Bài 1: Giới thiệu chung về học phần

1. Thông tin chung

\*Nội dung học phần

-Các cơ chế nền tảng của điện toán đám mây

1. Cơ sở hạ tầng đám mây

-Máy chủ

-Máy chủ nhỏ gọn

-Máy chủ dạng Rack

-Blade

-Trung tâm dữ liệu

+Hệ thống làm mát

+Nguồn dự phòng

+Hệ thống chữa cháy

+Hệ thống đảm bảo an ninh

+Hệ thống giám sát

+Hệ thống bảo đảm kết nối

1. Đám mây

-Đám mây: trung tâm dịch vụ

-Điện toán đám mây: việc chuyển đổi công nghệ thông tin từ sản phẩm sang dịch vụ

\*Các mô hình dịch vụ đám mây

IaaS < PaaS < SaaS < EaaS (everything as a service)

1. Các loại cloud

-Public cloud

-Private cloud

-Hybrid cloud

Chapter 4: Fundamental concepts and models

\*Các vai sử dụng trong cloud computing

1. Cloud provider
2. Cloud consumer
3. Cloud service owner
4. Cloud resource administrator
5. Cloud auditor
6. Cloud broker
7. Cloud carrier

Biên của dịch vụ (Boundary)

-Organization boundary

-Trust boundary

Chapter 5: Cloud-Enabling technology

1. Broadband networks and Internet architecture
2. DC technology

-Ảo hóa

-Trung tâm dữ liệu: là cơ sở hạ tầng công nghệ thông tin đặc biệt chứa tài nguyên IT tập trung như server, db, hệ thống phần mềm

1. Công nghệ ảo hóa

-Các loại tài nguyên có thể ảo hóa: server, storage, network

-Độc lập về phần cứng

Q: (i) Thiết lập máy ảo lên trên 1 máy ảo khác được ko?

(ii) Liệt kê điều kiện/hãng hệ điều hành

Tìm hiểu lỗi thiết kế trong chip Intel dẫn đến việc tốc độ của các dịch vụ trên cloud giảm đi 15-30% (kể từ giữa năm 2018 đến nay)

Lý giải: (i) cách vá lỗi; (ii) lý do vá lỗi dẫn đến chậm tốc độ máy chủ

**Chapter 7: An toàn thông tin trong điện toán đám mây**

1. Một số khái niệm

-Tính bí mật (confidentiality)

-Tính toàn vẹn (integrity)

-Tính chính xác (Authenticity)

-Tính sẵn sàng (Availability)

-Hiểm họa (threat)

-Lỗ hổng (vulnerability)

-Rủi ro (risk)

-Security controls – các biện pháp đề phòng

-Security mechanism – các thành phần tạo nên giải pháp an ninh

-Security policies – thiết lập luật/quy định

2. Tác nhân tạo hiểm họa (threat agents)

-Threat agents

->Thực thể gây ra hiểm họa

->Bên trong hoặc bên ngoài

->Con người hoặc chương trình máy tính

-Trong số các tác nhân gây ra hiểm họa

+Trusted attacker

+Malicious insiders

-> Là tác nhân nguy hiểm nhất

-Anonymous Attacker

3.Malicious an ninh trong cloud

-Nghe lén

-Sửa đổi bất hợp pháp

-Từ chối dịch vụ (DoS)

-Xác thực không đủ hiệu quả

-Tất công vào tầng ảo hóa

-Chồng lấn vùng tin tưởng

-Lỗi trong lập trình

**Chapter 10: Cơ chế an ninh trong điện toán đám mây**

1. Mã hóa

-Mã đối xứng

-Mã bất đối xứng

2. Hàm băm

3. Chữ ký số

-IAM

-SSO

-H-VSI

B.T.V.N: Khái niệm, vai trò, ví dụ về trường hợp sử dụng của chữ ký số (Digital signature) và Cơ sở hạ tầng khóa công khai (PKI – Public Key Infrastructure) trong Cloud Computing (Chuẩn bị PPT)

-Khuyến khích tìm hiểu tài liệu về công nghệ mà các hãng Amaron, Microsoft sử dụng trong nền tảng cloud của họ

**Các nội dung đã học**

1. Cơ bản
2. Công nghệ đảm bảo cho cloud computing
3. Cơ chế về an ninh, an toàn thông tin
4. Các cơ chế an ninh, an ninh thông tin trong điện toán đám mây
5. Chữ ký số
6. PKI

**Cơ chế của điện toán đám mây**

1. Logical network perimeter (LNP)

-LNP: thiết lập đường biên trên mạng ảo nhằm bao trọn và phân tách các tài nguyên IT bên cloud.

(Các tài nguyên IT đó “có thể” phân tán về mặt vật lý)

-LNP: có thể được thực thi để phân tích các tài nguyên IT từ người sử dụng cloud và điều khiển băng thông thông quan thiết bị mạng

Bao gồm: tường lửa, mạng ảo, …

1. Máy chủ ảo (Virtual Server)

-Là phần mềm ảo hóa bắt trước dịch vụ thật

-Việc ảo hóa máy chủ ảo từ “image file” thông qua tiến trình cấp phát tài nguyên nhanh chóng và theo nhu cầu

-VIM (virtual infrastructure manager)

3.

4. Trình theo dõi sử dụng cloud (Cloud usage monitor)

-Monitoring agent

-Resource agent

-Polling agent

BTVN.3:

1. Tìm hiểu các cloud services cung cấp bởi:

-Amazon;

-Microsoft;

-Google;

-IBM;

2. Xác định 01 PaaS cụ thể cho mỗi nhà cung cấp, so sánh SLA của 04 PaaS này

(G-MAFIA (Google, Microsoft, Amazon, Facebook, IBM, Apple) <> BAT (Baidu, Alibaba, Tencent))

1. Tìm hiểu các cloud services cung cấp bởi các nhà cung cấp dịch vụ của Việt Nam

Chuẩn bị ra ppt

BTVN.4:

(1) Cài đặt, sử dụng CloudSIM để thiết lập trung tâm dữ liệu trên PC

(2) Thử nghiệm với 02 cấu hình nhất định, thiết lập các request với số lượng khác nhau và đánh giá khả năng phản hồi của hệ thống.

(Và đưa vào báo cáo các hình minh họa tương ướng);

Ngày 25/09 Nộp báo cáo (bản mềm, qua email);

**Cloud computing: Architecture**

Có tổng số: 21 architecture trong cloud computing

Chapter 11: Fundamental Cloud

11.1: Workload Distribution Architecture

11.2: Resource Fooling Architecture

11.3: Dynamic Scalability Architecture

11.4: Elastic Resource Capacity Architecture

11.5: Service Load Balancing Architecture

11.6: Cloud Bursting Architecture

11.7 Elastic Disk Evisioning Architecture

11.8: Redudant Storage Architecture

Chapter 12: Advanced Cloud Architecture

12.1: Hypervisor Clustering Architecture

12.2: Load balanced Virtual Server instances architecture

12.3: Non-Disruptive service relocation architecture

12.4: Zoro downtime architecture

12.5: Cloud balancing architecture

12.6: Resource reservation architecture

12.7: Dynamic failure detection and recovery architecture

12.8: Bare-metal provisioning architecture

12.9: Rapid provisioning architecture

12.10: Storage workload management architecture

Chapter 13: Specialized cloud architectures

13.1: Direct I/O access architecture

13.2: Direct LUN access architecture

13.3: Dynamic data normalization architecture

13.4: Elastic network capacity architecture

13.5: cross-storage device vertical tiering architecture

13.6: intra-storage device vertical data tiering architecture

13.7: load balanced virtual switches architecture

13.8: multipath resource access architecture

13.9: persistent architecture configuration architecture

13.10: redundant physical connection for

Nhóm 2: Đề 1 12.1-12.2

<https://bit.ly/2HjS7C9>

1. Workload Distribution A
2. Resource Pooling (chung/gộp) A
3. Dynamic Scalability A
4. Elastic resource capacity architecture
5. Service load balancing architecture

**Hệ thống quản lý tệp GFS và HDFS**

1. Lý do cần có GFS

-GFS: google file system

-Google của 1 hệ thống quản lý trên hệ thống máy rẻ tiền và không đáng tin cậy

-GFS được thiết kế cho G-apps

-G-apps đc thiết kế cho GFS

-Giả định:

+máy tính luôn hỏng

+lượng file cần quản lý lớn

+kích thước file lớn

-Các thành phần chính

+master: chứa metadata

+chunkserver: chưa dữ liệu

+client: tạo và/hoặc sử dụng dữ liệu

B.T.V.N.5:

Các nhóm: Cài đặt máy ảo có hỗ trợ sẵn Hadoop. Cloudera Hadoop (hoặc tương đương)

-Thực hiện quản lý tệp trên HDFS (qua GUI và lệnh)

-Thực hiện copy dữ liệu giữa máy ảo (Linux) và HDFS

-Làm việc với Hadoop (xem ví dụ liên quan) và thực nghiệm các ví dụ tính toán trên nên tảng MapReduce (Word count)

Lưu ý: Lựa chọn phiên bản nhẹ nhất có thể

**Mô hình lập trình MapReduce**

\*Mô hình lập trình tuần tự:

-1 CPU

-Chương trình trên 1 máy đơn lẻ

-Hệ quản lý tệp truyền thống

-Hệ quản trị csdl quan hệ (RDBMS)

-Khi có nhiều máy -> sử dụng các hệ quản lý tệp đặc thù HDFS

-Làm sao để tận dùng nhiều máy cùng làm việc (tính toán) -> MapReduce

Làm sao ->Tính toán song song (trên 1 máy)/(trên 1 card chuyên dùng: FPGA,GPU)

-Hệ quản trị csdl cũng thay đổi SQL -> no SQL (not only SQL)

-Gợi ý cuối kỳ:

+Làm ứng dụng PaaS

+Khai thác sử dụng hệ quản trị CSDL trên Cloud

+Xây dựng ứng dụng MapReduce

+Xây dựng ứng dụng Machine Learning trên Cloud

+Thiết lập triển khai cloud (có tạo máy ảo)

Hbase

Google App Engine