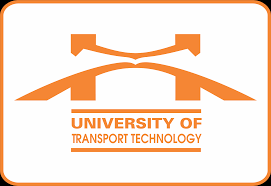
**TRƯỜNG ĐẠI HỌC CÔNG NGHỆ GIAO THÔNG VẬN TẢI**

**KHOA CÔNG NGHỆ THÔNG TIN**

**-----o0o-----**

****

**BÁO CÁO MÔN**

**ĐIỆN TOÁN ĐÁM MÂY**

**Tên đề tài:**

**Tìm hiểu về an toàn bảo mật trong công nghệ đám mây**

|  |  |
| --- | --- |
| **Giảng Viên Hướng Dẫn:** | **Mạc Văn Quang** |
| **Nhóm Thực Hiện:** | **12** |
| **Sinh Viên Thực Hiện:** | **Phùng Đức Vinh**  **Nguyễn Thế Hiệp** |

**HÀ NỘI 2023**

Mục Lục

[LỜI MỞ ĐẦU 3](#_Toc146272438)

[CHƯƠNG 1 TỔNG QUAN VỀ ĐIỆN TOÁN ĐÁM MÂY 4](#_Toc146272439)

[1.1. Định nghĩa điện toán đám mây 4](#_Toc146272440)

[1.2 Lịch sử hình thành và phát triển của điện toán đám mây 5](#_Toc146272441)

[1.3 Công nghệ ứng dụng trong điện toán đám mây 6](#_Toc146272442)

[1.4 Những ưu điểm và nhược điểm của điện toán đám mây 8](#_Toc146272443)

[1.4.1 Ưu điểm của điện toán đám mây 8](#_Toc146272444)

[1.4.2 Nhược điểm của điện toán đám mây 9](#_Toc146272445)

[1.5 Một số nhà cung cấp dịch vụ điện toán đám mây 11](#_Toc146272446)

[1.5.1 Trên thế giới 11](#_Toc146272447)

[1.5.2 Tại Việt Nam 12](#_Toc146272448)

[CHƯƠNG 2 : BẢO VỆ THÔNG TIN TRONG ĐIỆN TOÁN ĐÁM MÂY 14](#_Toc146272449)

[2.1.Khái niệm an toàn bảo mật thông tin 14](#_Toc146272450)

[2.2. Các vấn đề về an toàn bảo mật trong điện toán đám mây 15](#_Toc146272451)

[2.2.1 Phân loại bảo mật đám mây 15](#_Toc146272452)

[2.2.2 Một số vấn đề an toàn bảo mật dữ liệu trong các tầng dịch vụ 16](#_Toc146272453)

[2.2.3 Một số lỗ hổng về an toàn bảo mật trong hệ thống đám mây 19](#_Toc146272454)

[2.2.4 Một số phương pháp chủ đạo hacker thường sử dụng để tấn công kho dữ liệu đám mây 20](#_Toc146272455)

[2.3 Giải pháp bảo vệ dữ liệu cho điện toán đám mây 21](#_Toc146272456)

[2.3.1 Lập chiến lược quy trình đảm bảo an toàn bảo mật hệ thống 22](#_Toc146272457)

[2.3.2 Một số biến pháp đảm bảo an toàn bảo mật được áp dụng phổ biến trong hệ thống đám mây 22](#_Toc146272458)

# **LỜI MỞ ĐẦU**

**1.Đặt vấn đề**

Trong những năm gần đây, Điện toán đám mây (Cloud Computing, viết tắt là CC) đã có những bước tiến vượt bậc. Như chúng ta biết, CC không phải là một công nghệ gì mới, mà là sự kết hợp nhiều công nghệ trước đây. Những công nghệ này đã hoàn thiện ở các mức độ khác nhau trong những ngữ cảnh khác nhau, chúng không được thiết kế như một thể thống nhất. Tuy nhiên, chúng đã tạo ra một hệ thống kỹ thuật cho CC. Những tiến bộ mới trong bộ vi xử lý, công nghệ ảo hóa, đĩa lưu trữ, kết nối internet băng thông rộng, các máy chủ rẻ, mạnh và nhanh đã kết hợp với nhau tạo ra CC.

Các lợi ích CC đem lại cho người dùng rất lớn, trên thực tế CC đã thật sự được quan tâm và sử dụng hiệu quả ở nhiều nước phát triển trên thế giới. Khả năng giải quyết và đáp ứng tốt các nhu cầu bức thiết trong nhiều lĩnh vực. Vì vậy, CC ngày càng được các tổ chức, doanh nghiệp và cá nhân sử dụng và CC sẽ là xu hướng phát triển trong tương lai.

Tuy nhiên điều mà các tổ chức, các doanh nghiệp, hoặc cá nhân e dè khi muốn chuyển đổi các ứng dụng quan trọng trong kinh doanh sang môi trường đám mây là do những thách thức có thể gặp phải như độ tin cậy, tính bảo mật, khả năng sẵn sàng của dịch vụ và hiệu xuất hoạt động. Trong đó, vấn đề bảo mật của CC là điều mà nhiều người quan tâm nhất. Dữ liệu của khách hàng được cung cấp CC bảo mật như thế nào? Người sử dụng tự bảo mật dữ liệu làm sao?

# **CHƯƠNG 1 TỔNG QUAN VỀ ĐIỆN TOÁN ĐÁM MÂY**

## 1.1. Định nghĩa điện toán đám mây

Điện toán đám mây (Cloud computing) là một xu hướng công nghệ nổi bật trên thế giới trong những năm gần đây và có những bước phát triển nhảy vọt về cả chất lượng, quy mô cung cấp và loại hình dịch vụ, với một loạt các nhà cung cấp nổi tiếng như Google, Amazon, Saleforce, Microsoft,…

Điện toán đám mây là mô hình điện toán mà mọi giải pháp liên quan đến công nghệ thông tin đều được cung cấp dưới dạng các dịch vụ qua mạng Internet, giải phóng người sử dụng khỏi việc phải đầu tư nhân lực, công nghệ và hạ tầng để triển khai hệ thống. Từ đó điện toán đám mây giúp tối giản chi phí và thời gian triển khai, tạo điều kiện cho người sử dụng nền tảng điện toán đám mây tập trung được tối đa nguồn lực vào công việc chuyên môn.

Lợi ích của điện toán đám mây mang lại không chỉ gói gọn trong phạm vi người sử dụng nền tảng điện toán đám mây mà còn từ phía các nhà cung cấp dịch vụ điện toán. Theo những đánh giá của nhóm IBM CloudBurst năm 2009, trên môi trường điện toán phân tán có đến 85% tổng năng lực tính toán trong trạng thái nhàn rỗi, thiết bị lưu trữ tăng 54% mỗi năm, khoảng 70% chi phí được dành cho việc duy trì các hệ thống thông tin. Công nghiệp phần mềm mất đi 40 tỷ USD hằng năm vì việc phân phối sản phẩm không hiệu quả, khoảng 33% khách hàng phàn nàn về các lỗi bảo mật do các công ty cung cấp dịch vụ. Những thống kê này đều chỉ đến một điểm quan trọng: mô hình hệ thống thông tin hiện tại đã lỗi thời và kém hiệu quả, cần phải chuyển sang một mô hình điện toán mới – đó là điện toán đám mây.

Theo định nghĩa của Viện Quốc gia Tiêu chuẩn và Công nghệ Mỹ (US NIST), điện toán đám mây là mô hình cho phép truy cập trên mạng tới các tài nguyên được chia sẻ (ví dụ: hệ thống mạng, máy chủ, thiết bị lưu trữ, ứng dụng và các dịch vụ) một cách thuận tiện và theo nhu cầu sử dụng. Những tài nguyên này có thể được cung cấp một cách nhanh chóng hoặc thu hồi với chi phí quản lý tối thiểu hoặc tương tác tối thiểu với nhà cung cấp dịch vụ.

Như vậy điện toán đám mây có thể coi là bước tiếp theo của ảo hóa, bao gồm ảo hóa phần cứng và ứng dụng, là thành phần quản lý, tổ chức, vận hành các hệ thống ảo hóa trước đó.

Điện toán đám mây có các đặc điểm chính sau :

*Tự phục vụ theo nhu cầu (On-Deman self-service):* Người sử dụng có thể tự cung cấp tài nguyên như máy chủ ảo, tài khoản, email… mà không cần có người tương tác với nhân viên của nhà cung cấp dịch vụ (nhân viên công nghệ thông tin).

*Mạng lưới truy cập rộng lớn (Broad Network Access):* Khách hàng có thể truy cập tài nguyên qua mạng máy tính (như mạng Internet) từ nhiều thiết bị khác nhau (điện thoại thông minh, máy tính bảng, máy tính xách tay...).

*Tài nguyên được chia sẻ (Resource Pooling):* Tài nguyên của các nhà cung cấp dịch vụ được chia sẻ tới nhiều khách hàng. Thông thường, các công nghệ ảo hóa được sử dụng để cho nhiều bên cùng thuê và cho phép tài nguyên được cấp phát động dựa theo nhu cầu của khách hàng.

*Tinh linh hoạt nhanh (Rapid elasticity):* Tài nguyên có thể được cung cấp và giải phóng nhanh, tự động dựa trên nhu cầu. Khách hàng có thể tăng hoặc giảm việc sử dụng dịch vụ đám mây một cách dễ dàng theo nhu cầu hiện tại của mình.

*Ước lượng dịch vụ (Measured service):* Khách hàng chỉ chi trả cho tài nguyên thực tế họ đã sử dụng. Thông thường, nhà cung cấp dịch vụ sẽ cung cấp cho khách hàng bảng điều khiển (dashboard) để họ có thể theo dõi việc sử dụng dịch vụ của họ.

Điện toán đám mây đã khắc phục được yếu điểm quan trọng của điện toán truyền thống về khả năng mở rộng và độ linh hoạt. Các công ty, tổ chức có thể triển khai ứng dụng và dịch vụ nhanh chóng, giảm chi phí và ít rủi ro về đầu tư.

## 1.2 Lịch sử hình thành và phát triển của điện toán đám mây

Khái niệm điện toán đám mây ra đời từ những năm 1950 khi máy chủ tính toán quy mô lớn (large-scale mainframe computers) được triển khai tại một số cơ sở giáo dục và tập đoàn lớn. Tài nguyên tính toán của các hệ thống máy chủ được truy cập từ các máy khách cuối (thin clients, terminal computers), từ đó khai sinh khái niệm "chia sẻ thời gian" (time- sharing) đặc tả việc cho phép nhiều người sử dụng cùng chia sẻ đồng thời một tài nguyên tính toán chung.

Trong những năm 1960 – 1990, xuất hiện luồng tư tưởng coi máy tính hay tài nguyên công nghệ thông tin có thể được tổ chức như hạ tầng dịch vụ công cộng (public utility). Điện toán đám mây hiện tại cung cấp tài nguyên tính toán dưới dạng dịch vụ và tạo cảm giác cho người dùng về một nguồn cung ứng là vô tận. Đặc tính này có thể so sánh tới các đặc tính của ngành công nghiệp tiêu dùng dịch vụ công cộng như điện và nước. Khi sử dụng điện hay nước, người dùng không cần quan tâm tới tài nguyên đến từ đâu, được xử lý, phân phối như thế nào, họ chỉ việc sử dụng dịch vụ và trả tiền cho nhà cung cấp theo lượng tiêu dùng của mình.

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.

Amazon cung cấp nền tảng Amazon Web Services (AWS) vào năm 2006, đánh dấu việc thương mại hóa điện toán đám mây. Từ đầu năm 2008, Eucalyptus được giới thiệu là nền tảng điện toán đám mây mã nguồn mở đầu tiên, tương thích với API của AWS. Tính tới thời điểm hiện tại, có rất nhiều các sản phẩm điện toán đám mây được đưa ra như Google App Engine, Microsoft Azure, Nimbus,...

## 1.3 Công nghệ ứng dụng trong điện toán đám mây

**Công nghệ ảo hóa**

Công nghệ ảo hóa (virtualization) là công nghệ quan trọng nhất ứng dụng trong điện toán đám mây. Công nghệ ảo hóa là công nghệ cho phép tạo ra các thực thể ảo có tính năng tương đương như các thực thể vật lý, ví dụ như thiết bị lưu trữ, bộ vi xử lý,... Ảo hóa phần cứng (hardware virtualization) tham chiếu tới việc tạo ra các máy ảo (virtual machine) mà hoạt động với hệ điều hành được cài đặt như một máy tính vật lý thực. Ví dụ, một máy ảo chạy hệ điều hành Ubuntu có thể được tạo ra trên một máy tính thực cài hệ điều hành Windows.

Ảo hoà phần cứng cho phép chia nhỏ tài nguyên vật lý để tối ưu hóa hiệu năng sử dụng. Điều này được thể hiện qua việc có thể khởi tạo nhiều máy ảo với năng lực tính toán và năng lực lưu trữ bé hơn trên duy nhất một máy chủ vật lý. Máy chủ vật lý được gọi là host machine còn máy ảo (virtual machine) được gọi là máy khách (guest machine). Khái niệm "host" và "guest" được sử dụng để phân biệt phần mềm chạy trên máy tính vật lý hay phần mềm chạy trên máy ảo. Phần mềm hay firmware tạo máy ảo được gọi là hypervisor hay virtual machine manager.

**Công nghệ tự động hóa giảm sút điều phối tài nguyên**

Công nghệ giám sát điều phối tài nguyên động là nền tảng để điện toán đám mây thực hiện cam kết chất lượng cung cấp dịch vụ điện toán. Với công nghệ điều phối tài nguyên động, việc lắp đặt thêm hay giảm bớt các tài nguyên máy chủ vật lý hoặc máy chủ lưu trữ dữ liệu được thực hiện tự động để hệ thống điện toán luôn đáp ứng được giao kèo trong hợp đồng dịch vụ đã ký với bên người sử dụng.

**Công nghệ phân tán, hệ phân tán**

Điện toán đám mây là một dạng hệ phân tán xuất phát từ yêu cầu cung ứng dịch vụ cho lượng người sử dụng khổng lồ. Tài nguyên tính toán của điện toán đám mây là tổng thể kết hợp của hạ tầng mạng và hàng nghìn máy chủ vật lý phân tán trên một hay nhiều trung tâm dữ liệu số (data centers).

**Công nghệ Web 2.0**

Web 2.0 là nền tảng công nghệ phát triển các sản phẩm ứng dụng hướng dịch vụ trên nền điện toán đám mây. Công nghệ Web 2.0 phát triển cho phép phát triển giao diện ứng dụng web dễ dàng và nhanh chóng và trên nhiều thiết bị giao diện khác nhau. Web 2.0 phát triển làm xóa đi khoảng cách về thiết kế giao diện giữa ứng dụng máy tính thông thường và ứng dụng trên nền web, cho phép chuyển hóa ứng dụng qua dịch vụ trên nền điện toán đám mây mà không ảnh hưởng đến thói quen người sử dụng.

## 1.4 Những ưu điểm và nhược điểm của điện toán đám mây

### **1.4.1 Ưu điểm của điện toán đám mây**

*Triển khai nhanh chóng:* So với phương pháp thông thường triển khai một ứng dụng trên internet, người dùng phải thực hiện một loạt các công việc như mua sắm thiết bị (hoặc thuê thiết bị từ bên thứ ba), cài đặt và cấu hình phần mềm, đưa các ứng dụng vào đám mây, việc sử dụng điện toán đám mây giúp loại bỏ một số công việc đòi hỏi thời gian lớn. Bên cạnh đó, khả năng tăng hoặc giảm sự cung cấp tài nguyên nhanh chóng theo nhu cầu tiêu dùng của ứng dụng tại các thời điểm khác nhau nhờ công nghệ ảo hóa của điện toán đám mây cũng là một trong những đặc điểm vượt trội của công nghệ này, thể hiện khả năng triển khai nhanh đáp ứng đòi hỏi tài nguyên tức thời của ứng dụng.

*Giảm chi phí:* Chi phí được giảm đáng kể do chi phí vốn đầu tư được chuyển sang chi phí duy trì hoạt động. Điều này làm giảm những khó khăn khi người dùng cần tính toán xử lý các tác vụ trong một lần duy nhất hoặc không thường xuyên do họ có thể đi thuê cơ sở hạ tầng được cung cấp bởi bên thứ ba.

*Đa phương tiện truy cập:* Sự độc lập giữa thiết bị và vị trí làm cho người dùng có thể truy cập hệ thống bằng cách sử dụng trình duyệt web mà không quan tâm đến vị trí của họ hay thiết bị nào mà họ đang dùng, ví dụ như PC, mobile. Vì cơ sở hạ tầng off-site (được cung cấp bởi đối tác thứ ba) và được truy cập thông qua Internet, do đó người dùng có thể kết nổi từ bất kỳ nơi nào.

*Chia sẻ:* Việc cho thuê và chia sẻ tài nguyên giữa các người dùng với nhau làm giảm chỉ phí đầu tư hạ tầng tính toán giữa một phạm vi lớn người dùng. Sự chia sẻ này cũng cho phép tập trung cơ sở hạ tầng để phục vụ các bài toán lớn với chi phí thấp hơn việc đầu tư hệ thống máy chủ tính toán từ đầu.

*Độ tin cậy:* Nền tảng đám mây thiết kế bảo trì bởi đội ngũ chuyên gia nhiều kinh nghiệm về hệ thống. Quá trình khôi phục sao lưu sau sự cố thường nhanh chóng do luôn làm việc với hệ thống lớn và gặp lỗi tương tự nhau.

*Tính co dãn linh động:* Tính co dãn thể hiện sự linh động trong việc cung cấp tài nguyên tính toán theo nhu cầu thực tế của người dùng hoặc các ứng dụng dịch vụ.

*Bảo mật:* Các nhà cung cấp luôn chú trọng nâng cao công nghệ và đặt ra những rào cản để tăng tính an toàn cho dữ liệu. Nhà cung cấp dành nhiều nguồn lực cho việc giải quyết các vấn đề bảo mật mà nhiều khách hàng không có đủ chi phí để thực hiện.

### **1.4.2 Nhược điểm của điện toán đám mây**

*Chi phí:* Giảm chi phí đầu tư ban đầu là ưu điểm của điện toán đám mây. Tuy nhiên, nó cũng là một vấn đề phải tranh cãi khi người sử dụng điện toán đám mây luôn phải duy trì trả phí sử dụng dịch vụ. So với tự chủ đầu tư hạ tầng, người sử dụng điện toán đám mây không có tài sản sau khấu hao chi phí đầu tư.

*Các công cụ giám sát và quản lý:* Công cụ giám sát và bảo trì chưa hoàn thiện và khả năng giao tiếp với các đám mây là có giới hạn, mặc dù thông báo gần đây của BMC, CA Novell cho rằng các ứng dụng quản lý trung tâm dữ liệu đang được cải tiến để cung cấp kiểm soát tốt hơn dữ liệu trong điện toán đám mây Amazon EC2 và các dịch vụ đám mây.

*Chuẩn hóa đám mây:* Chuẩn hóa giao tiếp và thiết kế đám mây chưa được thông qua. Mỗi nền tảng cung cấp các giao diện quản lý và giao tiếp ứng dụng API khác nhau. Hiện nay, các tổ chức như Distributed Management Task Force, Cloud Security Alliance và Open Cloud Consortium đang phát triển các tiêu chuẩn về quản lý tương thích, di chuyển dữ liệu, an ninh và các chức năng khác của điện toán đám mây.

*Tính sẵn sàng:* Tính sẵn sàng là ưu điểm của đám mây trong lý thuyết. Tuy nhiên, trên thực tế với các đám mây hiện thời, tính sẵn sàng đôi khi không được đảm bảo và cũng là một trở ngại hiện nay, khi chỉ có một số ít nhà cung cấp dịch vụ cam kết được về sự sẵn sàng và liên tục của dịch vụ, về thời gian sửa chữa và phục hồi dữ liệu.

*Vấn đề tuân thủ hợp đồng cũng trở nên phức tạp:* Những nhà cung cấp dịch vụ điện toán đám mây có thể chuyển dữ liệu tới quốc gia khác có giá điện rẻ hơn, nhưng luật lỏng lẽo hơn mà người sử dụng dịch vụ điện toán không được thông tin. Điều này hoàn toàn có thể vì đám mây là trong suốt với người dùng.

*Tính riêng tư:* Hầu hết các hợp đồng thể hiện giao kèo giữa nhà cung cấp và người dùng điện toán đám mây hứa hẹn một viễn cảnh trong đó dữ liệu khách hàng luôn an toàn và riêng tư. Tuy nhiên, tính riêng tư trong điện toán đám mây cũng là một vấn đề đáng quan tâm vì hạ tầng an toàn thông tin cho đám mây hiện vẫn đang là một chủ đề nghiên cứu trong giới khoa học.

*Cấp độ dịch vụ:* Điện toán đám mây cung cấp dịch vụ theo yêu cầu, tuy nhiên trong thực tế, các gói dịch vụ thường được định nghĩa trước và người sử dụng căn cứ vào nhu cầu và khả năng để chọn dịch vụ sẵn có. Ví dụ, việc tự cấu hình chi tiết thông số các máy ảo hiện tại chưa thực hiện được. Như vậy, khả năng để thích ứng yêu cầu cấp dịch vụ cho các nhu cầu cụ thể của một doanh nghiệp là ít hơn so với các trung tâm dữ liệu xây dựng riêng với mục đích là để tiếp tục mục tiêu nâng cao khả năng kinh doanh của công ty.

*Khả năng tích hợp với hạ tầng thông tin sẵn có của tổ chức:* Việc tích hợp điện toán đám mây vào hạ tầng sẵn có của khách hàng chưa có mô hình và cách thức thực hiện cụ thể. Các mô hình kết nối đám mây riêng và đám mây thương mại vẫn đang được nghiên cứu.

## 1.5 Một số nhà cung cấp dịch vụ điện toán đám mây

### **1.5.1 Trên thế giới**

**1. Microsoft**

Microsoft Azure được xem là nền tảng dịch vụ đám mây tốt nhất hiện nay. Công nghệ được phát triển bởi Microsoft từ năm 2010. Nó cung cấp hàng loạt các gói giải pháp phù hợp với mọi loại hình kinh doanh. Doanh nghiệp có thể chạy bất kỳ dịch vụ nào trên đám mây của họ. Hoặc bạn có thể kết hợp nó với trung tâm dữ liệu hoặc hạ tầng đang có. Với Azure, người dùng được hỗ trợ di chuyển dữ liệu lên cloud dễ dàng và nhanh chóng hơn. Đồng thời, giúp tiết kiệm chi phí về cơ sở hạ tầng và vận hành máy chủ tại chỗ.

**2. Amazon Web Service (AWS)**

Amazon Web Service (AWS) là một nền tảng đám mây phổ biến nhất. Amazon cung cấp một loạt các dịch vụ IaaS, PaaS và sử dụng những dịch vụ web tích hợp để xây dựng các giải pháp doanh nghiệp. AWS là đơn vị đầu tiên cung cấp hạ tầng điện toán đám mâynhư một dịch vụ năm 2008. AWS cung cấp quyền quản trị rộng rãi. Và luôn sẵn sàng thông qua một trang web khách hàng đảm bảo tính bảo mật. Đồng thời, AWS cho phép người dùng tối ưu hóa hạ tầng theo nhu cầu. Và người dùng có 3 sự lựa chọn chi trả khác nhau là “dùng đến đâu trả đến đó”, “tiết kiệm khi đặt chỗ trước và “sử dụng nhiều hơn, trả ít hơn”.

**3. Google Cloud Platform (GCP)**

Google là nhà cung cấpđiện toán đám mây mạnh mẽ. Google Cloud Platform (GCP) cung cấp một loạt các dịch vụ bao gồm những giải pháp IaaS, PaaS. Điều này cho phép người dùng tạo giải pháp kinh doanh bằng dịch vụ web mô-đun do Google cung cấp. Hạ tầng bảo mật nhiều lớp của GCP giúp cho dữ liệu lưu trữ của người dùng được bảo vệ. Thêm vào đó, Google Cloud Platform bao gồm nhiều công cụ đảm bảo hiệu suất và quản lý nhất quán, mang đến các giải pháp đám mây linh hoạt và hiệu quả.

**4. IMB Cloud**

IBM Cloud là các dịch vụ điện toán đám mâybởi công ty công nghệ nổi tiếng IBM. Giải pháp này cung cấp PaaS, SaaS và IaaS, dựa trên cả máy chủ ảo, máy chủ vật lý, mạng công cộng và mạng quản lý. Dịch vụ đám mây IBM Cloud trao cho người dùng toàn quyền quản lý và truy cập duy nhất vào cơ sở hạ tầng. Điều này giúp cải thiện tối đa hiệu suất làm việc. Đồng thời, IBM cũng cung cấp khả năng tùy biến tài nguyên máy chủ ở mức cao nhất. Công nghệ giúp doanh nghiệp hoàn toàn chủ động trong việc chi trả cho những gì mình sử dụng.

**5 .Oracle Cloud Infrastructure**

Hạ tầng Oracle Cloud là một dịch vụ đám mây khác từ công ty điện toán khổng lồ Oracle Corp. Các dịch vụ của Oracle đặc biệt mạnh mẽ trong việc hỗ trợ những công việc khác nhau. Đặc biệt là IoT, OLTP, AI và machine learning. Hai dịch vụ chính gồm: kiến trúc đám mây và lưu trữ dữ liệu. Chúng được thiết kế để phục vụ cho nhu cầu của các doanh nghiệp và tập đoàn lớn, về quản lý dữ liệu, cơ sở dữ liệu, ứng dụng; các công cụ quản lý, truyền thông xã hội, phân tích dữ liệu lớn (Big Data) cho thông tin chi tiết về kinh doanh.

**6. Vmware Cloud**

VMware là công ty ảo hóa hàng đầu thế giới. Nền tảng đám mây cung cấp toàn quyền truy cập vào dữ liệu và ứng dụng từ nhiều thiết bị. Đồng thời cung cấp một cấu trúc phần mềm tích hợp ngay từ ban đầu và có thể được sử dụng tại chỗ. Nhờ đó, doanh nghiệp để triển khai môi trường điện toán đám mâyriêng hoặc dưới dạng dịch vụ từ môi trường điện toán đám mây công cộng với những thao tác vận hành đơn giản và đồng nhất.

### **1.5.2 Tại Việt Nam**

**1. Viettel Cloud**

Nền tảng Viettel Cloud được ra mắt vào năm 2018 và hiện sở hữu 5 trung tâm dữ liệu đạt chuẩn quốc tế với hơn 23.000 m2 sàn, 4.000 racks thiết bị.

Các nền tảng Cloud của Viettel tập trung ứng dụng cho các lĩnh vực viễn thông, an ninh mạng, CNTT với số lượng tài nguyên là hơn 17.000 máy chủ có năng lực lưu trữ trên 30.000 Terabyte dữ liệu.

**2. VNG Cloud**

VNG chính thức cung cấp dịch vụ Cloud Server vào năm 2018 và chính thức đổi tên thành VNG Cloud và năm 2019. VNG Cloud được tập trung vào việc cung cấp giải pháp cho nhiều ngành công nghiệp với các sản phẩm dịch vụ đi kèm hỗ trợ. Đây cũng là đơn vị đồng hành cùng các StartUp trong chương trình Shark Tank và Start Up Wheel.

**3. CMC Cloud**

Là Nhà cung cấp dịch vụ cloud từ rất sớm vào năm 2017, [CMC Cloud](https://cloud.cmctelecom.vn/) được cho là nền tảng điện toán đám mây tiên phong cung cấp dịch vụ cloud server có chất lượng ổn định tại Việt Nam. CMC Cloud cũng là nền tảng điện toán đám mây duy nhất tại Việt Nam hiện đang kết nối trực tiếp tới nền tảng điện toán đám mây của 3 hãng công nghệ lớn là AWS, Microsoft và Google. Bên cạnh đó Nhà cung cấp CMC Cloud là CMC Telecom còn là Nhà cung cấp dịch vụ [hội tụ](https://cmctelecom.vn/) và tích hợp đa dịch vụ CNTT trên nền tảng điện toán đám mây từ kênh truyền internet, Thoại, Giải Pháp tổng đài, Cloud Camera, CDN, … nên có khả năng cung cấp dịch vụ đa dạng. Riêng nền tảng CMC Cloud hiện có trên 30 giải pháp dịch vụ đáp ứng nhu cầu của doanh nghiệp SME, ENT, các mô hình tập đoàn, … trong và ngoài nước.

**4. BizFly**

BizFly là nền tảng điện toán đám mây của VCCorp, vốn xuất thân từ một đơn vị hoạt động trong lĩnh vực báo chí truyền thông. Vào năm 2018 thì giải pháp VCCloud của VCCorp chính thức được đổi tên thành BizFly và ra mắt hệ sinh thái BizFly Cloud với 15 dịch vụ đáp ứng hầu hết các nhu cầu về hạ tầng cho doanh nghiệp.

**CHƯƠNG 2 : BẢO VỆ THÔNG TIN TRONG ĐIỆN TOÁN ĐÁM MÂY**

**2.1.Khái niệm an toàn bảo mật thông tin**

An toàn bảo mật thông tin là một tập hợp các biện pháp, quy tắc và các công nghệ được sử dụng để bảo vệ thông tin quan trọng khỏi sự truy cập, sử dụng, tiết lộ, sửa đổi hoặc hủy hoại trái phép. Trong ngữ cảnh công nghệ thông tin và cloud computing, an toàn bảo mật thông tin là một khía cạnh quan trọng để đảm bảo rằng dữ liệu và các tài nguyên liên quan đến dữ liệu được bảo vệ khỏi các mối đe dọa và rủi ro. Dưới đây là một số lý do vì sao phải thiết lập bảo mật trong công nghệ cloud:

+Bảo vệ Dữ liệu Khách Hàng: Các tổ chức lưu trữ dữ liệu của khách hàng trên các nền tảng cloud. Việc thiết lập bảo mật đảm bảo rằng thông tin cá nhân và dữ liệu quan trọng của khách hàng được bảo vệ khỏi việc truy cập trái phép.

+Đối phó với Các Mối Đe Dọa Mới: Các mối đe dọa và phương thức tấn công liên tục thay đổi và phát triển. Thiết lập bảo mật trong công nghệ cloud cho phép các tổ chức duyệt qua các biện pháp bảo mật mới và điều chỉnh chiến lược bảo mật để đối phó với chúng.

+Bảo Vệ Khỏi Mất Mát Dữ Liệu: Dữ liệu quan trọng có thể mất mát do lỗi kỹ thuật, lỗi người dùng hoặc tấn công mạng. Các biện pháp bảo mật trong công nghệ cloud giúp bảo vệ dữ liệu khỏi mất mát hoặc hỏng hóc.

+Tuân thủ Quy định: Nhiều quy định và luật pháp yêu cầu các tổ chức bảo vệ thông tin cá nhân và dữ liệu khách hàng. Thiết lập bảo mật trong công nghệ cloud giúp các tổ chức tuân thủ các quy định này, tránh vi phạm pháp luật và các hình phạt liên quan.

+Bảo vệ Khỏi Mất Kiểm Soát: Cloud computing thường bao gồm việc chia sẻ tài nguyên với các dịch vụ bên ngoài. Việc thiết lập bảo mật đảm bảo rằng các tổ chức không mất kiểm soát hoặc kiểm soát một cách nghiêm ngặt việc sử dụng các tài nguyên này.

+Xây Dựng Tinh Thần Tin Tưởng: Bảo mật là một yếu tố quan trọng để xây dựng tinh thần tin tưởng của khách hàng. Khách hàng sẽ cảm thấy an tâm hơn khi biết rằng dữ liệu của họ được bảo vệ chặt chẽ trên các nền tảng cloud.

+Giảm Rủi Ro Kinh Tế: Một việc vi phạm bảo mật có thể dẫn đến các tổn thất kinh tế đáng kể, bao gồm chi phí khôi phục, phạt và thiệt hại về danh tiếng. Bảo mật tốt giúp giảm thiểu rủi ro kinh tế này.

## 2.2. Các vấn đề về an toàn bảo mật trong điện toán đám mây

### **2.2.1 Phân loại bảo mật đám mây**

Hiện tại được chia ra thành 3 kiểu Cloud cần được bảo mật đó là: Private (cá nhân), Public (công cộng) và Hybrid. Mỗi loại đều có một tính năng riêng phụ thuộc vào mức độ cần thiết của doanh nghiệp

Private Compute Cloud (cơ sở hạ tầng điện toán đám mây cá nhân) được đặt tại các trung tâm dữ liệu của khách hàng hoặc tại các nhà cung cấp dịch vụ, bao gồm ảo hóa và mạng được định nghĩa phần mèm (SDN). Toàn bộ khối lượng công việc của khách hàng chạy trên các Server riêng, kho lưu trữ dành riêng và ở cấp độ của các thiết bị kết nối vật lý riêng biệt cho một khách hàng. Tất cả được tổng hợp lại và chia sẻ trên mạng, hay mạng nội bộ công ty, trên Internet, hhách hàng cũng có thể cài đặt cách truy cập kết nối chia sẻ cho riêng mình,

Public Compute Cloud (cơ sở hạ tầng điện toán đám mây công cộng) cũng được đặt tại trung tâm dữ liệu của khách hàng nhưng chỉ khác với các đám mây cá nhân là đám mây công cộng cung cấp tại nhiều vị trí địa lý, mở rộng phạm vi hơn. Khối lượng công việc đang được di chuyển sang các đám mây IaaS như AWS và Azure, và áp dụng các ứng dụng phần mềm như một dịch vụ SaaS. Do đó mà toàn bộ khối lượng công việc của khách hàng trên các máy chủ vật lý hay kho lưu trữ vật lý và kết nối vật lý đều được chia sẻ công khai giữa các khách hàng với nhau. Tuy mọi công việc đều chia sẻ công khai giữa các khách hàng nhưng không có nghĩa là mỗi khách hàng đều có quyền truy cập vào hệ thống lẫn nhau.

Hybrid Cloud đơn thuần chỉ là một phần trong cơ sở điện toán đám mây của khách hàng lai giữa phần cứng và phần mềm, nằm giữa Private Cloud và Public Cloud

### **2.2.2 Một số vấn đề an toàn bảo mật dữ liệu trong các tầng dịch vụ**

Công nghệ điện toán đám mây hay ảo hóa máy chủ bao gồm các thành phần là tài nguyên vật lý, các phần mềm ảo hóa, máy ảo, hệ điều hành. Tuy nhiên những thành phần này đều tồn tại các vấn đề bảo mật.

*Vấn đề 1. Bảo mật ứng dụng*

Người sử dụng thường truy nhập các ứng dụng đám mây thông qua trình duyệt web. Sai sót trong các trang web có thể tạo nên những lỗ hổng của dịch vụ SaaS. Tin tặc từ đó có thể gây thương tổn tới các máy tính của người sử dụng để thực hiện các hành vi ác ý hoặc ăn trộm các thông tin nhạy cảm. ATBM trong dịch vụ SaaS không khác với trong các ứng dụng web thông thường. Có thể tham khảo thêm về những vấn đề ATBM ứng dụng web thông qua bài viết “The most critical web application security risks” do OWASP (Open Web Application Security Project) xuất bản.

*Vấn đề 2. Nhiều người thuê đồng thời (multi-tenancy)*

Các dịch vụ SaaS có thể được xây dựng theo ba mô hình:

- Mô hình khả mở (scalability model): Mỗi người sử dụng được cấp một thể hiện đã chuyên biệt hóa của phần mềm. Mặc dù có nhiều nhược điểm, nhưng mô hình này lại không tạo nên những vấn đề lớn về an toàn và bảo mật.

- Mô hình cấu hình qua siêu dữ liệu (configurability via metadata): Mỗi người cũng có một thể hiện riêng của phần mềm, tuy nhiên các thể hiện này dùng chung một mã nguồn, sự khác biệt chỉ là cấu hình của phần mềm thông qua các siêu dữ liệu.

- Mô hình nhiều người thuê đồng thời: Trong mô hình này, một thể hiện duy nhất của ứng dụng được chia sẻ cho nhiều người thuê. Khi đó tài nguyên sẽ được sử dụng hiệu quả (mặc dù tính khả mở sẽ giảm đi). Trong mô hình này, do dữ liệu của các người dùng được lưu trữ trên cùng một cơ sở dữ liệu nên nguy cơ về rò rỉ dữ liệu có thể xảy ra.

*Vấn đề 3. Bảo mật dữ liệu*

Trong SaaS, dữ liệu thường được xử lý dưới dạng bản rõ và được lưu trữ trên đám mây. Nhà cung cấp dịch vụ SaaS sẽ phải chịu trách nhiệm về bảo mật dữ liệu trong khi chúng được xử lý và lưu trữ. Việc sao lưu dữ liệu rất phổ biến trong các hệ thống đám mây cũng tạo nên những vấn đề phát sinh cho bảo mật dữ liệu, nhất là khi nhà cung cấp dịch vụ ký hợp đồng sao lưu lại với một đối tác thứ ba không đáng tin cậy.

*Vấn đề 4. Truy cập dịch vụ*

Việc các dịch vụ SaaS hỗ trợ khả năng truy cập thông qua trình duyệt mang lại nhiều thuận lợi, ví dụ như chúng có thể dễ dàng được truy cập từ các thiết bị kết nối mạng khác PC như điện thoại hay máy tính bảng. Tuy nhiên, điều này lại tạo nên những nguy cơ mới về ATBM như các phần mềm ăn trộm dữ liệu trên di động, mạng Wifi không an toàn, kho ứng dụng không an toàn,...

*An toàn và bảo mật trong các dịch vụ nền tảng*

PaaS hỗ trợ việc xây dựng các ứng dụng đám mây mà không cần quan tâm tới vấn đề thiết lập và duy trì hạ tầng phần cứng hay môi trường phần mềm. Vấn đề ATBM trong PaaS liên quan tới hai khía cạnh: bảo mật trong nội tại của dịch vụ PaaS và bảo mật trong phần mềm của khách hàng triển khai trên nền dịch vụ PaaS. Nội dung tiếp theo giới thiệu một số vấn đề về ATBM trong tầng dịch vụ nền tảng.

*Vấn đề 5. An toàn và bảo mật của bên thứ ba*

Dịch vụ PaaS thường không chỉ cung cấp môi trường phát triển ứng dụng của nhà cung cấp dịch vụ mà đôi khi cho phép sử dụng những dịch vụ mạng của bên thứ ba. Những dịch vụ này thường được đóng gói dưới dạng thành phần trộn (mashup). Chính vì vậy, ATBM trong các dịch vụ PaaS cũng phụ thuộc vào ATBM của chính các mashup này.

*Vấn đề 6. Vòng đời của ứng dụng*

Việc cung cấp ứng dụng đòi hỏi nhà cung cấp dịch vụ PaaS phải hỗ trợ tốt cho những thay đổi của ứng dụng. Đồng thời, người phát triển cần phải lưu ý rằng sự thay đổi của các thành phần ứng dụng trong quá trình nâng cấ đôi khi gây các vấn đề về an toàn bảo mật.

*Vấn đề 7. Ảo hóa*

Công nghệ ảo hóa cho phép người sử dụng dễ dàng tạo lập, sao chép, chia sẻ, di trú và phục hồi các máy ảo trên đó thực thi các ứng dụng. Công nghệ này tạo nên một tầng phần mềm mới trong kiến trúc phần mềm của hệ thống. Chính vì vậy nó cũng mang đến những nguy cơ mới về ATBM.

*Vấn đề 8. Giám sát máy ảo*

Thành phần giám sát máy ảo (virtual machine monitor – VMM) hay còn gọi là supervisor có trách nhiệm giám sát và quản lý các máy ảo được tạo trên máy vật lý. Chính vì vậy, nếu VMM bị tổn thương, các máy ảo do nó quản lý cũng có thể bị tổn thương. Di trú máy ảo từ một VMM này sang một VMM khác cũng tạo nên những nguy cơ mới về ATBM.

*Vấn đề 9. Tài nguyên chia sẻ*

Các máy ảo trên cùng một hệ thống chia sẻ một số tài nguyên chung như CPU, RAM, thiết bị vào ra,... Việc chia sẻ này có thể làm giảm tính ATBM của mỗi máy ảo. Ví dụ, một máy ảo có thể đánh cắp thông tin của máy ảo khác thông qua bộ nhớ chia sẻ. Hơn nữa nếu khai thác một số kênh giao tiếp ngầm giữa các máy ảo, các máy ảo có thể bỏ qua mọi quy tắc bảo mật của VMM.

*Vấn đề 10. Kho máy ảo công cộng*

Trong môi trường IaaS, ảnh máy ảo là một mẫu sẵn có để tạo nên các máy ảo. Một hệ thống đám mây có thể cung cấp một số ảnh máy ảo trong một kho công cộng để người dùng có thể dễ dàng tạo nên máy ảo theo nhu cầu của mình. Đôi khi hệ thống đám mây có thể cho phép người sử dụng tự tải ảnh máy ảo của mình lên kho công cộng này. Điều này tạo nên một nguy cơ về bảo mật khi tin tặc tải lên những ảnh máy ảo có chứa mã độc và người sử dụng có thể dùng những ảnh này để tạo máy ảo của họ. Hơn nữa, qua việc tải ảnh máy ảo lên kho công cộng, người dùng cũng có nguy cơ mất đi những dữ liệu nhạy cảm của mình trong ảnh máy ảo đã tải. Ảnh máy ảo cũng tạo ra nguy cơ về bảo mật khi chúng không được vá lỗi giống như các hệ thống đang vận hành.

Vấn đề 11. Phục hồi máy ảo

Người sử dụng có thể phục hồi máy ảo về một trạng thái đã được lưu trữ trước đó. Tuy nhiên, nguy cơ về ATBM lại phát sinh khi những lỗi được vá mới không áp dụng cho trạng thái máy ảo cũ

*Vấn đề 12. Mạng ảo*

Mạng ảo có thể được chia sẻ bởi nhiều người thuê trong một vùng chứa tài nguyên. Khi đó, các vấn đề ATBM có thể phát sinh giữa các người thuê chia sẻ chung mạng ảo này như việc một máy ảo có thể nghe trộm các bản tin gửi cho máy ảo khác trên cùng mạng.

### **2.2.3 Một số lỗ hổng về an toàn bảo mật trong hệ thống đám mây**

**Giao diện người dùng sử dụng API không an toàn**

**-**Chứng nhận sử dụng hợp lệ yếu

-Việc kiểm tra xác quyền không đủ

-Thiếu kiểm tra tính hợp lệ của dữ liệu

**Tài nguyên phân bố không giới hạn**

Hệ thống có thể gặp phải tình huống dành sẵn quá nhiều tài nguyên nếu như việc đánh giá về tài nguyên sử dụng không chính xác.

**Các lỗ hổng liên quan đến dữ liệu**

-Khả năng phân tách yếu cho những dữ liệu có nguồn gốc khác nhau nhau dẫn đến chúng dễ bị đánh cắp.

-Dữ liệu không xóa được hoàn toàn.

-Dữ liệu sao lưu bởi bên thứ 3 không đáng tin cậy.

-Người sử dụng thường không biết vị trí lưu trữ dữ liệu.

-Dữ liệu thường được lưu trữ,di chuyển và xử lý dưới dạng bản rõ.

**Lỗ hổng trong máy ảo**

**-**Tồn tại những kênh giao tiếp không tường minh.

-Cấp phát và giải phóng tài nguyên không hạn chế trong máy ảo.

-Di trú không được kiểm xoát.

-Không kiểm xoát snapshot có thể dẫn đến rò rỉ dữ liệu.

-Các máy ảo có IP có thể quan sát được đám mây, do vậy tin tặc có thể định vị được 1 máy ảo cần tấn công

**Lỗ hổng trong ảnh máy ảo**

-Máy ảnh ảo được đặt trong kho lưu trữ công cộng 1 cách không kiểm xoát.

-Mảnh ảnh ảo không thể vá lỗi vì chúng không hoạt động

**Lỗ hổng trong Hypervisor**

**-**Khả năng cấu hình linh động trong hypervisor có thể khiến chúng bị khai thác.

**Lỗ hổng trong mạng ảo**

-Khi chia sẻ các cầu nối ảo giữa các máy ảo

### **2.2.4 Một số phương pháp chủ đạo hacker thường sử dụng để tấn công kho dữ liệu đám mây**

**Tấn công API**

Rò rỉ thông tin xác thực API hoặc API bị định cấu hình sai là một trong những lỗ hổng phổ biến mở đường cho hacker xâm nhập vào các nền tảng đám mây. Khi kẻ tấn công có được một trong các khóa truy cập, chúng sẽ sử dụng nó chiếm truy cập và kiểm soát một phần máy chủ, sau đó thực hiện lệnh gọi API đối với các hoạt động độc hại hoặc leo thang đặc quyền hệ thống. Thông thường, các khóa được sẽ được rò rỉ/chia sẻ thông qua GitHub, BitBucket… dưới dạng hình ảnh được chia sẻ và ảnh chụp nhanh.

Vụ rò rỉ dữ liệu gần đây ảnh hưởng tới hơn 6,5 triệu công dân Israel là ví dụ điển hình về hình thức tấn công này.

Việc để lộ khóa API cũng có thể là một sai sót của các nhà phát triển như đã xảy ra với Starbuck. Nếu khóa API bị lộ và rơi vào tay hacker, chúng sẽ có quyền truy cập vào các hệ thống nội bộ và thao túng danh sách người dùng được ủy quyền.

Sự cố rò rỉ API lớn nhất được ghi nhận vào tháng 3 năm 2019, khi một nhóm các nhà nghiên cứu bảo mật phát hiện ra 100.000 kho lưu trữ GitHub bị rò rỉ token API và khóa mật mã, có thể truy cập tự do trong khoảng thời gian 6 tháng, gây thiệt hại nặng nề cho các tổ chức có liên quan.

**Cấu hình sai**

Cơ sở dữ liệu và máy chủ bị định cấu hình sai là một trong những nguyên nhân phổ biến đằng sau không ít thảm họa bảo mật đám mây.

Tài nguyên dựa trên điện toán đám mây rất phức tạp và thay đổi liên tục, khiến người quản lý hệ thống gặp khó khăn khi cấu hình. Hacker, đặc biệt là các những nhóm được tài trợ, luôn nhắm vào lỗ hổng cấu hình sai trên các máy chủ đám mây để triển khai ransomware và backdoor nhằm khai thác tiền điện tử hoặc đánh cắp dữ liệu nhạy cảm. Một số máy chủ đám mây lớn đã từng trở thành nạn nhân của hình thức tấn công này bao gồm máy chủ WebLogic của Oracle, Atlassian Confluence và máy chủ email Microsoft Exchange.

**Giả mạo yêu cầu phía máy chủ**

SSRF (Server Side Request Forgery) - giả mạo yêu cầu từ phía máy chủ - là một hình thức tấn công cho phép hacker thay đổi tham số được sử dụng trên ứng dụng web để tạo hoặc kiểm soát các yêu cầu từ máy chủ dễ bị tấn công.

SSRF là hình thức tấn công có xu hướng nở rộ trong thời gian gần đây, liên quan thực tiếp đến quyền truy cập cấu hình, nhật ký, thông tin đăng nhập và nhiều loại dữ liệu khác trong cơ sở hạ tầng đám mây.

Vụ vi phạm dữ liệu với quy mô cực lớn xảy gần đây nhắm vào tổ chức Capital One cho thấy tiềm năng và mức độ rủi ro của SSRF. Những kẻ tấn công đã triển khai thành công một chiến dịch SSRF quy mô lớn để chiếm đoạn thông tin xác thực AWS, sau đó sử dụng dữ liệu này đánh cắp thông tin cá nhân của hơn 100 triệu khách hàng Capital One.

## 2.3 Giải pháp bảo vệ dữ liệu cho điện toán đám mây

### **2.3.1 Lập chiến lược quy trình đảm bảo an toàn bảo mật hệ thống**

Để đảm bảo an toàn cho các và bảo mật cho hệ thống đám mây, các nhà quản lý dịch vụ đám mây cần những chiến lược và quy trình hoàn chỉnh thay vì áp dụng những kĩ thuật ứng phó đơn lẻ, rời rạc. Nếu chúng ta xem xét các sự cố an toàn và bảo mật là một dạng rủi ro của hệ thống thì việc đảm bảo an toàn và bảo mật cho hệ thống có thể được thực hiện theo một quy trình quản lý rủi ro :

*Bước 1*. Lập kế hoạch: Mục tiêu của bước này là nhận định những nguy cơ về an toàn và bảo mật; xác định các cơ chế kiểm soát an toàn và bảo mật (security controls) hiệu quả nhằm giải quyết các nguy cơ; lên kế hoạch cho việc thực hiện các cơ chế kiểm soát an toàn và bảo mật này.

*Bước 2.* Triển khai: Bao gồm việc cài đặt và cấu hình cho các cơ chế kiểm soát an toàn và bảo mật*.*

*Bước 3.* Đánh giá: Đánh giá tính hiệu quả của của các cơ chế kiểm soát và định kỳ xem xét tính đầy đủ của cơ chế kiểm soát.

*Bước 4*. Duy trì: Khi hệ thống và các cơ chế kiểm soát đã vận hành, cần thường xuyên cập nhật những thông tin mới về các nguy cơ ATBM.

Cơ chế kiểm soát an toàn và bảo mật (security controls) được hiểu như một kỹ thuật, một hướng dẫn hay một trình tự được định nghĩa tường minh giúp ích cho việc phát hiện, ngăn chặn, hoặc giải quyết các sự cố về an toàn bảo mật.

Năm 2013, liên minh an toàn và bảo mật trong điện toán đám mây (CSA) xuất bản tài liệu CSA Cloud Control Matrix phiên bản 3.0 (viết tắt là CSA CCM v3.0). Tài liệu này đề xuất một tập hợp bao gồm hơn một trăm hai mươi cơ chế kiểm soát an toàn và bảo mật nhằm trợ giúp các nhà cung cấp dịch vụ đám mây dễ dàng ứng phó với các nguy cơ về ATBM.

### **2.3.2 Một số biến pháp đảm bảo an toàn bảo mật được áp dụng phổ biến trong hệ thống đám mây**

**Bảo mật trung tâm dữ liệu**

Bảo mật mức vật lý: Các công ty như Google, Microsoft, Yahoo, Amazon và một số nhà khai thác trung tâm dữ liệu đã có nhiều năm kinh nghiệm trong việc thiết kế, xây dựng và vận hành các trung tâm dữ liệu quy mô lớn. Những kinh nghiệm này đã được áp dụng cho chính nền tảng cơ sở hạ tầng điện toán đám mây của họ. Kỹ thuật tiên tiến trong việc bảo mật mức vật lý là đặt các trung tâm dữ liệu tại các cơ sở khó nhận biết với những khoảng sân rộng và vành đai kiểm soát được đặt theo tiêu chuẩn quân sự cùng với các biên giới tự nhiên khác.

Những nhân viên được cấp phép phải sử dụng phương pháp xác thực hai bước không ít hơn ba lần mới có thể truy cập vào tầng trung tâm dữ liệu. Thông thường, tất cả khách tham quan hay các nhà thầu phải xuất trình căn cước và phải đăng ký. Sau đó họ tiếp tục được hộ tống bởi đội ngũ nhân viên được cấp phép.

Các công ty cung cấp dịch vụ đám mây đôi khi thiết lập trung tâm dữ liệu với mức độ tiên tiến vượt xa so với các trung tâm dữ liệu của các công ty dịch vụ tài chính. Máy chủ của các trung tâm dữ liệu này được đặt vào hầm trú ẩn kiên cố không dễ dàng vượt qua như chúng ta vẫn thấy trong các bộ phim gián điệp.

**Các biện pháp kiểm soát truy cập**

Tiếp theo vấn đề bảo mật mức vật lý là các kỹ thuật kiểm soát những đối tượng có thể truy nhập vào đám mây. Dĩ nhiên điều này là cực kỳ cần thiết, bởi vì thiếu nó, tin tặc có thể truy nhập vào các máy chủ của người sử dụng, đánh cắp thông tin hoặc sử dụng chúng cho các mục đích xấu. Chúng ta hãy lấy ví dụ về cách thức kiểm soát truy nhập của Amazon Web Services (cũng tương tự như với một số đám mây khác). Cách thức kiểm soát này được thức hiện qua nhiều bước, thường bắt đầu với thông tin thẻ tín dụng của khách hàng.

**Bảo mật dữ liệu và mạng**

Bảo mật hệ điều hành: Bảo mật mức hệ thống có nhiều cấp độ: bảo mật cho hệ điều hành của máy chủ vật lý; bảo mật cho hệ điều hành của các máy ảo chạy trên nó; tường lửa và bảo mật cho các API.

Để bảo mật cho máy chủ vật lý, Amazon yêu cầu người quản trị sử dụng khóa SSH để truy nhập vào các máy bastion. Bastion là các máy được thiết kế đặc biệt và không cho phép người sử dụng truy nhập tới chúng. Sau khi đã truy nhập được vào bastion, người quản trị có thể thực hiện một số lệnh với mức ưu tiên cao lên các máy chủ vật lý. Khi người quản trị đã hoàn tất công việc, quyền truy nhập của họ vào các máy bastion sẽ bị rút

Bảo mật mạng: Các đám mây công cộng thường cung cấp một hệ thống tường lửa để ngăn chặn các truy nhập trái phép. Hệ thống tường lửa nội bộ được sử dụng để kiểm soát sự trao đổi nội tại bên trong đám mây. Thông thường người sử dụng cần định nghĩa tường minh các cổng cần mở cho các giao dịch nội bộ này. Việc kiểm soát và thay đổi các luật tường lửa do mỗi máy ảo tự đảm nhận, tuy nhiên hệ thống đám mây sẽ yêu cầu giấy phép X.509 khi người sử dụng thực hiện các thay đổi này trên máy ảo. Trong mô hình cung cấp dịch vụ của Amazon EC2, quản trị viên của hệ thống đám mây và quản trị viên của các máy ảo là hai đối tượng khác nhau. AWS khuyến khích người sử dụng tự định nghĩa thêm các luật tường lửa cho các máy ảo của mình.

Thông thường, tường lửa cho mỗi máy ảo mặc định sẽ từ chối mọi kết nối tới các cổng người sử dụng sẽ phải cân nhắc cẩn thận cho việc mở cổng nào phù hợp với ứng dụng của mình. Các đám mây công cộng thường là đích ngắm của các tấn công trên mạng internet như DDoS.