TỔNG QUAN VỀ ĐIỆN TOÁN ĐÁM MÂY VÀ CÁC VẤN ĐỀ THÁCH THỨC BẢO MẬT

Vũ Thi Lưu*, Trần Thị Thu Huyền, Nguyễn Thị Huyền

Khoa Công nghệ thông tin, Học viện Nông nghiệp Việt Nam

Tác giả liên hệ: vtluu@vnua.edu.vn

Ngày nhận bài: 18.10.2023 Ngày chấp nhận: 16.10.2024

TÓM TẮT

Trong những năm gần đây, điện toán đám mây đang phát triển rất mạnh mẽ trong lĩnh vực khoa học máy tính. Nó đóng một vai trò và vị trí quan trọng trong quá trình triển khai các dự án công nghệ thông tin. Nó có kiến trúc tính toán mạnh mẽ dựa trên mạng Internet. Công nghệ này đem lại nhiều sự tiện lợi cho phía người dùng, tuy nhiên nỗi lo sợ lớn nhất là sự an toàn và bảo mật của nó. Khi việc sử dụng đám mây ngày càng gia tăng thì những thách thức về bảo mật cũng tăng theo. Chính vì thế nhiều tổ chức cũng đã triển khai các dự án để cung cấp các giải pháp bảo mật tốt hơn cho khách hàng. Mặt khác, các chuyên gia bảo mật cũng đang nỗ lực nghiên cứu các giải pháp bảo mật tốt hơn. Bài viết này trình bày tổng quan về tình hình phát triển của điện toán đám mây, ưu điểm của nó mang lại, các mô hình triển khai và các dịch vụ của điện toán đám mây cung cấp. Đồng thời, bài báo tổng hợp những những thách thức quan trọng trong vấn đề bảo mật và quyền riêng tư trong điện toán đám mây, phân loại các giải pháp đa dạng hiện có, so sánh điểm mạnh và hạn chế của chúng cũng như các định hướng nghiên cứu trong tương lai.

Từ khóa: Điện toán đám mây, bảo mật mạng, IaaS, PaaS, SaaS.

Overview of Cloud Computing and Security Challenges

ABSTRACT

In recent years, cloud computing is growing very strongly in computer science. It plays an important role and position in the process of implementing information technology projects. It has a powerful computing architecture based on the Internet. This technology brings many conveniences to users, but the biggest fear is its safety and security. Security challenges increased with increased cloud usage. That's why many organizations have also implemented projects to provide better security solutions for customers. On the other hand, security experts are also making efforts to research better security solutions. This article presents an overview of the development of cloud computing, its advantages, deployment models and services provided by cloud computing. At the same time, the article summarizes the important challenges in security and privacy in cloud computing, classifies the diverse existing solutions, and compares their strengths and limitations as well as the future research directions.

Keywords: Cloud computing, Network security, IaaS, PaaS, SaaS.

1. ĐẶT VẤN ĐỀ

Điện toán đám mây đang nhanh chóng chiếm ưu thế lớn trong bối cảnh phát triển mạnh mẽ của công nghệ 4.0 hiện nay. Nó đóng một vai trò quan trọng trong vấn đề chuyển đổi các mô hình triển khai truyền thống từ đầu tư sang trả phí theo dịch vụ thuê bao. Điện toán đám mây là một chiến lược mang lại nhiều lợi thế về chi phí trực tiếp cho khách hàng với khả năng biến một trung tâm dữ liệu mà phải đầu tư rất nhiều chi phí thành các dịch vụ có thể định giá được. Nó cho phép người tiêu dùng vượt qua những trở ngại kinh tế và kỹ thuật khi mới thành lập tổ chức và giúp cho các tổ chức mới thành lập trong thời gian ngắn có thể vận hành và phát triển các ứng dụng phần mềm mà không cần đầu tư nhiều về cơ sở hạ tầng. Nó thực sự đem lại nhiều hữu ích cho tất cả các loại hình doanh nghiệp với nhiều ưu điểm khác nhau. Trong đó ưu điểm khả năng mở rộng và tính co giãn của điện toán đám mây đã giúp các

khách hàng tự động mở rộng hoặc thu hẹp quy mô một cách nhanh chóng và linh hoạt. Ngoài ra nó còn cung cấp cho khách hàng các dịch vụ có độ tin cậy cao, thời gian đáp ứng nhanh chóng và sự linh hoạt để xử lý các biến động theo nhu cầu sử dụng (Mell & Grance, 2011).

Đám mây là tập hợp các máy tính được ảo hóa và kết nối với nhau bao gồm hệ thống song song và phân tán, chúng có thể được trình bày và cung cấp tự động tài nguyên máy tính dựa trên các thỏa thuận mức dịch vụ (SLA) được thiết lập giữa khác giữa khách hàng và nhà cung cấp dịch vụ (Buyya & cs., 2008). Các lợi thế của việc sử dụng điện toán đám mây là cung cấp vô hạn tài nguyên máy tính, chi phí thấp, kiểm soát bảo mật, hypervisor bảo vệ, độ co giãn với khả năng mở rộng hoặc thu hẹp linh hoạt và khả năng chịu lỗi với hiệu suất cao. Nhiều công ty như là Microsoft, Google, Amazon, IBM,… đã phát triển đám mây hệ thống máy tính và cung cấp một lượng lớn khách hàng bằng cách nâng cao các dịch vụ của họ (Zhou & cs., 2010). Tuy nhiên, việc sử dụng và triển khai trên điện toán đám mây vẫn có những các rào cản như vấn đề bảo mật, quyền riêng tư, việc tuân thủ các quy định và các vấn đề pháp lý. Nguyên nhân dẫn đến rào cản đó là do mô hình điện toán đám mây tương đối mới và có rất nhiều vấn đề liên quan đến bảo mật ở tất cả các mức độ như máy chủ lưu trữ, mạng, dữ liệu và ứng dụng có thể được thực hiện (Rosado & cs., 2012). Việc quản lý dữ liệu và dịch vụ là mối quan tâm rất lớn khi cơ sở dữ liệu và phần mềm ứng dụng di chuyển đám mây đến các trung tâm dữ liệu lớn. Nó có thể phát sinh nhiều thách thức về bảo mật trong sử dụng điện toán đám mây bao gồm quyền riêng tư, kiểm soát, ảo hóa và khả năng cao truy cập lỗ hổng bảo mật, quản lý xác thực thông tin và danh tính, độ tin cậy, xác thực của thiết bị trả lời và tính toàn vẹn được thể hiện qua báo cáo của Gartener năm 2008. Ngày nay việc sử dụng các dịch vụ điện toán đám mây ngày càng phổ biến hơn vì các nhà cung cấp dịch vụ đã đảm bảo độ bảo bảo mật với các quy định và kiểm soát phức tạp hơn.

Từ những thảo luận phía trên có thể thấy điện toán đám mây cung cấp nhiều dịch vụ và tiện ích hơn là mô hình IT truyền thống. Tuy nhiên, nhiều khách hàng vẫn còn quan ngại về vấn đề an toàn bảo mật khi sử dụng điện toán đám mây. Ngày nay, việc bảo mật thông tin dữ liệu là rất cần thiết và cực kỳ quan trọng, giá trị của dữ liệu chúng ta không thể đo được. Chính vì thế việc giữ an toàn bảo mật cho dữ liệu trong môi trường mạng là rất quan trọng. Dựa theo báo cáo của Gartner và kết quả tổng hợp của (Manish & cs., 2019) *thì* trên 70% các giám đốc kỹ thuật CTO (Chief Technical Officers) phụ trách cho các doanh nghiệp IT cho rằng nguyên nhân chính khiến các dịch vụ điện toán đám mây vẫn chưa hoàn toàn được sử dụng phổ biến là các vấn đề về quyền riêng tư và bảo mật thông tin. Theo quan điểm của đa số người dùng thì một số vấn đề liên quan đến trở ngại trong quá trình triển khai công nghệ điện toán đám mây trong nghiên cứu của Trần Cao Đệ (2013) là:

Chưa kiểm soát được vấn đề an ninh do bên thứ 3 phụ trách hoặc của nhà cung cấp dịch vụ

Các hợp đồng giữa người dùng điện toán đám mây và các nhà cung cấp điện toán đám mây thiếu sự đảm bảo an toàn, an ninh hoặc chưa được ràng buộc chặt chẽ.

Ngày càng có nhiều các cuộc tấn công nguy hiểm vào các máy chủ tập trung của các dịch vụ đám mây.

Chính vì thế trong bài báo này, chúng tôi đã tổng hợp các vấn đề thách thức về an toàn bảo mật, nguy cơ có thể xảy ra trên môi trường điện toán đám mây, kèm theo một số giải pháp cũng như các nghiên cứu đã và đang triển khai để giải quyết vấn đề liên quan đến bảo mật trên đám mây. Từ đó cung cấp cho người dùng cái nhìn tổng quan và kiến thức căn bản để người dùng có nhiều sự lựa chọn cũng như các phương án phù hợp để triển khai các hệ thống trên môi trường đám mây. Bài báo này, chúng tôi trình bày tổng quan về kiến trúc điện toán đám mây trong phần 2 với các mô hình triển khai đám mây, mô hình dịch vụ đám mây, đặc trưng cơ bản của đám mây, bảo mật đám mây. Phần 3 của bài báo sẽ trình bày về các thách thức trong vấn đề bảo mật của đám mây. Phần 4 là phân tích và thảo luận các vấn đề liên quan đến bảo mật. Cuối cùng là kết luận những vấn đề thách thức bảo mật trong điện toán đám mây.

2. KIẾN TRÚC ĐIỆN TOÁN ĐÁM MÂY

Theo định nghĩa của Viện Quốc gia Tiêu chuẩn và Công nghệ Mỹ (US NIST) (Mell & cs., 2011), 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 được thu hồi lại với chi phí quản lý tối thiểu. Như vậy, hiểu một cách đơn giản, mô hình điện toán đám mây cung cấp cho người sử dụng, các tổ chức, doanh nghiệp sử dụng tài nguyên công nghệ thông tin dưới dạng các dịch vụ. Cho phép người sử dụng lựa chọn các dịch vụ linh hoạt, theo yêu cầu, giảm thiểu chi phí đầu tư cơ sở hạ tầng.

Kiến trúc điện toán đám mây được triển khai dưới 4 mô hình sau: đám mây công cộng, đám mây riêng, đám mây cộng đồng, và đám mây lai. Các mô hình triển khai thể hiện cách mà cơ sở hạ tầng đám mây cung cấp các dịch vụ đám mây cho khách hàng thuê. Các mô hình dịch vụ đám mây luôn sẵn sàng cho khách hàng bao gồm dịch vụ cơ sở hạ tầng (Infrastructure as a Service - IaaS), dịch vụ nền tảng (Platform as a Service - PaaS) và dịch vụ phần mềm (Software as a Service - SaaS). Với mỗi mô hình dịch vụ trong đám mây sẽ có mức độ yêu cầu bảo mật khác nhau. Nhà cung cấp dịch vụ đám mây chịu trách nhiệm cung cấp dịch vụ, quản lý phân phối tài nguyên và tính bảo mật. Kiến trúc điện toán đám mây được thể hiện ở hình 1.

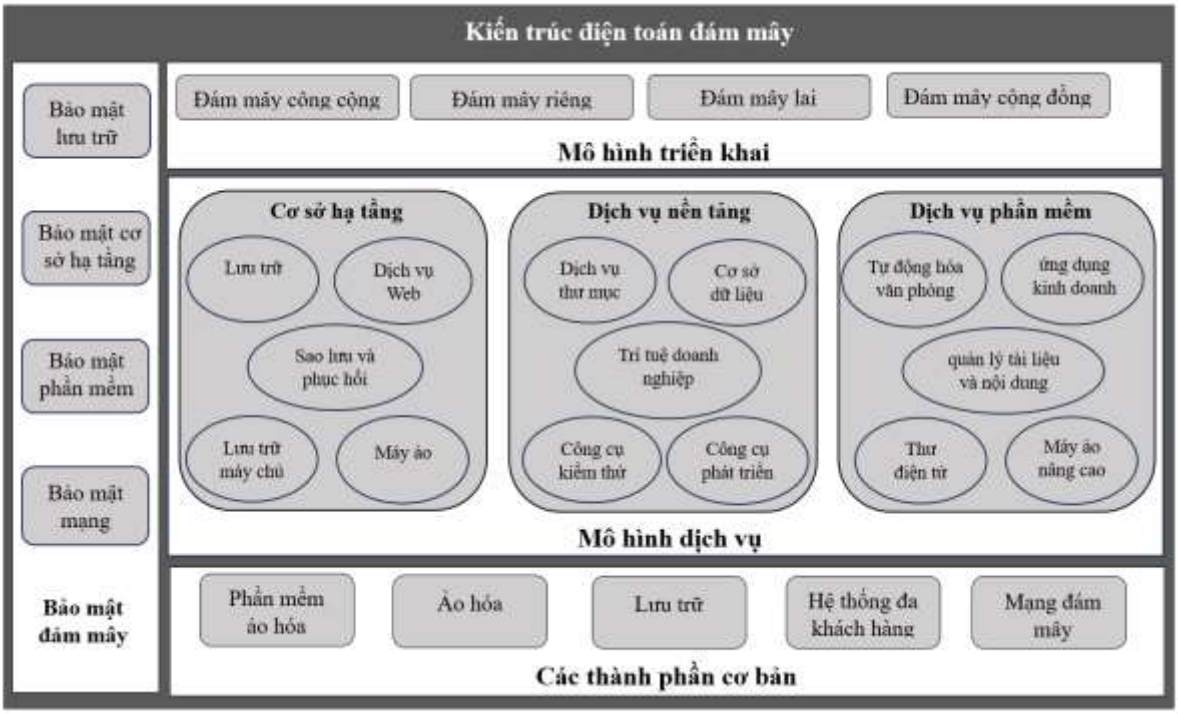
2.1. Mô hình triển khai điện toán đám mây

Đám mây công cộng - Public Cloud: đám mây công cộng có nghĩa là toàn bộ cơ sở hạ tầng điện toán được đặt trên cơ sở của một công ty điện toán đám mây cung cấp dịch vụ điện toán. Do đó, khách hàng không có quyền kiểm soát vật lý đối với cơ sở hạ tầng, chúng thuộc sở hữu của nhà cung cấp dịch vụ. Khách hàng và nhà cung cấp tài nguyên làm việc với nhau dựa trên các thỏa thuận mức dịch vụ. Một số nhà cung cấp dịch vụ đám mây công cộng nổi tiếng như Microsoft, Google, Amazon, VMware, IBM, Sun và Rackspace. Với mô hình triển khai công cộng, nguồn tài nguyên được cung cấp cho nhiều người dùng và dễ dàng truy cập. Ngoài ra, nhiều tác nhân tham gia vào việc vận hành đám mây và tài nguyên được công khai cho khách hàng. Chính vì thế khiến họ khó bảo vệ được tài nguyên khỏi các cuộc tấn công vào hệ thống. Hơn nữa, hệ thống lại nằm ngoài tường lửa nên gặp nhiều khó khăn đảm bảo một số vấn đề như quyền riêng tư, quyền truy cập dữ liệu và bảo mật cho khách hàng. Đây là mô hình được đánh giá kém an toàn hơn các mô hình triển khai khác và nó phù hợp với doanh nghiệp quy mô vừa và nhỏ.

Đám mây riêng - Private Cloud: Với mô hình đám mây này, cơ sở hạ tầng đám mây được quản lý và được duy trì bởi một tổ chức mà có thỏa hiệp nhiều khách hàng. Các tài nguyên được cung cấp nội bộ cho các tổ chức tạo đám mây riêng với máy chủ vật lý và lớp ảo hóa đặt phía trên. Vì thế, các ứng dụng có thể triển khai trên chính máy chủ điều khiển vật lý đó mà không cần sử dụng các máy chủ của Microsoft hoặc Amazon. Với mô hình triển khai này, cơ sở hạ tầng sẽ được thiết lập riêng. Do đó có thể đảm bảo an ninh vật lý và an toàn hơn so với đám mây công cộng vì khả năng hoạt động nội bộ của nó. Tuy nhiên, chi phí triển khai theo mô hình này thì tốn kém hơn do phải đầu tư cơ sở hạ tầng và đào tạo nhân lực chuyên môn cao như quản trị server, chuyên gia ảo hóa, chuyên gia mạng.

Đám mây cộng đồng - Community Cloud: Đây là dạng đám mây mà hạ tầng được chia sẻ bởi một vài tổ chức. Nó hỗ trợ một vài thứ chung của cộng đồng đó, chẳng hạn như nhiệm vụ, chính sách bảo mật, các chuẩn dùng chung,…

Đám mây lai - Hybrid Cloud: Đám mây lai là sự kết nhiều mô hình đám mây khác nhau như đám mây công cộng, đám mây riêng hoặc đám mây cộng đồng. Nó cung cấp nhiều lợi ích hơn so với các mô hình triển khai khác nhau và có thể được lưu trữ bên trong và bên ngoài của đám mây. Mô hình này khá phổ biến vì nó có khả năng tiết kiệm chi phí, có tính đàn hồi và cho phép kiểm soát linh hoạt khi cần thiết.



Nguồn: Muhammad & cs. (2017).

Hình 1. Kiến trúc điện toán đám mây

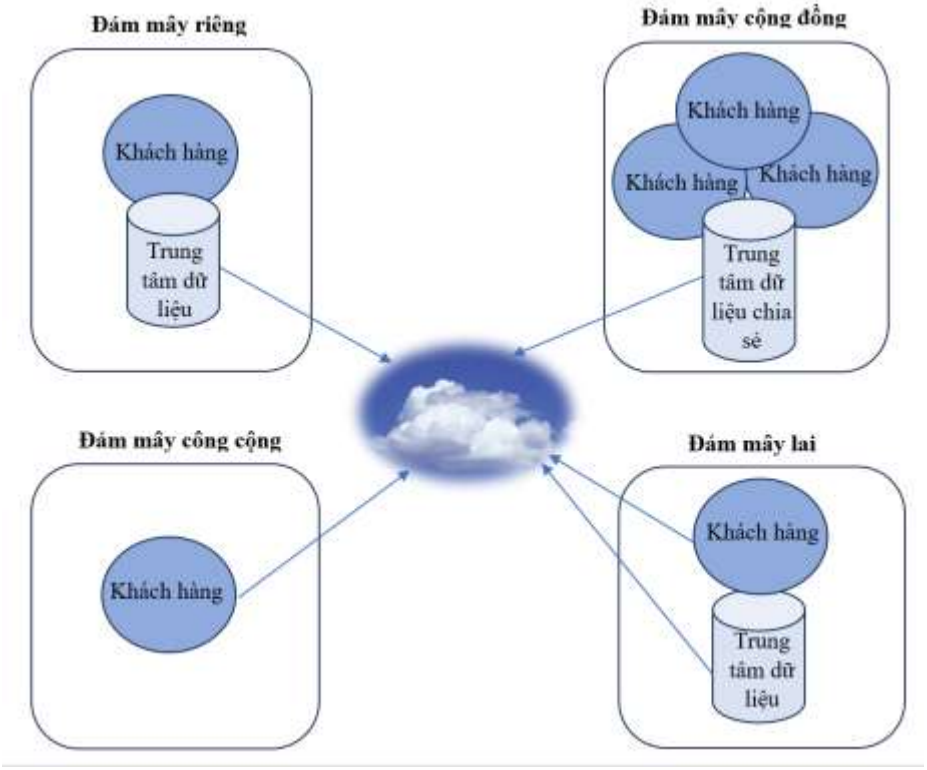
2.2. Mô hình dịch vụ đám mây

Dịch vụ cơ sở hạ tầng - Infrastructure as a Service: là mô hình dịch vụ điện toán đám mây phổ biến nhất, cung cấp cơ sở hạ tầng cơ bản về máy chủ ảo, mạng, hệ điều hành và các ổ lưu trữ. Điều này mang lại sự linh hoạt, độ tin cậy và khả năng mở rộng mà nhiều công ty mong muốn tìm kiếm, các công ty không cần đầu tư toàn bộ cơ sở hạ tầng vật lý, tiết kiệm chi phí và thúc đẩy tăng trưởng kinh doanh. IaaS là dịch vụ có thể chạy trong cơ sở hạ tầng công cộng, tư nhân hoặc kết hợp.

Dịch vụ nền tảng - Platform as a Service: Mô hình dịch vụ này nằm trên lớp IaaS, khách hàng có khả năng triển khai trên hạ tầng điện toán đám mây bằng việc sử dụng các chương trình, framework, môi trường phát triển tích hợp, ngôn ngữ lập trình, các thư viện, dịch vụ, công cụ phát triển được hỗ trợ từ bên thứ ba. Các ứng dụng web có thể được tạo dễ dàng và nhanh chóng thông qua PaaS với sự linh hoạt và mạnh mẽ của các dịch vụ trong mô hình này hỗ trợ. Nếu nhiều nhà phát triển làm việc trên một dự án thì các giải pháp PaaS có khả năng triển khai và mở rộng dễ dàng. Các nhà cung cấp nổi tiếng cho mô hình PaaS gồm là: Microsoft Azure, Apprenda, Stackato, VMware, Google App Engine... Với dịch vụ này, máy ảo được sử dụng như một chất xúc tác và nó bắt buộc phải bảo vệ khỏi các cuộc tấn công của phần mềm độc hại trên đám mây. Việc kiểm tra xác thực hợp lệ trong quá trình truyền dữ liệu trên các kênh mạng là rất quan trọng và cần duy trì tính toàn vẹn của các ứng dụng. Tính bảo mật của PaaS có thể bị xâm phạm trong quá trình triển khai ứng dụng của khách hàng hoặc thời gian chạy của ứng dụng.

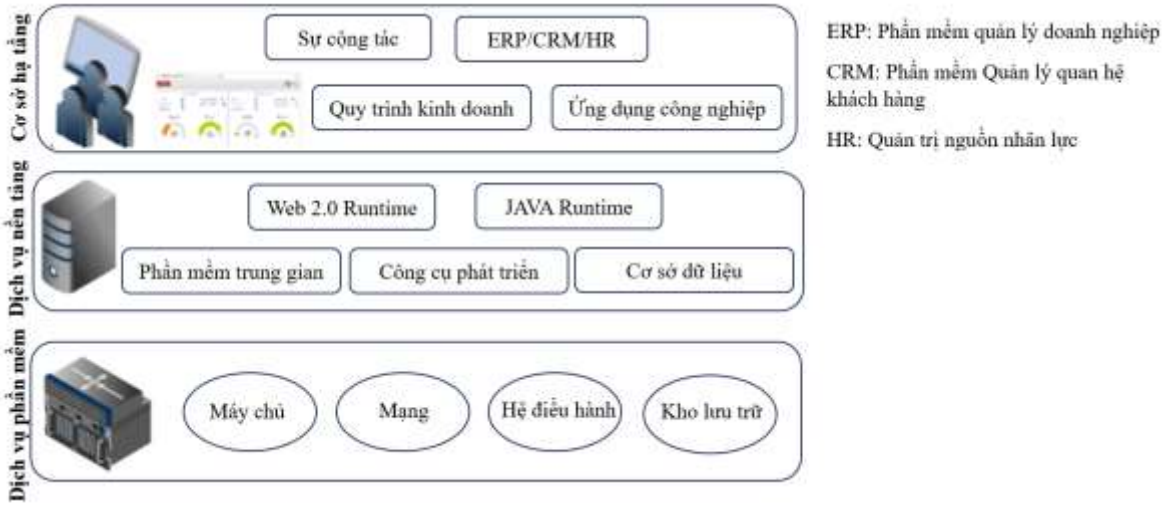
Dịch vụ phần mềm - Software as a Service: Mô hình dịch vụ này là lớp trên cùng cho phép khách hàng sử dụng các dịch vụ phần mềm của nhà cung cấp ứng dụng được triển khai trên hạ tầng điện toán đám mây. Ứng dụng có thể truy cập từ các thiết bị khác nhau thông qua giao diện người dùng chẳng hạn như một trình duyệt web (ví dụ như email trên web),

hoặc qua giao diện của chương trình. Khách hàng không quản lý hoặc kiểm soát cơ sở hạ tầng điện toán đám mây nằm bên dưới nhưng có thể thiết lập cấu hình cho ứng dụng phù hợp với mình. Hiện tại đa số chúng ta đang sử dụng phần mềm trên điện toán đám mây của Google như: Gmail, Google Docs, trình tìm kiếm của Google... Dịch vụ phần mềm được cung cấp dựa theo cơ chế dịch vụ web (web service) và các cổng thông tin điện tử (portal).



Nguồn: Manish & cs. (2019).

Hình 2. Kiểu triển khai đám mây

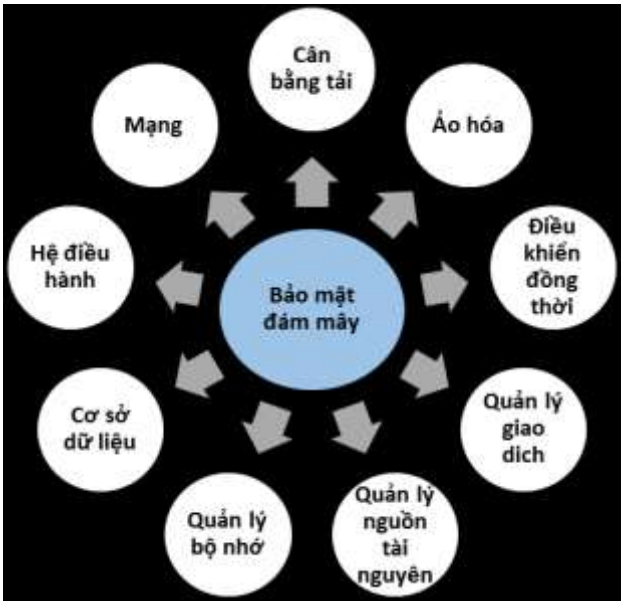


Nguồn: Osama & cs. (2014).

Hình 3. Mô hình dịch vụ đám mây

Bảng 1. Nhà cung cấp mô hình dịch vụ tương ứng trên các mô hình triển khai đám mây

Dịch vụ/ Mô hình triển khai	Dịch vụ cơ sở hạ tầng (IaaS)	Dịch vụ nền tảng (PaaS)	Dịch vụ phần mềm (SaaS)
Đám mây công cộng	Rackspace, Amazon EC2	VMware, Microsoft Azure, CloudFoundry.com, Google App Engine	Office 365, QuickBooks online, Salesforce.com
Đám mây riêng	OpenStack, Hyper-V, VMware, CloudStack	Stackato, Apprenda	Cisco WebEx
Đám mây lai	Rackspace, Custom	Cloud Foundry, Custom	Rackspace
Đám mây cộng đồng	NYSE Capital	NYSE Capital	Salesforce



Hình 4. Các yếu tố ảnh hưởng đến hiệu suất của đám mây (Iqbal, 2019)

Các mô hình dịch vụ trên chúng được thể hiện qua hình 3. Trong đó IaaS là mô hình dịch vụ tầng cơ sở hạ tầng dưới cùng, ở giữa là tầng dịch vụ nền tảng (PaaS) và trên cùng là tầng dịch vụ phần mềm (SaaS). Vì vậy an ninh của hệ thống phụ thuộc vào an ninh của mỗi tầng được thiết kế và cài đặt kèm theo như là một dịch vụ hay tiện ích.

Các nhà cung cấp đã sử dụng mô hình dịch vụ đám mây tương ứng trên các mô hình triển khai đám mây được thể hiện trong bảng 1.

3. THÁCH THỨC BẢO MẬT TRONG ĐIỆN TOÁN ĐÁM MÂY

3.1. Yếu tố ảnh hưởng đến bảo mật đám mây

Theo nghiên cứu được tổng hợp trong bài báo của Iqbal (2019) hiệu suất hoạt động của điện toán đám mây bị ảnh hưởng bởi nhiều yếu tố vì nó được bao quanh bởi nhiều công nghệ được thể hiện trong hình 4 như là: cân bằng tải, mạng, điều khiển đồng thời, ảo hóa, hệ điều hành, cơ sở dữ liệu, quản lý bộ nhớ... Trong đó, yếu tố mạng kết nối điện toán đám mây với thế giới bên ngoài phải được bảo mật. Yếu tố ảo hóa phải được thực hiện một cách an toàn khi ánh xạ với các hệ thống vật lý. Yếu tố cân bằng tải liên quan đến việc xử lý lưu lượng yêu cầu đến đôi khi làm quá tải máy chủ. Ngoài ra, cần có các thuật toán khai thác dữ liệu phù hợp được áp dụng để đối phó với các cuộc tấn công nguy hiểm.

3.2. Thách thức bảo mật trong điện toán đám mây

Bên cạnh các lợi ích và mà điện toán đám mây đem lại thì vẫn còn nhiều khó khăn và

thách thức gặp phải khi các doanh nghiệp triển khai dự án trên không gian đám mây. Theo một cuộc khảo sát được thực hiện bởi Gartner và nghiên cứu được tổng hợp từ Manish & cs. (2019) có hơn 70% giám đốc kỹ thuật cho rằng lý do chủ yếu khiến các dịch vụ điện toán đám mây không được sử dụng phổ biến chính là vấn đề bảo mật thông tin và quyền riêng tư. Đó cũng chính là lý do khiến các công ty, doanh nghiệp ngần ngại chuyển cơ sở hạ tầng của họ lên đám mây. Dưới đây là một số thách thức về vấn đề bảo mật được đề cập đến trong nghiên cứu của Manish & cs. (2019), Nasarul (2017) và Mohammad & cs. (2024).

Quyền riêng tư của dữ liệu (Privacy data): Quyền riêng tư của dữ liệu rất quan trọng đối với việc triển khai hệ thống trên điện toán đám mây. Hầu hết các tổ chức, doanh nghiệp cảm thấy an toàn hơn khi họ đặt thông tin dữ liệu trên chính trang web của họ hơn là đám mây. Người sử dụng các dịch vụ đám mây hầu như không có khái niệm về nơi lưu thông tin, ngày chuyển, hoạt động của đám mây, v.v. Nhiều câu hỏi băn khoăn được người sử dụng đặt ra như là: Thông tin có bị sao lưu lại không? Các tệp tin được tạo và xóa như thế nào? Người dùng nào có thể truy nhập thông tin? Vị trí lưu dữ liệu?…

Tính bảo mật của dữ liệu (Confidentiality of data): Tính bảo mật liên quan đến quyền riêng tư của dữ liệu, đảm bảo rằng chỉ những người dùng được phê duyệt mới có thể xem thông tin. Nhà cung cấp dịch vụ có nhiệm vụ cung cấp các cơ chế bảo mật. Và giải pháp cho tính bảo mật dữ liệu đó chính là mã hóa. Hiện tại, cũng có nhiều thuật toán đối xứng và bất đối xứng được sử dụng để bảo mật dữ liệu, mặc dù vậy nhưng vẫn còn nhiều vấn đề quan tâm được đặt ra như là: Thông tin, dữ liệu được mã hóa và giải mã ở đâu (phía máy khách hoặc phía đám mây)? Thông tin có thể bị tìm kiếm dưới dạng mã hóa như thế nào? Mối đe dọa nào có thể xảy ra khi truyền thông tin giữa máy khách tới đám mây? Việc lạm dụng thông tin của nhà cung cấp dịch vụ? Lỗi sử dụng khóa của nhà cung cấp dịch vụ?…

Dữ liệu còn lại trên đám mây (Data remance): Đề cập đến phần còn lại của dữ liệu còn sót lại trên đám mây sau khi chu kỳ sử dụng của nó đã hết hoặc sau khi phương tiện lưu trữ được format - định dạng hoặc dùng lại. Dữ liệu sót lại đó có thể bị truy cập hoặc lấy ra từ phương tiện khác. Hiện tại không có tiêu chuẩn rõ ràng nào cho vấn sử dụng lại phương tiện lưu trữ. Việc lưu trữ dữ liệu còn sót lại này gây khó khăn cho việc sử dụng tài nguyên phần cứng từ đám mây. Hầu hết người dùng không biết tài nguyên và dung lượng lưu trữ được phân bổ, do vậy có thể người dùng bị khóa trong một nhà cung cấp dịch vụ. Hiện tại có nhiều kỹ thuật khác nhau đã được phát triển để truy cập dữ liệu sót lại như làm sạch hoặc tiêu hủy. Phương pháp cụ thể của các kỹ thuật này là ghi đè, khử từ, mã hóa và phá hủy phương tiện (Data Remanence, https://en.wikipedia.org/wiki/Data_remanence).

Tính toàn vẹn của dữ liệu (Data integrity): Thông tin chỉ có thể được sửa đổi bởi những người dùng có thẩm quyền. Tuy nhiên, dữ liệu trên đám mây có thể bị thay đổi bởi một người dùng nào đó mà không có thẩm quyền hoặc ủy quyền. Chính vì thế, để đảm bảo tính toàn vẹn thì nhà cung cấp dịch vụ đám mây sẽ có thêm cam kết để đảm bảo chắc chắn rằng dữ liệu không được sửa đổi bởi bất kỳ một người dùng không có thẩm quyền. Thêm nữa, tính toàn vẹn dữ liệu còn được thể hiện khi dữ liệu truyền từ một đám mây này đến một đám mây khác mà vẫn đảm bảo toàn vẹn dữ liệu.

Truyền dữ liệu (Transmission of data): Hầu hết thời gian thông tin được truyền giữa đám mây và người tiêu dùng. Dữ liệu ban đầu được gửi từ trang web của khách hàng đến đám mây và thông tin được trả về sau các truy vấn từ đám mây đến máy khách. Mã hóa được sử dụng để cung cấp bảo mật trong khi thông tin đang được truyền đi. Tuy nhiên, hầu hết thời gian dữ liệu được truyền đi mà không được mã hóa vì phải mất rất nhiều thời gian để mã hóa và giải mã dữ liệu cho mỗi thao tác. Kẻ xâm nhập có thể theo dõi thông tin liên lạc trong quá trình chuyển giao; làm gián đoạn quá trình truyền thông tin, sử dụng sai thông tin,...

Vi phạm dữ liệu: Như đã đề cập ở trên, nhiều người dùng và tổ chức từ các nơi khác nhau trên thế giới chia sẻ môi trường đám mây; thông tin quý giá của họ được lưu trữ ở một địa điểm nào đó. Tuy nhiên bất kỳ sự cố nào đó trên đám mây cũng có thể làm lộ những dữ liệu nhạy cảm cho người dùng của các tổ chức khác cùng chia sẻ kho lưu trữ dữ liệu. Ngoài ra, do có nhiều khách hàng cùng thuê hoặc sử dụng các ứng dụng khác nhau trên các máy ảo có thể chia sẻ cùng một cơ sở dữ liệu, nên bất kỳ sự cố hỏng hóc nào xảy ra sẽ ảnh hưởng đến những người khác chia sẻ cùng một cơ sở dữ liệu.

Bên thứ ba xử lý dữ liệu (Third party handling data): Dữ liệu trên đám mây được xử lý và quản lý bởi bên thứ ba, chính vì thế vấn đề lớn nhất là các biện pháp bảo mật được bên thứ ba sử dụng và điều gì đảm bảo rằng dữ liệu được bảo mật vì không bên thứ ba nào có thể cung cấp sự bảo mật dữ liệu 100%. Vì vậy, không có sự đảm bảo nào là thích hợp về bảo mật dữ liệu.

Tính khả dụng: Tính khả dụng của hệ thống điện toán đám mây mọi lúc mọi nơi là rất quan trọng đối với sự thành công của điện toán đám mây. Hầu hết các giải pháp Công nghệ Thông tin yêu cầu dịch vụ mọi lúc vì các dịch vụ quan trọng mà họ cung cấp, bất kỳ sự gián đoạn dịch vụ nào cũng có thể dẫn đến mất mát, mất niềm tin của người tiêu dùng. Tiêu biểu là các cuộc tấn công như từ chối dịch vụ được sử dụng để từ chối tính khả dụng của dữ liệu. Nếu kẻ tấn công sử dụng tất cả các tài nguyên có sẵn, những người khác không thể sử dụng các tài nguyên đó, điều này có thể dẫn đến từ chối dịch vụ và truy cập chậm vào các tài nguyên đó.

Tấn công mạng (Cyber attack): Mối quan tâm bảo mật quan trọng nhất trong điện toán đám mây là tấn công mạng. Có nhiều cách tấn công khác nhau được tiến hành trên dữ liệu như phát tán các phần mềm độc hại, mã độc, từ đó khai thác sức mạnh của dịch vụ đám mây để tấn công các máy tính khác. Các phần mềm độc hại được thiết kế để lây lan với tốc độ rất nhanh, vì thế việc nắm bắt và ngăn chặn được nó sẽ làm cho dữ liệu trên đám mây an toàn bảo mật hơn (Arjun, 2023).

Tấn công từ bên trong (Insider attack): Những người tấn công từ bên trong hệ thống hay còn gọi là nội gián, đó có thể là những nhân viên được ủy quyền, được các nhà cung cấp dịch vụ đám mây chỉ định để quản lý và duy trì đám mây. Đôi khi những người này có khả năng đánh cắp hoặc làm hỏng, phá hủy dữ liệu nhạy cảm của tổ chức trên đám mây và chuyển thông tin nhạy cảm này cho các tổ chức khác trong cùng một đám mây nhằm phá hoại, gây tổn thất tài chính, hiệu suất công việc, thiệt hại thương hiệu… Những kẻ nội gián này có thể được trả tiền cho công việc này. Các nhà cung cấp dịch vụ đôi khi không kiểm soát được hết các vấn đề xảy ra đối với các nhân viên của họ.

Các vấn đề về API: Đây là giao diện lập trình phần mềm để tương tác với các dịch vụ đám mây. Khi các hãng thứ 3 sử dụng các API thiếu bảo mật này để tạo phần mềm, tài khoản và dữ liệu của người dùng có thể bị ảnh hưởng thông qua các ứng dụng đó. Có nhiều giải pháp được đề xuất để tránh các giao diện và API không an toàn như là phân tích mô hình bảo mật của nhà cung cấp đám mây cho các giao diện, tăng cường kiểm soát truy cập và xác thực mạnh mẽ khi truyền dữ liệu và khi sử dụng các API thì phải hiểu rõ nguyên lý của nó (Anamika & cs., 2023).

Vị trí dữ liệu (Data location): Vị trí dữ liệu đề cập đến việc dữ liệu được lưu trữ và xử lý ở đâu trên hạ tầng đám mây của nhà cung cấp dịch vụ. Một số vấn đề về bảo mật dữ liệu có liên quan đến vị trí dữ liệu cần quan tâm được đề cập trong các nghiên cứu của Kumar & cs. (2013) và Hussain & cs. (2023):

Luật pháp và sự tuân thủ: Nhiều quốc gia và vùng lãnh thổ có các quy định về bảo mật và quyền riêng tư dữ liệu. Việc lưu trữ dữ liệu ở một quốc gia nào đó có thể đòi hỏi tuân thủ những quy định cụ thể về bảo mật và quyền riêng tư của quốc gia đó.

An toàn dữ liệu: Chọn đúng vị trí lưu trữ dữ liệu có thể ảnh hưởng đến mức độ an toàn của dữ liệu. Một số quốc gia có các tiêu chuẩn bảo mật cao hơn và hạ tầng an toàn hơn, trong khi ở các quốc gia khác, rủi ro bảo mật có thể cao hơn.

Khả năng truy cập của nhà cung cấp dịch vụ: Cho dù chúng ta có biết dữ liệu lưu trữ ở đâu thì nhà cung cấp dịch vụ đám mây vẫn có thể có quyền truy cập vào dữ liệu của bạn cho mục đích hỗ trợ kỹ thuật hoặc kiểm tra an ninh. Điều này đặt ra câu hỏi về khả năng kiểm soát và quản lý dữ liệu.

Sự thay đổi vị trí dữ liệu: Trong môi trường đám mây, dữ liệu của bạn có thể được di chuyển tự động giữa các trung tâm dữ liệu để tối ưu hiệu suất hoặc đáp ứng nhu cầu. Điều này có thể làm tăng rủi ro về bảo mật và tuân thủ quy định.

Để giải quyết các vấn đề bảo mật liên quan đến vị trí dữ liệu trong điện toán đám mây, chúng ta nên xem xét cẩn thận hợp đồng với nhà cung cấp dịch vụ để hiểu rõ về cách họ quản lý dữ liệu và tuân thủ quy định về bảo mật và quyền riêng tư. Đồng thời, nắm vững các quy định pháp lý liên quan đến dữ liệu và tuân thủ chúng một cách chính xác.

Chiếm đoạt tài khoản hoặc dịch vụ: Khi người dùng sử dụng mật khẩu để truy cập vào các dịch vụ đám mây có thể tài khoản và mật khẩu của họ bị lấy cắp mất. Khi đó dữ liệu của khách hàng có thể bị, thay đổi, xóa hoặc bị bán cho người khác. Để tránh gặp phải vấn đề này, có nhiều giải pháp được đề xuất để tránh bị chiếm đoạt tài khoản hoặc dịch vụ như:

- Ngăn chặn việc chia sẻ thông tin đăng nhập của khách hàng.

- Sử dụng hệ thống xác thực hai yếu tố.

- Giám sát tất cả các hoạt động để phát hiện truy cập trái phép.

Ngoài ra còn một số mối nguy hiểm khác cho các đám mây đến từ phía bên ngoài được đề cập theo nghiên cứu của Tadapaneni (2020):

Tấn công từ chối dịch vụ: Máy chủ bị đánh sập bằng cách tạo ra lưu lượng lớn truy cập ảo từ tin tặc làm cho hệ thống bị tiêu thụ hết tài nguyên dẫn đến tắc nghẽn và sập mạng.

Tấn công sử dụng SQL (Structured Query Language injection Attack): Tin tặc sử dụng các truy vấn SQL tấn công trực tiếp vào cơ sở dữ liệu lấy thông tin đặc biệt như tên người dùng và mật khẩu.

Quét cổng (Port scanning): Tin tặc sử dụng kỹ thuật để cố gắng tìm hiểu các cổng đang được máy chủ đám mây sử dụng với mục đích truy cập vào thông tin được lưu trữ trên đám mây.

Theo dõi mạng (Network sniffing): Tin tặc dựa vào quá trình theo dõi tất cả mạng giữa các đám mây với nhau hoặc giữa đám mây với người dùng để nắm bắt phương thức xác thực đã được sử dụng.

Tấn công chéo (Cross-site Scripting attack): Tấn công được thực hiện bằng cách nhúng các liên kết hoặc tệp độc hại lên trang web, nếu người dùng mở liên kết đó sẽ vô tình chia sẻ quyền kiểm soát hoặc quyền truy cập cho tin tặc.

Như vậy bảo mật trong điện toán đám mây là vấn đề phức tạp và quan trọng, ngoài các khía cạnh mà chúng tôi đã tổng hợp kèm theo các giải pháp gợi ý để giải quyết nhằm đảm bảo an toàn cho dữ liệu và dịch vụ của người dùng thì cần có nghiên cứu chuyên sâu từ chuyên gia của các nhà cung cấp dịch vụ để đưa ra giải pháp tổng thể đem lại niềm tin cho người dùng khi sử dụng dịch vụ trong môi trường điện toán đám mây. Phần tiếp theo, bài báo sẽ tổng hợp thêm một vài giải pháp để hỗ trợ bảo mật trong điện toán đám mây.

4. MỘT SỐ GIẢI PHÁP BẢO MẬT ĐÃ ĐƯỢC NGHIÊN CỨU VÀ TRIỂN KHAI TRONG ĐIỆN TOÁN ĐÁM MÂY

4.1. Mã hóa dữ liệu

Mã hóa dữ liệu là công nghệ chuyển hóa dữ liệu này thành một dạng dữ liệu mới mà người dùng không thể đọc hoặc hiểu được nó. Bằng cách sử dụng các thuật toán lồng vào nhau, thường dựa trên một khóa để mã hóa dữ liệu. Nếu chúng ta sử dụng mật khẩu yếu, tin tặc có thể phá mã hóa và truy cập tập tin, làm thất bại mục đích của mã hóa. Mã hóa được cho là cách tiếp cận tốt hơn để đảm bảo các yêu cầu về tính bí mật, tính toàn vẹn và tính không khước từ (nghĩa là không chối bỏ được việc mình đã làm). Với giải pháp này, dữ liệu phải được mã hóa

trước khi gửi lên đám mây. Chủ sở hữu dữ liệu có thể cho phép một số thành viên cụ thể có quyền truy cập vào dữ liệu đó (Rao & cs., 2015). Tệp hoặc dữ liệu được gửi lên đám mây phải được mã hóa trước, sau đó nhà cung cấp đám mây phải mã hóa lại; quá trình này được gọi là mã hóa nhiều tầng. Người ta đã quan sát thấy rằng sự kết hợp của các thuật toán mã hóa khác nhau giúp mã hóa dữ liệu tốt hơn. Kết quả thực nghiệm cho thấy sự kết hợp thuật toán mã hóa RSA+IDEA[1] cho hiệu suất mã hóa cao hơn trong việc bảo mật dữ liệu (Chennam & cs., 2017; Yan & cs. 2017; Sandeep, 2023).

Tuy nhiên, mã hóa không thể giải quyết hết được vấn đề bảo mật, bởi nguyên nhân của rò rỉ thông tin bao gồm cả việc tồn tại các lỗ hổng như XSS (Cross-site scripting - tấn công chéo trang) hay SQL injection, cũng như việc sử dụng mật khẩu khẩu quá ngắn hoặc dễ đoán… Bản thân việc mã hóa không ngăn chặn được thông tin bị đánh cắp, mất mật khẩu sẽ dẫn tới mất gói dữ liệu, dẫn đến không đảm bảo được tính an toàn, toàn vẹn về mặt dự phòng dữ liệu. Bên cạnh đó, đa phần các công nghệ quản lý khóa mã được sử dụng rộng rãi hiện nay cũng có thể tiềm ẩn những rủi ro. Thực tế chưa có phát biểu nào khẳng định sự đảm bảo tuyệt đối về tính an toàn bảo mật của dữ liệu.

4.2. Thẩm quyền pháp lý

Thẩm quyền pháp lý của điện toán đám mây và các khía cạnh rất cơ bản của môi trường đám mây như vấn đề ảo hóa, dữ liệu phân tán động, các yếu tố đa quốc gia làm cho việc bảo vệ dữ liệu trở nên phức tạp. Người dùng thường không biết rằng dữ liệu của họ nằm ở đâu trên đám mây. Ví dụ, một khách hàng từ Việt Nam có thể đang sử dụng máy chủ được triển khai tại Hoa Kỳ, sử dụng ứng dụng đã được phát triển tại Nhật Bản và lưu trữ dữ liệu quan trọng của mình tại một trung tâm dữ liệu được đặt tại Thụy Sĩ (Sony & cs., 2013). Do đó, tài nguyên được phân bổ cho người dùng nên được đánh dấu để thực hiện chắc chắn rằng dữ liệu được tách biệt (Harfoushi & cs., 2014).

4.3. Từ chối dịch vụ phân tán (DdoS - Distributed Denial of Service)

Từ chối dịch vụ phân tán là một loại tấn công trong đó kẻ tấn công tạo ra một số máy tấn công (zombie) bằng cách lây nhiễm máy qua internet (Deepali & cs., 2017; Somani & Gaurav, 2016; Paharia & cs., 2017; Arjun, 2023). Sau đó, những máy bị nhiễm này được sử dụng để tấn công nạn nhân. Khi các cuộc tấn công/lưu lượng truy cập từ rất nhiều máy bị nhiễm được hướng đến đối với một nạn nhân, tài nguyên của nó như CPU, băng thông và bộ nhớ bắt đầu cạn kiệt và tài nguyên cụ thể trở nên không khả dụng đối với người dùng. Để đối phó với điều này, nghiên cứu của Deepali & cs. (2017) đã giới thiệu một lớp có tên là lớp sương mù nằm giữa máy chủ đám mây và người dùng. Tất cả các yêu cầu gửi đến máy chủ đều được lọc qua lớp sương mù này và các cuộc tấn công DDoS (Distributed Denial of Service) được giảm thiểu.

4.4. Chữ ký số

Chữ ký số là công cụ mạnh để bảo mật dữ liệu trong điện toán đám mây (Merkle & cs., 1989). Trong nghiên cứu của Rewagad & Pawar (2013) đã đề xuất giải pháp sử dụng chữ ký số để bảo mật dữ liệu cùng với trao đổi khóa Diffie Hellman với thuật toán mã hóa AES (Advanced Encryption Standard). Cơ sở trao đổi khóa Diffie Hellman đánh dấu rằng nó vô dụng nếu khóa bị hack trong quá trình truyền vì nó vô dụng nếu không có khóa riêng của người dùng, khóa này chỉ giới hạn cho người dùng hợp pháp. Cơ chế ba chiều này được đề xuất trong bài báo đó khiến hệ thống bảo mật khó bị hack hơn, do đó có thể bảo vệ dữ liệu tốt hơn.

5. KẾT LUẬN

Điện toán đám mây đã và đang phát triển rất mạnh mẽ với những ưu điểm của nó đem lại. Tuy nhiên nó gặp phải một số thách thức liên

[1] RSA: Thuật toán mã hóa lấy tên 3 chữ cái đầu của 3 tác giả tạo ra (Ron Rivest, Adi Shamir và Len Adleman)
IDEA: International Data Encryption Algorithm - Thuật toán mật mã hóa dữ liệu quốc tế

quan đến vấn đề an ninh và bảo mật, đây là trở ngại chính trong việc áp dụng và triển khai nó với quy mô rộng rãi. Mối lo ngại về bảo mật đám mây trở nên phức tạp hơn khi nhiều lĩnh vực khác nhau liên tục xâm nhập vào ngành điện toán đám mây. Bài viết này đã tổng hợp kiến thức cơ bản về điện toán đám mây, kiến trúc và các mô hình dịch vụ nó cung cấp, đồng thời đề cập đến các thách thức bảo mật kèm một số giải pháp cho những vấn đề đã được phân tích tổng hợp từ các nghiên cứu được thu thập. Từ đó cung cấp cho người dùng cái nhìn tổng quan và những thách thức bảo mật, giúp người dùng có thêm phương án lựa chọn khi triển khai các dự án trên điện toán đám mây. Đây cũng là vấn đề để các chuyên gia bảo mật, các nhà nghiên cứu khoa học, tổ chức cung cấp dịch vụ đang tiếp tục tìm hiểu, nghiên cứu phát triển để có nhiều giải pháp hơn nữa nâng cao chất lượng dịch vụ và sự an toàn bảo mật cho người dùng.

TÀI LIỆU THAM KHẢO

Anamika Agarwal, Satya Bhushan Verma, Bineet Kumar Gupta (2023). A Review of Cloud Security Issues and Challenges. Adcaij advances in distributed computing and artificial intelligence journal. 12(1): e31459.

Arjun Reddy Kunduru (2023). Security Concerns and Solutions for Enterprise Cloud Computing Applications. Asian Journal of Research in Computer Science. 15(4): 24-33.

Buyya R., Yeo C.S. & Venugopal S. (2008). Market-oriented cloud computing: Vision, hype, and reality for delivering IT services as computing utilities. Proceedings of the 10th IEEE International Conference on High Performance Computing and Communications. pp. 5-13

Chennam K.K., Muddana L. & Aluvalu R.K. (2017). Performance Analysis of Various Encryption Algorithms for Usage in Multistage Encryption for securing data in Cloud. 2nd IEEE International Conference on Recent trends in Electronics, Information & Communication Technology (RTEICT). pp. 2030-2033.

Data Remanence. Retrieved from https://en.wikipedia. org/ wiki/Data_remanence on Oct 15, 2023.

Deepali Bhushan K. (2017). DDoS Attack Defense Framework for Cloud using Fog Computing (2017). 2nd IEEE International Conference on Recent trends in Electronics, Information & Communication Technology (RTEICT). India. pp. 534-538.

Brodkin, J. (2008). Gartener: Seven cloud-computing security risks. Truy cập từ trang gartner-seven-cloud-computing-security-risks.html: https://www.infoworld.com/article/2652198/gartner-seven-cloud-computing-security-risks.html ngày 15/12/2023

Harfoushi O., Alfawwaz B. & Ghatasheh N.A. (2014). Data Security Issues and Challenges in Cloud Computing: A conceptual Analysis and Review. Communications and Network. 6(1): 15-21.

Hussain Akbar, Muhammad Zubair & Muhammad Shairoze Malik (2023). Security Issues and challenges in Cloud Computing. International Journal for Electronic Crime Investigation. 7(1).

Iqbal Ahmed (2019). A brief review: security issues in cloud computing and their solutions. Telecommunication Computing Electronics and Control journal. 17(6): 2812, 2817.

Kumar P. Singh & Arri H. (2013). Data Location in Cloud Computing. International Journal for Science and Emerging Technologies with Latest Trends.

Manish Kumar Khandelwala & Hukam Chand Sainib (2019). Review on Security Challenges of Cloud Computing. International Conference on Advancements in Computing & Management (ICACM-2019). pp. 1031-1037.

Merkle Ralph C (1989). A Certified Digital Signature. CRYPTO. New York. pp. 218-238.

Mell P. & Grance T. (2011). The NIST definition of cloud computing. Special Publication. 800-145.

Mohammad Ahmar Khan, Dr. Pratibha Gupta, Abdulsatar Abduljabbar Sultan, Dr. Preeti Singh Shivam & Dr. Melanie Lourens (2024). Security in Cloud Computing: Issues and Challenges1Dr. International journal of intelligent systems and applications in engineering. ISSN: 2147-67992

Muhammad Faheem Mushtaq, Urooj Akram, Irfan Khan, Sundas Naqeeb Khan, Asim Shahzad & Arif Ullah (2017). Cloud Computing Environment and Security Challenges: A Review. International Journal of Advanced Computer Science and Applications. 8(10).

Nasarul Islam K.V. (2017). Review on Benefits and Security Challenges of Cloud Computing. (IJCSIT) International Journal of Computer Science and Information Technologies. 8(2): 224-228.

Osama Harfoushi, Bader Alfawwaz, Nazeeh A. Ghatasheh, Ruba Obiedat, Mua'ad M. Abu-Faraj & Hossam Faris (2014). Data Security Issues and Challenges in Cloud Computing: A Conceptual Analysis and Review. Journal of Communications and Network. 6(1): 15-21.

Paharia Bhumika & Bhushan K (2018). DDoS Detection and Mitigation in Cloud Via FogFiter: A Defence Mechanism. 9th International Conference on Computing, Communication and Networking Technologies (ICCCNT). IEEE. pp. 1-7.

Rosado D.G., Gomez R., Mellado D. & Fernández-Medina E. (2012). Security analysis in the migration to cloud environments. Future Internet. 4(4): 469-487.

Rao R.V. & Selvamani K. (2015). Data Security Challenges and its Solutions in Cloud Computing. Procedia Computer Science. 48: 204-209.

Rewagad P. & Pawar Y. (2013). Use of Digital Signature with Diffie Hellman Key Exchange and AES Encryption Algorithm to Enhance Data Security in Cloud Computing. International Conference on Communication Systems and Network technologies. India. 437-439.

Sandeep Reddy Gudimetla (2023). Data encryption in cloud storage. International Research Journal of Modernization in Engineering Technology and Science. 6: 2582-5208.

Somani & Gaurav (2016). DDoS attacks in cloud computing: Collateral damage to non-targets. Computer Networks. 109: 157-171.

Sony R., Rao S.K.D. & Prasad D.B. (2013). Data Protection and Cloud Computing: A Jurisdictional Aspect. Law Journal of Higher School of Economics. Annual review. pp. 81-91.

Trần Cao Đệ (2013). Tổng quan về an ninh trên điện toán đám mây. Tạp chí Khoa học Trường Đại học Cần Thơ. tr. 46-53

Yan Z., Deng R.H. & Varadharajan V. (2017). Cryptography Data Security in Cloud Computing. Information Sciences. 387: 53-55.

Zhou M., Zhang R., Xie W., Qian W. & Zhou A. (2010). Security and privacy in cloud computing: A survey. Semantics Knowledge and Grid (SKG), 6th International Conference. pp. 105-112.