# HỌC VIỆN CÔNG NGHỆ BƯU CHÍNH VIỄN THÔNG


## BÀI GIẢNG MÔN

# *ĐIỆN TOÁN ĐÁM MÂY*
# *(Cloud computing)*

**Giảng viên:** ThS. Hoàng Thị Thu

**Điện thoại/E-mail:** 0326189970 thuht@ptit.edu.vn

**Bộ môn:** Mạng viễn thông – Khoa Viễn thông 1

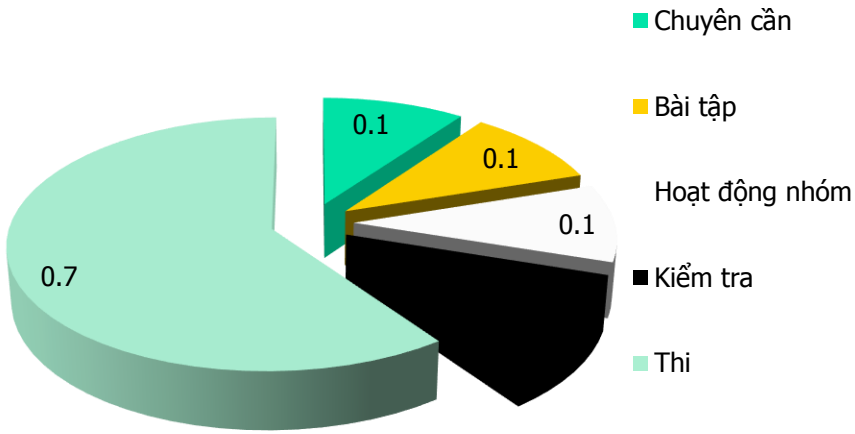
**Học kỳ/Năm biên soạn:** II/ 2022-2023

# Định hướng ban đầu

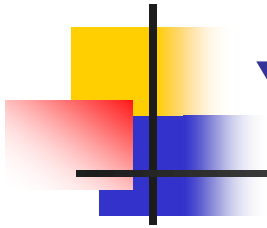
- Giới thiệu về môn học, giảng viên
- Hỏi đáp sinh viên có nền tảng gì
- Làm quen với sinh viên: Lớp trưởng, lớp phó, số lượng nam nữ
- Thông tin liên hệ: sđt, email
- Danh sách lớp với 4 cột điểm.
- Nhắc sinh viên ghi số thứ tự ở bìa vở môn học, sau này cần cho các bài kiểm tra, bài tập (khi có danh sách chính thức)

# Đánh giá môn học

| | |
|---|---|
| Chuyên cần | • 10% (Đánh giá dựa trên số giờ đi học, ý thức chuẩn bị bài và tinh thần tích cực thảo luận) |
| Bài tập, thảo luận, hoạt động nhóm | • 10% - đánh giá nội dung riêng từng cá nhân |
| Kiểm tra | • 10% (viết – 2 bài, lấy trung bình) |
| Bài thi cuối kỳ | • 70% thi viết (ôn theo đề cương và bài giảng) |




***Bài thi cuối kỳ không được sử dụng tài liệu ngoài tài liệu được phát trong phòng thi (nếu có)***



# Yêu cầu của môn học

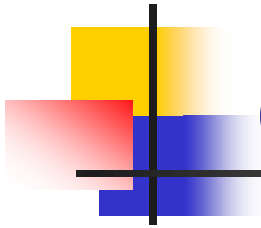
- Tinh thần đóng góp, ý kiến trong khóa học
- Giữ trật tự, không gây ảnh hưởng tới bạn xung quanh
- Đi học đầy đủ
- Nộp bài tập lớn đúng hạn

# Mục tiêu môn học

- Trang bị cho sinh viên các kiến thức nền tảng về điện toán đám mây và các giải pháp ứng dụng của điện toán đám mây trong mạng truyền thông. Nội dung chính của học phần gồm các khái niệm, các mô hình dịch vụ đám mây, các mô hình triển khai đám mây, các công nghệ nền tảng cho điện toán đám mây và an ninh trên đám mây.
- Đồng thời, môn học giúp sinh viên nghiên cứu và phát triển các ứng dụng trên nền tảng điện toán đám mây dựa trên các kiến thức nền tảng đã học.

# Nội dung môn học Internet và giao thức (45 tiết=3tc, Lớp chính quy)

- **Lý thuyết:** 24 tiết
  - **C1- Tổng quan về Điện toán đám mây**
  - **C2- Kiến trúc điện toán đám mây**
  - **C3- Truy nhập và lưu trữ dữ liệu**
  - **C4- Bảo mật trong điện toán đám mây**
  - **2 tiết kiểm tra**
  - **2 tiết ôn tập**
- **Bài tập:** 6 tiết – làm nhóm.
- **Thi cuối kỳ:** Thi viết
- **Giờ tự học:** 0 tiết



# Chương 4: Bảo mật trong ĐTĐM

## Nội dung chương 4

- 4.1 Khái quát nguy cơ và tác động tới điện toán đám mây
- 4.2 Mã hóa dữ liệu đám mây
- 4.3 Bảo mật hệ thống điều hành
- 4.4. Bảo mật cho giải pháp ảo hóa
- 4.5 Kết luận chương

## 4.1.KHÁI QUÁT NGUY CƠ VÀ TÁC ĐỘNG TỚI ĐIỆN TOÁN ĐÁM MÂY

- ĐTĐM tạo ra nhiều lợi ích cho NTD dịch vụ điện toán nhưng cũng có những lo ngại về bảo mật.
- Do sự chia sẻ lớn của cơ sở hạ tầng và tài nguyên => rủi ro bảo mật.
- Hệ thống bảo mật dựa trên đám mây cần giải quyết tất cả các nhu cầu cơ bản của một hệ thống thông tin như tính bảo mật, tính toàn vẹn, tính sẵn có của thông tin, quản lý danh tính, xác thực và ủy quyền.

## 4.1.KHÁI QUÁT NGUY CƠ VÀ TÁC ĐỘNG TỚI ĐIỆN TOÁN ĐÁM MÂY

# Nguyên lý bảo mật chung

- Việc triển khai cơ chế quản lý danh tính và kiểm soát truy cập trong doanh nghiệp hết sức cần thiết.
- Bảo mật hệ thống máy tính: bảo vệ cả hệ thống và cả dữ liệu mà nó lưu trữ.
- Cách bảo mật như một khía cạnh quan trọng của kiến trúc đám mây trải dài trên tất cả các lớp của mô hình tham chiếu.
- Bảo mật trong đám mây gồm bảo mật vật lý (cơ sở hạ tầng) đến bảo mật ứng dụng.

## 4.1.KHÁI QUÁT NGUY CƠ VÀ TÁC ĐỘNG TỚI ĐIỆN TOÁN ĐÁM MÂY

# Trách nhiệm liên quan

- Nhà cung cấp phải đảm bảo an ninh cho CSHT của chính mình cũng như dữ liệu,ứng dụng của khách hàng.
- NTD phải xác minh và đảm bảo rằng nhà cung cấp đã sử dụng tất cả các biện pháp bảo mật có thể để đảm bảo an toàn cho các dịch vụ.
- Nhà cung cấp phải thiết lập mối quan hệ tin cậy với NTD của mình. Cả hai bên có ý tưởng rõ ràng về trách nhiệm của mình đối với việc quản lý bảo mật.

## 4.1.KHÁI QUÁT NGUY CƠ VÀ TÁC ĐỘNG TỚI ĐIỆN TOÁN ĐÁM MÂY

# Thoả thuận mức dịch vụ SLA

- Thiết lập mối quan hệ tin cậy giữa nhà cung cấp dịch vụ và NTD => SLA nêu chi tiết về các khả năng ở cấp độ dịch vụ mà các nhà cung cấp hứa hẹn sẽ cung cấp và các yêu cầu/mong đợi mà NTD đã nêu.
- Tài liệu SLA nên bao gồm các vấn đề bảo mật.
- SLA giữa nhà cung cấp dịch vụ đám mây (CSP) và NTD đề cập chi tiết về khả năng bảo mật của các giải pháp và các tiêu chuẩn bảo mật cần được duy trì bởi các nhà cung cấp dịch vụ.

## 4.1.KHÁI QUÁT NGUY CƠ VÀ TÁC ĐỘNG TỚI ĐIỆN TOÁN ĐÁM MÂY

# Đe doạ, tính rủi ro

- Đe doạ là một sự kiện có thể gây hại cho hệ thống. Nó có thể làm hỏng độ tin cậy của hệ thống và làm giảm tính bảo mật, tính khả dụng/tính toàn vẹn của thông tin được lưu trữ trong hệ thống.
- Rủi ro là khả năng một mối đe dọa khai thác các lỗ hổng, gây hại cho hệ thống. Rủi ro xảy ra khi mối đe dọa và lỗ hổng hệ thống chồng chéo lên nhau, đây là viễn cảnh khi đe dọa thành hiện thực.

## 4.1.KHÁI QUÁT NGUY CƠ VÀ TÁC ĐỘNG TỚI ĐIỆN TOÁN ĐÁM MÂY

# Đe doạ, tính rủi ro

- **Nghe trộm**: Cuộc tấn công này bắt các gói dữ liệu trong quá trình truyền mạng và tìm kiếm thông tin nhạy cảm để tạo nền tảng cho một cuộc tấn công.
- **Gian lận (Fraud):** Nó được thực hiện thông qua các giao dịch ngụy biện và việc thay đổi dữ liệu một cách sai lệch để tạo ra một số lợi nhuận bất hợp pháp.
- **Trộm cắp**: ăn cắp bí mật thương mại hoặc dữ liệu để thu lợi. Nó cũng có thể là tiết lộ thông tin trái pháp luật để gây ra thiệt hại.

## 4.1.KHÁI QUÁT NGUY CƠ VÀ TÁC ĐỘNG TỚI ĐIỆN TOÁN ĐÁM MÂY

# Đe doạ, tính rủi ro

- **Phá hoại**: thực hiện thông qua nhiều cách khác nhau như phá vỡ tính toàn vẹn của dữ liệu (được gọi là phá hoại dữ liệu), trì hoãn sản xuất, tấn công từ chối dịch vụ (DoS),…
- **Tấn công bên ngoài**: Chèn mã độc hại hoặc vi rút vào ứng dụng hoặc hệ thống thuộc loại mối đe dọa này.

## 4.1.KHÁI QUÁT NGUY CƠ VÀ TÁC ĐỘNG TỚI ĐIỆN TOÁN ĐÁM MÂY

# Mối đe doạ với ĐTĐM

- **Cơ sở hạ tầng**: mối đe dọa về bảo mật cơ sở hạ tầng cấp độ ứng dụng, cấp độ máy chủ/cấp độ mạng.
- **Thông tin**: dữ liệu của người dùng
- **Kiểm soát truy cập**: xác thực và quản lý uỷ quyền thích hợp cho các ứng dụng.

## 4.1.KHÁI QUÁT NGUY CƠ VÀ TÁC ĐỘNG TỚI ĐIỆN TOÁN ĐÁM MÂY

# Bảo mật với CSHT ĐTĐM

- Kiểm soát quyền truy cập vào các tài nguyên vật lý hỗ trợ CSHT đám mây.
- Bảo mật cơ sở hạ tầng có thể được phân thành ba loại như cấp độ mạng, cấp độ máy chủ và cấp độ dịch vụ.

## 4.1.KHÁI QUÁT NGUY CƠ VÀ TÁC ĐỘNG TỚI ĐIỆN TOÁN ĐÁM MÂY

# Bảo mật với CSHT ĐTĐM

- **Cấp độ mạng**: đảm bảo tính bảo mật, tính toàn vẹn và tính sẵn sàng của dữ liệu.
- Sử dụng các kỹ thuật mã hóa và chữ ký điện tử.
- Được triển khai tại chỗ/tại cơ sở của nhà cung cấp, phụ thuộc vào tiềm năng của kiến trúc sư CSHT

## 4.1.KHÁI QUÁT NGUY CƠ VÀ TÁC ĐỘNG TỚI ĐIỆN TOÁN ĐÁM MÂY

# Bảo mật với CSHT ĐTĐM

- **Cấp máy chủ**: đảm bảo không có mối đe dọa mới nào xảy ra đối với các máy chủ dành riêng cho ĐTĐM.
- Các đám mây liên kết với nhau khả năng của hàng trăm nút điện toán.

## 4.1.KHÁI QUÁT NGUY CƠ VÀ TÁC ĐỘNG TỚI ĐIỆN TOÁN ĐÁM MÂY

# Bảo mật với CSHT ĐTĐM

**Mức ứng dụng**:

- Ở cấp độ IaaS: người dùng chủ yếu chịu trách nhiệm quản lý và bảo mật các máy chủ ảo mà họ làm việc cùng với các nhà cung cấp.
- Ở cấp độ PaaS: bảo mật nền tảng và các ứng dụng của NTD triển khai trên nền tảng PaaS.
- Ở cấp độ SaaS: nhà cung cấp có trách nhiệm quản lý bộ ứng dụng hoàn chỉnh mà họ cung cấp cho NTD.

## 4.1.KHÁI QUÁT NGUY CƠ VÀ TÁC ĐỘNG TỚI ĐIỆN TOÁN ĐÁM MÂY

# An toàn và bảo mật của hệ thống vật lí

- Cơ sở cung cấp điện liên tục (UPS).
- Các biện pháp an toàn chống cháy thích hợp để giảm thiểu thiệt hại trong trường hợp thiên tai.
- Cơ sở làm mát và thông gió thích hợp.
- Hạn chế nghiêm ngặt đối với quyền truy cập vật lý vào máy chủ. Những người không được phép không được phép tiếp cận khu vực này.
- Các biện pháp bảo vệ vật lý được liệt kê ở trên cũng cần được duy trì cho tất cả các thiết bị liên quan đến mạng (chẳng hạn như bộ định tuyến) và cáp.

# 4.2. Mã hoá dữ liệu đám mây

## Bảo mật dữ liệu

- Xác định dữ liệu yêu cầu mã hóa.
- Mạng công cộng: truyền dữ liệu qua các mạng công cộng như internet.
- Mạng riêng: truyền dữ liệu qua mạng riêng được bảo mật chẳng hạn như mạng cục bộ được thiết lập cho địa điểm văn phòng.
- Thiết bị cục bộ: truyền dữ liệu giữa các thiết bị cục bộ như máy tính, thiết bị lưu trữ dữ liệu và thiết bị ngoại vi.

# 4.2. Mã hoá dữ liệu đám mây

## Bảo mật dữ liệu

- Công nghệ bao gồm mạng, cơ sở dữ liệu, hệ điều hành, ảo hóa, lập lịch tài nguyên, quản lý giao dịch, cân bằng tải, kiểm soát luồng và quản lý bộ nhớ.
- Bảo mật dữ liệu bao gồm việc mã hóa dữ liệu cũng như đảm bảo rằng các chính sách thích hợp được thực thi để chia sẻ dữ liệu.

# 4.2. Mã hoá dữ liệu đám mây

## Bảo mật dữ liệu

- Truyền dữ liệu: là quá trình gửi dữ liệu số hoặc dữ liệu tương tự qua một phương tiện truyền thông tới một hoặc nhiều thiết bị máy tính, mạng, truyền thông hoặc điện tử.
- Bảo mật ảo hóa: các biện pháp, thủ tục và quy trình chung để đảm bảo việc bảo vệ cơ sở hạ tầng ảo hóa/môi trường ảo hóa.

# 4.2. Mã hoá dữ liệu đám mây

## Bảo mật dữ liệu

- An ninh mạng: đảm bảo an ninh cho các tài sản của tổ chức đó và tất cả lưu lượng truy cập mạng.
- Tính toàn vẹn của dữ liệu xác định dữ liệu nào trong hệ thống máy tính có thể được chia sẻ với bên thứ ba.
- Bảo mật dữ liệu: "tính toàn vẹn dữ liệu" đề cập đến tính chính xác và tính nhất quán của dữ liệu được lưu trữ trong cơ sở dữ liệu, kho dữ liệu, trung tâm dữ liệu hoặc cấu trúc khác.

# 4.2. Mã hoá dữ liệu đám mây

## Bảo mật dữ liệu

- Vị trí dữ liệu: Lưu trữ đám mây là một mô hình lưu trữ dữ liệu máy tính, trong đó dữ liệu kỹ thuật số được lưu trữ trong các nhóm logic.
- Tính sẵn có của dữ liệu: thuật ngữ được một số nhà sản xuất bộ nhớ máy tính và nhà cung cấp dịch vụ lưu trữ (SSP).

# 4.2. Mã hoá dữ liệu đám mây

## Kỹ thuật mã hoá trong đám mây

- Mã hóa đám mây là việc chuyển đổi dữ liệu của khách hàng sử dụng dịch vụ Đám mây thành văn bản mã.
- Mã hóa dựa trên thuộc tính (ABE): mã hóa khóa công khai, trong đó khóa bí mật của người dùng và bản mã phụ thuộc vào các thuộc tính.

# 4.2. Mã hoá dữ liệu đám mây

## Bảo mật với CSHT ĐTĐM

- Mã hóa đồng hình hoàn toàn (FHE): cho phép tính toán trên dữ liệu được mã hóa, đồng thời cho phép tính tổng và tích của dữ liệu được mã hóa mà không cần giải mã.
- Mã hóa có thể tìm kiếm (SE): hệ thống mật mã có chức năng tìm kiếm an toàn trên dữ liệu được mã hóa. SE dựa trên mật mã khóa bí mật (hoặc khóa đối xứng) và SE dựa trên mật mã khóa công khai.

# 4.2. Mã hoá dữ liệu đám mây

## Mã hóa dựa trên thuộc tính khóa-chính sách phi tập trung

- Các mô-đun con: thiết lập toàn cầu, thiết lập quyền hạn, cấp khóa, mã hóa và giải mã.
- Thiết lập toàn cầu: mô-đun này nhận tham số bảo mật làm tham số hệ thống đầu vào và đầu ra.
- Thiết lập quyền hạn: các tham số hệ thống có được từ thiết lập chung để tạo các khóa công khai và riêng tư cho các thuộc tính mà nó duy trì.

# 4.2. Mã hoá dữ liệu đám mây

## Mã hóa dựa trên thuộc tính khóa-chính sách phi tập trung

- Phát hành khóa: người dùng và quyền hạn về thuộc tính tương tác thông qua giao thức cung cấp khóa ẩn danh để xác định một tập hợp các thuộc tính thuộc về người dùng.
- Mã hóa: thuật toán mã hóa lấy một tập hợp các thuộc tính được duy trì bởi quyền hạn về thuộc tính và dữ liệu làm đầu vào.

# 4.2. Mã hoá dữ liệu đám mây

## Mã hóa dựa trên thuộc tính khóa-chính sách phi tập trung

- Giải mã: thuật toán giải mã lấy thông tin xác thực giải mã được cấp lại từ các quyền hạn về thuộc tính và bản mã làm đầu vào => Việc giải mã sẽ thành công nếu và chỉ khi các thuộc tính người dùng thỏa mãn cấu trúc truy cập.

# 4.2. Mã hoá dữ liệu đám mây

## Trò chơi bảo mật

- Người dùng gửi một danh sách các bộ thuộc tính và các quyền hạn về thuộc tính gồm các cơ quan có thẩm quyền cho hệ thống.
- Hệ thống tạo ra các khóa công khai và riêng tư tương ứng với các thuộc tính và quyền hạn được cung cấp bởi người dùng.
- Cung cấp các khóa công khai và riêng tư tương ứng với các quyền bị hỏng cho đối thủ chỉ các khóa công khai tương ứng với các quyền hạn còn lại cho đối thủ.

# 4.2. Mã hoá dữ liệu đám mây

## Trò chơi bảo mật

- ***Truy vấn khoá bí mật***: kẻ thù được phép thực hiện bất kỳ số lượng truy vấn khóa bí mật nào mà anh ta muốn chống lại quyền hạn.
- Yêu cầu duy nhất là đối với mỗi người dùng, phải có ít nhất một quyền thuộc tính không bị hỏng mà từ đó kẻ thù có thể nhận được không đủ số lượng khóa bí mật.

# 4.2. Mã hoá dữ liệu đám mây

## Trò chơi bảo mật

- **Thách thức:** Đối thủ gửi hai bản tin *m*0 và *m*1 đến đối thủ ở miền thuần túy.
- Kẻ thách thức chọn ngẫu nhiên một trong các bản tin và mã hóa nó và gửi bản mã cho kẻ thù.

# 4.2. Mã hoá dữ liệu đám mây

## Trò chơi bảo mật

- **Tiếp tục truy vấn khoá bí mật**: Kẻ thù được phép thực hiện nhiều truy vấn khóa bí mật hơn miễn là anh ta đáp ứng yêu cầu được đưa ra trước đó.

# 4.2. Mã hoá dữ liệu đám mây

## Trò chơi bảo mật

- **Đoán:** bây giờ đối thủ đoán xem bản tin nào đã được mã hóa bởi đối thủ.
- Kẻ thù được cho là thành công nếu anh ta đoán đúng bản tin với xác suất 1 + s, theo đó s là một hàm không đáng kể.

# 4.2. Mã hoá dữ liệu đám mây

## Trò chơi bảo mật

- **Mã hoá đồng hình hoàn toàn (FHE)**
- Hệ thống liên quan đến nhiều bên đóng ba vai trò quan trọng trong việc tính toán riêng, những người dùng thuê ngoài tính toán cho một bên từ xa (Đám mây) với dữ liệu bí mật của họ được bảo vệ khỏi sự thẩm vấn trái phép; các nút tính toán đồng hình (HC) được cung cấp bởi các dịch vụ Đám mây bằng cách sử dụng các phiên bản dựa trên CPU, GPU.

# 4.2. Mã hoá dữ liệu đám mây

## Trò chơi bảo mật

- **Mã hoá đồng hình hoàn toàn (FHE)**
- Trước tiên, người dùng xác minh cấu hình của Đám mây thông qua giám sát từ xa và thiết lập khóa bí mật được chia sẻ với các nút khởi động.
- Sau khi xử lý, người dùng cung cấp các tham số mã hóa của họ cũng như khóa bí mật và khóa công khai cho các nút khởi động thông qua kênh bí mật đã được thiết lập.

# 4.2. Mã hoá dữ liệu đám mây

## Trò chơi bảo mật

- **Mã hoá đồng hình hoàn toàn (FHE)**
- Dữ liệu của người dùng được mã hóa theo khóa bí mật đồng hình sẽ được gửi đến các nút HC để thực hiện các phép tính đồng hình.
- Nếu tính toán yêu cầu dữ liệu riêng tư từ nhiều người dùng, mỗi người dùng sẽ gửi dữ liệu được mã hóa bằng khóa riêng của họ đến các nút HC.

# 4.2. Mã hoá dữ liệu đám mây

## Trò chơi bảo mật

- **Mã hoá đồng hình hoàn toàn (FHE)**
- Khi cần khởi động chuỗi ký tự trong tính toán đồng hình, bản mã trung gian dự kiến được gửi từ các nút HC đến các nút khởi động.
- Các nút khởi động, chạy bên trong một mã hóa an toàn, trước tiên phải giải mã bản mã, sau đó mã hóa lại bằng khóa bí mật và gửi bản mã được làm mới trở lại các nút HC.

# 4.2. Mã hoá dữ liệu đám mây

## Trò chơi bảo mật

- **Mã hoá đồng hình hoàn toàn (FHE)**
- Sau khi hoàn thành toàn bộ quá trình tính toán đồng hình, bản mã được gửi từ nút HC trở lại người dùng. Người dùng giải mã bản mã để lấy kết quả tính toán.

# 4.2. Mã hoá dữ liệu đám mây

## Trò chơi bảo mật

- **Mã hoá có thể tìm kiếm**
- Mã hóa có thể tìm kiếm hoạt động bằng cách hiển thị phân đoạn thông tin của ngữ cảnh có thể được sử dụng để xác định ngữ cảnh.
- Mã hóa có thể tìm kiếm cho phép xác định nội dung được mã hóa dựa trên một số phân đoạn thông tin có sẵn về nội dung mà không để lộ nội dung đó.

# 4.3. Bảo mật cho hệ điều hành

- Một hệ điều hành cho phép nhiều ứng dụng chia sẻ tài nguyên phần cứng của một hệ thống vật lý tuân theo một bộ chính sách.
- Bảo vệ các ứng dụng chống lại các cuộc tấn công nguy hiểm.
- Dữ liệu được đưa vào hệ thống có thể chứa mã độc; đây có thể là trường hợp của một ứng dụng Java hoặc dữ liệu được trình duyệt nhập từ một trang web độc hại.

# 4.3. Bảo mật cho hệ điều hành

- Điều kiện cần (nhưng không phải điều đủ) để đạt tính bảo mật là các hệ thống con được giao nhiệm vụ thực hiện các chức năng liên quan đến bảo mật phải có khả năng chống giả mạo và không thể bị vượt qua. Một hệ điều hành nên giới hạn một ứng dụng trong một miền bảo mật duy nhất.

# 4.3. Bảo mật cho hệ điều hành

- Một giải pháp cho vấn đề đường dẫn tin cậy là phân rã một cơ chế phức tạp thành một số thành phần với các vai trò được xác định rõ ràng.
- Ví dụ, cơ chế kiểm soát truy cập cho không gian ứng dụng có thể bao gồm các thành phần thực thi và quyết định.

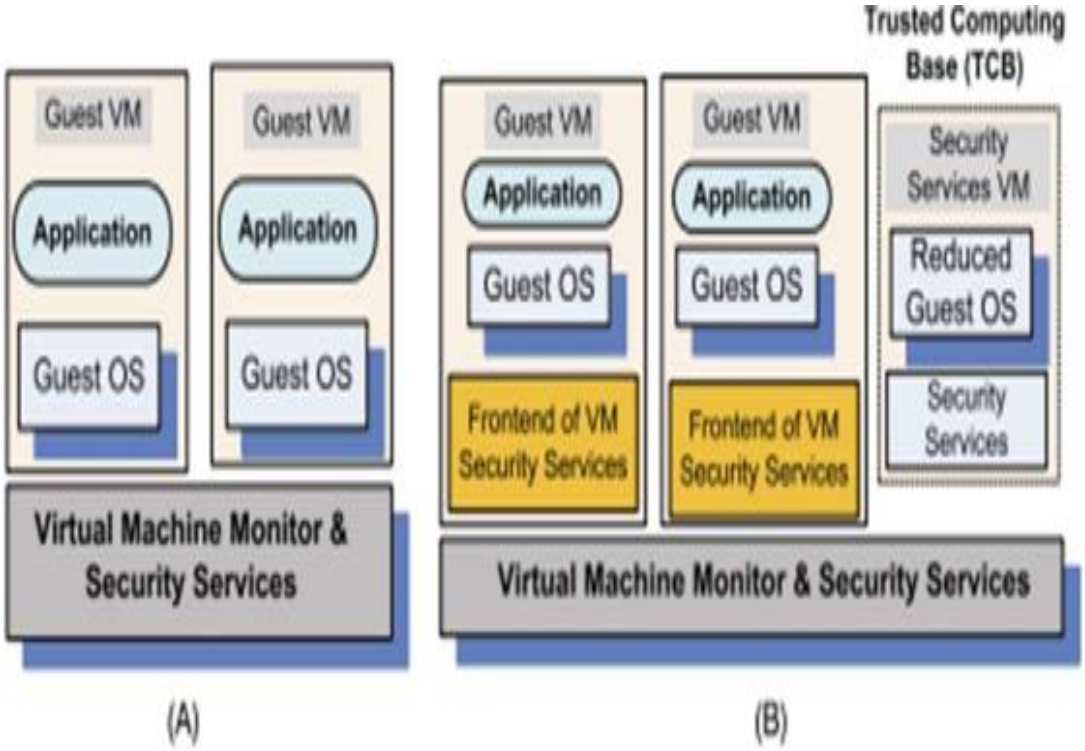
# 4.3. Bảo mật cho hệ điều hành

- Hệ điều hành chỉ cung cấp các cơ chế yếu để các ứng dụng xác thực lẫn nhau và không có đường dẫn tin cậy giữa người dùng và ứng dụng.
- Những thiếu sót này thêm vào những thách thức của cung cấp bảo mật trong môi trường máy tính phân tán.

# 4.3. Bảo mật cho hệ điều hành

## Bảo mật máy ảo

Công nghệ VM cung cấp sự cách ly chặt chẽ hơn giữa các máy ảo với nhau so với việc cách ly các quy trình trong một hệ điều hành truyền thống.




*Hình 4.1: (a) Các dịch vụ bảo mật ảo (b) Một máy ảo bảo mật chuyên dụng*

# 4.3. Bảo mật cho hệ điều hành

## Bảo mật máy ảo

- (i) Chi phí phần cứng cao hơn vì một hệ thống ảo đòi hỏi nhiều tài nguyên hơn như chu kỳ CPU, bộ nhớ, đĩa và băng thông mạng;
- (ii) Chi phí phát triển bộ hypervisor và sửa đổi hệ điều hành chủ trong trường hợp ảo hóa;
- (iii) Chi phí ảo hóa khi hypervisor liên quan đến các hoạt động đặc quyền.

# 4.3. Bảo mật cho hệ điều hành

## Bảo mật máy ảo

- Thiếu tài nguyên và từ chối dịch vụ đối với một số máy ảo.
- Các cuộc tấn công kênh bên máy ảo.
- Triển khai máy ảo giả mạo hoặc không an toàn.
- Sự hiện diện của hình ảnh máy ảo không an toàn và bị giả mạo trong kho hình ảnh máy ảo.

# 4.3. Bảo mật cho hệ điều hành

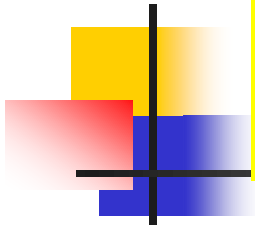
## Các mối đeo dọa bảo mật bởi hệ điều hành quản lý

- Hypervisor phải dựa vào hệ điều hành quản lý để tạo máy ảo và truyền dữ liệu vào và ra từ máy ảo khách tới các thiết bị lưu trữ và giao diện mạng.
- Hệ điều hành quản lý hỗ trợ các công cụ quản trị, di chuyển trực tiếp, trình điều khiển thiết bị và trình giả lập thiết bị.

# 4.3. Bảo mật cho hệ điều hành

## Các mối đeo dọa bảo mật bởi hệ điều hành quản lý

1. Phân bổ bộ nhớ trong không gian địa chỉ Dom0 và tải hạt nhân của hệ điều hành khách từ bộ nhớ thứ cấp.
2. Phân bổ bộ nhớ cho máy ảo mới và sử dụng ánh xạ nước ngoài để tải hạt nhân vào máy ảo mới.



# 4.3. Bảo mật cho hệ điều hành

## Các mối đeo dọa bảo mật bởi hệ điều hành quản lý

3. Thiết lập các bảng trang ban đầu cho máy ảo mới
4. Giải phóng ánh xạ ngoại trên bộ nhớ máy ảo mới, thiết lập thanh ghi CPU ảo và khởi chạy máy ảo mới

# 4.3. Bảo mật cho hệ điều hành

## Các mối đeo dọa bảo mật bởi hệ điều hành quản lý

Để triển khai một hệ thống thời gian chạy an toàn, chúng ta phải chặn và kiểm soát các siêu cuộc gọi được sử dụng để liên lạc giữa một Dom0 không thể tin cậy và một DomU mà chúng ta muốn bảo vệ.

# 4.3. Bảo mật cho hệ điều hành

## Các mối đeo dọa bảo mật bởi hệ điều hành quản lý

- Tính riêng tư và tính toàn vẹn của CPU của máy ảo.
- Tính riêng tư và tính toàn vẹn của bộ nhớ ảo VM
- Sự mới mẻ của CPU ảo và bộ nhớ của máy ảo. Giải pháp là thêm vào mã băm một số phiên bản.

# 4.3. Bảo mật cho giải pháp ảo hoá

- Ảnh hưởng tiêu cực đến hiệu suất, do chi phí bổ sung.
- Nhu cầu về các hệ thống mạnh hơn để chạy nhiều máy ảo.

# 4.3. Bảo mật cho giải pháp ảo hoá

- Hỗ trợ mô hình phân phối IaaS. Người dùng IaaS chọn một ảnh phù hợp với môi trường ứng dụng cục bộ, sau đó tải lên và chạy ứng dụng trên đám mây bằng ảnh này.
- Tăng độ tin cậy. Hệ điều hành với tất cả các ứng dụng đang chạy dưới nó có thể được sao chép và chuyển sang chế độ chờ nóng trong trường hợp hệ thống bị lỗi.

# 4.3. Bảo mật cho giải pháp ảo hoá

- Cơ chế đơn giản để thực hiện các chính sách quản lý tài nguyên. Một hệ điều hành và các ứng dụng chạy dưới nó có thể được chuyển đến một máy chủ khác để cân bằng tải của hệ thống.
- Cải thiện khả năng phát hiện xâm nhập. Trong môi trường ảo, clone có thể tìm kiếm các mẫu đã biết trong hoạt động của hệ thống và phát hiện nếu có xâm nhập.

# 4.3. Bảo mật cho giải pháp ảo hoá

- Bảo mật nhật ký và bảo vệ chống xâm nhập. Khi được triển khai ở cấp hệ điều hành, tính năng phát hiện xâm nhập có thể bị vô hiệu hóa và kẻ xâm nhập có thể sửa đổi nhật ký.
- Bảo trì và kiểm tra phần mềm hiệu quả và linh hoạt hơn.

# 4.3. Bảo mật cho giải pháp ảo hoá

## Các mối đe dọa bảo mật ảo hóa

- **Máy chủ duy nhất:** chia sẻ tài nguyên làm cho ảo hóa hiệu quả chi phí. Một bộ tài nguyên điện toán vật lý có thể thực hiện nhiều mục đích và chạy một số máy ảo.
- **Các mối đe dọa đối với trình ảo hóa:** bảo mật và tính ổn định của bất kỳ môi trường ảo hóa nào phụ thuộc rất nhiều vào khả năng của trình ảo hóa để bảo vệ chính mình khỏi các cuộc tấn công.

# 4.3. Bảo mật cho giải pháp ảo hoá

## Các mối đe dọa bảo mật ảo hóa

- **Cấu hình phức tạp:** ảo hóa thêm một lớp trừu tượng khác vì thế gia tăng sự phức tạp cho các hệ thống điện toán.
- **Phân cấp đặc quyền**: tấn công leo thang đặc quyền xảy ra khi người dung/một số ứng dụng có quyền truy cập vào nhiều tài nguyên hoặc chức năng hơn so với chúng được hưởng do một số lỗ hổng thiết kế trong hệ thống.

# 4.3. Bảo mật cho giải pháp ảo hoá

## Các mối đe dọa bảo mật ảo hóa

- **Các máy ảo không hoạt động**: các máy ảo không còn hoạt động/ở trạng thái ngủ đông, thường tự động di chuyển ra khỏi hệ thống giám sát.
- **Hợp nhất các vùng tin cậy khác nhau**: khối lượng công việc của các cấp tin cậy khác nhau từ các khu vực khác nhau hợp nhất lên cùng một hệ thống vật lý cơ bản mà không có được sự tách biệt.

# 4.3. Bảo mật cho giải pháp ảo hoá

## Khuyến nghị bảo mật ảo hoá

- **Làm cứng máy ảo:** trong ảo hóa máy chủ, người dùng có quyền truy cập gián tiếp vào tài nguyên điện toán thông qua các máy ảo.
- **Làm cứng Trình ảo hóa:** Trình ảo hóa là thành phần chủ chốt trong ảo hóa. Bất kỳ giao tiếp nào giữa các máy ảo và các tài nguyên cơ bản đều được hướng qua trình ảo hóa.

# 4.3. Bảo mật cho giải pháp ảo hoá

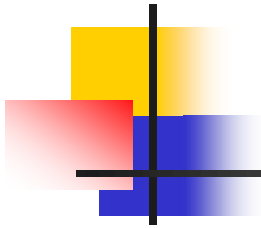
## Khuyến nghị bảo mật ảo hoá

- **Hạn chế quyền truy cập vật lý vào máy chủ:** bất kỳ lỗ hổng nào của hệ thống máy chủ đều phơi bày toàn bộ môi trường ảo với rủi ro.
- **Việc thực hiện hàm chính đơn cho mỗi VM:** mặc dù các máy ảo có khả năng xử lý nhiều tác vụ, nhưng nó làm cho môi trường ảo hóa an toàn hơn nếu các quy trình chính được tách ra giữa các VM khác nhau.

# 4.3. Bảo mật cho giải pháp ảo hoá

## Khuyến nghị bảo mật ảo hoá

- **Sử dụng truyền thông bảo mật:** thiết lập các cơ chế truyền thông có bảo mật cung cấp bảo vệ cho hệ thống điện toán.
- **Sử dụng NIC riêng biệt cho VM nhạy cảm:** các máy ảo xử lý dữ liệu nhạy cảm sẽ thu hút sự chú ý nhiều hơn từ tin tặc trên mạng.



# Kết luận chương 4

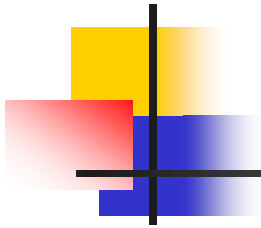
- Các khía cạnh liên quan tới vấn đề bảo mật ĐTĐM.
- Bảo vệ từ các giải pháp truy nhập, tới hệ điều hành, phần mềm và tới các ứng dụng.

# Câu hỏi ôn tập chương 4

1. Khái quát nguy cơ và tác động tới điện toán đám mây
2. Tầm quan trọng của SLA
3. Mối đe dọa đối với điện toán đám mây
4. Bảo mật với cơ sở hạ tầng điện toán đám mây
5. Bảo mật cấp độ mạng
6. Bảo mật cấp máy chủ
7. Bảo mật mức ứng dụng

# Câu hỏi ôn tập chương 4

8. Mã hóa dữ liệu đám mây
9. Kỹ thuật mã hóa trong đám mây
10. Mã hóa dựa trên thuộc tính khóa-chính sách phi tập trung
11. Bảo mật cho hệ điều hành
12. Bảo mật máy ảo
13. Các mối đeo dọa bảo mật bởi hệ điều hành quản lý
14. Bảo mật cho giải pháp ảo hóa
15. Các mối đe dọa bảo mật ảo hóa



# KẾT LUẬN

- Mô hình, kiến trúc hệ thống, giải pháp công nghệ ĐTĐM.
- Các vấn đề kỹ thuật và giải pháp thực hiện trong các mô hình điện toán đám mây.
- Các phương pháp truy nhập và lưu trữ thông tin dữ liệu
- Vấn đề bảo mật điện toán đám mây: giải pháp truy nhập, hệ điều hành, phần mềm và các ứng dụng.