HỌC VIỆN CÔNG NGHỆ BƯU CHÍNH VIỄN THÔNG
Khoa viễn thông 1

Điện toán đám mây

Nguyễn Văn Thăng
Email: thangnv@ptit.edu.vn

2025

MỤC TIÊU MÔN HỌC

- Kiến thức:
  - 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
- Kỹ năng:
  - Sinh viên có khả năng phân tích và đánh giá được lợi ích của việc triển khai các ứng dụng trên nên tảng đám mây so với kiến trúc thông thường, có khả năng lựa chọn các mô hình phù hợp với yêu cầu của từng loại đám mây, và có khả năng nghiên cứu và phát triển các ứng dụng trên nền tảng điện toán đám mây dựa trên các kiến thức nền tảng đã học
- Thái độ:
  - Tham gia đầy đủ các giờ lý thuyết, thảo luận nhóm và thực hiện các bài tập được giao. Sẵn sàng và vận dụng hiệu quả kiến thức vào bài toán thực tiễn.

TÀI LIỆU VÀ ĐÁNH GIÁ MÔN HỌC

- Tài liệu tham khảo
  - Điện toán đám mây. Bài giảng của bộ môn Mạng viễn thông, Học viện Công nghệ Bưu chính Viễn thông, 2021
  - Marinescu, Dan C. Cloud computing: theory and practice. Morgan Kaufmann, 2017
  - Comer, Douglas E. The Cloud Computing Book: The Future of Computing Explained. Chapman and Hall/CRC, 2021.
- Đánh giá
  - Chuyên cần: 10%
  - Kiểm tra: 10%
  - Bài tập và thảo luận: 10%
  - Thi kết thúc học phần: 70%

Các nội dung chính

- TỔNG QUAN VỀ ĐIỆN TOÁN ĐÁM MÂY
- KIẾN TRÚC ĐIỆN TOÁN ĐÁM MÂY
- TRUY NHẬP VÀ LƯU TRỮ DỮ LIỆU
- BẢO MẬT ĐIỆN TOÁN ĐÁM MÂY

4. BẢO MẬT ĐIỆN TOÁN ĐÁM MÂY

❑ Khái quát nguy cơ và tác động

Điện toán đám mây mang đến nhiều lợi ích, nhưng cũng tiềm ẩn nhiều rủi ro bảo mật. Bài viết này thảo luận về các vấn đề bảo mật trong điện toán đám mây, các giải pháp và trách nhiệm của nhà cung cấp và người tiêu dùng dịch vụ.

1. Vấn đề bảo mật

- Chia sẻ cơ sở hạ tầng và tài nguyên trong mô hình điện toán đám mây dẫn đến các vấn đề bảo mật mới.
- Các rủi ro bảo mật truyền thống cũng tồn tại trong môi trường điện toán đám mây.

2. Giảm thiểu rủi ro

- Hiểu biết kiến trúc đám mây và lựa chọn triển khai phù hợp.
- Bảo mật là trách nhiệm chung của nhà cung cấp và người tiêu dùng dịch vụ.

4. BẢO MẬT ĐIỆN TOÁN ĐÁM MÂY

❑ Khái quát nguy cơ và tác động

Chia sẻ cơ sở hạ tầng và lo ngại về bảo mật

- So sánh với địa điểm công cộng, tiềm ẩn rủi ro cho dữ liệu nhạy cảm.
- Việc di chuyển dữ liệu ra khỏi mạng doanh nghiệp cần được kiểm soát chặt chẽ.

Các nguyên lý bảo mật chung

- Bảo mật dữ liệu: Mã hóa dữ liệu, kiểm soát truy cập, quản lý bản quyền.
- Bảo mật ứng dụng: Xác thực, ủy quyền, kiểm soát truy cập, mã hóa ứng dụng.
- Bảo mật cơ sở hạ tầng: An ninh vật lý, kiểm soát truy cập, bảo mật mạng.
- Quản lý danh tính và truy cập: Xác thực, ủy quyền, quản lý tài khoản.
- Giám sát và tuân thủ: Giám sát hoạt động, phát hiện xâm nhập, tuân thủ quy định.

4. BẢO MẬT ĐIỆN TOÁN ĐÁM MÂY

Trách nhiệm bảo mật trong điện toán đám mây

Hai góc độ: Nhà cung cấp dịch vụ: Đảm bảo an ninh cơ sở hạ tầng, dữ liệu và ứng dụng của khách hang; Người tiêu dùng dịch vụ: Xác minh và đảm bảo nhà cung cấp sử dụng biện pháp bảo mật phù hợp.

Vai trò của nhà cung cấp

- Kinh nghiệm và chuyên môn về bảo mật.
- Thiết lập mối quan hệ tin cậy với người tiêu dùng.
- Xác định rõ ràng trách nhiệm bảo mật.

Vai trò của người tiêu dùng

- Thuê chuyên gia kỹ thuật đánh giá rủi ro bảo mật.
- Đảm bảo an toàn cho ứng dụng và dữ liệu.
- Yêu cầu điều tra để đảm bảo quá trình bảo mật liên tục.

4. BẢO MẬT ĐIỆN TOÁN ĐÁM MÂY

❑ Tầm quan trọng của SLA trong điện toán đám mây

Thỏa thuận mức dịch vụ (SLA) là Thiết lập mối quan hệ tin cậy giữa nhà cung cấp dịch vụ và người tiêu dùng. Nêu chi tiết các khả năng dịch vụ và yêu cầu/mong đợi của cả hai bên. Có giá trị pháp lý và tham khảo trong tranh chấp. Nên được xem xét bởi chuyên gia pháp lý trước khi ký kết.

SLA và bảo mật

- SLA nên bao gồm các vấn đề bảo mật một cách chi tiết.
- Xác định trách nhiệm bảo mật của cả hai bên.

Nội dung SLA về bảo mật

Khả năng bảo mật của các giải pháp đám mây.

Tiêu chuẩn bảo mật mà nhà cung cấp dịch vụ cần duy trì.

Định nghĩa vi phạm bảo mật theo quan điểm của người tiêu dùng.

4. BẢO MẬT ĐIỆN TOÁN ĐÁM MÂY

❑ Đe dọa, tính dễ bị tổn thương và rủi ro trong điện toán đám mây

Mối đe dọa phổ biến

- Nghe trộm: Bắt gói dữ liệu trong quá trình truyền mạng để tìm kiếm thông tin nhạy cảm.
- Gian lận: Thực hiện giao dịch ngụy biện và thay đổi dữ liệu trái phép để thu lợi bất hợp pháp.
- Trộm cắp: Ăn cắp bí mật thương mại hoặc dữ liệu để thu lợi hoặc tiết lộ thông tin trái phép.
- Phá hoại: Phá vỡ tính toàn vẹn dữ liệu, trì hoãn sản xuất, tấn công từ chối dịch vụ (DoS), v.v.
- Tấn công bên ngoài: Chèn mã độc hại hoặc vi rút vào ứng dụng hoặc hệ thống.

Đặc điểm bảo mật trong điện toán đám mây

- Hệ thống tiện ích công cộng với tài nguyên dùng chung.
- Cơ chế bảo mật cần được kiểm tra và tổ chức phù hợp.

4. BẢO MẬT ĐIỆN TOÁN ĐÁM MÂY

❑ Bảo mật với cơ sở hạ tầng điện toán đám mây

Bảo mật cơ sở hạ tầng điện toán đám mây

- Bảo mật cơ sở hạ tầng: Kiểm soát quyền truy cập vào các tài nguyên vật lý hỗ trợ cơ sở hạ tầng đám mây.
- Liên quan đến cả nhà cung cấp IaaS, PaaS và SaaS.

Phân loại

- Cấp độ mạng: Bảo mật mạng, tường lửa, v.v.
- Cấp độ máy chủ: Bảo mật hệ điều hành, ứng dụng, v.v.
- Cấp độ dịch vụ: Bảo mật dữ liệu, truy cập, v.v.

Thách thức

- Bản chất năng động của môi trường đám mây.
- Quản trị bảo mật liên tục.

4. BẢO MẬT ĐIỆN TOÁN ĐÁM MÂY

Mã hóa dữ liệu đám mây

- Chuyển đổi dữ liệu của khách hàng thành văn bản mã.
- Dịch vụ được cung cấp bởi nhà cung cấp dịch vụ lưu trữ đám mây.
- Nâng cao bảo mật dữ liệu trong môi trường đám mây.

Mã hóa dựa trên thuộc tính (ABE)

- Mã hóa khóa công khai.
- Khóa bí mật và bản mã phụ thuộc vào thuộc tính của người dùng.
- Chỉ giải mã được nếu tập hợp thuộc tính của khóa người dùng khớp với bản mã.

Chính sách mật mã ABE (CP-ABE)

- Bộ mật mã kiểm soát chiến lược truy cập.
- Tập trung vào việc thiết kế cấu trúc truy cập.

4. BẢO MẬT ĐIỆN TOÁN ĐÁM MÂY

❑ Mã hóa dữ liệu đám mây

Chính sách khóa ABE (KP-ABE)

- Tập thuộc tính mô tả văn bản được mã hóa.
- Khóa cá nhân liên kết với chính sách cụ thể.

Mã hóa đồng hình hoàn toàn (FHE)

- **Cho phép tính toán trên dữ liệu được mã hóa.**
- **Tính tổng và tích dữ liệu mà không cần giải mã.**

Mã hóa có thể tìm kiếm (SE)

- Tìm kiếm an toàn trên dữ liệu được mã hóa.
- Hai loại: SE khóa bí mật và SE khóa công khai.
- SE khóa đối xứng sử dụng chỉ mục từ khóa để cải thiện hiệu quả tìm kiếm.

4. BẢO MẬT ĐIỆN TOÁN ĐÁM MÂY

Bảo mật cho hệ điều hành

- Hệ điều hành cho phép nhiều ứng dụng chia sẻ tài nguyên phần cứng.
- Chức năng quan trọng: bảo vệ ứng dụng khỏi tấn công.
- Bài viết thảo luận về các vấn đề bảo mật trong hệ điều hành.

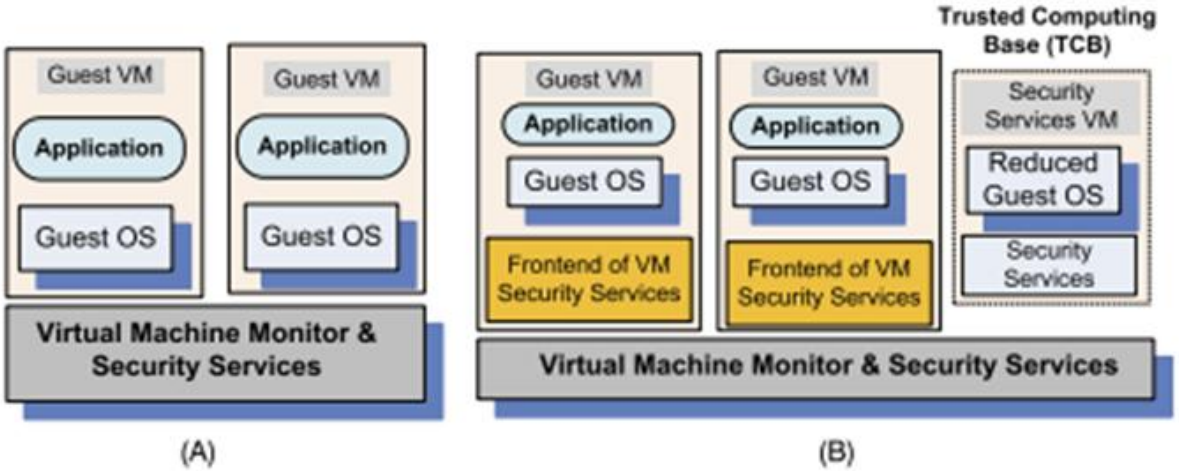
Các chính sách bảo mật

- Kiểm soát truy cập: Quy định cách hệ điều hành cấp quyền truy cập vào các đối tượng hệ thống.
- Xác thực: Xác định cơ chế xác thực người dùng.
- Mật mã: Chỉ định cơ chế bảo vệ dữ liệu.
- Hệ thống con bảo mật: Cần chống giả mạo và không thể bị vượt qua.
- Miền bảo mật: Hạn chế ứng dụng trong một miền duy nhất.

4. BẢO MẬT ĐIỆN TOÁN ĐÁM MÂY

❑ Bảo mật máy ảo

Các dịch vụ bảo mật ảo thường được cung cấp bởi hypervisor



(A) Các dịch vụ bảo mật ảo (B) Một máy ảo bảo mật chuyên dụng

4. BẢO MẬT ĐIỆN TOÁN ĐÁM MÂY

Bảo mật máy ảo

Nhóm bảo mật NIST phân loại các mối đe dọa bảo mật trong môi trường ảo hóa thành hai nhóm chính:

1. Mối đe dọa dựa trên hypervisor

Thiếu tài nguyên và từ chối dịch vụ. Nguyên nhân do giới hạn tài nguyên được cấu hình không phù hợp hoặc máy ảo giả mạo vượt qua giới hạn tài nguyên.

Tấn công kênh bên máy ảo. Nguyên nhân do thiếu sự cách ly lưu lượng giữa các máy ảo,

Giới hạn của thiết bị kiểm tra gói, hay sử dụng phiên bản VM không an toàn.

2. Mối đe dọa dựa trên máy ảo

Triển khai máy ảo giả mạo hoặc không an toàn. Nguyên nhân do cấu hình sai điều khiển truy cập quản trị VM.

Hình ảnh máy ảo không an toàn và bị giả mạo. Nguyên nhân do thiếu kiểm soát truy cập kho lưu trữ hình ảnh, hay thiếu cơ chế xác minh tính toàn vẹn hình ảnh.

4. BẢO MẬT ĐIỆN TOÁN ĐÁM MÂY

❑ Bảo mật cho giải pháp ảo hóa

Mối quan hệ phức tạp giữa ảo hóa và bảo mật

- Ảo hóa an ninh: Tăng cường bảo mật cho hệ thống bằng cách sử dụng ảo hóa.
- Bảo mật ảo hóa: Bảo vệ hệ thống ảo hóa khỏi các mối đe dọa.

Tác động của ảo hóa đối với bảo mật

- Nhiễm virus có thể kéo dài vô thời hạn: Máy ảo bị nhiễm có thể được khôi phục và lây nhiễm sang các hệ thống khác.
- Khó khăn trong việc đạt trạng thái ổn định: Môi trường ảo luôn thay đổi và khó kiểm soát.
- Lỗ hổng do khả năng khôi phục trạng thái: Kẻ tấn công có thể truy cập mật khẩu và số nonce được lưu trữ trong bộ nhớ.
- Giảm độ tin cậy: Khó khăn trong việc xác định danh tính của các hệ thống ảo.
- Nguy cơ rò rỉ dữ liệu nhạy cảm: Dữ liệu nhạy cảm có thể được lưu trữ trên nhiều máy chủ và khó kiểm soát.

4. BẢO MẬT ĐIỆN TOÁN ĐÁM MÂY

Các mối đe dọa bảo mật ảo hóa

Bên cạnh các mối đe dọa truyền thống của hệ thống điện toán truyền thống, ảo hóa còn tiềm ẩn những rủi ro bảo mật riêng biệt.

Mối đe dọa đối với máy chủ

- Chia sẻ tài nguyên khiến máy chủ ảo dễ bị tấn công.
- Vi phạm bảo mật ở cấp độ tài nguyên vật lý có thể ảnh hưởng đến nhiều hệ thống.

Mối đe dọa đối với trình ảo hóa

- Bảo mật và tính ổn định của môi trường ảo hóa phụ thuộc vào khả năng bảo vệ của trình ảo hóa.
- Vi phạm bảo mật ở cấp độ ảo hóa khiến toàn bộ môi trường dễ bị tổn thương.

Cấu hình phức tạp

- Ảo hóa thêm một lớp trừu tượng, làm tăng sự phức tạp của hệ thống.
- Cấu hình không phù hợp có thể dẫn đến các lỗ hổng bảo mật.

4. BẢO MẬT ĐIỆN TOÁN ĐÁM MÂY

Các mối đe dọa bảo mật ảo hóa

Leo thang đặc quyền

- Tin tặc có thể lợi dụng lỗ hổng để truy cập trái phép vào nhiều tài nguyên hoặc chức năng.

Máy ảo không hoạt động

- Dữ liệu nhạy cảm trong các máy ảo không hoạt động có thể bị lộ.
- Mất quyền truy cập vào các máy ảo này tạo ra rủi ro bảo mật.

Hợp nhất các vùng tin cậy khác nhau

- Hợp nhất các khối lượng công việc với mức độ tin cậy khác nhau có thể gây nguy hiểm cho các ứng dụng nhạy cảm.

4. BẢO MẬT ĐIỆN TOÁN ĐÁM MÂY

Khuyến nghị bảo mật ảo hóa

Bổ sung phần cứng máy ảo

- Cấu hình máy ảo mạnh mẽ và đúng cách.
- Giữ phần mềm máy ảo được cập nhật.

Bảo vệ trình ảo hóa

- Triển khai trình ảo hóa một cách vững chắc.
- Bảo vệ trình ảo hóa khỏi các cuộc tấn công.

Bảo vệ hệ điều hành máy chủ

- Cấu hình hệ điều hành máy chủ an toàn.
- Vá lỗi hệ điều hành máy chủ thường xuyên.

4. BẢO MẬT ĐIỆN TOÁN ĐÁM MÂY

Khuyến nghị bảo mật ảo hóa

Hạn chế quyền truy cập vật lý vào máy chủ

- Ngăn chặn truy cập trái phép vào hệ thống máy chủ.
- Sử dụng các biện pháp bảo mật vật lý.

Việc thực hiện hàm chính đơn cho mỗi VM

- Tách biệt các quy trình chính giữa các VM khác nhau.
- Hạn chế tác động của các lỗ hổng bảo mật.

Sử dụng truyền thông bảo mật

- Mã hóa dữ liệu truyền qua mạng.
- Sử dụng các kỹ thuật truyền thông an toàn.

Sử dụng NIC riêng biệt cho VM nhạy cảm

- Bảo vệ dữ liệu nhạy cảm khỏi tin tặc.
- Giảm thiểu rủi ro tấn công.

4. BẢO MẬT ĐIỆN TOÁN ĐÁM MÂY

Câu hỏi cuối chương

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
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

Thank for your attention!