ĐẠI HỌC QUỐC GIA HÀ NỘI

**TRƯỜNG ĐẠI HỌC CÔNG NGHỆ**

**NGUYỄN VIỆT DŨNG**

# BẢO VỆ THÔNG TIN TRONG MÔI TRƯỜNG ẢO HÓA

Chuyên ngành: Hệ thống thông tin

Mã số: 60480104

TÓM TẮT LUẬN VĂN THẠC SĨ

Hà Nội – 2016

# 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<br>Integrity-tính toàn vẹn<br>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 |

# 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.

**Commented [t1]:** Phần note vàng theo em nên Remove đi

**Commented [t2]:** Gồm 3 Mục tiêu chính
-Hiểu rõ các nguy cơ, mối đe dọa an ninh thông tin trong môi trường ảo hóa và điện toán đám mây
-Tăng cường an ninh cho môi trường ảo hóa và điện toán đám mây
- ứng dụng giải pháp an ninh ảo hóa cho doanh nghiệp thực tế

**Commented [t3]:** -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
-Làm rõ các mối đe dọa an ninh đối với môi trường ảo hóa
- Đi sâu cơ chế, giải pháp kỹ thuật để bảo vệ thông tin trong môi trường ảo hóa và điện toán đám mây
- Thực hiện triển khai giải pháp an ninh đề xuất cho một tổ chức, doanh nghiệp tại việt nam để bảo vệ môi trường ảo hóa và điện toán đám mây

**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….

**Bố cục luận văn bao gồm 4 chương:**

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

Tìm hiểu, làm rõ các khái niệm, đặc trưng, mô hình triển khai, kiến trúc của môi trường Ảo hóa và Điện toán đám mây

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

Tìm hiểu phân tích các nguy cơ và thách thức anh ninh thông tin trong môi trường Ảo hóa và Điện toán đám mây

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

Đề xuất các giải pháp bảo vệ thông tin trong môi trường Ảo hóa và Điện toán đám mây

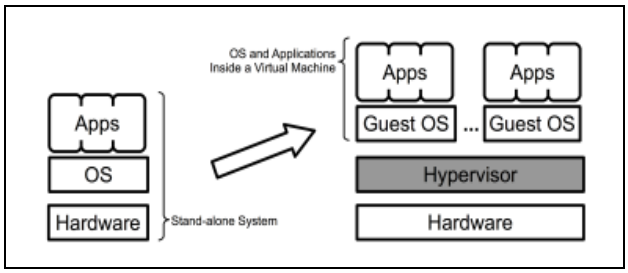
Chương 4 - TƯ VẤN, TRIỂN KHAI GIẢI PHÁP BẢO VỆ NỀN TẢNG ẢO HÓA CHO TỔ CHỨC, DOANH NGHIỆP TẠI VIỆT NAM

# 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

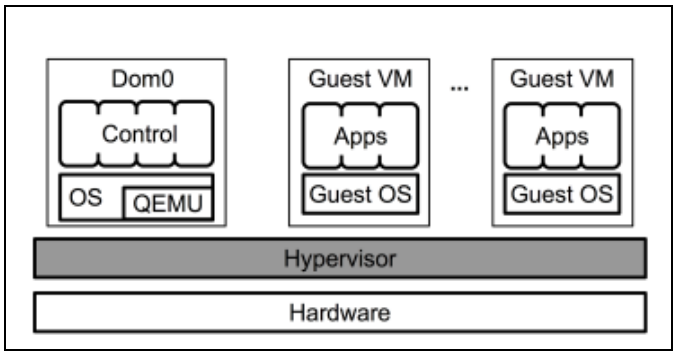
Định nghĩa Ảo hóa: Ảo hóa là công nghệ được thiết kế tạo ra tầng trung gian giữa hệ thống phần cứng máy tính và phần mềm chạy trên nó. Từ một máy vật lý có thể tạo ra nhiều máy ảo độc lập. Mỗi máy ảo đều được thiết lập một hệ thống riêng rẽ với hệ điều hành, ảo hóa mạng, ảo hóa hóa lưu trữ và các ứng 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: Hệ điều hành và ứng dụng một máy ảo*

### 1.1.2. Phân loại nền tảng Ảo hóa

#### *1.1.2.1. Kiểu 1: "Bare Metal Hypervisor"*

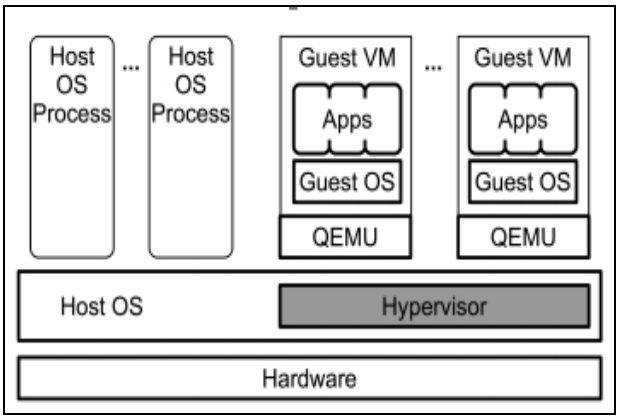



*Hình 02: hypervisor kiểu 1-Hệ thống Xen*

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.

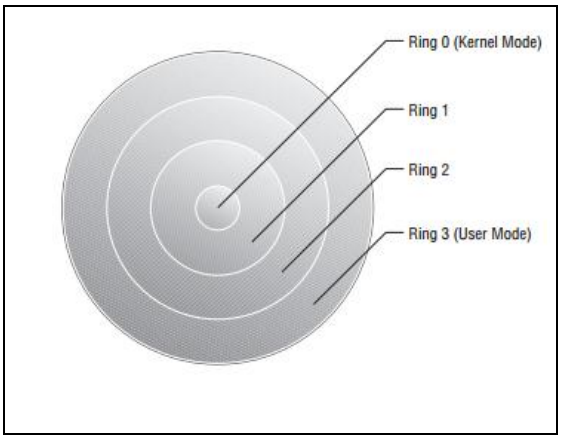
#### *1.1.2.2. Kiểu 2: "Hosted Hypervisor"*




*Hình 03: hypervisor kiểu 2-Hệ thống KVM*

Loại nền tảng Ảo hóa số hai này chạy trên hệ điều hành như 1 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.

### 1.1.3. Ảo hóa kiến trúc vi xử lý x86




*Hình 04: mức đặc quyền vi xử lý x86*

## 1.2. KHÁI NIỆM ĐIỆN TOÁN ĐÁM MÂY

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".

## 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 05: Mô hình ba dịch vụ điện toán đám mây*

### 1.4.1. Hạ tầng hướng dịch vụ

### 1.4.2. Dịch vụ nền tảng

### 1.4.3. Dịch vụ Phần mềm

## 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.

### 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.

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

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

### 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. 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.

### 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.

### 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 kịp thời hoặc cấu hình 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.

### 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.

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

Ảo hóa là một hệ thống động, sự kết hợp nhiều hệ thống ảo hóa 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.

#### 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.

#### 2.1.6. Tranh chấp tài nguyên.

Hệ thống bảo mật truyền thống như 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. máy chủ vật lý, nó có khả năng làm giảm hiệu suất của máy chủ.

#### 2.1.7. Thiếu tính tuân thủ-thiếu công cụ kiểm soát, đánh giá

Mức độ tích hợp cao hơn cũng đồng nghĩa với việc đặt ra sự đòi hỏi lớn hơn về khả năng đảm bảo sự tuân thủ, đặc biệt là giữa các ứng dụng cực kỳ quan trọng. Các bản sao lưu và ảnh máy ảo được tạo ra hàng ngày, hàng giờ và tự động lưu trữ trong môi trường ảo hóa, rất khó để biết được chúng được lưu trữ ở đâu, ai di chuyển và sao chép chúng. Rất khó để truy vết được sao chép trái phép dữ liệu

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

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

Bảng 1: 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] | |
| 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. |
| Tấn công từ bên ngoài | 1/. Tấn công khai thác lỗ hổng trong phần mềm, ứng dụng |

| | |
|---|---|
| hệ thống: | 2/. Xâm nhập trái phép.<br>3/. Sử dụng kỹ thuật lừa đảo để đánh cắp tài khoản và mật khẩu truy cập hệ thống.<br>4/. Tấn công vào phiên làm việc hợp lệ trên máy tính.<br>5/. Lây nhiễm mã độc, virus |
| 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. |
| Thất thoát dữ liệu | 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. |
| **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: | |
| 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: | 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. |
| Tấn công từ chối 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 | 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 2: Các rủi ro An ninh thông tin đối với điện toán đám mây [5]

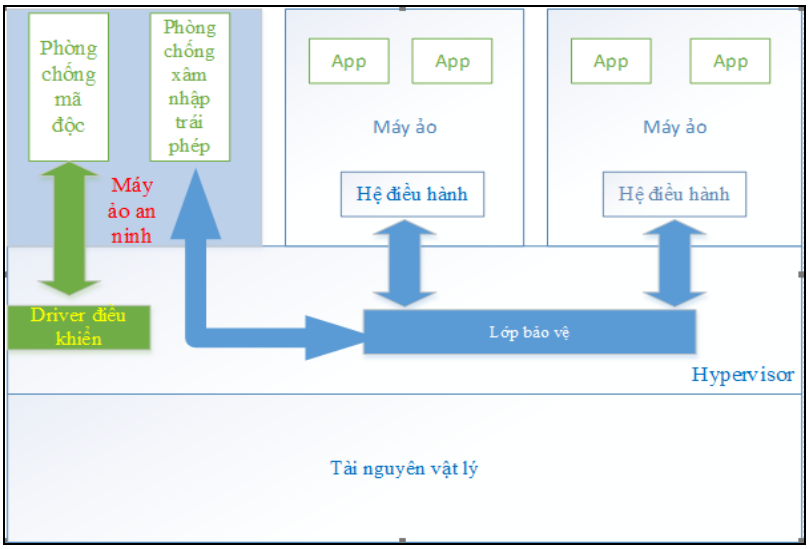
| Rủi ro | Mô tả |
|---|---|
| Tài khoản đặc quyền | Nhà cung cấp dịch vụ điện toán đám mây có quyền truy cập không giới hạn vào dữ liệu người dùng. |
| Ví trí lưu trữ dữ liệu | Khách hàng có thể không biết nơi lưu trữ dữ liệu của họ trên đám mây, có thể có nguy cơ dữ liệu bí mật được lưu trữ cùng với 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 | 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. |
| 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

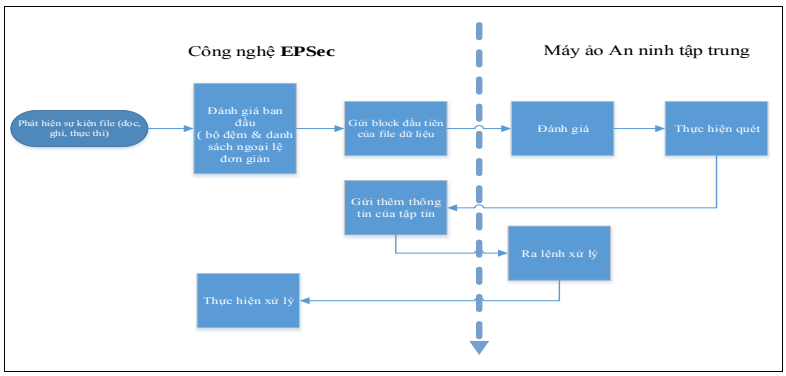
Giải pháp Agentless không cần cài đặt bất kì phần mềm bảo mật nào trên máy ảo. Giải pháp sử dụng một máy ảo an ninh tích hợp với tầng phần mềm lõi của ảo hóa và các driver điều khiển để bảo vệ máy ảo. Kiến trúc Agentless giải quyết được các nguy cơ tấn công chéo giữa các máy ảo, kiểm soát dữ liệu ra 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.




*Hình 6: 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 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 7: Phát hiện 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

### 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

### 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

1/. Thiết lập tường lửa giữa các lớp mạng ảo và các máy ảo với nhau.

2/. Triển khai hệ thống phát hiện và phòng chống xâm nhập trên mạng phát hiện và ngăn chặn các tấn công mạng

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 và sử dụng 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

#### 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 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

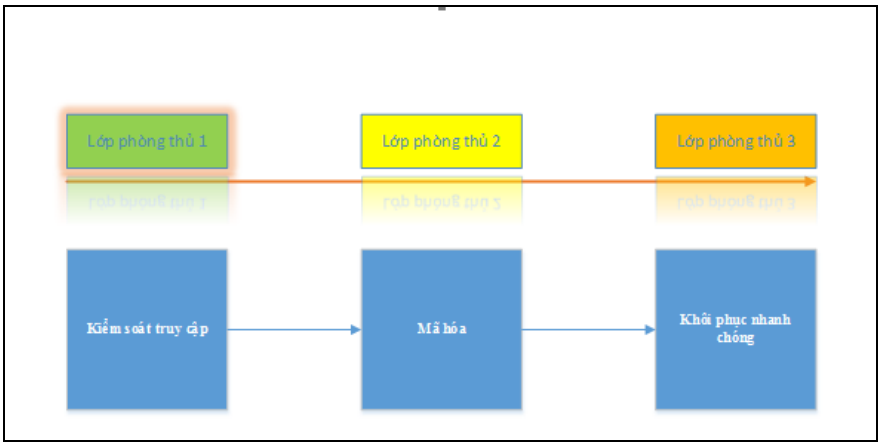
1/. Thực hiện đầy đủ sao lưu ảnh chụp trạng thái máy ảo có đầy đủ cấu hình bao gồm ổ đĩa cứng ảo để khách hàng có có thể dễ dàng khôi phục các dữ liệu và máy ảo ban đầu.
2/. Sử dụng mã hóa bảo vệ luồng dữ liệu khi sao lưu ngăn chặn tin tặc chặn bắt gói tin.
3/. Thiết lập mật khẩu bảo vệ các file sao 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




*Hình 08: Mô hình bảo vệ dữ liệu*

### 4.1.1. Lớp phòng thủ thứ nhất "Kiểm soát truy cập"

#### *4.1.1.1. Quyền tối thiểu*

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.

#### *4.1.1.2. Quản lý tài khoản*

### 4.1.2. Lớp phòng thủ thứ hai "mã hóa"

1/. Ngăn chặn và giới hạn mối đe dọa nội bộ truy cập trái phép dữ liệu Khách hàng của nhân viên nhà cung cấp điện toán đám mây

2/. Ngăn chặn và giới hạn mối đe dọa truy cập dữ liệu từ bên ngoài của hacker, đối thủ cạnh tranh

Tổ chức, doanh nghiệp lưu trữ dữ liệu cá nhân trên Điện toán đám mây cần thực hiện biện pháp như sau:

1/. Mã hóa dữ liệu khi lưu trữ trong ổ cứng của máy ảo

2/. Mã hóa dữ liệu khi lưu trữ trong các phương tiện lưu trữ/dịch vụ dù ở định dạng khối hay tầng file.

3/. Mã hóa trong bản ghi cơ sở dữ liệu.

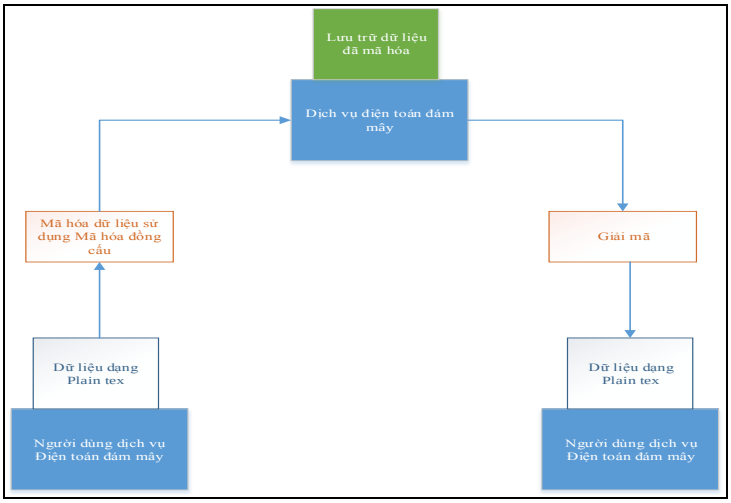
4/. Mã hóa dữ liệu khi truyền trên mạng.

#### *4.1.3.1. Khái niệm, tính chất "mã hóa đồng cấu"*

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

#### *4.1.3.2. Sử dụng mã hóa đồng cấu mã hóa dữ liệu trong điện toán đám mây*




*Hình 09: Mô hình sử dụng mã hóa đồng cấu mã hóa dữ liệu điện toán đám mây*

#### *4.1.3.3. Khái niệm mã hóa đồng cấu đầy đủ*

[9] 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.

#### *4.1.3.4. 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:

$[q_0p+2r_0, q_1p+2r_1, \ldots, q_tp+2r_t] = (x_0, x_1, \ldots, x_t)$

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: $c \pmod{p} = 2 \cdot r + b \pmod{p} = 2 \cdot r + b$

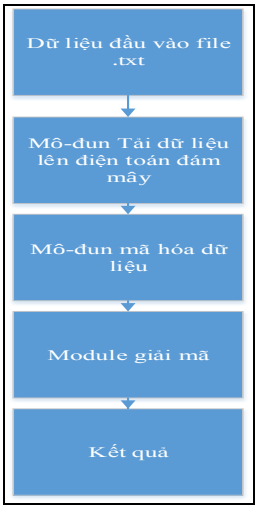
Thuật toán mã hóa đồng cấu đầy đủ gặp phải 2 vấn đề

1/. Bản mã có kích thước lớn

2/. Độ nhiễu cao mỗi lần tính toán.

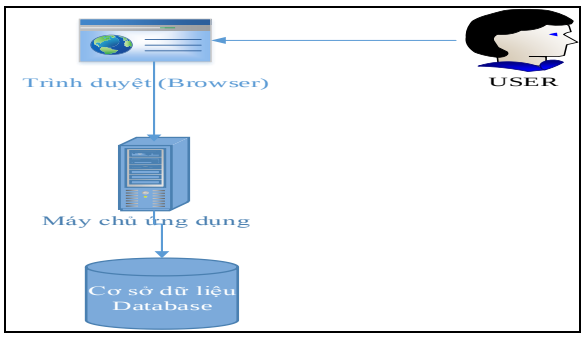
#### *4.1.3.5. Triển khai xây dựng công cụ mã hóa dữ liệu điện toán đám mây sử dụng thuật toán mã hóa đồng cấu đầy đủ*

Thiết kế chương trình




*Hình 10: Thiết kế chương trình*

Kiến trúc chương trình




*Hình 11: Kiến trúc chương trình*

#### 4.1.3. Lớp phòng thủ thức ba "khôi phục nhanh chóng"

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.

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

##### *4.1.4.1. Kiểm soát an ninh môi trường vật lý điện toán đám mây*

##### *4.1.4.2. 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.

##### *4.1.4.3. 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

##### *4.1.4.4. Phân loại và dãn 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.

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

# 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.

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

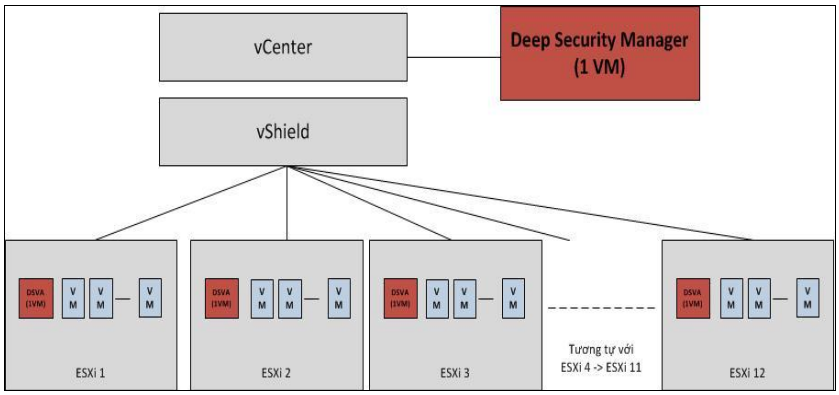
Ngăn chặn các tấn SQL injection and XSS trên ứng dụng, Che chắn lỗ hổng đã biết và chưa biết trong các trang web và các ứng dụng như Shellshock và Heartbleed
Cung cấp chi tiết, báo cáo có thể kiểm tra tài liệu đó ngăn chặn các cuộc tấn công và tình trạng tuân thủ chính sách, và các chính sách mã hóa 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.

## 4.2. TRIỂN KHAI GIẢI PHÁP

### 4.2.1. Mô hình triển khai




*Hình 13: 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.

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. Tính năng tường lửa Tính năng lọc gói tin **Deep Packet Inspection** bao gồm các thành phần IPS/IDS, web application Protection, Application control. Tính năng giám sát thay đổi tập tin quan trọng. 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.

# 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.