa chọn ngẫu nhiên 4 bít K '= 12 sau đó tính
P0=105195802851194030592932060756553342783557414664099137669178122750463891978223732486512473766558 1
P1=108711192381463276648158124169700408733775019967891779423494587651257282914457503860391386 7044349
Bước 3: số được mã hóa N=9
Bước 4,5: Thực hiện mã hóa và nhận được
C=351538953026924605522606341314706595021760530379264175431646490079339093623377137387891293 7 87689.
Bước 6: Giải mã được thực hiện và nhận lại bản rõ N = 9



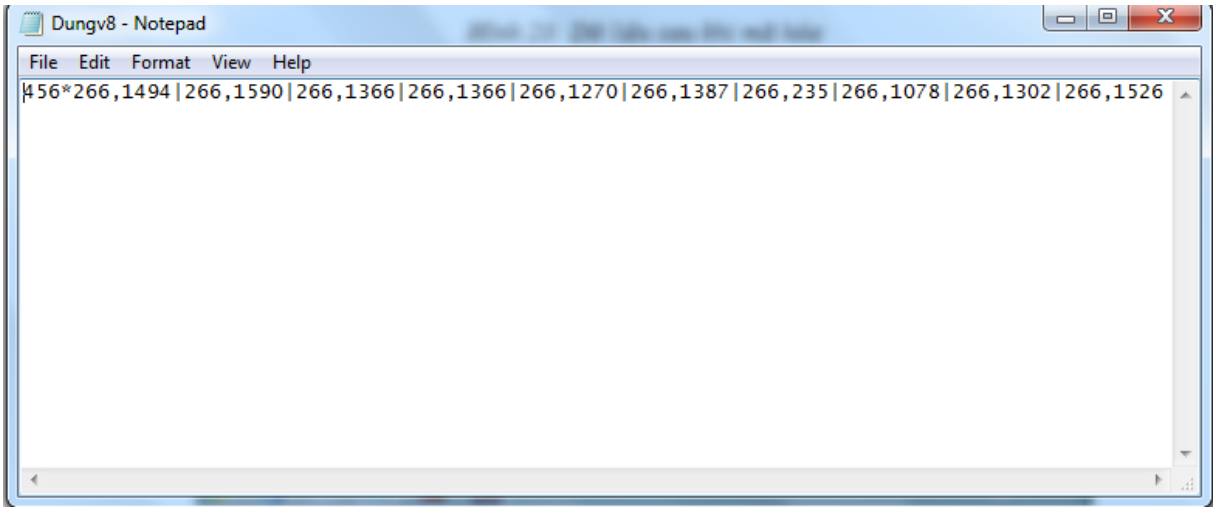
Hình 18: Thuật toán chương trình

Kết quả
Dữ liệu dạng bản rõ trước khi mã hóa



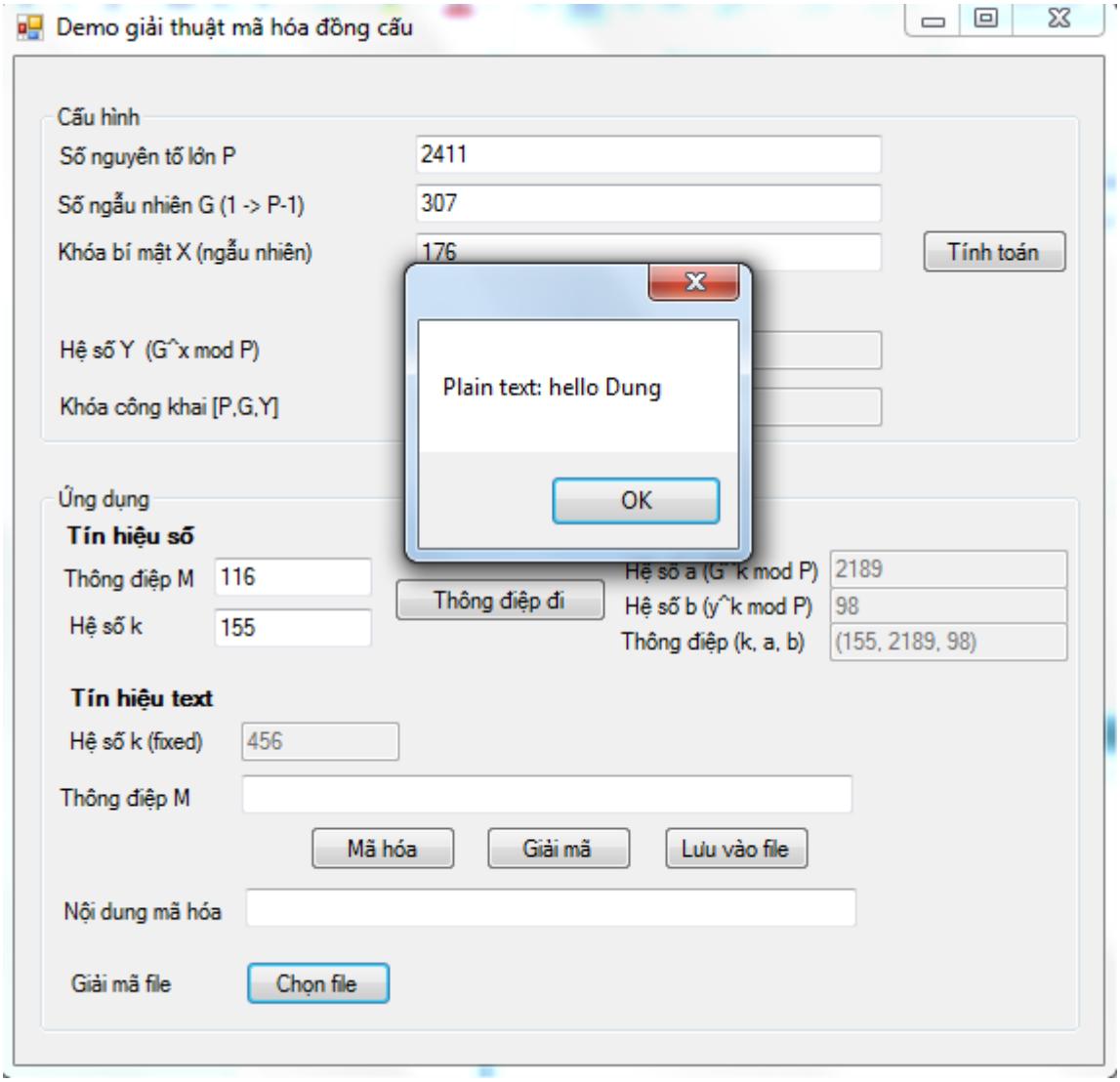
Hình 19: Dữ liệu dạng bản rõ trước khi mã hóa

Dữ liệu sau khi mã hóa



Hình 20: Dữ liệu sau khi mã hóa

Dữ liệu sau khi giải mã giữ nguyên nội dung



Hình 21: Dữ liệu sau khi giải mã

3.2.3. Lớp phòng thủ thứ ba khôi phục nhanh chóng

Lớp bảo vệ cuối cùng bảo vệ dữ liệu là khả khôi phục dữ liệu hoặc di chuyển một cách nhanh chóng trong trường hợp xảy ra sự cố hoặc theo yêu cầu của Khách hàng. Tổ chức cung cấp dịch vụ điện toán đám mây cần tuân thủ các nguyên tắc cơ bản sau nhằm đảm bảo dữ liệu khôi phục nhanh chóng và đầy đủ [6].

1/. 100% dữ liệu phải được sao lưu. Các bản sao lưu phải đầy đủ và nhất quán được lưu trữ theo nguyên tắc 3-2-1. Mỗi file dữ liệu có ít nhất ba bản (1 bản gốc và 2 bản sao lưu, ít nhất một trong ba bản đó có sẵn trực tuyến khi cần). Lưu trên ít nhất 2 thiết bị lưu trữ khác nhau có ít nhất bản sao lưu tĩnh đặt tại địa điểm cách xa và độc lập địa điểm lưu trữ dữ liệu gốc.

2/. Có quy trình sao lưu và phục hồi chia rõ vai trò của từng cá nhân tổ chức.

3/. Thường xuyên đào tạo, diễn tập kịch bản khôi phục hệ thống dữ liệu nhằm đảm bảo độ tin cậy phương tiện truyền thông và toàn vẹn thông tin.

3/. Tổ chức phải có các cơ sở trung tâm dữ liệu thay thế tương đương (trung tâm dữ liệu dự phòng). Các trung tâm dữ liệu phải được giữ cách xa địa điểm chịu rủi ro về

xác suất môi trường cao, địa điểm nguy cơ cháy nổ như trạm xăng dầu, kho vũ khí. Khoảng cách từ trung tâm dữ liệu chính đến trung tâm dữ liệu dự phòng đảm bảo tối thiểu 30km.

4/. Tổ chức phải có kế hoạch đảm bảo tính liên tục kinh doanh, thường xuyên diễn tập kế hoạch và kiểm thử đảm bảo tính liên tục kinh doanh

5/. Bảo vệ tính bí mật và toàn vẹn, tính sẵn sàng của dữ liệu sao lưu tại các trung tâm lưu trữ như mã hóa, đặt mật khẩu file mã hóa.

6/. Sao lưu dữ liệu người dùng trong hệ thống điện toán đám mây phù hợp với yêu cầu thời gian phục hồi và điểm khôi phục mục tiêu của Khách hàng

7/. Sao lưu thông tin hệ thống chứa trong các hệ thống thông tin phù hợp với yêu cầu thời gian phục hồi và điểm khôi phục mục tiêu.

3.2.4. Một số biện pháp phòng thủ bổ sung nhằm bảo vệ dữ liệu trong môi trường điện toán đám mây

3.2.4.1. Kiểm soát an ninh môi trường vật lý điện toán đám mây

Đơn vị cung cấp dịch vụ điện toán đám mây cần phải xây dựng và thường xuyên cập nhật quy định kiểm soát an ninh môi trường vật lý điện toán đám mây:

1/. Việc ra vào phải được kiểm soát bằng thẻ từ, vân tay.

2/. Sử dụng khóa vật lý hoặc thẻ vật lý để truy cập trung tâm dữ liệu điện toán đám mây, có đầy đủ quy trình cấp phát và thay thế khi chìa khóa bị mất và cán bộ chuyển hoặc nghỉ việc.

3/. Quyền truy cập vào khu vực trung tâm dữ liệu chỉ được cấp cho các nhân viên vận hành hoặc nhân viên kỹ thuật liên quan trực tiếp đến hệ thống. Những nhân viên của bên thứ ba/cung cấp dịch vụ thực hiện dịch vụ bảo trì hay các dịch vụ khác phải giấy ủy quyền và giới thiệu rõ ràng được giám sát chặt chẽ bởi nhân viên của nhà cung cấp dịch vụ Điện toán đám mây.

4/. Trung tâm dữ liệu phải có camera giám sát. Camera giám sát phải được đặt vị trí phù hợp để giám sát tối thiểu nơi vào ra của cửa khu vực quan trọng. Lịch sử lưu trữ dữ liệu của Camera tối thiểu là 3 tháng.

5/. Tất cả dữ liệu về các truy cập ra vào trong các khu vực trung tâm dữ liệu đều phải được lưu dưới dạng nhật ký. Mọi hoạt động được thực hiện trong khu vực trung tâm dữ liệu Điện toán đám mây phải được ghi nhận, giám sát và định kỳ rà soát nhật ký truy cập.

6/. Có quy trình cho phép di dời hoặc chuyển nhượng phần cứng, phần mềm hoặc dữ liệu đến một cơ sở khác.

7/. Trung tâm dữ liệu cần sử dụng hệ thống điện dự phòng đảm bảo hệ thống không bị ngắt điện đột ngột: sử dụng UPS, thiết bị máy phát chạy xăng hoặc dầu. Có giải pháp phòng cháy chữa cháy chuyên dụng cho hệ thống trung tâm dữ liệu điện toán đám mây. Cảnh báo kịp thời xảy ra cháy nổ. Duy trì nhiệt độ và độ ẩm trung tâm dữ liệu,

thường xuyên giám sát và có báo cáo điều chỉnh nhiệt độ và độ ẩm khi các thông số vượt ngưỡng cho phép.

3.2.4.2. Kiểm soát thay đổi hạ tầng, cấu hình hệ thống điện toán đám mây

Nhà cung cấp dịch vụ điện toán đám mây phải có tài liệu mô tả quy trình thay đổi của tổ chức. Các chính sách cần được xây dựng, ban hành và thường xuyên cập nhật để quản lý rủi ro liên quan đến việc áp dụng các thay đổi vào hệ thống hạ tầng quan trọng của điện toán đám mây (vật lý và ảo hóa). Cần có những chính sách, thủ tục, bản kê danh sách các phần mềm và sử dụng biện pháp giám sát kỹ thuật để hạn chế và giám sát việc cài đặt các phần mềm trái phép trên các hệ thống máy chủ, máy tính ảo hay thay đổi cơ sở hạ tầng như mạng và các thành phần hệ thống khác trong hệ thống điện toán đám mây. Các thay đổi hạ tầng có rủi ro ảnh hưởng đến tính liên tục hoạt động của Khách hàng cần phải được thông báo ít nhất trước 5 ngày cho Khách hàng trước khi thực hiện thay đổi. Thường xuyên đào tạo nâng cao nhận thức an ninh thông tin và tuân thủ quy trình thay đổi và các quy định vận hành hệ thống.

3.2.4.3. An toàn phát triển ứng dụng trong điện toán đám mây

Tổ chức phát triển ứng dụng trong điện toán đám mây cần tuân thủ các nguyên tắc sau

1/. Xây dựng các bộ tiêu chuẩn phát triển ứng dụng an toàn.

2/. Thực hiện kiểm thử ứng dụng được phát triển trước khi cho phép đi vào hoạt động.

3/. Định kỳ rà soát và đánh giá an ninh thông tin cho ứng dụng phát triển trong điện toán đám mây

4/. Triển khai các API kiểm soát an toàn thông tin ứng dụng trong điện toán đám mây

3.2.4.4. Phân loại và dán nhãn dữ liệu theo các tiêu chí cụ thể.

Dữ liệu lưu trữ trong điện toán đám mây cần được phân loại và dán nhãn. Nhằm đánh dấu các dữ liệu quan trọng và bí mật để có biện pháp bảo vệ phù hợp. phân tách dữ liệu theo nguyên tắc: các dữ liệu nhạy cảm bí mật không lưu trữ cùng dữ liệu khác, và phải có biện pháp bảo vệ riêng cho các dữ liệu bí mật. Dữ liệu của tổ chức phải được phân loại và dán nhãn. Đề xuất chia làm ba loại như sau:

1/. Dữ liệu bí mật: số thẻ tín dụng, thông tin an ninh quốc gia, dữ liệu khách hàng, bí mật kinh doanh. Khi các dữ liệu bị mất gây thiệt hại to lớn cho tổ chức doanh nghiệp

2/. Dữ liệu nhạy cảm

3/. Thông tin công cộng

Chương 4 - TƯ VẤN, TRIỂN KHAI GIẢI PHÁP BẢO VỆ NỀN TẢNG ẢO HÓA CHO TỔ CHỨC, DOANH NGHIỆP TẠI VIỆT NAM

4.1. TƯ VẤN, THIẾT KẾ GIẢI PHÁP

Dựa trên tổng hợp, phân tích và đánh giá cũng như kinh nghiệm triển khai hệ thống Bảo vệ dữ liệu cho môi trường Ảo hóa, tác giả tư vấn tổ chức doanh nghiệp nên triển khai bộ giải pháp của hãng bảo mật Trend Micro để bảo vệ cho môi trường Ảo hóa. Bộ giải pháp kết hợp hai giải pháp như sau:

Giải pháp Hybrid Cloud Security (Deep Security) được thiết kế đặc biệt dành cho môi trường ảo hóa, giải pháp có khả năng bảo vệ máy chủ ảo trong môi trường Ảo hóa trước nguy cơ lây nhiễm mã độc hại, Virus, xâm nhập trái phép, vv.... Giải pháp Deep Security sử dụng kiến trúc agentless giúp giải quyết vấn đề xung đột tài nguyên do cơn bão anti-virus thường thấy khi thực hiện quét toàn hệ thống và update các mẫu nhận dạng virus mới, giúp giảm thiểu độ phức tạp trong vận hành bảo mật và cho phép các tổ chức gia tăng mật độ máy ảo, tăng tốc ảo hóa

Giải pháp mã hóa dữ liệu SecureCloud giúp mã hóa an toàn dữ liệu trong môi trường Ảo hóa và điện toán đám mây. Giải pháp SecureCloud tập trung bảo vệ an toàn tính bí mật của dữ liệu.

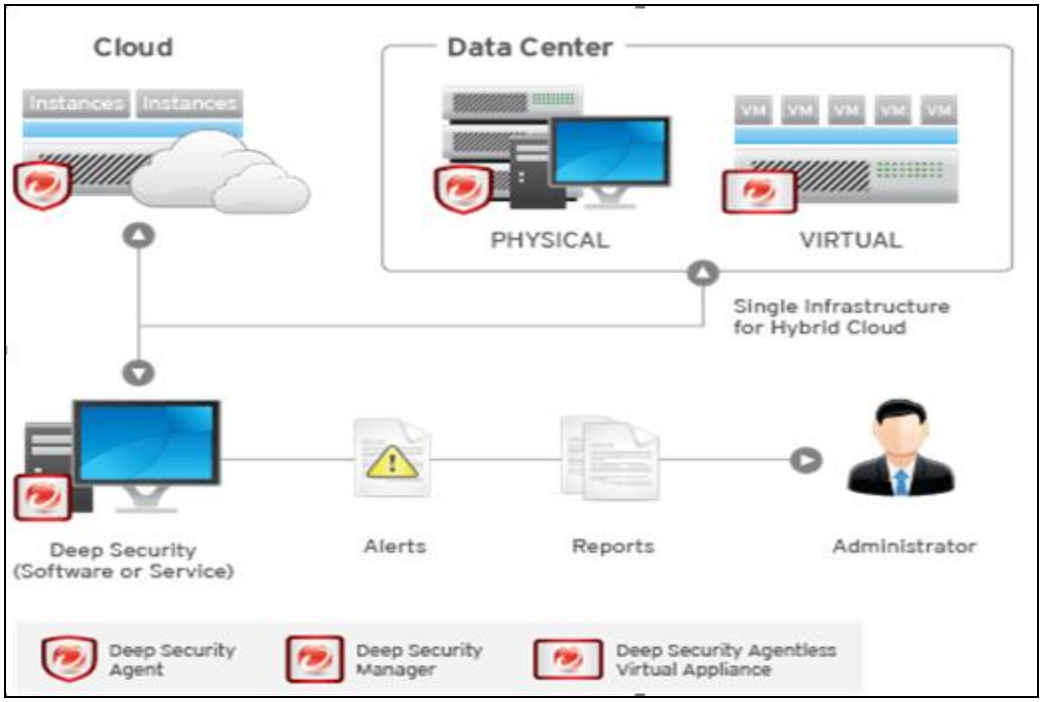
Một số đặc điểm nổi bật của giải pháp bảo mật cho môi trường Ảo hóa và Điện toán đám mây của hãng Trendmicro:

Được thành lập vào năm 1988 với hơn 20 năm hoạt động hãng Trend Micro chuyên cung cấp các giải pháp an ninh thông tin cho người dùng cá nhân và các tổ chức. Trendmicro là tổ chức dẫn đầu trong việc nghiên cứu và cung cấp giải pháp bảo vệ môi trường Ảo hóa và Điện toán đám mây. Giải pháp sử dụng kiến trúc Agentless, phát hiện và xử lý phần mềm độc hại, xâm nhập trái phép không cần cài trên từng máy ảo (Anti-malware Agentless) được thiết kế chuyên biệt cho các môi trường Ảo hóa và điện toán đám mây.

Khả năng tương thích với hầu hết các nền tảng ảo hóa và Điện toán đám mây phổ biến hiện nay: VMware vCloud Air, Amazon Elastic Compute Cloud (Amazon EC2), and Microsoft Azure [10]. Kết hợp chặt chẽ và tận dụng các API công nghệ của VMware vShield Endpoint và VMware vShield Endpoint Drivers

Tiết kiệm chi phí: theo tính toán của Trend Micro, với cùng một hạ tầng IT, nếu chuyển sang sử dụng Deep Security Anti-mailware Agentless, một tổ chức có 1.000 máy chủ ảo có thể tiết kiệm ít nhất nửa triệu đô-la trong khoảng thời gian 3 năm

Cung cấp các giải pháp an ninh thông tin chuyên biệt cho môi trường Ảo hóa và điện toán đám mây



Hình 22: Giải pháp bảo vệ Ảo hóa và Điện toán đám mây Trendmicro

Giải pháp an toàn mạng ảo bao gồm phòng chống xâm nhập, truy cập trái phép qua mạng để bảo vệ hệ thống trước các khai thác các lỗ hổng bảo mật chưa được vá lỗi và stateful tường lửa kiểm soát các port cần kết nối giúp cung cấp các lớp bảo vệ quanh mỗi máy ảo

Ngăn chặn các tấn công SQL injection and XSS trên ứng dụng, Che chắn lỗ hổng đã biết và chưa biết trong các trang web và các ứng dụng như Shellshock và Heartbleed

Cung cấp chi tiết, báo cáo có thể kiểm tra tài liệu đó ngăn chặn các cuộc tấn công và tình trạng tuân thủ chính sách, và các chính sách mã hóa cho các máy chủ

Xác định các hoạt động và hành vi đáng ngờ từ đó có các biện pháp phòng ngừa sớm như cảnh báo.

Phát hiện và ngăn chặn một loạt các mối đe dọa đến máy chủ, máy tính ảo, bao gồm mã độc hại, virus, các mối đe dọa web, phần mềm gián điệp, rootkits, sâu mạng và các tấn công nâng cao.

Giải pháp mã hóa SecureCloud sử dụng thuật toán mã hoá chuẩn an toàn AES 256 bit được tổ chức FIPS 140-2 cấp chứng chỉ. Giúp mã hóa toàn bộ dữ liệu, máy ảo và toàn bộ ổ đĩa máy ảo theo thời gian thực. Giải pháp mã hóa SecureCloud quản lý khóa giải mã an toàn. Không lưu trữ trên nhà cung cấp dịch vụ Điện toán đám mây. Sử dụng chuẩn giao thức quản lý khóa an toàn. Giải pháp mã hóa SecureCloud cho phép kiểm toán báo cáo và cảnh báo việc sử dụng và quản lý khóa và truy cập dữ liệu mã hóa. Giải pháp mã hóa SecureCloud hỗ trợ mã hóa cho đa nền tảng hệ điều hành khác nhau

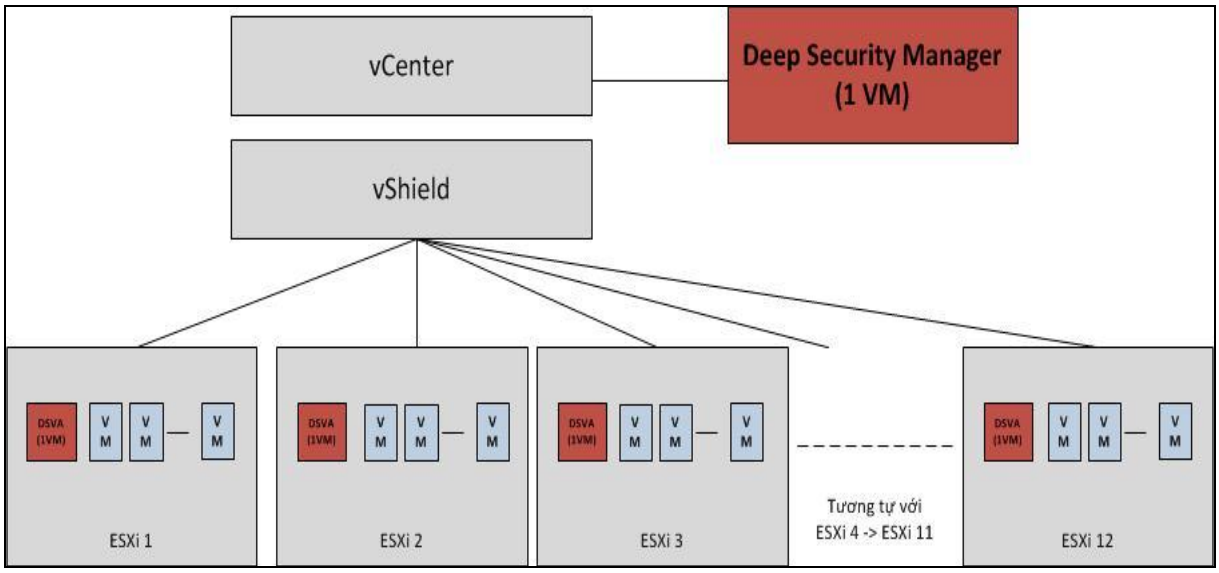
Bảng 5: So sánh giải pháp Deep Security Trendmicro và một số giải pháp an ninh khác dựa trên tổng hợp, đánh giá và quan điểm cá nhân của tác giả

Tiêu chí so sánh (Yes: đáp ứng đầy đủ No: không đáp ứng hoặc đáp ứng không đầy đủ Thang điểm tính từ 1, 2, 3, 4, 5. 5 là điểm cao nhất)	Deep Security TrendMicro	MCafee Move	Symantec Data Center Security
Tính năng quan trọng: Agentless Antivirus – quét toàn bộ máy ảo, quét virus theo thời gian thực Agentless phát hiện và ngăn chặn xâm nhập trái phép Giám sát toàn vẹn dữ liệu Quản trị chính sách tập trung Báo cáo và cảnh báo kịp thời đầy đủ thông tin	Yes	No (chỉ hỗ trợ Agentless cho Antivirus	No (chỉ hỗ trợ Agentless cho Antivirus
Giải pháp toàn diện, hỗ trợ đa nền tảng: vật lý, Ảo hóa, và Điện toán đám mây	yes	no	no
Dễ dàng triển khai, tích hợp	5	4	4
Hoạt động ổn định	5	4	5
Hỗ trợ kỹ thuật	4	3	4
Tiết kiệm hiệu năng	4	3	3

4.2. TRIỂN KHAI GIẢI PHÁP

Đề tài áp dụng các biện pháp đề xuất để triển khai giải pháp bảo vệ dữ liệu cho hệ thống Ảo hóa đặt tại một trung tâm dữ liệu mới của Hải Quan đặt tại Lô E3 - Đường Dương Đình Nghệ - Cầu Giấy - Hà Nội

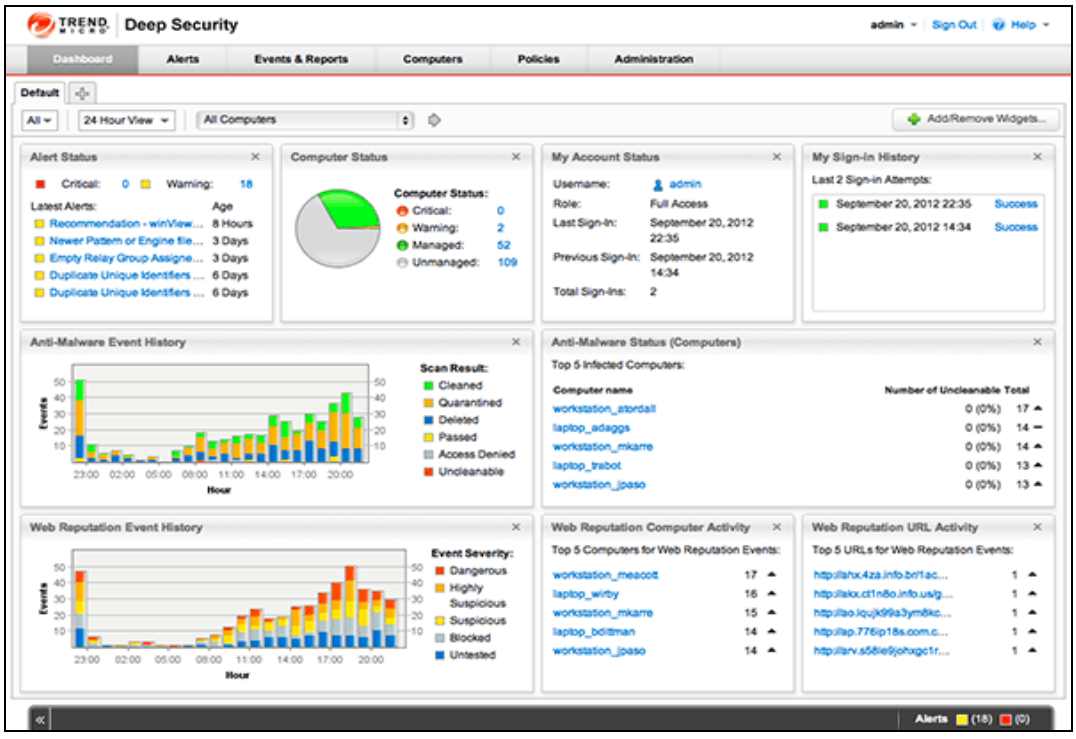
4.2.1. Mô hình triển khai



Hình 23: Mô hình triển khai hệ thống Deep Security

4.2.2. Thành phần giải pháp

Deep Security Manager. Là công cụ quản trị tập trung mạnh mẽ cho phép quản trị viên tạo ra các chính sách an ninh và áp dụng chúng vào máy chủ, theo dõi các cảnh báo và đưa ra các hành động phản ứng để đối phó với các mối đe dọa, phân phối các bản cập nhật bảo mật cho các máy chủ, và tạo các báo cáo. Tính năng mới Event Tagging cho phép quản lý một số lượng lớn các sự kiện.



Hình 24: Giao diện thành phần Deep Security Manager

Deep Security Virtual Appliance: Là một máy ảo bảo mật được xây dựng cho các môi trường ảo hóa cung cấp các module chống mã độc , kiểm tra tính toàn vẹn.

Virtual Appliance bảo vệ các máy ảo khác cùng hệ thống của mình mà các máy ảo khác không cần cài bất cứ 1 thành phần gì.

Smart Protection Network. Deep Security được tích hợp với kiến trúc cloud-client thế hệ mới để cung cấp sự bảo vệ theo thời gian thực khỏi các mối đe dọa mới xuất hiện bằng cách liên tục đánh giá và phân tích danh tiếng của các websites, nguồn emails và files.

Vcenter: thành phần quản trị tập trung các server ảo hóa ESX được phát triển bởi hãng Vmware

Vshield Endpoint là thành phần Antivirus và Anti-Malware cho máy ảo của hãng Vmware

Vshield manager: Quản lý tập trung các thành phần security (vShield) của hãng Vmware

4.2.3. Các tính năng chính triển khai

Tính năng phát hiện và xử lý mã độc hại trên các máy Ảo: các loại mã độc Deep Security có thể phát hiện và xử lý bao gồm VirusTrojans,Backdoor, Worms, Network viruses, Rootkits, Spyware/grayware. Chức năng chống mã độc hoạt động real time bảo vệ máy ảo 24/7.

Tính năng tường lửa Ảo: tính năng này giúp giảm thiểu các tấn công vào các server trong tất cả các môi trường vật lý, điện toán đám mây, và ảo hóa; ngăn chặn các cuộc tấn công như từ chối dịch vụ và phát hiện quét thăm dò và quản trị tập trung chính sách tường lửa của các máy chủ. Tính năng quản trị tập trung chính sách cho các máy chủ firewall bao gồm các mẫu cho các kiểu máy chủ phổ biến Tính năng lọc chi tiết theo địa chỉ IP & MAC, theo dịch vụ, cổng kết nối. Hỗ trợ tất cả các giao thức TCP, UDP, ICMP, IGMP

Tính năng lọc gói tin **Deep Packet Inspection** bao gồm các thành phần IPS/IDS, web application Protection, Application control có khả năng:

Bảo vệ chống lại các nguy cơ đã biết và các cuộc tấn công zero-day bằng cách chặn các lỗ hổng khai thác không giới hạn.

Bảo vệ những lỗ hổng chưa được biết đến trước những khai thác điểm yếu, che chắn các lỗ hổng trong ứng dụng web cho đến khi việc sửa chữa lỗi hoàn thành.

Chống lại các tấn công SQL injection, cross-site scripting, phát hiện và ngăn chặn các phần mềm độc hại truy cập vào mạng

Phát hiện các đáng ngờ trong luồng dữ liệu Vào/ra chẳng hạn như các giao thức được cho phép trên các cổng tiêu chuẩn về giao thức , nôi dung để tìm ra dấu hiệu của cuộc tấn công hoặc vi phạm chính sách

Bảo vệ các lỗ hổng trước những khai thác điểm yếu cho đến lần bảo trì window kế tiếp.

Tính năng giám sát thay đổi tập tin quan trọng. Tính năng giám sát các tập tin quan trọng của hệ điều hành hoặc các khóa regitry để phát hiện mã độc hại cũng như sự thay đổi bất thường

Theo dõi những tập tin quan trọng của hệ điều hành và ứng dụng, chẳng hạn như các thư mục, các khóa registry để phát hiện mã độc hại và những thay đổi bất thường.

Phát hiện việc sửa đổi và tạo mới các file hệ thống và thông báo lại theo thời gian thực

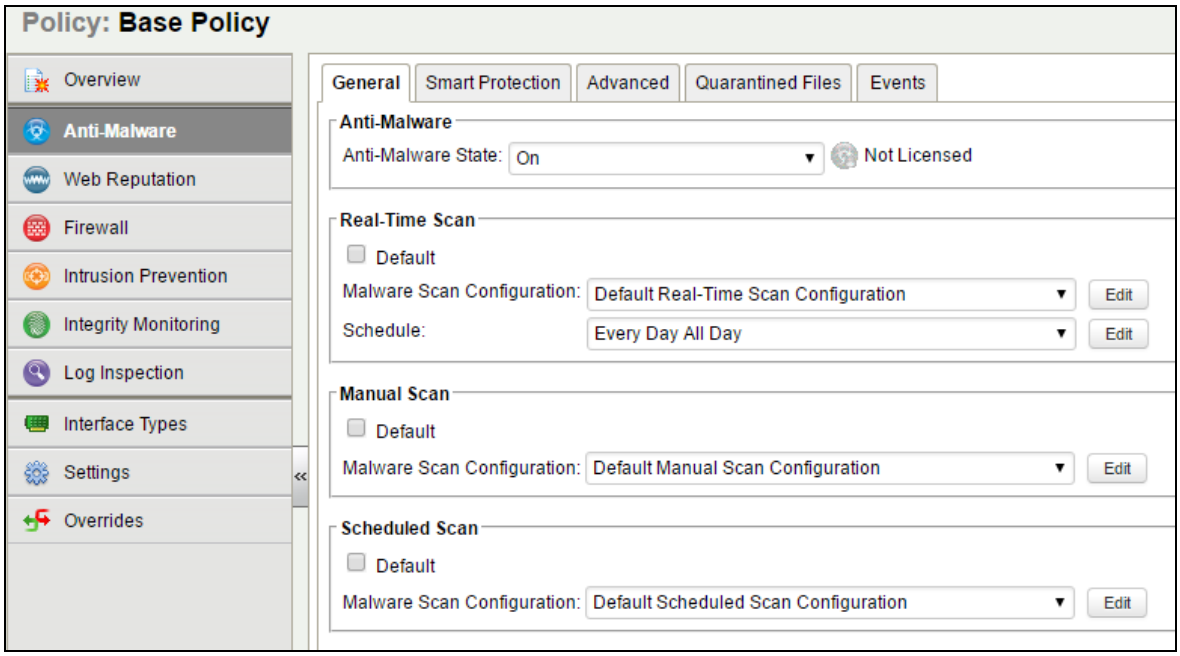
Cho phép kiểm soát theo ý muốn, có thể theo lịch hoặc kiểm soát theo thời gian thực, kiểm tra đặc tính tập tin và theo dõi từng thư mục cụ thể.

Tính năng này cũng bảo vệ hypervisor khỏi các tấn công khai thác bằng cách cung cấp giám sát sự toàn vẹn của hypervisor tận dụng công nghệ TPM/TXT.

Tính năng Log Inspection: thu thập và phân tích các log của hệ điều hành và ứng dụng để tìm ra các sự kiện an ninh, tối ưu hóa việc xác định các sự kiện an ninh quan trọng trong các log sự kiện.

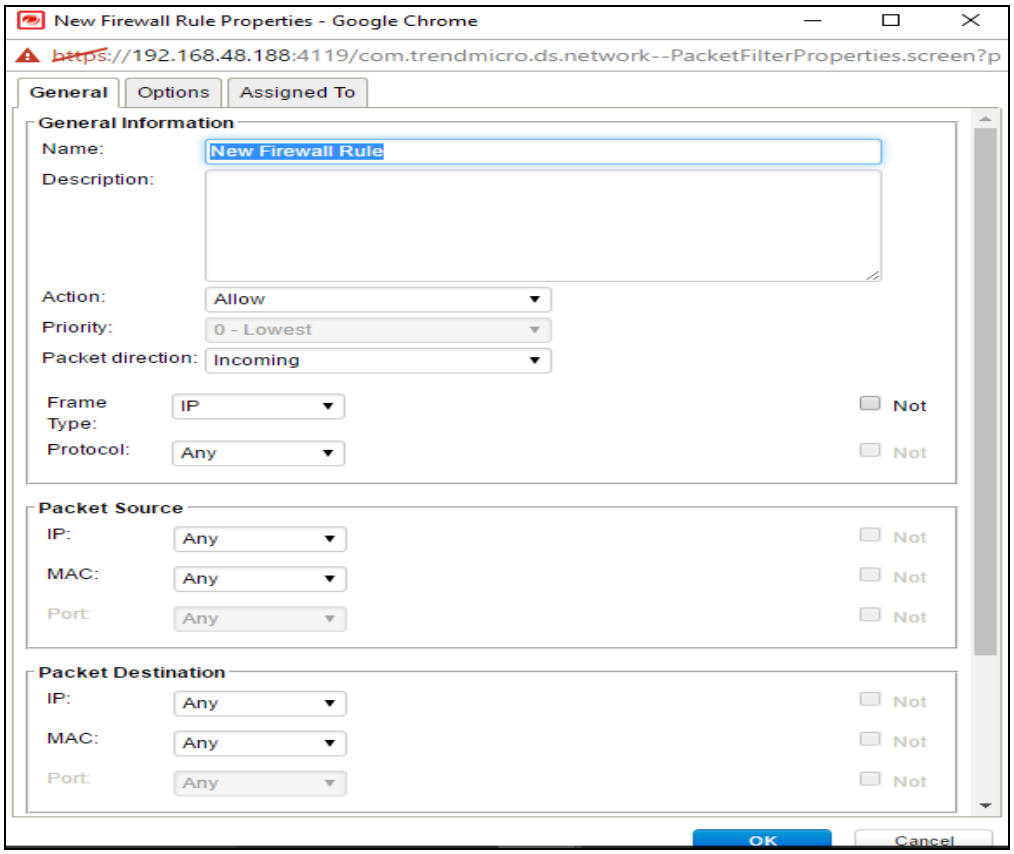
4.2.4. Cấu hình thiết lập chính sách bảo vệ

Cấu hình thiết lập tính năng Anti-Malware. Chọn tính năng Anti-Malware chọn thẻ General cấu hình bật tính năng Antimalware



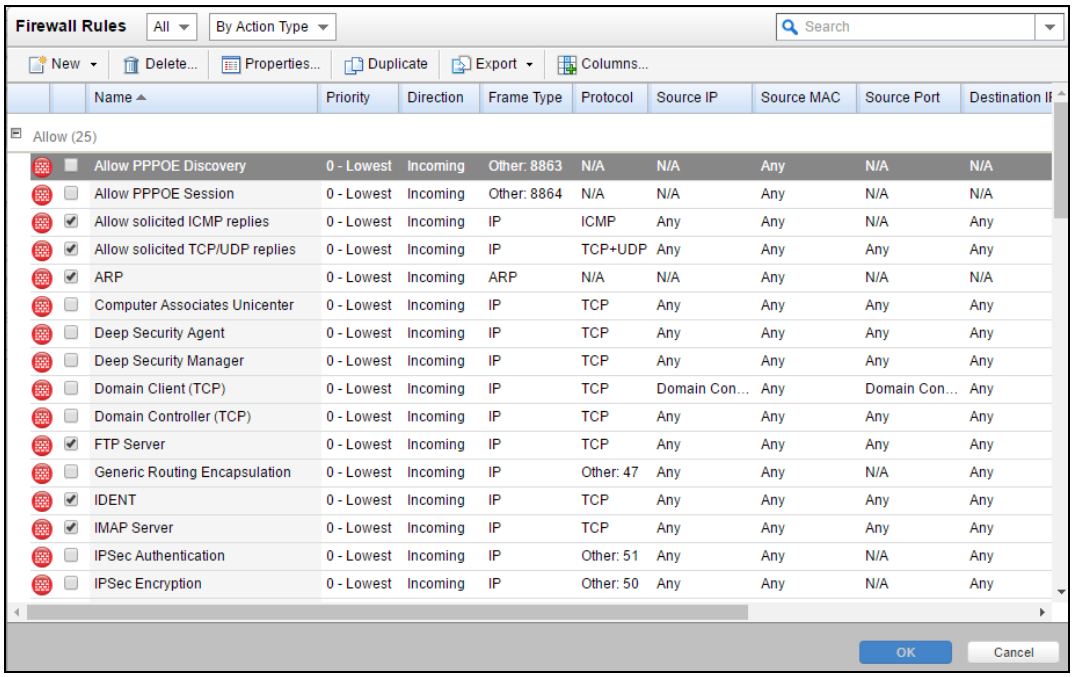
Hình 25: thiết lập tính năng phòng chống mã độc

Cấu hình thiết lập chính sách tường lửa bảo vệ các lớp mạng Ảo



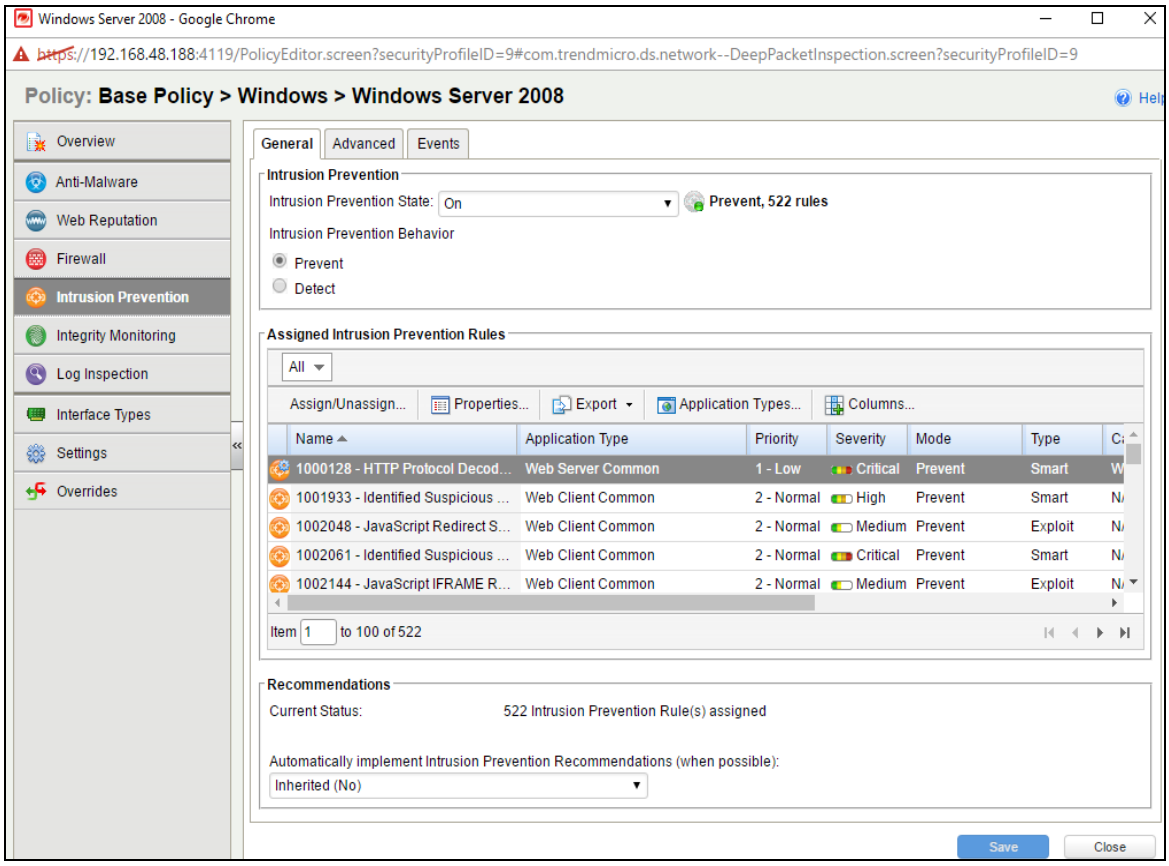
Hình 26: cấu hình chính sách tường lửa

Cấu hình chính sách tường lửa ứng dụng

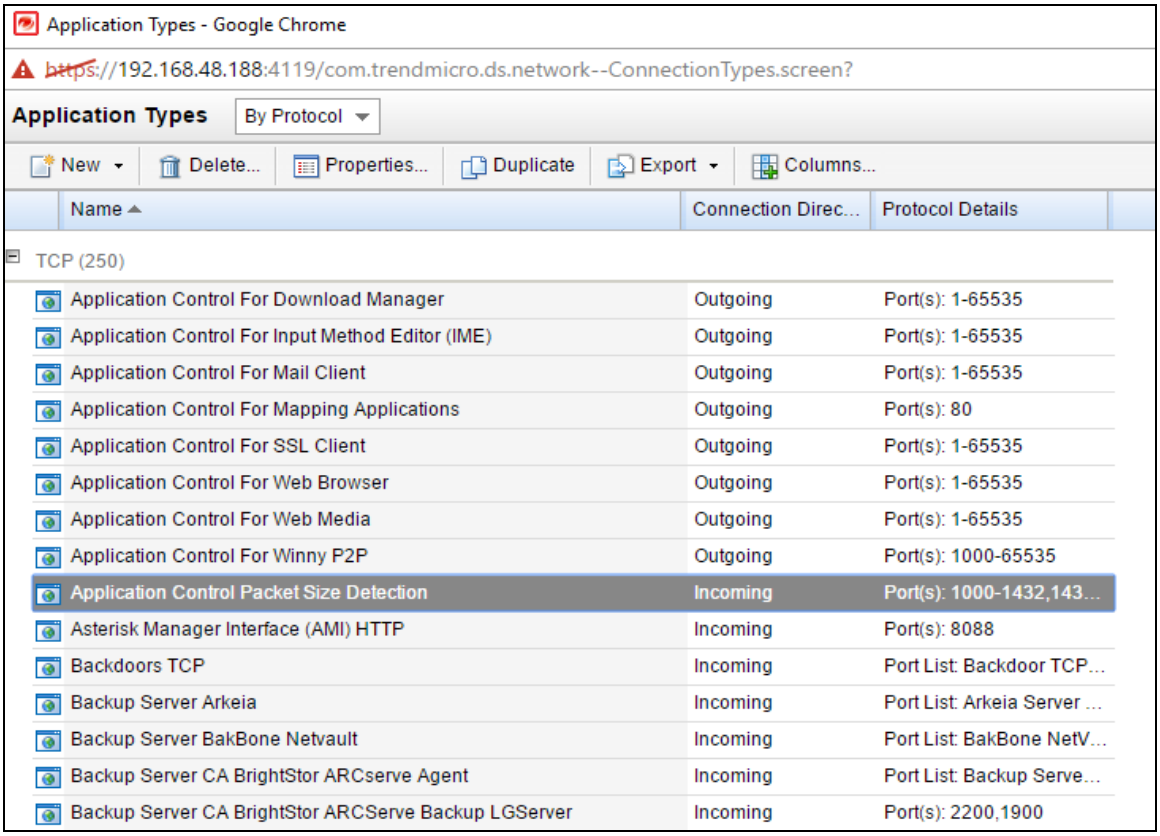


Hình 27: cấu hình chính sách tường lửa ứng dụng

Cấu hình tính năng Deep Packet Inspection

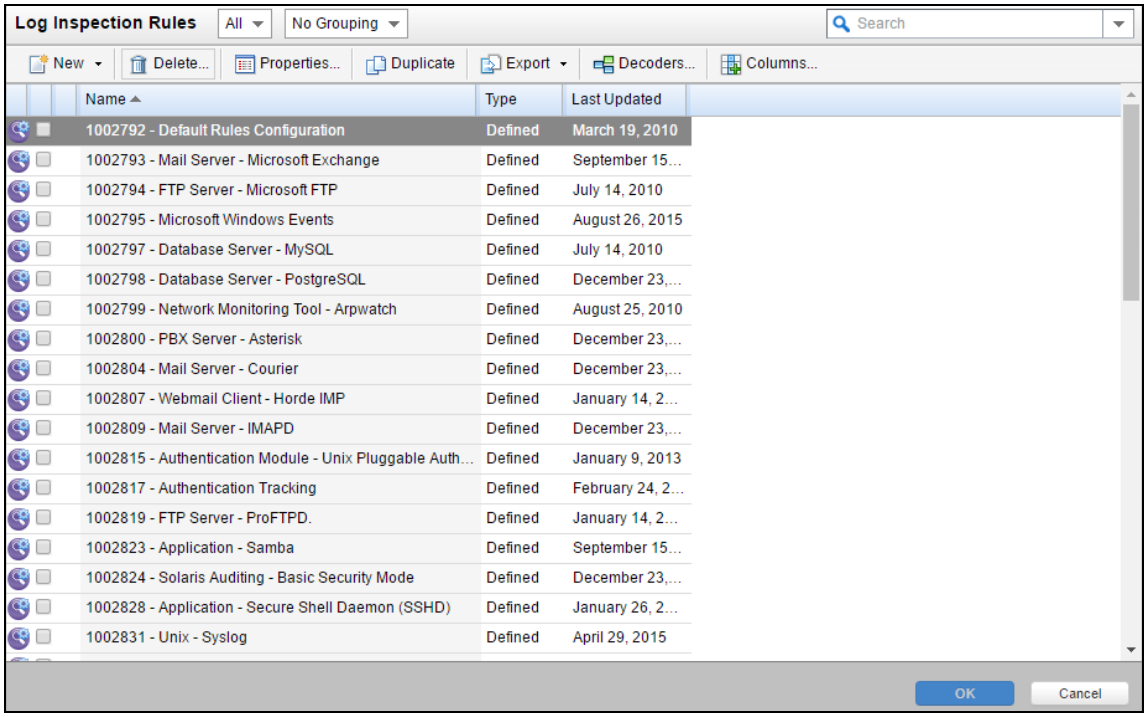


Hình 28: cấu hình tính năng Deep Packet Inspection

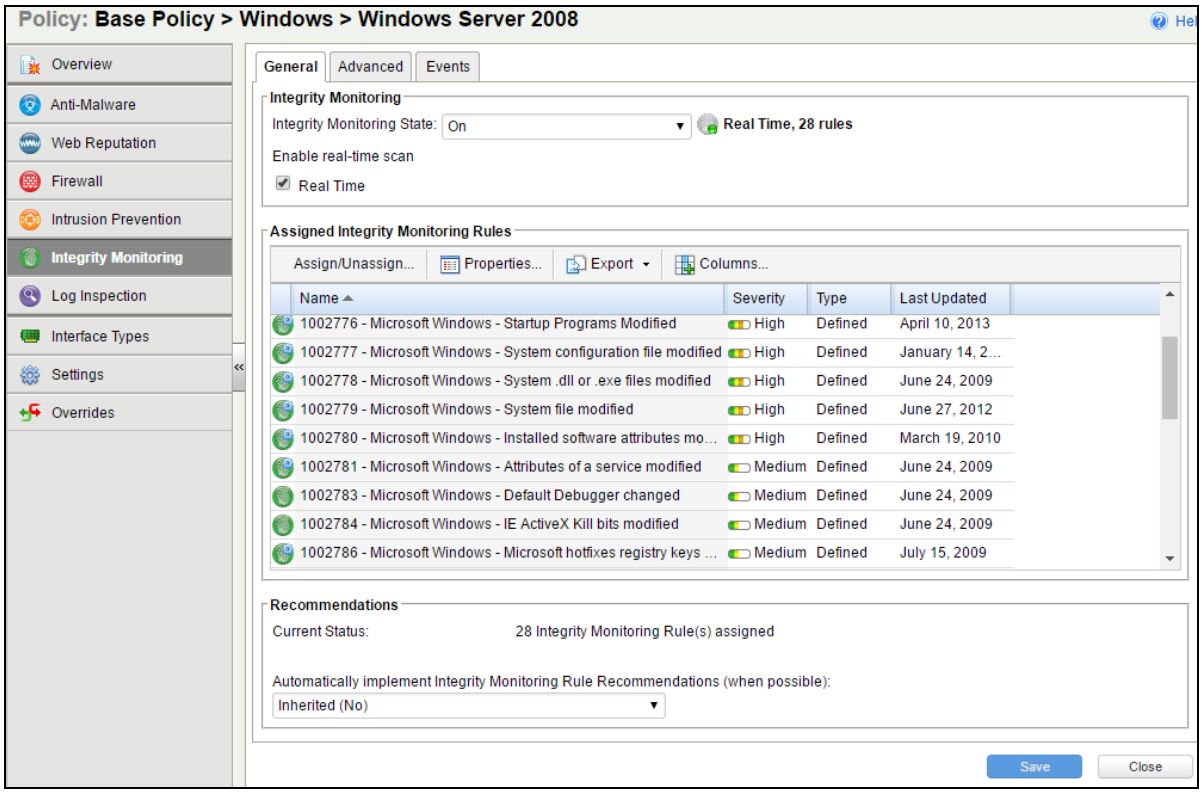


Hình 29: cấu hình tính năng Deep Packet Inspection

Cấu hình tính năng Integrity Monitoring

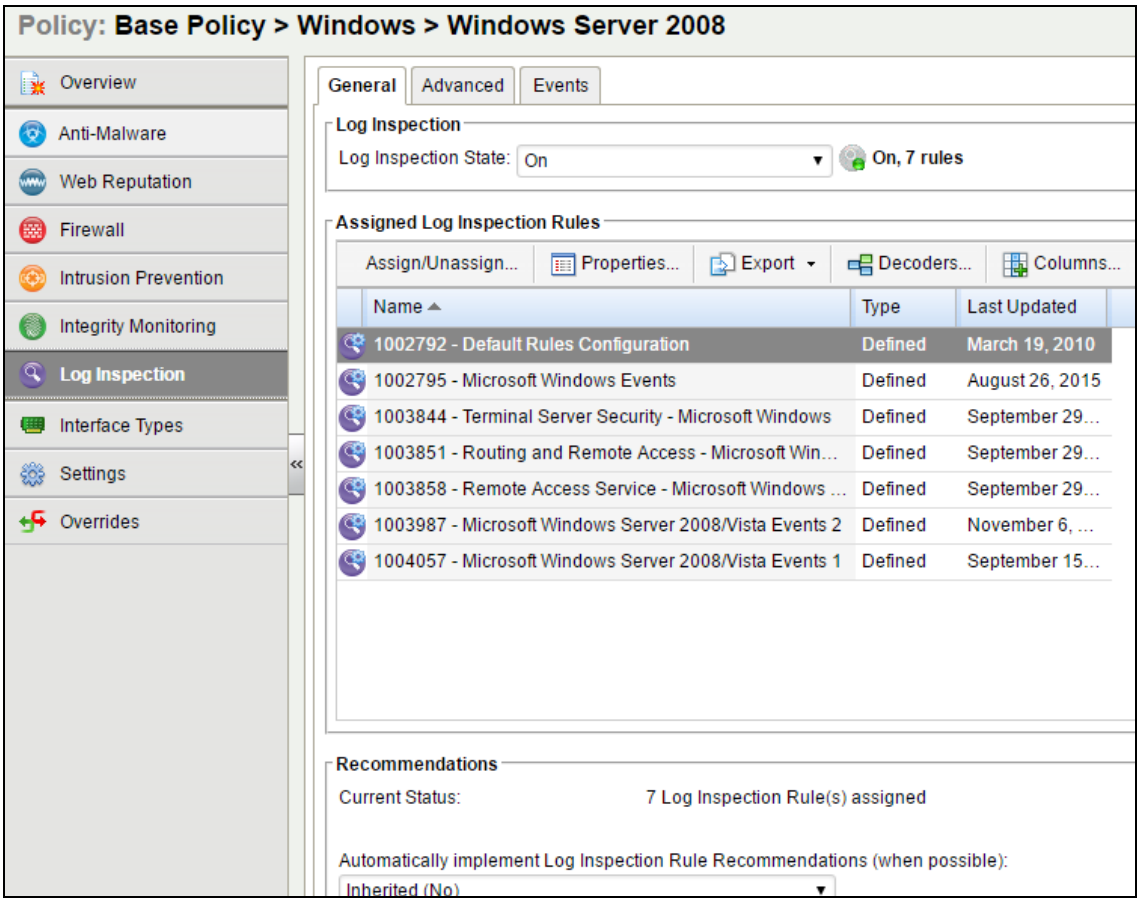


Hình 30: cấu hình giám sát thay đổi cấu hình



Hình 31: cấu hình giám sát thay đổi cấu hình

Cấu hình tính năng Log Inspection



Hình 32: Cấu hình tính năng Log Inspection

4.2.5. Kết quả đạt được sau khi triển khai giải pháp Deep Security tại Trung tâm dữ liệu

Sử dụng tài nguyên hiệu quả hơn so với các giải pháp anti-malware truyền thống. Giải pháp giúp tối ưu hoá, tiết kiệm, loại bỏ chi phí triển khai nhiều phần mềm trên từng máy chủ ảo bằng một máy chủ ảo đa tính năng và được quản lý tập trung.

Cải thiện việc quản trị bảo mật trong môi trường VMware bằng cách giảm sự phức tạp khi phải cấu hình thường xuyên update, và patch các agents

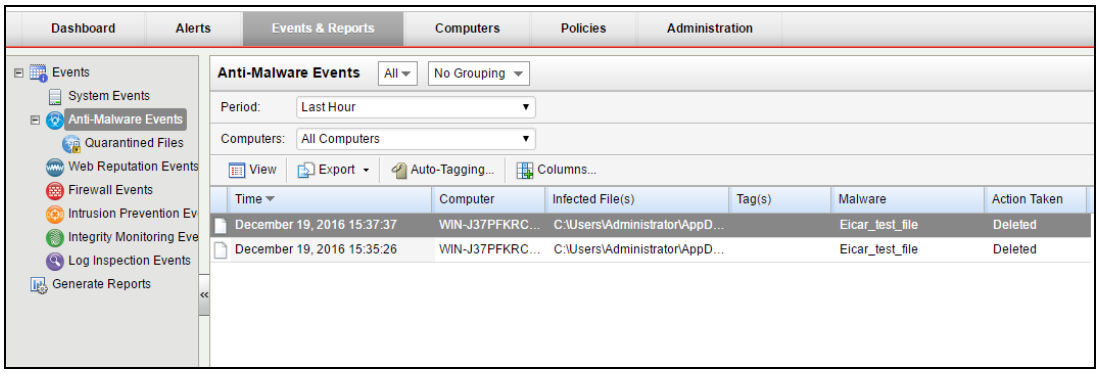
Phát hiện và xóa malware khỏi các virtual servers trong thời gian thực với độ ảnh hưởng đến hiệu năng nhỏ nhất.

Bảo vệ các điểm yếu đã biết và chưa biết trong các ứng dụng và hệ điều hành, phát hiện các hành vi đáng ngờ, cho phép chủ động các biện pháp phòng chống

Tận dụng năng lực về việc đánh giá danh tiếng web của một trong những cơ sở dữ liệu về danh tiếng lớn nhất thế giới để theo dõi độ tin cậy của các websites và bảo vệ người sử dụng khỏi việc truy cập vào các sites bị lây nhiễm đó

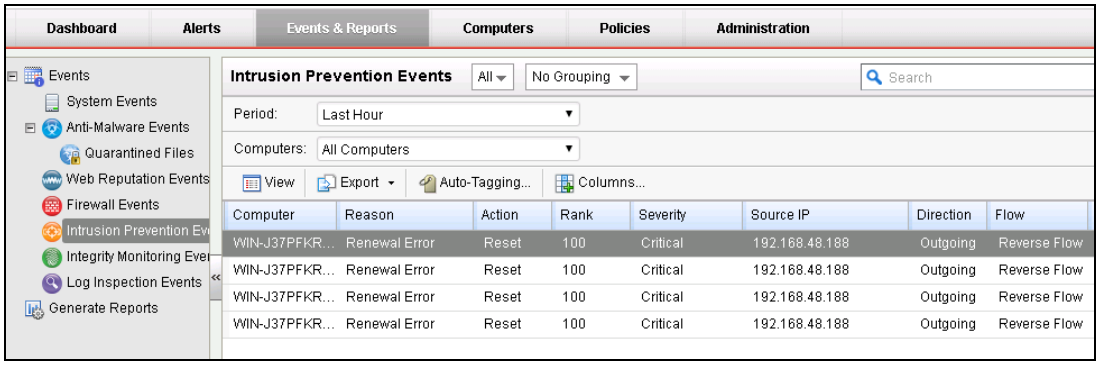
Cung cấp thông tin chi tiết, báo cáo chỉnh sửa về tài liệu ngăn ngừa các cuộc tấn công và tình trạng tuân thủ chính sách An ninh thông tin của tổ chức.

Kết quả: tính năng Anti-Malware phát hiện mã độc lây nhiễm vào máy ảo



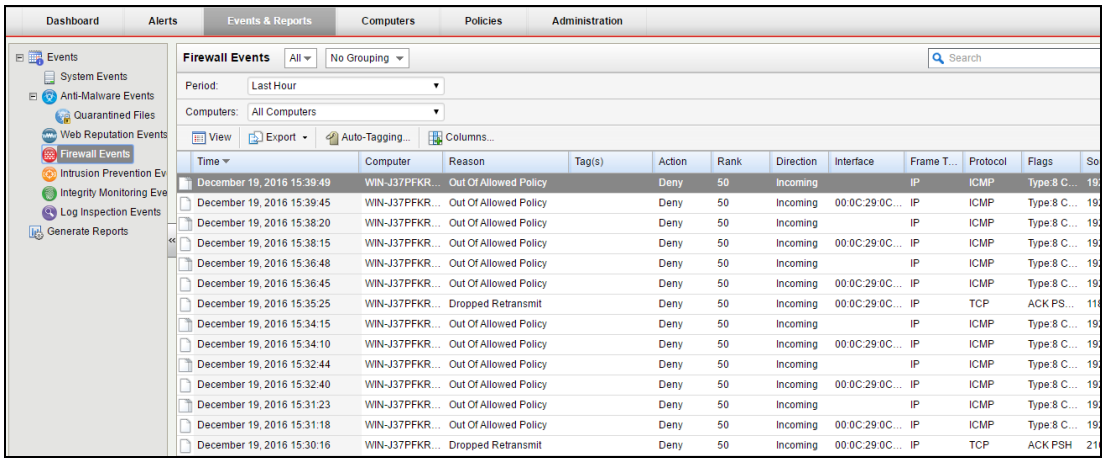
Hình 33: Kết quả hoạt động tính năng Anti-Malware

Kết quả hoạt động tính năng Deep Packet Inspection phát hiện tấn công vào máy ảo



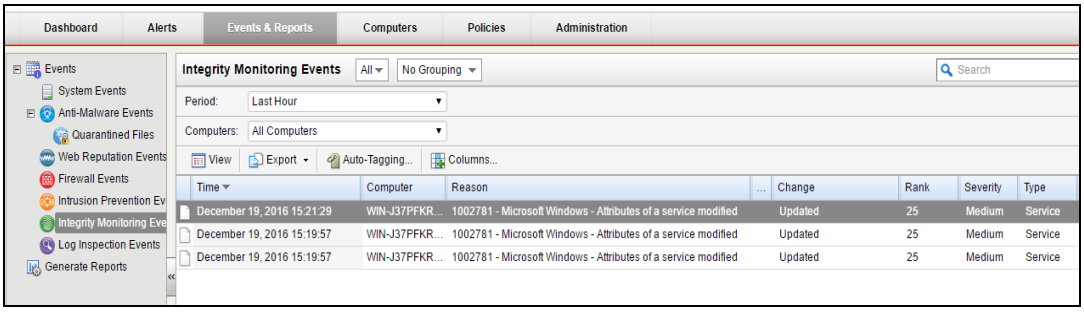
Hình 34: Kết quả hoạt động tính năng Deep Packet Inspection

Kết quả hoạt động tính năng Firewall ngăn chặn các kết nối không được chính sách của tổ chức



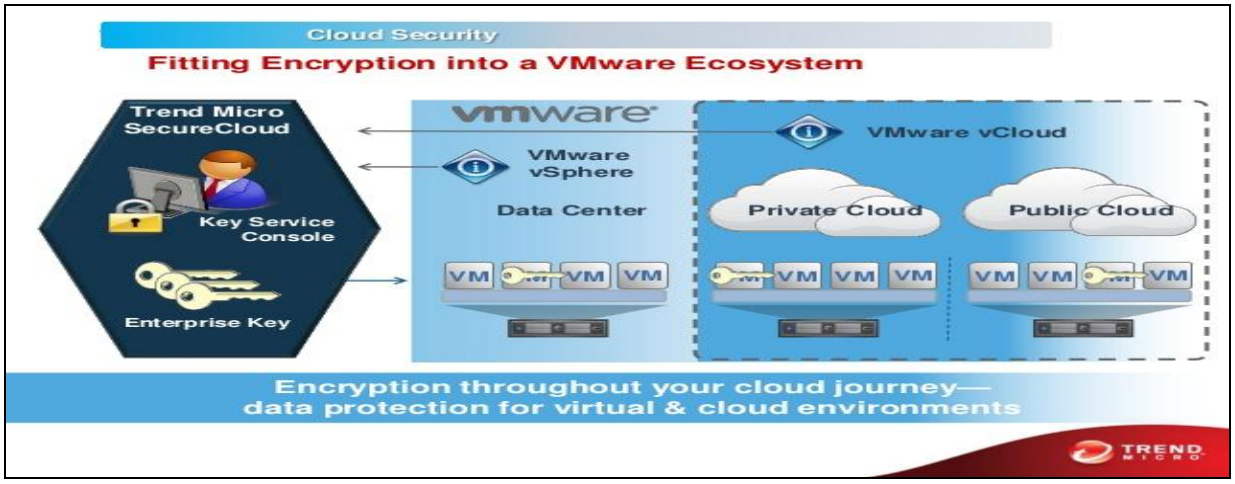
Hình 35: Kết quả hoạt động tính năng tường lửa

Kết quả tính năng Integrity Monitoring phát hiện được các thay đổi file cấu hình trái phép trên máy ảo



Hình 36: Tính năng giám sát phát hiện thay đổi file cấu hình trái phép

Triển khai giải pháp mã hóa SecureCloud mã hóa dữ liệu lưu trữ trên điện toán đám mây Amazon EC và Microsoft Azure. Mô hình triển khai

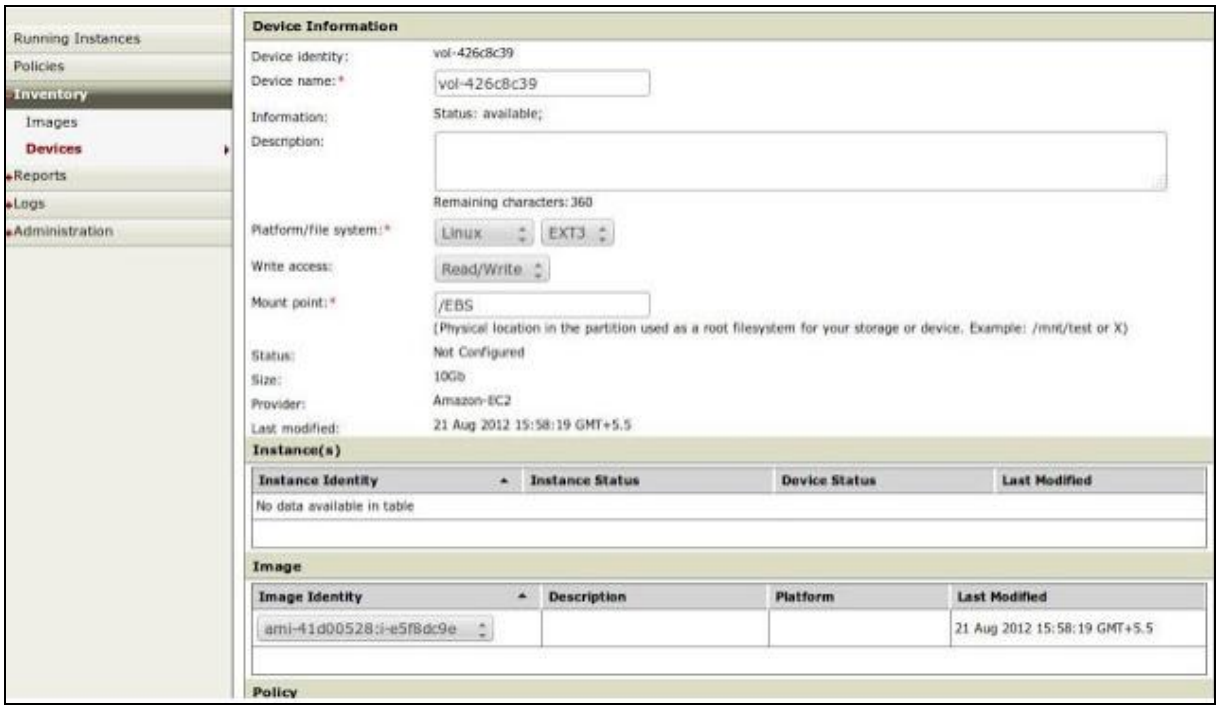


Hình 37: Mô hình triển khai giải pháp mã hóa Trendmicro dữ liệu trên điện toán đám mây

Cài đặt thành phần quản trị khóa tập trung: cài đặt webserver (Microsoft IIS), cài đặt cơ sở dữ liệu quản lý tài khoản và khóa, cài đặt thành phần mã hóa SecureCloud Agents, tích hợp Amazon EC2

Hình 38: tích hợp dịch vụ Điện toán đám mây

Tiến hành cấu hình thiết bị cần mã hóa dữ liệu



Hình 39: Cấu hình thiết bị mã hóa

Cấu hình chi tiết thu mục cần mã hóa dữ liệu

Hình 40:Cấu hình thư mục cần mã hóa

KẾT LUẬN

Trong kỷ nguyên công nghệ hiện nay Ảo hóa và điện toán đám mây đang dần trở nên phổ biến và là thành phần quan trọng đối với tổ chức, doanh nghiệp. Việc bảo vệ dữ liệu trong môi trường Ảo hóa đã trở nên cần thiết hơn bao giờ hết.

Đề tài đã thành công trong việc nhận dạng, tìm hiểu và phân tích đầy đủ, chính xác một số mối nguy cơ và thách thức an ninh thông tin nghiêm trọng đối với môi trường Ảo hóa và Điện toán đám mây hiện tại và tương lai:

1/. Tồn tại lỗ hổng trong phần mềm lõi của nền tảng ảo hóa,

2/. Tấn công chéo giữa các máy ảo

3/. Thất thoát dữ liệu giữa các thành phần ảo hóa.

4/. Lây nhiễm mã độc hại, virus

Bên cạnh đó đề tài đã đề xuất được các giải pháp đơn giản và hiệu quả nhằm giải quyết tận gốc các mối nguy cơ và thách thức trong môi trường Ảo hóa và Điện toán đám mây, các đề xuất này có khả năng áp dụng thực tế trong các đơn vị và doanh nghiệp:

1/. Xây dựng kiến trúc ảo hóa an toàn

2/. Sử dụng công nghệ phòng chống mã độc chuyên biệt cho môi trường ảo hóa.

3/. Áp dụng phương thức phòng thủ nhiều lớp theo chiều sâu để bảo vệ dữ liệu trong môi trường Ảo hóa và Điện toán đám mây: lớp kiểm soát truy cập, mã hóa dữ liệu và lớp khôi phục nhanh chóng.

4/. Xây dựng bộ chính sách tuân thủ đối với tổ chức cung cấp dịch vụ điện toán đám mây

Các giải pháp trong đề tài giúp cho các tổ chức, doanh nghiệp có thể lên kế hoạch về các vấn đề cần xử lý để đảm bảo tính bí mật, tính toàn vẹn và tính sẵn sàng của dữ liệu trong môi trường Ảo hóa và Điện toán đám mây.

Trong thời gian tới tác giả sẽ tiếp tục nghiên cứu mở rộng và phát triển các biện pháp bảo vệ thông tin trong môi trường Ảo hóa và Điện toán đám mây, phát triển ứng dụng mã hóa dữ liệu sử dụng thuật toán mã hóa đồng cấu đầy đủ.

TÀI LIỆU THAM KHẢO

1. James Michael Stewart and Mike Chapple and Darril Gibson (2015), "Certified Information Systems Security Professional Study Guide Seventh Edition", *John Wiley & Sons, Inc.*
2. Dave Shackleford (2011)"Virtualization Security", *John Wiley & Sons, Inc.*
3. Peter Mell and Timothy Grance (2011), "The NIST Definition of Cloud Computing", *Special Publication 800-145*
4. Ronald L. Krutz and Russell, (2011)"A Comprehensive Guide to Secure Cloud Computing", *John Wiley & Sons, Inc.*
5. Wayne Jansen and Timothy Grance (December 2011) ,"Guidelines on Security and Privacy in Public Cloud Computing",
6. Lee Newcombe (July 2012), "Securing Cloud Services", *IT Governance Publishing.*
7. Dai Yuefa, Wu Bo, Gu Yaqiang, Zhang Quan, Tang Chaojing (2009),"Data Security Model for Cloud Computing", ISBN 978-952-5726-06-0.
8. Craig Gentry, Fully Homomorphic Encryption Using Ideal Lattices, STOC '09: Proceedings of the 41st annual ACM symposium on Theory of computing, DOI:10.1145/1536414.1536440 September 2009.
9. Tebaa, M.; El Hajji, S.; El Ghazi, A., "Homomorphic encryption method applied to Cloud Computing," in Network Security and Systems (JNS2), 2012 National Days of , vol., no., pp.86-89, 20-21 April 2012
10. IDC Custom Solutions (Mar 2016), Server Security: Virtualization & Cloud Changes Everything,