HỌC VIỆN CÔNG NGHỆ BƯU CHÍNH VIỄN THÔNG
KHOA AN TOÀN THÔNG TIN

BÁO CÁO BÀI TẬP LỚN
HỌC PHẦN: AN TOÀN HỆ ĐIỀU HÀNH
MÃ HỌC PHẦN: INT1484

ĐỀ TÀI: ĐIỆN TOÁN ĐÁM MÂY

Các sinh viên thực hiện (trưởng nhóm xếp số 1):

B22DCAT113	Lê Quang Hiệp
B22DCAT115	Bùi Trung Hiếu
B22DCAT132	Phí Công Huân
B22DCAT133	Trần Ngọc Huân
B22DCAT136	Nguyễn Văn Hùng
B22DCAT137	Phạm Mạnh Hùng

Tên nhóm: 04

Tên lớp: Nhóm 01

Giảng viên hướng dẫn: PGS.TS. Hoàng Xuân Dậu

HÀ NỘI 3-2025

PHÂN CÔNG NHIỆM VỤ NHÓM THỰC HIỆN

TT	Công việc / Nhiệm vụ	SV thực hiện	Thời hạn hoàn thành
1	Nhóm trưởng: Phân công, chia việc, giám sát tiến trình, tổ chức buổi họp, kiểm tra nội dung, chính tả, hình thức báo cáo. Làm nội dung: Cơ chế hoạt động điện toán đám mây Thuyết trình	Lê Quang Hiệp	03/03/2025 11/03/2025
2	Tìm hiểu tổng quan Điện toán đám mây: Lịch sử, khái niệm, tổng hợp nội dung toàn bài Làm báo cáo bản Word	Nguyễn Văn Hùng	03/03/2025 08/03/2025
3	Làm nội dung: Kiến trúc điện toán đám mây Cơ chế hoạt động điện toán đám mây Làm báo cáo bản Word	Phí Công Huân	03/03/3025
4	Làm nội dung: Các thành phần điện toán đám mây Làm slide	Phạm Mạnh Hùng	03/03/2025 08/03/2025
5	Làm nội dung: Các thành phần điện toán đám mây Làm slide	Trần Ngọc Huân	03/03/2025 08/03/2025
6	Làm nội dung: Ưu và nhược điểm điện toán đám mây Vấn đề an ninh Tổng kết	Bùi Trung Hiếu	03/03/2025

NHÓM THỰC HIỆN TỰ ĐÁNH GIÁ

TT	SV thực hiện	Thái độ tham gia	Mức hoàn thành CV	Kỹ năng giao tiếp	Kỹ năng hợp tác	Kỹ năng lãnh đạo
1	Lê Quang Hiệp	5	5	4	5	3
2	Nguyễn Văn Hùng	5	5	4	4	
3	Phí Công Huân	5	4	4	4	
4	Phạm Mạnh Hùng	5	4	4	4	
5	Trần Ngọc Huân	5	4	4	4	
6	Bùi Trung Hiếu	5	4	4	5	

Ghi chú:

- Thái độ tham gia: Đánh giá điểm thái độ tham gia công việc chung của nhóm (từ 0: không tham gia, đến 5: chủ động, tích cực).
- Mức hoàn thành CV: Đánh giá điểm mức độ hoàn thành công việc được giao (từ 0: không hoàn thành, đến 5: hoàn thành xuất sắc).
- Kỹ năng giao tiếp: Đánh giá điểm khả năng tương tác, giao tiếp trong nhóm (từ 0: không hoặc giao tiếp rất yếu, đến 5: giao tiếp xuất sắc).
- Kỹ năng hợp tác: Đánh giá điểm khả năng hợp tác, hỗ trợ lẫn nhau, giải quyết mâu thuẫn, xung đột
- Kỹ năng lãnh đạo: Đánh giá điểm khả năng lãnh đạo (từ 0: không có khả năng lãnh đạo, đến 5: có khả năng lãnh đạo tốt, tổ chức và điều phối công việc trong nhóm hiệu quả).

MỤC LỤC

DANH MỤC CÁC HÌNH VẼ

DANH MỤC CÁC BẢNG BIỂU

DANH MỤC CÁC TỪ VIẾT TẮT

Từ viết tắt	Thuật ngữ tiếng Anh/Giải thích	Thuật ngữ tiếng Việt/Giải thích
NIST	National Institute of Standards and Technology	Viện Tiêu chuẩn và Công nghệ Quốc gia
SSD	Solid State Drive	Ổ cứng thể rắn
SAN	Storage Area Network	Mạng lưu trữ
NAS	Network Attached Storage	Lưu trữ gắn mạng
CPU	Central Processing Unit	Bộ xử lý trung tâm
RAM	Random Access Memory	Bộ nhớ truy cập ngẫu nhiên
IaaS	Infrastructure as a Service	Cơ sở hạ tầng như một dịch vụ
PaaS	Platform as a Service	Nền tảng như một dịch vụ
SaaS	Software as a Service	Phần mềm như một dịch vụ
API	Application Programming Interface	Giao diện lập trình ứng dụng
BLP	Bit-level Parallelism	Song song mức bit
ILP	Instruction-level Parallelism	Song song cấp độ lệnh
DLP	Data-level Parallelism	Song song cấp độ dữ liệu
TLP	Task-level Parallelism	Song song cấp độ tác vụ
SIMD	Single Instruction Multiple Data	Một lệnh - Nhiều dữ liệu
HTTP	Hypertext Transfer Protocol	Giao thức truyền tải siêu văn bản
HTTPS	Hypertext Transfer Protocol Secure	Giao thức truyền tải siêu văn bản bảo mật
FTP	File Transfer Protocol	Giao thức truyền tệp tin
CDN	Content Delivery Network	Mạng phân phối nội dung
TLS/SSL	Transport Layer Security / Secure Sockets Layer	Bảo mật lớp truyền tải / Lớp cổng bảo mật
VPN	Virtual Private Network	Mạng riêng ảo
MFA	Multi-Factor Authentication	Xác thực đa yếu tố
2FA	Two-Factor Authentication	Xác thực hai yếu tố
MITM	Man-in-the-Middle Attack	Tấn công người đứng giữa
DDoS	Distributed Denial of Service	Tấn công từ chối dịch vụ phân tán
SLA	Service Level Agreement	Thỏa thuận mức dịch vụ

CSP	Cloud Service Provider	Nhà cung cấp dịch vụ đám mây
IDS/IPS	Intrusion Detection System / Intrusion Prevention System	Hệ thống phát hiện xâm nhập / Hệ thống ngăn chặn xâm nhập
XSS	Cross-Site Scripting	Tấn công kịch bản chéo trang
WAF	Web Application Firewall	Tường lửa ứng dụng web
Host OS	Host Operating System	Hệ điều hành máy chủ
PKI	Public Key Infrastructure	Cơ sở hạ tầng khóa công khai
IAM	Identity and Access Management	Quản lý danh tính và truy cập
SSO	Single Sign-On	Đăng nhập một lần

MỞ ĐẦU

Với sự phát triển không ngừng của công nghệ thông tin và ứng dụng của nó trong cuộc sống ngày nay, điện toán đám mây đã trở thành một phần quan trọng của xã hội con người. Bài tập lớn này nhằm mục đích nghiên cứu sâu hơn về các khái niệm, kiến trúc, cơ chế hoạt động và các vấn đề an toàn bảo mật của điện toán đám mây trong môi trường thực tế.

Bài tập lớn này sẽ giúp bạn có cái nhìn tổng quan và dễ hiểu hơn về lĩnh vực ngày một đang phát triển này.

Báo cáo bài tập lớn gồm 4 chương với nội dung chính như sau:

- Chương 1 nghiên cứu tổng quan về điện toán đám mây bao gồm khái quát về lịch sử, khái niệm, đặc điểm, các thành phần, ưu nhược điểm điện toán đám mây.

- Chương 2 thực hiện việc phân tích nguyên tắc hoạt động, đặc điểm, ưu nhược điểm các loại kiến trúc điện toán đám mây bao gồm kiến trúc song song, kiến trúc phân tán, kiến trúc tương tác điện toán đám mây.

- Chương 3 tìm hiểu cơ chế hoạt động điện toán đám mây, cụ thể là lưu trữ, truy xuất và quản lý dữ liệu, sử dụng tài nguyên, ảo hóa và quản lý tự động cùng với khả năng truy cập.

- Chương 4 cuối cùng là các vấn đề an ninh và bảo mật điện toán đám mây trong đó có khái quát nguy cơ, ảnh hưởng của các mối đe dọa bảo mật, đồng thời biết về thỏa thuận mức dịch vụ giữa người dùng và nhà cung cấp, xác định trách nhiệm bảo mật trong mô hình điện toán đám mây.

CHƯƠNG 1. TỔNG QUAN VỀ ĐIỆN TOÁN ĐÁM MÂY

1.1 Lịch sử ra đời của điện toán đám mây

Khái niệm điện toán đám mây đã trải qua một quá trình phát triển lâu dài từ những năm 1950 khi các tổ chức lớn sử dụng máy chủ tính toàn quy mô lớn (large-scale mainframe computer). Do chi phí cao của phần cứng, xuất hiện nhu cầu phát triển công nghệ cho phép 'một máy tính có thể được sử dụng bởi hai hoặc nhiều người cùng một lúc", từ đó khai sinh ra tiền thân của điện toán đám mây, những máy tính cổ xưa, khổng lồ sử dụng các cuộn băng từ để làm bộ nhớ.

Năm 1969, JCR Licklider đã giúp phát triển ARPANET (Mạng lưới Cơ quan Dự án Nghiên cứu Tiên tiến), một phiên bản "rất" thô sơ của Internet. JCR, hay "Lick", vừa là nhà tâm lý học vừa là nhà khoa học máy tính, và đã thúc đẩy một tầm nhìn được gọi là "Mạng máy tính liên thiên hà", trong đó mọi người trên hành tinh sẽ được kết nối với nhau thông qua máy tính và có thể truy cập thông tin từ bất kỳ đâu. Mạng máy tính liên thiên hà, hay còn gọi là internet, là cần thiết để truy cập vào đám mây.

Những năm 1990, các công ty viễn thông từ chỗ cung ứng kênh truyền dữ liệu điểm tới điểm (point-to-point data circuits) riêng biệt đã bắt đầu cung ứng các dịch vụ mạng riêng ảo với giá thấp. Thay đổi này tạo tiền đề để các công ty viễn thông sử dụng hạ tầng băng thông mạng hiệu quả hơn. Điện toán đám mây mở rộng khái niệm chia sẻ băng thông mạng này qua việc cho phép chia sẻ cả tài nguyên máy chủ vật lý bằng việc cung cấp các máy chủ ảo.

Sự phát triển tiếp theo là Amazon Web Services trong năm 2002, trong đó cung cấp các dịch vụ dựa trên đám mây bao gồm lưu trữ, tính toán và ngay cả trí tuệ nhân tạo thông qua Amazon Mechanical Turk.

Năm 2006, Amazon ra mắt điện toán đám mây Elastic Compute của nó (EC2) là một dịch vụ web thương mại cho phép các công ty nhỏ, cá nhân thuê máy tính mà trên đó để chạy các ứng dụng máy tính của mình. Đây là dịch vụ cơ sở hạ tầng điện toán đám mây có thể truy cập rộng rãi đầu tiên.

Một cột mốc lớn khác năm 2009, với Web 2.0 là bước tiến triển lớn, Google và các công ty khác bắt đầu cung cấp các ứng dụng doanh nghiệp dựa trên trình duyệt. Tính tới thời điểm hiện tại, có rất nhiều sản phẩm điện toán đám mây được đưa ra như Google App Engine, Microsoft Azure, Nimbus,...

1.2 Khái niệm về điện toán đám mây

Theo định nghĩa chính thức của NIST, "Điện toán đám mây là mô hình cho phép truy cập mạng phổ biến, thuận tiện, theo yêu cầu vào các nhóm tài nguyên tính toán chia sẻ được cấu hình (VD: mạng, máy chủ, lưu trữ, ứng dụng và dịch vụ) mà nó dễ dàng được cung cấp và được phát hành với nỗ lực quản lý tối thiểu hoặc tương tác tối thiểu giữa các nhà cung cấp dịch vụ."

Các dịch vụ phổ biến điển hình của điện toán đám mây như Google Drive, Dropbox, OneDrive, iCloud, ... Người dùng chỉ cần đăng ký tài khoản và sử dụng dịch vụ miễn phí

và trả phí theo nhu cầu của bản thân. Người dùng có thể lưu trữ tài liệu của họ lên tài khoản của mình và truy cập sử dụng bất cứ lúc nào, bất kể vị trí miến là có kết nối mạng.

1.3 Đặc điểm của điện toán đám mây

Điện toán đám mây có 5 đặc trưng cơ bản để phân biệt với các hình thức máy chủ khác trước đây:

- Tự phục vụ nhu cầu (On-demand self-service): Cung cấp cho người dùng có thể chủ động sử dụng tài nguyên số bao gồm mạng, server, lưu trữ, ứng dụng, dịch vụ,... mà không cần phụ thuộc vào nhà cung cấp hosting.
- Truy cập mọi lúc mọi nơi (Broad network access): Có thể truy cập tài khoản điện toán đám mây và sử dụng ở bất cứ nơi đâu có mạng.
- Hồ chứa tài nguyên (Resource pooling): Các nhà cung cấp dịch vụ điện toán đám mây sẽ có các trung tâm dữ liệu với cơ sở hạ tầng hiện đại, đáp ứng nhu cầu đa dạng của người dùng.
- Co dãn nhanh chóng (Rapid elasticity or expansion): Cho phép người dùng chủ động nâng cấp hoặc giảm lượng tài nguyên cần sử dụng theo nhu cầu.
- Đo lường dịch vụ (Measured service): Dịch vụ cloud ghi và báo cáo lưu lượng sử dụng của khách hàng. Khách hàng có thể biết chính xác lưu lượng tài nguyên mình đã sử dụng.

1.4 Các thành phần của điện toán đám mây

1.4.1 Phần cơ sở

Phần cơ sở trong kiến trúc điện toán đám mây là nền tảng vật lý và công nghệ, bao gồm các tài nguyên phần cứng và phần mềm quản lý, tạo nên môi trường đám mây. Đây là lớp cơ bản nhất, cung cấp các dịch vụ và tài nguyên cần thiết để các lớp khác hoạt động hiệu quả.

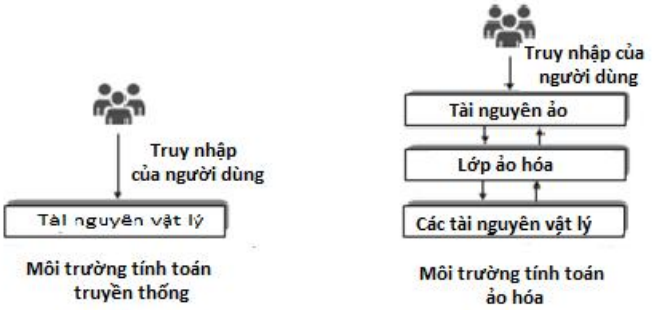
1.4.1.1 Phần cứng trung tâm dữ liệu

- Phần cứng trung tâm là nền tảng của bất kỳ đám mây nào, là nơi chạy các máy chủ, lưu trữ và nối mạng.
- Máy chủ (Servers): Các hệ thống máy tính mạnh mẽ, xử lý và lưu trữ dữ liệu, chạy các ứng dụng và dịch vụ đám mây. Trong môi trường đám mây, máy chủ thường được ảo hóa để tạo ra nhiều máy ảo
- Thiết bị lưu trữ (Storage Devices): Hệ thống lưu trữ dữ liệu như ổ cứng, SSD, SAN, NAS, hoặc hệ thống lưu trữ phân tán đảm bảo dữ liệu được lưu trữ an toàn và truy cập nhanh chóng. Nó được sử dụng để lưu trữ dữ liệu, bao gồm bộ nhớ chính và bộ nhớ dự phòng.
- Thiết bị mạng (Networking Equipment): Thiết bị mạng có trách nhiệm kết nối các máy chủ và cung cấp kết nối mạng an toàn và đáng tin cậy. Hệ thống mạng bao gồm bộ định tuyến, switch, firewall, và các giao thức kết nối.

- Hệ thống an ninh: Để bảo vệ trung tâm dữ liệu khỏi sự truy cập trái phép, các hệ thống an ninh như tường lửa và hệ thống phát hiện xâm nhập được sử dụng.

1.4.1.2 Ảo hóa

Ảo hóa đề cập đến việc thể hiện các tài nguyên điện toán vật lý ở dạng mô phỏng thông qua phần mềm. Lớp phần mềm đặc biệt này (được cài đặt trên các máy vật lý) được gọi là lớp ảo hóa. Lớp này biến đổi các tài nguyên điện toán vật lý thành dạng ảo mà người dùng sử dụng để đáp ứng nhu cầu tính toán của họ. Hình 1 đại diện cho khái niệm cơ bản về ảo hóa ở dạng đơn giản hóa.



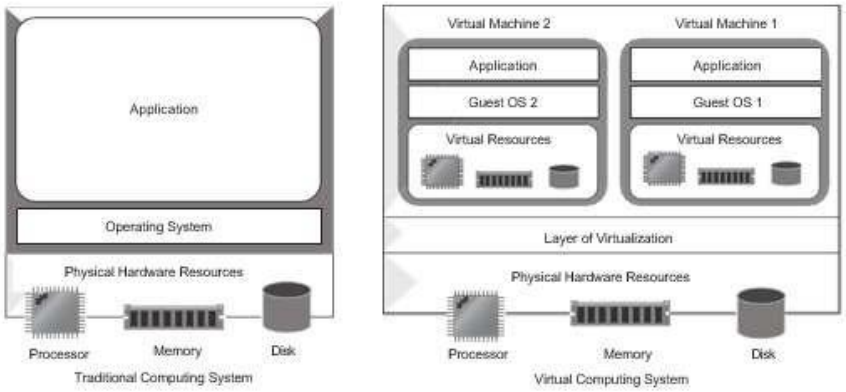
Hình 1 Tương tác trong môi trường điện toán truyền thống và ảo hóa

Ảo hóa cung cấp một mức độ trừu tượng hóa logic giải phóng phần mềm do người dùng cài đặt (bắt đầu từ hệ điều hành và các hệ thống khác cũng như phần mềm ứng dụng) khỏi một bộ phần cứng cụ thể. Thay vào đó, người dùng cài đặt mọi thứ trên môi trường hoạt động logic (thay vì vật lý) đã tạo ra thông qua ảo hóa.

Trừu tượng là quá trình che giấu các đặc điểm phức tạp và không thiết yếu của một hệ thống. Thông qua trừu tượng, một hệ thống có thể được trình bày theo cách đơn giản cho một số sử dụng cụ thể sau khi bỏ qua các chi tiết không cần thiết với người dùng. Trong điện toán, sự trừu tượng được thực hiện thông qua các lớp phần mềm. Lớp hệ điều hành có thể được coi là một lớp trừu tượng.

Lớp ảo hóa là một tập hợp các chương trình điều khiển tạo ra môi trường cho các máy ảo chạy trên. Lớp này cung cấp quyền truy cập vào các tài nguyên hệ thống cho các máy ảo. Nó cũng kiểm soát và giám sát việc thực hiện các máy ảo trên nó. Lớp phần mềm này được gọi là Giám sát viên ảo hoặc máy ảo (VMM).

Lớp ảo hóa cũng tạo điều kiện cho sự tồn tại của nhiều VM, chúng không bị ràng buộc chia sẻ kernel hệ điều hành. Vì lý do này, có thể chạy các hệ điều hành khác nhau trong các máy ảo đó như được tạo ra trên một trình ảo hóa. Lớp ảo hóa cung cấp một bảng điều khiển hệ thống quản trị thông qua đó môi trường hệ thống ảo (như số lượng thành phần ảo hoặc dung lượng của các thành phần) có thể được quản lý.



Hình 2 Hệ thống điện toán thông thường và ảo hóa

1.4.1.3 Phần mềm quản lý hạ tầng

- Phần mềm quản lý tài nguyên: Giám sát, phân bổ tài nguyên như CPU, RAM, lưu trữ, đảm bảo hiệu suất và tối ưu hóa sử dụng tài nguyên.
- Phần mềm tự động hóa: Tự động triển khai và quản lý tài nguyên, giám sát và bảo trì hệ thống.
- Phần mềm bảo mật: Đảm bảo an toàn cho dữ liệu và ứng dụng trên đám mây thông qua việc mã hóa, xác thực và phát hiện mối đe dọa.

1.4.2 Phần nền tảng

Phần này cung cấp cơ sở hạ tầng cho ứng dụng, nó cung cấp sự truy cập đến các dịch vụ và hệ điều hành liên quan. Nó sử dụng các công cụ và ngôn ngữ lập trình do nhà cung cấp hỗ trợ, tạo ra mã code để lập trình web, lập trình di động cho người dùng sử dụng.

1.4.2.1 Hệ điều hành đám mây (Cloud Operating Systems)

Hệ điều hành đám mây là một loại hệ điều hành được thiết kế để hoạt động trong môi trường điện toán đám mây hoặc ảo hóa. Hệ điều hành quản lý hiệu quả quy trình vận hành cần thiết để quản lý cơ sở hạ tầng ảo.

VD: Microsoft Windows Azure và Google Chrome OS.

(a) Môi trường phát triển và triển khai (Development and Deployment Environments)

- Công cụ và dịch vụ hỗ trợ việc viết mã, kiểm thử và triển khai ứng dụng.

Ví dụ: Docker (containerization), Kubernetes (orchestration).

(b) Cơ sở dữ liệu (Database)

- Hệ thống cơ sở dữ liệu được vận hành trên nền tảng điện toán đám mây.
- Dịch vụ quản lý và lưu trữ dữ liệu có cấu trúc và phi cấu trúc

VD: MySQL, PostgreSQL, MongoDB.

(c) APIs

- Cung cấp các phương thức để ứng dụng tương tác với các ứng dụng khác.

VD: RESTful APIs, GraphQL,...

(d) Phần mềm trung gian (Middleware)

- Phần mềm trung gian là phần mềm mà các ứng dụng khác nhau sử dụng nó để giao tiếp với nhau. Do phần mềm trung gian cung cấp chức năng kết nối các ứng dụng. Ngoài ra phần mềm trung gian hỗ trợ giao tiếp và quản lý dữ liệu giữa các ứng dụng.

Ví dụ: Message brokers như RabbitMQ, Apache Kafka.

1.4.3 Phần người dùng

1.4.3.1 Giao diện người dùng (User Interface)

Giao diện người dùng trong đám mây chính là công cụ giúp người dùng truy cập, sắp xếp và quản lý dữ liệu của mình trên đám mây, có thể qua giao diện đồ họa hoặc dòng lệnh.

- Trình duyệt web: Công cụ phổ biến nhất để truy cập các dịch vụ đám mây, như Chrome, Firefox, Safari.
- Ứng dụng khách (Client Applications): Phần mềm được cài đặt trên thiết bị người dùng để truy cập dịch vụ đám mây, như ứng dụng lưu trữ đám mây (Google Drive, Dropbox) hoặc ứng dụng email (Outlook, Thunderbird).

1.4.3.2 Thiết bị người dùng (User Devices)

Máy tính cá nhân (PCs), laptop, thiết bị di động giúp người dùng truy cập dịch vụ mọi lúc, mọi nơi.

1.4.3.3 Cơ sở hạ tầng máy khách (Client Infrastructure)

Cơ sở hạ tầng máy khách chứa các ứng dụng và giao diện người dùng cần thiết để truy cập vào đám mây.

Đảm bảo thiết bị có đủ khả năng xử lý và tương thích với dịch vụ đám mây đồng thời có kết nối internet ổn định để truy cập dịch vụ.

1.5 Phân loại điện toán đám mây

1.5.1 Phân loại theo mô hình cung cấp dịch vụ

- Infrastructure as a Service - IaaS (Cơ sở hạ tầng dưới dạng dịch vụ)

IaaS - Infrastructure as a service là mức độ cơ bản nhất của một mô hình điện toán đám mây. Đây là mô hình kinh doanh phân phối cơ sở hạ tầng công nghệ thông tin như điện toán, lưu trữ và tài nguyên mạng trên cơ sở thanh toán theo mức sử dụng qua Internet. Khi sử dụng dịch vụ này, người dùng đã có một máy chủ ảo trên không gian đám mây để làm việc.

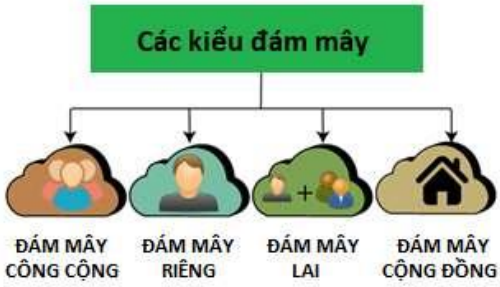
- Platform as a Service - PaaS (Nền tảng dưới dạng dịch vụ)

PaaS là mô hình điện toán đám mây trong đó nhà cung cấp bên thứ ba cung cấp các công cụ phần cứng và phần mềm từ đó người dùng có thể tập trung vào công tác triển khai cũng như quản lý các ứng dụng của mình.

- Software as a Service - SaaS (Phần mềm dưới dạng dịch vụ)

SaaS là dạng điện toán đám mây phổ biến nhất được định nghĩa là mô hình phân phối dịch vụ ứng dụng phần mềm. SaaS cung cấp sản phẩm hoàn chỉnh được nhà cung cấp dịch vụ vận hành và quản lý.

1.5.2 Phân loại theo phương pháp triển khai



Hình 3 Các kiểu đám mây

- Public Cloud: cơ sở hạ tầng được cung cấp cho công chúng hoặc nhóm công nghiệp lớn và thuộc sở hữu của một tổ chức bán dịch vụ đám mây.
- Private Cloud: cơ sở hạ tầng chỉ được vận hành cho một tổ chức.
- Hybrid Cloud: cơ sở hạ tầng là một thành phần của hai hoặc nhiều đám mây (công cộng và riêng tư) vẫn là các thực thể duy nhất nhưng được liên kết với nhau bằng công nghệ tiêu chuẩn hóa hoặc độc quyền cho phép dữ liệu và ứng dụng có khả năng chuyển dịch.
- Community Cloud: cơ sở hạ tầng được chia sẻ bởi một số tổ chức và hỗ trợ một cộng đồng cụ thể có chung mối quan tâm.

1.6 Ưu nhược điểm của điện toán đám mây

1.6.1 Ưu điểm

- **Cung cấp tài nguyên tính toán động:** Người dùng được đáp ứng nhanh chóng các nhu cầu như khởi tạo, nâng cấp, mua mới các phần mềm, ứng dụng,... Bởi vì, nhà cung cấp có khả năng huy động các nguồn tài nguyên nhàn rỗi trên Internet thời điểm đó để cung cấp cho khách hàng.
- **Tiết kiệm chi phí đầu tư hạ tầng và quản trị vận hành:** Điện toán đám mây giúp tiết kiệm chi phí vốn đáng kể vì không cần bất kỳ khoản đầu tư phần cứng vật lý nào, hay chi phí đào tạo để bảo trì phần cứng. Việc mua và quản lý thiết bị được thực hiện bởi nhà cung cấp dịch vụ đám mây. Khách hàng sử dụng dịch vụ điện toán đám mây chỉ việc trả phí cho nhu cầu của sử dụng của mình.
- **Giảm độ phức tạp trong cơ cấu của doanh nghiệp:** Doanh nghiệp có thể đưa các tất cả các quy trình làm việc của công ty lên hệ thống ĐTĐM và chia sẻ cho các nhân sự công ty để thực hiện theo, giúp nâng cao hiệu suất công việc.
- **Nhanh chóng, tiện lợi:** Khách hàng sẽ là người dùng cuối, họ chỉ cần tập trung vào công việc vì các vấn đề về kỹ thuật đã có nhà cung cấp chịu trách nhiệm.

- **An toàn và liên tục:** Những đơn vị cung cấp dịch vụ ĐTĐM sẽ có những trung tâm dữ liệu và đội ngũ kỹ thuật giàu kinh nghiệm luôn duy trì dịch vụ liên tục, ổn định và an toàn.
- **Loại bỏ được yếu tố vật lý và địa lý:** Người dùng có thể dễ dàng truy cập tài nguyên dữ liệu qua mạng Internet dễ dàng bằng thiết bị có kết nối Internet ở bất kỳ đâu mà không cần dùng các loại máy chủ riêng biệt.
- **Khả năng mở rộng và thu hẹp nhanh chóng:** Người dùng có thể mở rộng hoặc thu hẹp quy mô cơ sở dữ liệu, tài nguyên và nhu cầu sử dụng mà không bị hạn chế bởi các yếu tố như cấu hình máy chủ hoặc tài nguyên internet không đáp ứng.
- **Lợi thế chiến lược:** Điện toán đám mây cung cấp một lợi thế cạnh tranh so với đối thủ cạnh tranh của bạn. Đây là một trong những ưu điểm tốt nhất của dịch vụ Đám mây giúp bạn truy cập các ứng dụng mới nhất bất kỳ lúc nào mà không cần tốn thời gian và tiền bạc cho việc cài đặt.
- **Tốc độ cao:** Điện toán đám mây cho phép bạn nhận được các tài nguyên cần thiết cho hệ thống của mình trong vòng ít phút hơn.
- **Sao lưu và khôi phục dữ liệu:** Khi dữ liệu được lưu trữ trên Đám mây, việc sao lưu và phục hồi dữ liệu sẽ dễ dàng hơn, nếu không, đây sẽ là quá trình tốn nhiều thời gian nếu thực hiện tại cơ sở.
- **Độ tin cậy:** Độ tin cậy là một trong những lợi ích lớn nhất của đám mây lưu trữ. Bạn luôn có thể được cập nhật ngay lập tức về những thay đổi.

1.6.2 Nhược điểm

Bên cạnh những ưu điểm vượt trội thì điện toán đám mây cũng có những nhược điểm như sau:

- **Hiệu suất có thể thay đổi:** Khi bạn làm việc trong môi trường đám mây, ứng dụng của bạn đang chạy trên máy chủ, đồng thời cung cấp tài nguyên cho các doanh nghiệp khác. Bất kỳ hành vi tham lam hoặc Tấn công DDOS trên đối tượng thuê của bạn có thể ảnh hưởng đến hiệu suất của tài nguyên được chia sẻ của bạn.
- **Vấn đề kỹ thuật:** Công nghệ đám mây luôn dễ bị ngừng hoạt động và các vấn đề kỹ thuật khác. Thậm chí, các công ty cung cấp dịch vụ đám mây tốt nhất cũng có thể gặp phải loại rắc rối này mặc dù vẫn duy trì các tiêu chuẩn bảo trì cao.
- **Phụ thuộc vào mạng Internet:** ĐTĐM sử dụng Internet làm cầu nối giữa nhà cung cấp với người dùng, giữa các người dùng với nhau. Khi Internet gặp trục trặc, nó có thể không truy cập và sử dụng được.
- **Vấn đề bảo mật và quyền riêng tư:** Nếu như trước đây các toán bộ các thông tin được lưu giữ trong các ổ cứng thì người dùng có thể chủ động bảo vệ. Còn đối với điện toán đám mây, các dữ liệu được đưa lên không gian của nhà cung cấp. Điều này vẫn tiềm ẩn nguy cơ bị đánh cắp thông tin nếu như hệ thống bảo mật của nhà cung cấp dịch vụ kém.

- **Băng thông thấp hơn:** Nhiều nhà cung cấp dịch vụ lưu trữ đám mây giới hạn việc sử dụng băng thông của người dùng. Vì vậy, trong trường hợp tổ chức của bạn vượt quá mức cho phép nhất định, các khoản phí bổ sung có thể tốn kém đáng kể
- **Thiếu sự hỗ trợ:** Các công ty Điện toán đám mây không cung cấp hỗ trợ thích hợp cho khách hàng. Hơn nữa, họ muốn người dùng của mình phụ thuộc vào Câu hỏi thường gặp hoặc trợ giúp trực tuyến, đây có thể là một công việc tẻ nhạt đối với những người không rành về kỹ thuật.

Bất chấp tất cả những ưu điểm và nhược điểm của Điện toán đám mây, chúng ta không thể phủ nhận thực tế rằng Điện toán đám mây là phần phát triển nhanh nhất của điện toán dựa trên mạng. Hiện nay nhiều nhà cung cấp dịch vụ điện toán đám mây uy tín như VNPT Cloud đã có phương án khắc phục hiệu quả cho các nhược điểm trên.

Ví dụ: VNPT có nhiều trung tâm dữ liệu trên khắp cả nước nên có thể đảm bảo tốt về đường truyền và kết nối ổn định cho người dùng. Dịch vụ điện toán đám mây của VNPT Cloud được thiết kế với nhiều lớp bảo mật từ lớp vật lý tới lớp ảo. Người dùng có thể hoàn toàn yên tâm khi sử dụng dịch vụ điện toán đám mây ảo do VNPT cung cấp.

1.7 Kết chương

Chương này cung cấp một cái nhìn tổng quan về điện toán đám mây, bao gồm lịch sử phát triển, khái niệm, đặc điểm, và các thành phần của hệ thống điện toán đám mây. Ngoài ra, chương cũng phân loại các dịch vụ điện toán đám mây dựa trên mô hình cung cấp dịch vụ và phương pháp triển khai, cùng với những ưu nhược điểm khi áp dụng công nghệ này.

CHƯƠNG 2. KIẾN TRÚC ĐIỆN TOÁN ĐÁM MÂY

2.1 Kiến trúc song song

2.1.1 Giới thiệu chung

Kiến trúc song song là một kiểu kiến trúc máy tính trong đó nhiều bộ xử lý có thể thực hiện các tác vụ đồng thời. Kiến trúc này được sử dụng để cải thiện hiệu suất của các ứng dụng đòi hỏi tính toán cao.

Đặc điểm của kiến trúc song song:

- Tính song song: Nhiều bộ xử lý có thể thực hiện các tác vụ đồng thời.
- Tính đồng bộ: Các bộ xử lý có thể phối hợp hoạt động của chúng với nhau.
- Tính giao tiếp: Các bộ xử lý có thể trao đổi dữ liệu với nhau.

Ưu điểm	Nhược điểm
▪ Hiệu suất cao, có thể cải thiện hiệu suất của các ứng dụng đòi hỏi tính toán cao ▪ Dễ dàng mở rộng bằng cách thêm bộ xử lý mới ▪ Có thể linh hoạt sử dụng cho nhiều ứng dụng khác nhau	▪ Có thể phức tạp hơn các kiến trúc máy tính khác ▪ Khó khăn trong việc lập trình cho các hệ thống tuần tự ▪ Chi phí có thể đắt hơn các hệ thống tuần tự

Bảng 1. Ưu nhược điểm của kiến trúc song song

2.1.2 Các loại song song

Xử lý song song là một phần quan trọng của bất kỳ mô hình máy tính hiệu suất cao nào. Nó liên quan đến việc sử dụng một lượng lớn tài nguyên máy tính (CPU và bộ nhớ) để hoàn thành nhiệm vụ hoặc xử lý vấn đề phức tạp.

2.1.2.1 Song song mức bit (Bit-level parallelism - BLP)

Nguyên tắc hoạt động: Tăng kích thước từ (word size) của bộ xử lý, cho phép xử lý nhiều bit dữ liệu hơn trong một chu kỳ máy.

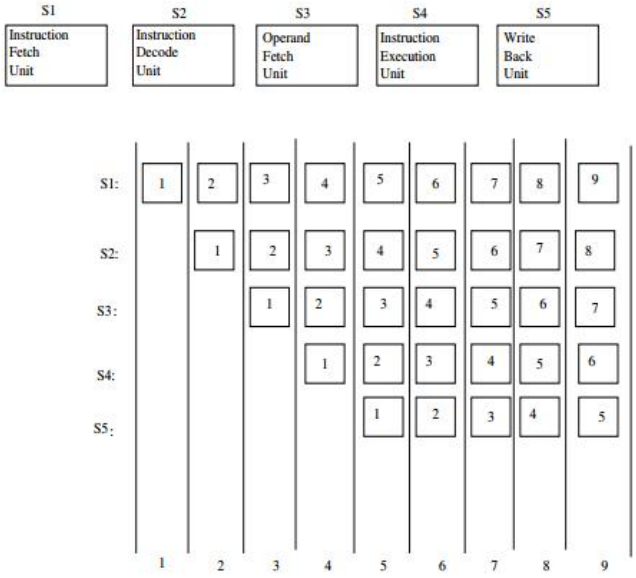
Ví dụ: Bộ xử lý 64-bit có thể xử lý 64 bit dữ liệu cùng lúc, nhanh gấp đôi so với bộ xử lý 32-bit.

Ưu điểm: Tăng tốc độ xử lý các phép toán số học và logic trên dữ liệu lớn.

Hạn chế: Hiệu quả giảm dần khi tăng kích thước từ vượt quá nhu cầu thực tế của ứng dụng.

2.1.2.2 Song song cấp độ lệnh (Instruction-level parallelism - ILP)

Nguyên tắc hoạt động: Thực thi nhiều lệnh cùng lúc bằng cách tận dụng các tài nguyên xử lý nhàn rỗi.



Hình 4 Các cấp độ lệnh song song

Kỹ thuật:

- Đường ống lệnh (pipelining): Chia quá trình thực thi lệnh thành nhiều giai đoạn và xử lý song song.
- Thực thi ngoài luồng (out-of-order execution): Thay đổi thứ tự thực thi lệnh để tránh tắc nghẽn.
- Dự đoán rẽ nhánh (branch prediction): Dự đoán kết quả của các lệnh rẽ nhánh để tiếp tục thực thi lệnh mà không bị gián đoạn.

Ưu điểm: Tăng hiệu suất đáng kể bằng cách tận dụng tối đa tài nguyên bộ xử lý.

Hạn chế: Phức tạp trong thiết kế và quản lý, đòi hỏi phần cứng và phần mềm hỗ trợ.

2.1.2.3 Song song cấp độ dữ liệu (Data-level parallelism - DLP)

Nguyên tắc hoạt động: Áp dụng cùng một phép toán trên nhiều phần tử dữ liệu cùng lúc.

Kiến trúc:

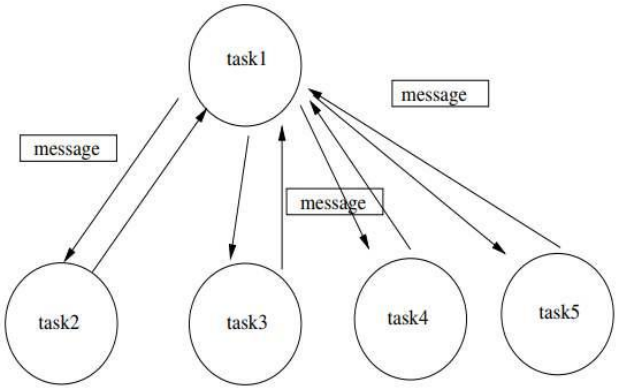
- SIMD (Single Instruction, Multiple Data): Thực hiện một lệnh trên nhiều dữ liệu đồng thời.
- Vector processing: Xử lý các vector (mảng) dữ liệu song song.

Ưu điểm: Tăng tốc đáng kể các ứng dụng xử lý dữ liệu lớn, đặc biệt là xử lý ảnh và video.

Hạn chế: Chỉ hiệu quả với các ứng dụng có thể vector hóa được.

2.1.2.4 Song song cấp độ tác vụ (Task-level parallelism - TLP)

Nguyên tắc hoạt động: Chia chương trình thành các tác vụ độc lập và thực thi chúng song song trên nhiều bộ xử lý hoặc lõi.



Hình 5 Song song cấp độ tác vụ

Kỹ thuật:

- Đa luồng (multithreading): Chia chương trình thành nhiều luồng thực thi song song trên cùng một bộ xử lý.
- Đa xử lý (multiprocessing): Chạy các tiến trình song song trên nhiều bộ xử lý.

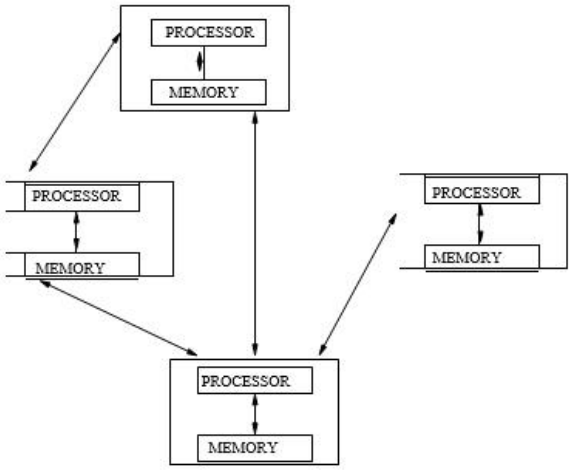
Ưu điểm: Tăng hiệu suất cho các ứng dụng có thể phân chia thành các tác vụ con độc lập.

Hạn chế: Đòi hỏi cơ chế đồng bộ hóa và giao tiếp giữa các tác vụ, có thể gây ra chi phí phát sinh.

2.2 Kiến trúc phân tán

2.2.1 Giới thiệu chung

Kiến trúc phân tán là một kiểu kiến trúc phần mềm trong đó các thành phần của hệ thống được phân phối trên nhiều máy tính hoặc nút mạng, giao tiếp và phối hợp với nhau để đạt được mục tiêu chung.



Hình 6 Hệ thống phân tán

Đặc điểm của kiến trúc phân tán:

- Tính phân tán: Các thành phần của hệ thống nằm trên nhiều máy tính hoặc nút mạng.
- Tính đồng thời: Nhiều thành phần có thể hoạt động đồng thời.
- Tính độc lập: Các thành phần có thể hoạt động độc lập với nhau.
- Tính mở rộng: Hệ thống có thể dễ dàng mở rộng bằng cách thêm các thành phần mới.
- Tính sẵn sàng: Hệ thống có thể tiếp tục hoạt động ngay cả khi một số thành phần bị lỗi.

Ưu điểm	Nhược điểm
▪ Dễ dàng mở rộng đáp ứng nhu cầu ngày càng tăng của người dùng ▪ Tính sẵn sàng cao, hệ thống có thể hoạt động ngay cả khi một số thành phần bị lỗi ▪ Có thể tận dụng sức mạnh tính toán của nhiều máy tính để đạt hiệu suất cao hơn ▪ Có thể linh hoạt triển khai trên nhiều nền tảng và môi trường khác nhau	▪ Hệ thống phân tán thường phức tạp hơn hệ thống tập trung ▪ Khó khăn trong việc quản lý so với hệ thống tập trung ▪ Có thể gặp nhiều vấn đề bảo mật hơn so với các hệ thống tập trung

Bảng 2. Ưu nhược điểm của kiến trúc phân tán

2.2.2 Mô hình tổ chức hệ thống

2.2.2.1 Hệ thống khách hàng - máy chủ (client-server)

Trong mô hình này, máy khách (client) gửi yêu cầu đến máy chủ (server) và máy chủ xử lý yêu cầu và trả về kết quả cho máy khách.

Ưu điểm:

- Tính bảo mật cao
- Dễ dàng quản lý và kiểm soát

Nhược điểm:

- "Điểm chết duy nhất" (Single Point of Failure) là thành phần duy nhất có khả năng phân phối dịch vụ, nếu gặp sự cố, cả hệ thống sẽ ngừng hoạt động.
- Tài nguyên sẽ trở nên khan hiếm nếu quá nhiều máy khách, hệ thống này không thể thu nhỏ và phát triển tùy theo nhu cầu.

2.2.2.2 Hệ thống ngang hàng (peer-to-peer)

Trong mô hình này, tất cả các máy tính trong mạng đều có vai trò như nhau và có thể giao tiếp trực tiếp với nhau.

Ưu điểm:

- Tính linh hoạt và khả năng mở rộng cao
- Không có điểm lỗi đơn

Nhược điểm:

- Tính bảo mật và độ tin cậy thấp hơn
- Khó khăn trong việc quản lý và kiểm soát

Tùy thuộc vào yêu cầu của ứng dụng, người ta có thể lựa chọn mô hình tổ chức hệ thống phù hợp. Ví dụ, mô hình khách hàng-máy chủ thường được sử dụng cho các ứng dụng yêu cầu tính bảo mật và độ tin cậy cao, trong khi mô hình ngang hàng thường được sử dụng cho các ứng dụng yêu cầu tính linh hoạt và khả năng mở rộng cao.

2.3 Kiến trúc tương tác điện toán đám mây

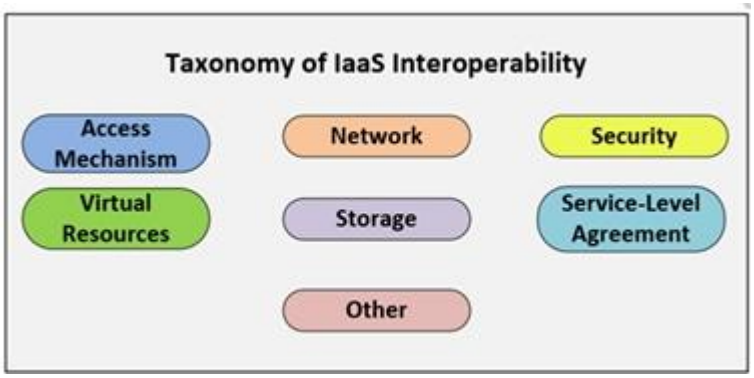
Khả năng tương tác trong đám mây có thể được coi và định nghĩa như một mô hình dịch vụ nên ta xem xét khả năng tương tác của các ứng dụng, nền tảng và quản lý.

- Khả năng tương tác của ứng dụng đám mây giải quyết các thành phần ứng dụng, cho dù chúng được triển khai dưới dạng IaaS, PaaS hay SaaS. Một thành phần ứng dụng có thể là một ứng dụng nguyên khối hoàn chỉnh hoặc một dịch vụ như một phần của ứng dụng phân tán. Các thành phần này cần các nền tảng tương ứng để triển khai các giao thức truyền thông và các tiêu chuẩn dữ liệu. Vì vậy, khả năng tương tác ứng dụng không thể thực hiện được nếu không có khả năng tương tác nền tảng đám mây.
- Khả năng tương tác của nền tảng đám mây liên quan đến các thành phần nền tảng, thường được triển khai dưới dạng PaaS hoặc IaaS. Trao đổi thông tin và khám phá dịch vụ yêu cầu các giao thức chuẩn để nhận ra các nền tảng có thể tương tác.
- Khả năng tương tác của quản lý đám mây nhắm vào các khía cạnh quản lý giữa các dịch vụ đám mây khác nhau được triển khai trên các cấp độ SaaS, PaaS hoặc IaaS. Mỗi nhà cung cấp có các tính năng và giao diện đám mây khác nhau để quản lý chúng. Vì vậy, khách hàng có thể có một cách tiếp cận riêng với quản lý hệ thống chung thông qua các giao diện tiêu chuẩn.

2.3.1 Khả năng tương tác mức IaaS

Khả năng tương tác trên mức IaaS của quản lý đám mây là hướng tới quản lý đơn giản và tiêu chuẩn hóa cơ sở hạ tầng của các hệ thống đám mây khác nhau. Việc quản lý bao gồm khởi tạo và kiểm soát các máy ảo, cho phép và khám phá các đặc trưng mạng, thiết lập và chỉnh sửa các quy tắc bảo mật, v.v. Hình 7 chỉ ra sự phân loại tương tác trong IaaS gồm:

- Cơ chế truy cập: xác định cách truy nhập một dịch vụ đám mây từ người dùng hay nhà phát triển phần mềm.
- Tài nguyên ảo: cung cấp dịch vụ dưới dạng một phần mềm hoàn chỉnh để cài đặt một máy ảo.
- Mạng: địa chỉ và giao diện lập trình ứng dụng (Application Programmable Interface).
- Lưu trữ: quản lý và tổ chức lưu trữ.
- Bảo mật: xác thực, ủy quyền, tài khoản người dùng và mã hóa.
- Thỏa thuận mức dịch vụ: định dạng kiến trúc, giám sát dịch vụ.



Hình 7 Phân loại các tương tác IaaS

2.3.2 Khả năng tương tác mức PaaS

Khả năng tương tác ở cấp độ PaaS nhằm trao đổi dữ liệu và dịch vụ đơn giản giữa các nền tảng khác nhau được lưu trữ trên các cơ sở hạ tầng khác nhau trên đám mây và việc tái sử dụng chúng hiệu quả mà không cần hỗ trợ từ phía người dùng.

Khi phân tích việc trao đổi dữ liệu, ta cần xem xét khả năng tương thích dữ liệu giữa các nền tảng khác nhau để thực hiện chuyển đổi định dạng nếu cần thiết. Khả năng tương tác của các dịch vụ được lưu trữ trên các nền tảng đám mây khác nhau sẽ tác động tới tính di động.

Ví dụ, để chuyển một dịch vụ từ đám mây này sang đám mây khác sử dụng nền tảng khác. Nếu các đám mây gốc và đích sử dụng cùng một môi trường, thì quá trình chuyển có thể thực hiện qua một quy trình đóng gói và sao chép đơn giản. Trong trường hợp các nền tảng khác nhau trên các đám mây gốc và đích, người ta phải bắt đầu một quy trình chuyển giao khác bao gồm đóng gói, sao chép, khởi tạo, cài đặt, triển khai và tùy chỉnh để cho phép khả năng tương tác. Tuy nhiên, vẫn có những vấn đề nảy sinh khi các dịch vụ được yêu cầu trên đám mây gốc không được đám mây đích hỗ trợ hoặc một sự phụ thuộc nào đó vào hệ điều hành cụ thể được lưu trữ trong đám mây gốc.

2.3.3 Khả năng tương tác mức SaaS

Khả năng tương tác ở cấp độ SaaS của các ứng dụng đám mây nhằm trao đổi dữ liệu và dịch vụ đơn giản giữa các ứng dụng khác nhau được lưu trữ trên các nền tảng và cơ sở hạ tầng khác nhau trên đám mây, và việc tái sử dụng chúng hiệu quả mà không cần hỗ trợ từ phía người dùng. Ngoài ra, loại khả năng tương tác này có thể được xem xét từ các miền ứng dụng khác nhau. Khả năng tương tác mức SaaS gồm 4 loại:

- Khả năng tương tác giữa các ứng dụng trong cùng một đám mây.
- Trao đổi dữ liệu và các yêu cầu hoạt động trong các ứng dụng trên các môi trường điện toán đám mây khác nhau.
- Các chương trình phần mềm được phân phối trong các môi trường đám mây khác nhau và tích hợp dữ liệu và ứng dụng trong đám mây theo một cách thống nhất.
- Di chuyển các ứng dụng từ một môi trường đám mây này sang môi trường khác.

Khi khách hàng chuyển đổi giữa hai nhà cung cấp đám mây ở cấp độ SaaS không liên quan đến việc chuyển các ứng dụng và dịch vụ, thay vào đó nó liên quan đến việc trao đổi dữ liệu có cấu trúc. Khả năng tương tác đám mây có lẽ là quan trọng nhất đối với việc giải quyết tính tương thích của dữ liệu. Nó không chỉ có nghĩa là chuyển dữ liệu có cấu trúc mà còn tất cả các quan hệ giữa chúng.

2.4 Kết chương

Chương này phân tích chi tiết các kiến trúc trong hệ thống điện toán đám mây, bao gồm kiến trúc song song, kiến trúc phân tán và kiến trúc tương tác trong môi trường đám mây. Chương cũng trình bày ưu nhược điểm của từng kiến trúc và những thách thức trong việc triển khai chúng.

CHƯƠNG 3. CƠ CHẾ HOẠT ĐỘNG ĐIỆN TOÁN ĐÁM MÂY

Điện toán đám mây hoạt động bằng cách cung cấp quyền cho người dùng tải lên và tải xuống thông tin được lưu trữ, thay vì yêu cầu người dùng sở hữu và quản lý phần cứng vật lý. Người dùng có thể truy cập dữ liệu từ mọi nơi. Hệ thống này dựa trên các công nghệ như ảo hóa, lưu trữ phân tán, cân bằng tải và tự động quản lý để đảm bảo hiệu suất và độ tin cậy cao.

Điện toán đám mây có thể được chia thành hai hệ thống. Một là front-end và một là back-end. Hai đầu kết nối với nhau nhờ sự hỗ trợ của kết nối Internet. Điện toán đám mây là sự kết hợp của các kỹ thuật front-end và back-end. Người dùng front-end tìm kiếm các giải pháp và chủ yếu giao diện thông qua điện thoại di động, máy tính xách tay và nhập các yêu cầu của họ vào trình duyệt. Nhà cung cấp dịch vụ từ back-end cung cấp các giải pháp bằng cách sử dụng máy ảo và sử dụng các cơ chế bảo mật và hệ thống lưu trữ.

Phần phụ trợ của đám mây là hệ thống và phần cuối là người dùng máy tính hoặc máy khách. Front-end của hệ thống có ứng dụng, được sử dụng để truy cập hệ thống đám mây. Hơn nữa, chương trình phụ trợ có nhiều máy tính, phần cứng, máy chủ và hệ thống lưu trữ dữ liệu khác nhau tạo thành đám mây.

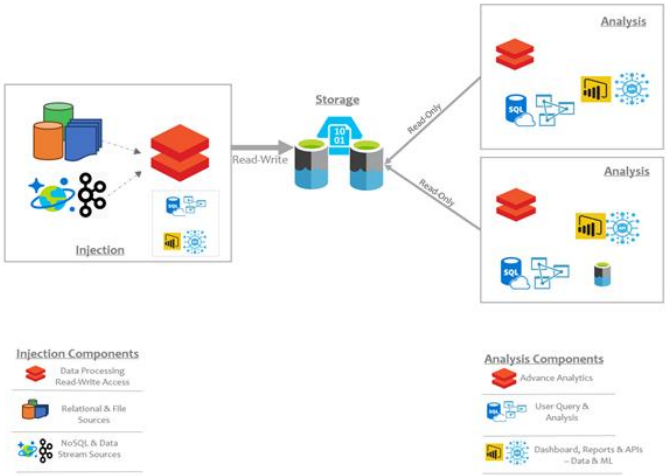
Tất cả các tính năng và chức năng này được quản lý bởi máy chủ trung tâm. Máy chủ trung tâm đảm bảo rằng mọi thứ chạy trơn tru và hoàn hảo.

Chẳng hạn, giải pháp mà người dùng tìm kiếm chủ yếu là một ứng dụng hoặc phần mềm. Sử dụng Giao diện người dùng đồ họa, máy khách giao tiếp với đám mây. Đám mây tìm kiếm dịch vụ trong các hệ thống lưu trữ rộng lớn và cung cấp cho người dùng phản hồi qua internet. Quy trình này tương đối tiết kiệm thời gian vì toàn bộ quy trình là ảo và cơ chế bảo mật vẫn còn nguyên vẹn. Ngoài ra, phạm vi rộng lớn mang lại sự đa dạng cho toàn bộ quy trình và giới thiệu cho người dùng thế giới dữ liệu lớn.

3.1 Cơ chế hoạt động của điện toán đám mây bao gồm:

3.1.1 Lưu trữ dữ liệu tập trung (Centralised data storage)

Dữ liệu của người dùng không được lưu trên máy tính cá nhân mà được lưu trữ trên các trung tâm dữ liệu (Data Centers) của nhà cung cấp dịch vụ đám mây.



Hình 8 Centralized data storage- Example

Các trung tâm dữ liệu này sử dụng hệ thống lưu trữ phân tán (Distributed Storage System), nơi dữ liệu được sao chép (Replication) trên nhiều máy chủ khác nhau để đảm bảo độ tin cậy (Reliability) và khả năng phục hồi dữ liệu (Data Recovery).

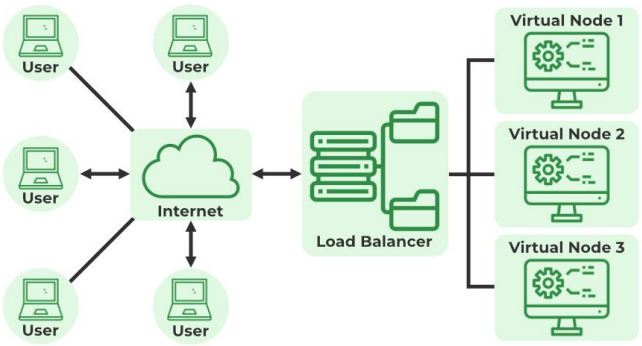
Người dùng truy cập dữ liệu thông qua giao thức mạng (HTTP, HTTPS, FTP, API RESTful) và có thể thao tác với dữ liệu qua các dịch vụ như Google Drive, Dropbox, OneDrive, AWS S3.

Ví dụ thực tế: khi tải ảnh lên Google Photos, hệ thống sẽ sao chép ảnh đó lên nhiều máy chủ ở các trung tâm dữ liệu khác nhau để đảm bảo bạn luôn có thể truy cập ngay cả khi một máy chủ bị lỗi.

3.1.2 Gộp chung tài nguyên (Resource Pooling)

Các nhà cung cấp dịch vụ đám mây sử dụng công nghệ ảo hóa (Virtualization) để chia sẻ một hệ thống tài nguyên vật lý giữa nhiều người dùng khác nhau.

Tài nguyên như CPU, RAM, bộ nhớ, băng thông mạng được tập trung trong một hệ thống lớn và được cấp phát động (Dynamic Allocation) theo nhu cầu của từng người dùng.



Hình 9 Resource Pooling

Khi có nhiều người dùng truy cập đồng thời, hệ thống sẽ tự động điều chỉnh để đảm bảo hiệu suất ổn định.

Ví dụ thực tế: khi bạn sử dụng một máy chủ ảo (VM) trên AWS EC2, thực tế bạn đang dùng một phần của một máy chủ vật lý được chia sẻ với nhiều người khác.

3.1.3 Truy xuất và quản lý dữ liệu (Data retrieval and management)

Người dùng có thể truy cập dữ liệu từ xa thông qua giao diện web, API hoặc ứng dụng.

Dữ liệu được lưu trữ tại nhiều trung tâm dữ liệu khác nhau và có thể được truy xuất nhanh chóng nhờ Content Delivery Network (CDN).

Hệ thống sử dụng cơ chế đồng bộ hóa dữ liệu (Data Synchronization) để đảm bảo khi dữ liệu thay đổi trên một thiết bị, nó sẽ được cập nhật trên tất cả các thiết bị khác.

Ví dụ thực tế: khi chỉnh sửa một tài liệu trên Google Docs từ điện thoại, thay đổi đó ngay lập tức xuất hiện trên máy tính của bạn mà không cần lưu thủ công.

3.1.4 Tính khả dụng theo yêu cầu (On-Demand Availability)

Người dùng có thể tự động tạo, thay đổi hoặc hủy bỏ tài nguyên theo nhu cầu sử dụng mà không cần liên hệ với nhà cung cấp dịch vụ.

Tài nguyên được tăng/giảm tự động (Auto Scaling) để phù hợp với tải công việc thực tế, giúp tiết kiệm chi phí.

Thanh toán theo mô hình Pay-as-you-go, chỉ trả tiền cho tài nguyên thực sự sử dụng.

Ví dụ thực tế: khi trang web thương mại điện tử của bạn có lượng truy cập tăng cao vào ngày giảm giá, hệ thống sẽ tự động tăng thêm máy chủ để đảm bảo trang web không bị sập.

3.1.5 Ảo hóa (Virtualization)

Hệ thống sử dụng Hypervisor để tạo ra các máy ảo (Virtual Machines - VMs) trên một máy chủ vật lý duy nhất.

Mỗi máy ảo hoạt động như một máy tính độc lập với hệ điều hành riêng, cho phép chạy nhiều ứng dụng cùng lúc mà không bị ảnh hưởng lẫn nhau.

Ngoài máy ảo, công nghệ Container (Docker, Kubernetes) giúp triển khai ứng dụng nhanh hơn mà không cần một hệ điều hành đầy đủ.

Ví dụ thực tế: khi bạn thuê một máy chủ đám mây trên Google Cloud, thực tế bạn đang sử dụng một máy ảo được chạy trên hạ tầng vật lý của Google.

3.1.6 Quản lý tự động (Automated Management)

Hệ thống đám mây sử dụng AI & Machine Learning để tự động giám sát, bảo trì và tối ưu hóa hệ thống.

Các nhiệm vụ như sao lưu dữ liệu (Backup & Recovery), cập nhật phần mềm và bảo mật hệ thống được thực hiện mà không cần sự can thiệp của con người.

Hệ thống giám sát theo thời gian thực để phát hiện và khắc phục sự cố ngay lập tức.

Ví dụ thực tế: dịch vụ AWS Backup tự động sao lưu dữ liệu hàng ngày mà không cần người dùng phải thực hiện thủ công.

3.1.7 Khả năng truy cập (Accessibility)

Người dùng có thể truy cập tài nguyên đám mây từ bất kỳ đâu miễn là có kết nối Internet.

Hệ thống xác thực đa yếu tố (Multi-Factor Authentication - MFA) giúp bảo vệ tài khoản khỏi truy cập trái phép.

Các nhà cung cấp dịch vụ đám mây sử dụng cơ sở hạ tầng mạng mạnh mẽ để đảm bảo tốc độ truy cập nhanh và ổn định.

Ví dụ thực tế: bạn có thể đăng nhập vào tài khoản Google từ điện thoại, laptop hoặc máy tính bảng mà không bị giới hạn bởi thiết bị cụ thể.

Tổng quan cơ chế hoạt động của điện toán đám mây được xây dựng trên ba phần chính:

- Cơ chế hạ tầng cung cấp nền tảng vật lý và ảo hóa để đảm bảo hiệu suất, khả năng mở rộng và truy xuất dữ liệu nhanh chóng.
- Cơ chế quản lý giúp điều phối tài nguyên, tối ưu hóa hiệu suất và kiểm soát chi phí dịch vụ.
- Cơ chế bảo mật bảo vệ dữ liệu và hệ thống khỏi các mối đe dọa bằng mã hóa, xác thực và phân quyền truy cập.

Giúp đảm bảo tính ổn định, hiệu suất và an toàn cho toàn bộ hệ thống.

- Thứ nhất, cơ chế hạ tầng là nền tảng của điện toán đám mây, bao gồm nhiều thành phần quan trọng. Hệ thống sử dụng biên giới mạng logic (Logical Network Boundary) để cô lập các tài nguyên đám mây và bảo vệ khỏi truy cập trái phép bằng tường lửa ảo và mạng ảo VLAN. Máy chủ ảo (Virtual Server) được tạo ra nhờ công nghệ ảo hóa, cho phép một máy chủ vật lý chạy nhiều máy ảo, giúp tối ưu hóa tài nguyên. Thiết bị lưu trữ đám mây (Cloud Storage Devices) hỗ trợ các mô hình lưu trữ như File, Block, Dataset và Object Storage, đảm bảo khả năng mở rộng và bảo vệ dữ liệu. Ngoài ra, hệ thống giám sát tài nguyên (Cloud Usage Monitoring) theo dõi việc sử dụng tài nguyên bằng các tác nhân giám sát, giúp nhà cung cấp điều chỉnh hiệu suất. Khi cần tăng cường khả năng hoạt động, cơ chế sao chép tài nguyên (Resource Replication) tạo ra các bản sao của máy chủ ảo để đảm bảo độ tin cậy và phục hồi nhanh chóng khi có sự cố.
- Thứ hai, cơ chế quản lý giúp điều phối tài nguyên và đảm bảo các dịch vụ đám mây hoạt động hiệu quả. Hệ thống quản lý từ xa (Remote Management System) cung cấp giao diện để người dùng giám sát và điều chỉnh dịch vụ. Hệ thống quản lý tài nguyên (Resource Management System) tự động phân bổ và tối ưu hóa tài nguyên dựa trên nhu cầu thực tế. Hệ thống quản lý SLA (SLA Management System) theo dõi mức độ tuân thủ cam kết chất lượng dịch vụ giữa nhà cung cấp và khách hàng.

Cuối cùng, hệ thống quản lý thanh toán (Billing Management System) tính toán chi phí dựa trên mức sử dụng thực tế theo mô hình Pay-as-you-go, giúp tối ưu hóa chi phí cho người dùng.

- Thứ ba, cơ chế bảo mật đảm bảo an toàn cho dữ liệu và hệ thống khỏi các mối đe dọa. Mã hóa (Encryption) được sử dụng để bảo vệ dữ liệu trong quá trình truyền tải và lưu trữ bằng các phương pháp mã hóa đối xứng và bất đối xứng. Băm dữ liệu (Hashing) giúp xác thực tính toàn vẹn của dữ liệu, đảm bảo không bị thay đổi trong quá trình truyền. Chữ ký số (Digital Signature) cung cấp khả năng xác thực và chống giả mạo tài liệu. Hạ tầng khóa công khai (Public Key Infrastructure - PKI) hỗ trợ quản lý khóa công khai và chứng chỉ số để xác thực danh tính giữa các bên. Ngoài ra, quản lý danh tính và truy cập (Identity and Access Management - IAM) kiểm soát quyền truy cập vào tài nguyên đám mây để ngăn chặn truy cập trái phép. Đăng nhập một lần (Single Sign-On - SSO) giúp người dùng có thể đăng nhập vào nhiều dịch vụ mà không cần xác thực lại nhiều lần. Cuối cùng, cơ chế nhóm bảo mật đám mây (Cloud-Based Security Group) phân chia tài nguyên thành các nhóm bảo mật riêng biệt để ngăn chặn tấn công và bảo vệ dữ liệu tốt hơn.

Nhờ sự kết hợp của ba cơ chế trên, điện toán đám mây có thể cung cấp một hệ thống linh hoạt, mạnh mẽ, dễ mở rộng và an toàn, giúp người dùng khai thác tài nguyên một cách tối ưu mà không cần đầu tư cơ sở hạ tầng vật lý.

3.2 Kết chương

Chương này giới thiệu các cơ chế hoạt động quan trọng của điện toán đám mây, bao gồm lưu trữ dữ liệu tập trung, gộp chung tài nguyên, quản lý tài nguyên tự động và các kỹ thuật ảo hóa. Ngoài ra, chương cũng phân tích tính sẵn sàng và linh hoạt của hệ thống điện toán đám mây trong việc cung cấp dịch vụ theo nhu cầu.

CHƯƠNG 4. AN NINH VÀ BẢO MẬT ĐIỆN TOÁN ĐÁM MÂY

4.1 Khái quát nguy cơ và tác động tới điện toán đám mây

4.1.1 Rủi ro bảo mật trong điện toán đám mây

- Chia sẻ tài nguyên: Môi trường đám mây hoạt động theo mô hình đa thuê (multi-tenancy), nơi nhiều khách hàng sử dụng cùng một cơ sở hạ tầng, có nguy cơ bị tấn công từ bên trong.
- Dữ liệu phân tán: Thông tin của khách hàng có thể được lưu trữ trên nhiều trung tâm dữ liệu khác nhau, dẫn đến rủi ro mất dữ liệu hoặc truy cập trái phép.
- Mất kiểm soát dữ liệu: Khi sử dụng đám mây, doanh nghiệp không trực tiếp kiểm soát hệ thống lưu trữ và vận hành dữ liệu của mình.
- Tấn công DDoS (Tấn công từ chối dịch vụ): Hacker có thể tấn công hệ thống bằng cách gửi lượng lớn yêu cầu giả mạo, làm quá tải hệ thống.
- Lỗ hổng trong API: Các dịch vụ đám mây thường cung cấp API để khách hàng kết nối và tương tác. Nếu API không được bảo mật tốt, hacker có thể lợi dụng để truy cập trái phép.

4.1.2 Ảnh hưởng của rủi ro bảo mật

Rủi ro bảo mật có thể gây ra hậu quả nghiêm trọng đối với doanh nghiệp, bao gồm:

- Rò rỉ dữ liệu quan trọng: Thông tin khách hàng, tài chính và dữ liệu nội bộ bị đánh cắp có thể dẫn đến gian lận, mất lợi thế cạnh tranh.
- Gián đoạn dịch vụ: Các cuộc tấn công mạng như DDoS có thể khiến hệ thống ngừng hoạt động, ảnh hưởng đến doanh thu và trải nghiệm khách hàng.
- Mất niềm tin và uy tín: Khi dữ liệu bị xâm phạm, khách hàng có thể lo ngại về an toàn thông tin và ngừng sử dụng dịch vụ.
- Tốn kém chi phí và rủi ro pháp lý: Doanh nghiệp phải chi nhiều tiền để khắc phục sự cố và có thể đối mặt với các án phạt nếu vi phạm quy định bảo mật.
- Nguy cơ mất quyền kiểm soát hệ thống: Hacker có thể chiếm quyền truy cập, mã hóa dữ liệu hoặc sử dụng hệ thống để thực hiện tấn công khác.

4.2 Các nguyên lý bảo mật chung

Để đảm bảo an toàn cho dữ liệu và hệ thống trên đám mây, cần tuân theo các nguyên lý sau:

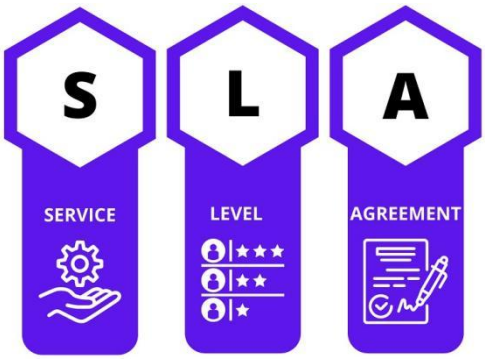
- Tính bảo mật dữ liệu (Confidentiality): ngăn chặn truy cập trái phép vào dữ liệu.
- Tính toàn vẹn dữ liệu (Integrity): đảm bảo dữ liệu không bị thay đổi trái phép.
- Tính sẵn có (Availability): dữ liệu và dịch vụ luôn sẵn sàng khi cần.
- Xác thực và ủy quyền: đảm bảo chỉ người dùng được phép mới có thể truy cập hệ thống.

- Ghi nhật ký và theo dõi: hệ thống cần có cơ chế giám sát để phát hiện các hoạt động bất thường.

4.3 Thoả thuận mức dịch vụ (SLA)

Thoả thuận mức dịch vụ (SLA) được sử dụng trong các ngành khác nhau để thiết lập mối quan hệ giữa nhà cung cấp dịch vụ và người tiêu dùng. SLA sẽ nêu chi tiết các khả năng ở cấp độ dịch vụ mà các nhà cung cấp hứa hẹn sẽ cung cấp và yêu cầu/mong đợi mà người tiêu dùng đã nêu.

Tài liệu SLA nên bao gồm các vấn đề bảo mật một cách chi tiết đầy đủ, như khả năng bảo mật của các giải pháp và các tiêu chuẩn cần nhà cung cấp duy trì, hay các thông tin rõ ràng về những gì người tiêu dùng coi là vi phạm bảo mật. Các hoạt động duy trì bảo mật mạnh mẽ cần xác định trách nhiệm của cả nhà cung cấp dịch vụ và người tiêu dùng dưới dạng văn bản.



Hình 10 Thỏa thuận mức dịch vụ

4.4 Trách nhiệm bảo mật trong mô hình điện toán đám mây

Mô hình bảo mật trong điện toán đám mây dựa trên mô hình chia sẻ trách nhiệm giữa:

- Nhà cung cấp dịch vụ đám mây (CSP - Cloud Service Provider): Chịu trách nhiệm bảo mật cơ sở hạ tầng, bao gồm phần cứng, mạng và hệ điều hành máy chủ.
- Người dùng dịch vụ đám mây (Cloud Consumer): Chịu trách nhiệm bảo mật dữ liệu, quyền truy cập, ứng dụng và cài đặt bảo mật riêng.
- Bên thứ ba (Cloud Auditors & Security Providers): Đánh giá, kiểm tra và hỗ trợ bảo mật dịch vụ đám mây.

Việc chia sẻ trách nhiệm này giúp tối ưu hóa bảo mật nhưng cũng đặt ra yêu cầu cao về phối hợp giữa các bên.

4.5 Các mối đe dọa bảo mật trong điện toán đám mây

4.5.1 Rủi ro từ cơ sở hạ tầng

Cơ sở hạ tầng đám mây bao gồm các máy chủ, trung tâm dữ liệu, hệ thống mạng và các dịch vụ hỗ trợ khác. Nếu không được bảo mật chặt chẽ, hệ thống này có thể trở thành mục tiêu của nhiều loại tấn công mạng:

- Tấn công từ bên trong: Một trong những mối đe dọa lớn nhất đến từ nội bộ nhà cung cấp dịch vụ đám mây. Nếu không có chính sách giám sát và kiểm soát truy

cập hợp lý, nhân viên nội bộ có thể lợi dụng quyền hạn để truy cập vào dữ liệu khách hàng, gây rò rỉ thông tin hoặc phá hoại hệ thống.

- Tấn công xen giữa (Man-in-the-Middle – MITM): Khi dữ liệu được truyền tải giữa người dùng và máy chủ đám mây, hacker có thể chặn luồng thông tin, đánh cắp dữ liệu hoặc thay đổi nội dung trong quá trình truyền. Nếu không có biện pháp mã hóa mạnh mẽ như TLS/SSL, dữ liệu có thể bị tổn thất nghiêm trọng.
- Lỗ hổng phần cứng: Các máy chủ vật lý vận hành dịch vụ đám mây cũng có thể bị tấn công. Nếu không được cập nhật bảo mật thường xuyên, phần cứng có thể trở thành mục tiêu của các cuộc tấn công nhắm vào firmware hoặc phần mềm điều khiển.

4.5.2 Rủi ro bảo mật dữ liệu

Dữ liệu là tài sản quan trọng nhất trong hệ thống đám mây, và các rủi ro bảo mật liên quan đến dữ liệu có thể gây hậu quả nghiêm trọng:

- Mất dữ liệu do lỗi hệ thống: Nếu hệ thống gặp sự cố nghiêm trọng, chẳng hạn như lỗi phần cứng, lỗi phần mềm hoặc thậm chí là thiên tai, dữ liệu có thể bị mất hoàn toàn nếu không có cơ chế sao lưu phù hợp.
- Truy cập trái phép: Các tài khoản quản trị bị lộ hoặc mật khẩu yếu có thể tạo điều kiện cho hacker xâm nhập vào hệ thống và đánh cắp dữ liệu. Tấn công brute-force hoặc phishing là những phương thức phổ biến để chiếm quyền kiểm soát tài khoản.
- Rò rỉ dữ liệu do lỗi con người: Một trong những nguyên nhân chính dẫn đến rủi ro bảo mật là do sai sót của con người. Ví dụ, nhân viên có thể vô tình gửi nhầm thông tin nhạy cảm, sử dụng mật khẩu dễ đoán hoặc không tuân thủ các chính sách bảo mật, tạo lỗ hổng cho hacker khai thác.

4.5.3 Kiểm soát truy cập và quyền hạn

Việc quản lý truy cập không chặt chẽ là một trong những nguyên nhân hàng đầu dẫn đến các vụ tấn công bảo mật:

- Thiếu chính sách phân quyền hợp lý: Nếu hệ thống không kiểm soát quyền hạn chặt chẽ, nhân viên có thể truy cập vào dữ liệu không thuộc phạm vi trách nhiệm của họ. Điều này làm tăng nguy cơ rò rỉ hoặc sửa đổi dữ liệu trái phép.
- Tài khoản không được giám sát: Những tài khoản cũ hoặc không còn được sử dụng nhưng chưa bị vô hiệu hóa có thể trở thành mục tiêu của hacker. Nếu không kiểm tra định kỳ, những tài khoản này có thể bị lợi dụng để xâm nhập hệ thống mà không bị phát hiện.
- Sử dụng chung tài khoản: Nếu nhiều người dùng chung một tài khoản mà không có cơ chế ghi nhật ký, rất khó để xác định ai đã thực hiện hành động nào trong hệ thống. Điều này gây khó khăn trong việc theo dõi và xử lý sự cố bảo mật.

4.6 Các cấp độ bảo mật trong điện toán đám mây

4.6.1 Bảo mật cấp độ mạng

Mạng là môi trường trung gian để dữ liệu được truyền tải giữa người dùng và các dịch vụ đám mây. Do đó, bảo mật mạng là yếu tố quan trọng giúp ngăn chặn các cuộc tấn công từ bên ngoài và đảm bảo dữ liệu không bị xâm phạm trong quá trình di chuyển.

Các biện pháp bảo mật mạng:

- Sử dụng VPN (Virtual Private Network): VPN giúp mã hóa toàn bộ luồng dữ liệu khi truyền tải giữa người dùng và máy chủ đám mây, giảm nguy cơ bị hacker chặn và đánh cắp thông tin.
- Triển khai tường lửa (Firewall): Tường lửa giúp kiểm soát lưu lượng truy cập vào hệ thống, ngăn chặn các kết nối trái phép và bảo vệ chống lại các cuộc tấn công mạng.
- Hệ thống phát hiện và ngăn chặn xâm nhập (IDS/IPS): Hệ thống IDS (Intrusion Detection System) giúp giám sát và phát hiện các hành vi tấn công đáng ngờ, trong khi IPS (Intrusion Prevention System) có thể chủ động ngăn chặn các mối đe dọa trước khi chúng gây thiệt hại cho hệ thống.
- Mã hóa dữ liệu trong quá trình truyền tải: Việc sử dụng giao thức bảo mật như TLS/SSL giúp bảo vệ dữ liệu khi được gửi đi trên mạng, ngăn chặn các cuộc tấn công kiểu "Man-in-the-Middle" (MITM).
- Phân đoạn mạng (Network Segmentation): Tạo các vùng mạng riêng biệt với chính sách truy cập khác nhau giúp giảm thiểu rủi ro tấn công lây lan trong toàn bộ hệ thống.

4.6.2 Bảo mật cấp máy chủ

Máy chủ là nền tảng cốt lõi trong hạ tầng đám mây, nơi lưu trữ và xử lý dữ liệu. Nếu máy chủ bị tấn công hoặc khai thác lỗ hổng, hacker có thể chiếm quyền điều khiển và truy cập vào dữ liệu quan trọng. Vì vậy, cần có các biện pháp bảo vệ nghiêm ngặt để giảm thiểu rủi ro.

Các biện pháp bảo mật máy chủ:

- Cập nhật bản vá bảo mật thường xuyên: Hệ điều hành và phần mềm trên máy chủ cần được cập nhật liên tục để khắc phục các lỗ hổng bảo mật, ngăn chặn hacker khai thác các điểm yếu trong hệ thống.
- Sử dụng hệ thống phát hiện xâm nhập (IDS): IDS giúp giám sát các hoạt động đáng ngờ trên máy chủ và gửi cảnh báo khi có dấu hiệu tấn công.
- Giới hạn quyền truy cập: Chỉ những tài khoản có quyền hạn thích hợp mới được phép thao tác trên máy chủ. Áp dụng nguyên tắc "Least Privilege" để hạn chế quyền truy cập không cần thiết.
- Bật chế độ ghi nhật ký (Logging): Ghi lại toàn bộ hoạt động trên máy chủ giúp phát hiện nhanh chóng các sự kiện bất thường và hỗ trợ điều tra khi xảy ra sự cố.

- Bảo vệ chống tấn công brute-force: Sử dụng CAPTCHA, khóa tài khoản sau một số lần đăng nhập sai hoặc áp dụng xác thực hai yếu tố để ngăn chặn hacker tấn công vào tài khoản quản trị máy chủ.
- Sao lưu dữ liệu định kỳ: Thực hiện sao lưu tự động để đảm bảo dữ liệu có thể khôi phục nếu xảy ra sự cố mất mát hoặc tấn công ransomware.

4.6.3 Bảo mật cấp ứng dụng

Ứng dụng chạy trên nền tảng đám mây thường là mục tiêu chính của các cuộc tấn công vì chúng có thể chứa nhiều lỗ hổng bảo mật, từ lỗi lập trình đến cấu hình sai. Do đó, bảo mật ứng dụng là một phần không thể thiếu trong việc bảo vệ hệ thống.

Các biện pháp bảo mật ứng dụng:

- Kiểm tra mã nguồn và vá lỗi bảo mật định kỳ: Thực hiện đánh giá bảo mật mã nguồn (code review) và kiểm thử bảo mật ứng dụng (penetration testing) để phát hiện các lỗ hổng có thể bị khai thác.
- Sử dụng xác thực hai yếu tố (2FA): Xác thực hai yếu tố giúp tăng cường bảo mật đăng nhập, đảm bảo chỉ những người dùng được ủy quyền mới có thể truy cập vào hệ thống.
- Cơ chế quản lý phiên (Session Management): Hệ thống cần quản lý phiên làm việc của người dùng một cách chặt chẽ, tự động đăng xuất khi không hoạt động trong một khoảng thời gian nhất định để tránh bị chiếm quyền điều khiển.
- Chống tấn công SQL Injection và XSS: Ứng dụng cần kiểm tra và lọc dữ liệu đầu vào từ người dùng để ngăn chặn các cuộc tấn công chèn mã độc vào cơ sở dữ liệu (SQL Injection) hoặc chèn mã JavaScript độc hại (Cross-Site Scripting – XSS).
- Bảo vệ API và giao thức truyền dữ liệu: Nếu ứng dụng sử dụng API để kết nối với các dịch vụ khác, cần xác thực và mã hóa dữ liệu truyền tải để tránh bị khai thác.
- Sử dụng Web Application Firewall (WAF): WAF giúp phát hiện và ngăn chặn các cuộc tấn công vào ứng dụng web, bảo vệ khỏi các mối đe dọa như DDoS, XSS và SQL Injection.

4.7 Bảo mật hệ điều hành và ảo hóa

Trong môi trường điện toán đám mây, bảo mật hệ điều hành và hệ thống ảo hóa là một yếu tố quan trọng để bảo vệ dữ liệu và tài nguyên khỏi các mối đe dọa từ cả bên trong lẫn bên ngoài. Hệ điều hành và các nền tảng ảo hóa chịu trách nhiệm quản lý tài nguyên, cung cấp dịch vụ và kiểm soát truy cập, do đó chúng trở thành mục tiêu hấp dẫn đối với tin tặc.

4.7.1 Nguy cơ bảo mật trong hệ thống ảo hóa

Công nghệ ảo hóa cho phép nhiều máy ảo (Virtual Machine - VM) chạy trên cùng một máy chủ vật lý, được quản lý bởi một hypervisor. Dù mang lại nhiều lợi ích như tối ưu tài nguyên và giảm chi phí, nhưng hệ thống ảo hóa cũng mang đến những rủi ro bảo mật đáng kể.

4.7.1.1 Tấn công vào hypervisor

Hypervisor (phần mềm quản lý máy ảo) là thành phần cốt lõi trong ảo hóa. Nếu hacker có thể khai thác lỗ hổng trong hypervisor, họ có thể:

- Thoát khỏi môi trường máy ảo (VM Escape): Tin tặc có thể vượt ra khỏi phạm vi của một máy ảo và xâm nhập vào hypervisor, từ đó kiểm soát toàn bộ hệ thống.
- Tấn công chéo máy ảo (VM-to-VM Attack): Nếu một máy ảo bị tấn công, hacker có thể sử dụng nó để xâm nhập vào các máy ảo khác chạy trên cùng một hypervisor.
- Tấn công từ bên trong: Nhân viên nội bộ có thể lợi dụng quyền truy cập để kiểm soát hypervisor và gây rủi ro cho toàn bộ hệ thống.

4.7.1.2 Các lỗ hổng trong hệ điều hành máy chủ

Hệ điều hành máy chủ (Host OS) là nền tảng mà hypervisor chạy trên đó. Nếu hệ điều hành này có lỗ hổng bảo mật, hacker có thể khai thác để:

- Tấn công từ bên ngoài: Kẻ xấu có thể khai thác lỗi hệ điều hành để truy cập trái phép vào hệ thống đám mây.
- Tấn công thông qua phần mềm lỗi thời: Nếu hệ điều hành không được cập nhật thường xuyên, nó có thể tồn tại những lỗ hổng nghiêm trọng.

4.7.1.3 Rủi ro từ cấu hình sai hoặc quản lý kém

- Nếu hệ thống ảo hóa không được cấu hình đúng cách, hacker có thể khai thác các điểm yếu để chiếm quyền điều khiển.
- Việc sử dụng mật khẩu yếu hoặc không có cơ chế xác thực mạnh có thể dẫn đến rủi ro bị xâm nhập.

4.7.2 Các mối đe dọa từ hệ điều hành quản lý

Hệ điều hành đóng vai trò cốt lõi trong việc điều hành máy chủ và các máy ảo. Nếu hệ điều hành có lỗ hổng bảo mật, kẻ tấn công có thể lợi dụng để giành quyền kiểm soát hệ thống. Các mối đe dọa chính bao gồm:

- Khai thác lỗ hổng phần mềm: Nếu hệ điều hành không được cập nhật thường xuyên, hacker có thể sử dụng các mã khai thác (exploit) để tấn công hệ thống.
- Tấn công leo thang đặc quyền (Privilege Escalation Attack): Nếu hacker tìm được một lỗi bảo mật trong hệ điều hành, họ có thể nâng quyền truy cập từ người dùng bình thường lên quản trị viên và kiểm soát toàn bộ hệ thống.
- Tấn công bằng mã độc (Malware Attack): Một số phần mềm độc hại có thể được cài đặt vào hệ điều hành để đánh cắp dữ liệu, chiếm quyền điều khiển hoặc làm gián đoạn dịch vụ.
- Tấn công từ nội bộ: Nhân viên hoặc người có quyền truy cập hệ điều hành có thể lạm dụng đặc quyền để đánh cắp dữ liệu hoặc thực hiện hành vi phá hoại.

4.8 Khuyến nghị bảo mật ảo hóa

Một yêu cầu cơ bản để ảo hóa thành công là thiết lập các cơ chế bảo mật để đối phó với các lỗ hổng của công nghệ hấp dẫn này. Về vấn đề này, ngoài các kỹ thuật truyền thống, một số biện pháp bảo mật khác là cần thiết để đảm bảo an toàn cho các hệ thống ảo hóa.

- 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. Tất cả các ứng dụng họ chạy hoặc bất kỳ tính toán nào họ thực hiện chỉ có thể được thực hiện trên VM. Các máy ảo mạnh mẽ và được cấu hình đúng sẽ không bao giờ cho phép bất kỳ ứng dụng nào bỏ qua chúng để truy cập trực tiếp vào các tài nguyên trình ảo hóa. Vì vậy, làm cứng các máy ảo nên được thực hiện nghiêm túc vì chúng đóng vai trò là lớp phòng thủ đầu tiên. Việc thực hiện có thể thay đổi theo các khuyến nghị của nhà cung cấp. Ngoài ra, cần giữ cho phần mềm máy ảo được cập nhật để đảm bảo rằng tất cả các lỗ hổng đã biết đã được sửa chữa.
- Làm cứng Trình ảo hóa (Hypervisor): 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. Vì vậy, không thể tránh khỏi việc tập trung vào sự bảo mật của trình ảo hóa và đảm bảo rằng nó được triển khai vững chắc. Điều này đảm bảo rằng ngay cả khi có lỗ hổng trong bất kỳ hệ thống khách nào (máy ảo), trình ảo hóa vẫn bảo vệ các VM khác và các tài nguyên cơ bản khỏi mọi cuộc tấn công hoặc vi phạm bảo mật sâu hơn.
- Làm cứng hệ điều hành máy chủ: Trong kỹ thuật ảo hóa máy chủ được lưu trữ, hệ điều hành máy chủ đóng vai trò quan trọng trong việc quản lý bảo mật của hệ thống vật lý. Mặc dù bất kỳ lỗ hổng nào trong cấu hình của hệ điều hành khách chỉ có thể ảnh hưởng đến môi trường máy ảo cụ thể, nhưng bất kỳ lỗ hổng nào trong hệ điều hành máy chủ có thể ảnh hưởng đến toàn bộ môi trường, bao gồm tất cả các máy khách. Ngoài ra, một hệ điều hành máy chủ thiếu bảo mật có thể làm suy yếu trình ảo hóa mà nó đang lưu trữ, khiến toàn bộ môi trường trở nên dễ bị tấn công.
- Hạn chế quyền truy cập vật lý vào máy chủ: Bất kỳ lỗ hổng nào của hệ thống máy chủ đều có thể khiến toàn bộ môi trường ảo hóa gặp rủi ro. Các hệ thống máy chủ phải được bảo vệ khỏi tất cả các truy cập bên ngoài trái phép. Bất kỳ quyền truy cập vật lý trái phép nào vào hệ thống máy chủ đều có thể khiến nó dễ bị tấn công theo nhiều cách.
- Thực hiện chức năng chính đơn cho mỗi VM: Mặc dù các máy ảo có khả năng xử lý nhiều tác vụ, nhưng việc tách riêng các chức năng chính giữa các VM khác nhau giúp môi trường ảo hóa an toàn hơn. Sự cô lập này ngăn các quá trình bị lộ và giảm khả năng hacker có thể làm hỏng nhiều chức năng quan trọng khi có một điểm yếu xuất hiện trong một máy ảo.
- Sử dụng truyền thông bảo mật: Thiết lập các cơ chế truyền thông bảo mật giúp bảo vệ hệ thống điện toán. Các kỹ thuật mã hóa nên được sử dụng để phòng thủ trước tin tặc. Các kỹ thuật phổ biến hiện nay bao gồm: HTTPS (HTTP Secure), VPN

(Mạng riêng ảo được mã hóa), TLS (Bảo mật lớp vận chuyển), SSH (Shell Secure), v.v.

- Sử dụng NIC riêng biệt cho VM nhạy cảm: Các máy ảo xử lý dữ liệu nhạy cảm thường là mục tiêu của tin tặc trên mạng. Trong trường hợp này, tốt hơn là sử dụng thẻ giao diện mạng vật lý riêng biệt (NIC) cho các máy ảo này thay vì chia sẻ một NIC giữa nhiều máy ảo.

4.9 Kết chương

Chương này tập trung vào các vấn đề an ninh và bảo mật trong điện toán đám mây, bao gồm những rủi ro bảo mật, tấn công mạng và mối đe dọa đối với dữ liệu lưu trữ trên đám mây. Chương cũng trình bày các nguyên tắc bảo mật chung, vai trò của các bên liên quan và các giải pháp bảo vệ để đảm bảo tính an toàn cho hệ thống.

KẾT LUẬN

Các kết quả đạt được (nêu các kết quả đã đạt được của BTL)

Nhóm thực hiện đề tài "Điện toán đám mây: Kiến trúc, cơ chế hoạt động, thành phần, ưu nhược điểm và vấn đề an toàn" đã hoàn thành việc nghiên cứu, phân tích và đánh giá các khía cạnh quan trọng của công nghệ điện toán đám mây. Đề tài đã thực hiện đầy đủ các nội dung đã đăng ký theo đề cương như sau:

- Nghiên cứu về kiến trúc tổng thể của điện toán đám mây, bao gồm mô hình dịch vụ (IaaS, PaaS, SaaS) và mô hình triển khai (Public Cloud, Private Cloud, Hybrid Cloud).
- Phân tích cơ chế hoạt động của hệ thống điện toán đám mây, bao gồm ảo hóa, phân bổ tài nguyên, quản lý dữ liệu và khả năng mở rộng linh hoạt.
- Tìm hiểu các thành phần cốt lõi của hệ thống điện toán đám mây, như máy chủ, trung tâm dữ liệu, phần mềm quản lý, API và cơ sở hạ tầng mạng.
- Đánh giá ưu và nhược điểm của điện toán đám mây, trong đó nêu bật các lợi ích như tối ưu chi phí, khả năng mở rộng, linh hoạt, cũng như những hạn chế như phụ thuộc vào nhà cung cấp, rủi ro mất dữ liệu và hiệu suất không ổn định.
- Phân tích vấn đề an ninh và an toàn, bao gồm rủi ro bảo mật, quyền riêng tư dữ liệu, tấn công mạng và các biện pháp bảo vệ như mã hóa, xác thực đa yếu tố và sao lưu dữ liệu.
- **Hướng phát triển (nêu hướng phát triển, bổ sung, nghiên cứu tiếp của BTL)**
- Đề tài này có thể được mở rộng theo các hướng sau:
- Nghiên cứu các công nghệ bảo mật tiên tiến dành cho điện toán đám mây, như Blockchain, AI trong bảo mật dữ liệu, và Zero Trust Security.
- Phát triển các giải pháp tối ưu hiệu suất trong điện toán đám mây, như phân phối tải, tối ưu hóa lưu trữ và giảm độ trễ trong truyền tải dữ liệu.
- Đánh giá tác động của điện toán đám mây đối với doanh nghiệp và ngành công nghiệp, từ góc độ kinh tế, vận hành và quản trị rủi ro.
- Khảo sát các xu hướng điện toán biên (Edge Computing) và điện toán không máy chủ (Serverless Computing) để cải thiện tốc độ xử lý và giảm chi phí vận hành.

TÀI LIỆU THAM KHẢO

[1] TS. Hoàng Trọng Minh, PGS. TS Trần Công Hùng, ThS. Nguyễn Thanh Trà. Bài giảng điện toán đám mây, Học viện Công Nghệ Bưu Chính Viễn Thông, 2022

[2] Huỳnh Quyết Thắng (chủ biên), Nguyễn Hữu Đức, Doãn Trung Tùng, Nguyễn Bình Minh, Trần Việt Trung. Điện toán đám mây, Trường Đại học bách khoa Hà Nội

[3] Các thành phần của điện toán đám mây hiện nay

[4] Điện toán đám mây là gì? Các thành phần của điện toán đám mây

[5] Cơ sở hạ tầng đám mây là gì? – Giải thích về cơ sở hạ tầng điện toán đám mây – AWS

[6] API là gì? - Giải thích về Giao diện lập trình ứng dụng - AWS

[7] 2 thành phần của dịch vụ đám mây: Front End và Back End | Tin tức

[8] Cấu trúc Đám mây là gì? Hướng dẫn về Thiết kế Đám mây

[9] Cloud Operating System (Cloud OS)

[10] Phần mềm trung gian là gì? - Giải thích về Phần mềm trung gian - AWS

[11] Platform Layer OverviewImpossible Cloud - User Interface (UI)

[12] Architecture of Cloud Computing - GeeksforGeeks

[13] A Brief History of Cloud Computing - DATAVERSITY

[14] Lịch Sử điện Toán đám Mây - DIGISTAR

[15] Ưu điểm & Nhược điểm của điện toán đám mây - Có nên dùng? - VNPT

[16] Ưu điểm và nhược điểm của Điện toán đám mây