Tạp chí Khoa học Trường Đại học Cần Thơ
website: sj.ctu.edu.vn

TỔNG QUAN VỀ AN NINH TRÊN ĐIỆN TOÁN ĐÁM MÂY

Trần Cao Đệ[1]
[1] Khoa Công nghệ Thông tin & Truyền thông, Trường Đại học Cần Thơ

Thông tin chung:
Ngày nhận: 03/09/2013
Ngày chấp nhận: 21/10/2013

Title:
Overview on cloud computing security

Từ khóa:
An toàn mạng, kiến trúc hướng dịch vụ, IaaS, PaaS, SaaS

Keywords:
Network security, Service oriented architecture, IaaS, PaaS, SaaS

ABSTRACT

In recent years cloud computing has emerged as a new development phase of the Internet. Cloud computing, its service models in particular, allows the use of hardware, software as services, that leads a fundamental change in the application of information technology in practice - shift from investment to the hire of computing resources. However, cloud adoption is still controversy issues surrounding the safety and security of system. This paper provides an overview on safety issues and security of cloud computing, from the perspective of architecture, services as well as main characters of cloud computing.

TÓM TẮT

Mấy năm gần đây điện toán đám mây (cloud computing) nổi lên như là một giai đoạn phát triển mới của Internet. Điện toán đám mây mà cụ thể là các mô hình dịch vụ của nó cho phép sử dụng phần cứng, phần mềm như là dịch vụ làm thay đổi căn bản việc ứng dụng công nghệ thông tin trong thực tiễn – chuyển từ đầu tư sang thuê bao. Tuy nhiên, việc chấp nhận điện toán đám mây vẫn còn khá dè dặt xoay quanh vấn đề an toàn và an ninh hệ thống. Bài viết này cung cấp một cái nhìn tổng quan về vấn đề an toàn và an ninh của điện toán đám mây, từ góc độ kiến trúc cho đến dịch vụ cũng như tính chất của đám mây điện tử.

1 GIỚI THIỆU

Điện toán đám mây đang nhanh chóng nổi lên như một xu hướng công nghệ, hầu hết các nhà cung cấp công nghệ hoặc sử dụng phần mềm, phần cứng và cơ sở hạ tầng đều có thể tận dụng. Công nghệ và kiến trúc dịch vụ điện toán đám mây cho phép khách hàng của các dịch vụ này không sở hữu tài sản trong các đám mây điện tử nhưng trả tiền trên cơ sở mỗi lần sử dụng. Về bản chất, họ đang thuê cơ sở hạ tầng vật lý và các ứng dụng trong kiến trúc dùng chung. Dịch vụ điện toán đám mây có thể từ lưu trữ dữ liệu cho đến các ứng dụng Web của người dùng cuối, cùng với các dịch vụ điện toán tập trung khác.

Một sự khác biệt quan trọng giữa mô hình tính toán truyền thống và điện toán đám mây là khả năng mở rộng và tính chất co giãn mà điện toán đám mây cung cấp. Thay vì một kiến trúc hệ thống tĩnh, điện toán đám mây hỗ trợ khả năng tự động mở rộng quy mô và nhanh chóng thu hẹp quy mô, 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 thông lượng và nhu cầu. Điện toán đám mây cũng hỗ trợ nhiều người dùng, cung cấp các hệ thống cấu hình trong suốt một cách thống nhất mang tính chia sẻ được. Công nghệ ảo hóa cho phép các nhà cung cấp điện toán đám mây để chuyển đổi một máy chủ thành nhiều máy ảo, do đó loại bỏ máy tính client-server với các hệ thống một mục đích. Điều này tối đa hóa khả năng phần cứng và cho phép khách hàng tận dụng triệt để và kinh tế theo quy mô sử dụng.

Theo nghiên cứu của Gartner đưa ra trong 4, doanh thu trên toàn thế giới từ điện toán đám mây năm 2009 là 58.6 tỷ USD, dự báo đạt 148 tỷ USD vào 2015. Nghiên cứu gần đây của IDC 4 chỉ rõ doanh thu trên toàn thế giới từ điện toán đám mây công cộng (public cloud) năm 2010 là hơn 21,5 tỷ USD và sẽ đạt 72,9 tỷ USD vào năm 2015, tốc độ tăng trưởng hàng năm là 27,6%. Tốc độ tăng trưởng này gấp hơn bốn lần so với tốc độ tăng trưởng dự báo cho toàn thị trường CNTT trên thế giới nói chung (6,7%). Cũng theo IDC, điện toán đám mây luôn nằm trong tốp 10 các công nghệ đình đám nhất trong các năm từ 2009 đến nay trong lĩnh vực công nghệ thông tin.

Mặc dù có những lợi ích và tiềm năng phát triển như vậy nhưng điện toán đám mây vẫn còn gặp nhiều dè dặt trong chấp nhận và nhân rộng chủ yếu là vấn đề an toàn. Tạm gác qua vấn đề kỹ thuật, từ quan điểm của người dùng thì các vấn đề chủ yếu cản trở việc chấp nhận điện toán đám mây là :

– Các doanh nghiệp giao việc quản lý an ninh cho một bên thứ ba nên có thể không kiểm soát được vấn đề an ninh.

– Tài sản của nhiều người thuê bao khác nhau nằm trong cùng một vị trí (server) và sử dụng cùng một dịch vụ mà không biết rõ cách thức kiểm soát an ninh, bảo mật của nhà cung cấp.

– Thiếu sự đảm bảo an toàn, an ninh trong các hợp đồng giữa người dùng (người thuê bao) điện toán đám mây và các nhà cung cấp điện toán đám mây.

– Các máy chủ tập trung các tài sản có giá trị và công khai cơ sở hạ tầng làm tăng xác suất các cuộc tấn công nguy hiểm.

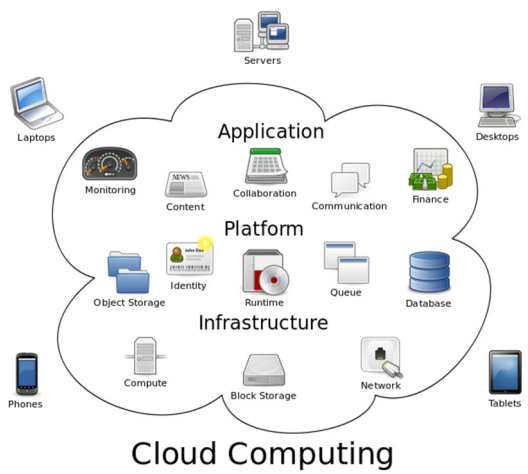
Bài viết này sẽ phân tích những thách thức và các vấn đề liên quan an ninh trên điện toán đám mây, những điểm yếu trong mô hình điện toán đám mây. Những vấn đề này sẽ được xem xét từ góc độ kiến trúc dịch vụ đến mô hình cùng với các đặc trưng của điện toán đám mây.

2 ĐIỆN TOÁN ĐÁM MÂY

2.1 Khái niệm

Thuật ngữ "Điện toán đám mây" (cloud computing) ra đời vào khoảng giữa năm 2007 nhằm để khái quát lại các hướng phát triển mới của công nghệ thông tin nhờ vào mạng Internet băng thông rộng và các trung tâm điện toán khổng lồ của các hãng công nghệ như Google, Amazon, IBM, Microsoft,… Điện toán đám mây gắn liền với một quan niệm mới về công nghệ thông tin, đó là: các nguồn lực điện toán khổng lồ như phần mềm, dữ liệu dịch vụ sẽ nằm tại các máy chủ ảo (đám mây) trên Internet thay vì trong máy tính của tổ chức, cá nhân để mọi người kết nối và sử dụng khi cần. Với các dịch vụ hạ tầng, phần mềm sẵn có trên Internet, doanh nghiệp không phải mua và duy trì hàng trăm, thậm chí hàng nghìn máy tính cũng như phần mềm cho công ty. Họ có thể thuê toàn bộ hạ tầng công nghệ thông tin như thuê bao điện thoại hay sử dụng điện, nước hàng ngày.

Theo định nghĩa của NIST 1: "Điện toán đám mây là một mô hình cho phép thuận tiện, truy cập mạng theo yêu cầu đến một nơi chứa các nguồn tài nguyên tính toán có thể chia sẻ và cấu hình được (ví dụ: mạng, máy chủ, lưu trữ, ứng dụng và dịch vụ), ở đó chúng có thể được cung cấp và phát hành nhanh chóng với nỗ lực quản lý hoặc tương tác với nhà cung cấp tối thiểu".



Hình 1: Minh họa cho điện toán đám mây theo Wikipedia 2

Điện toán đám mây đôi khi còn được coi là thế hệ Internet mới. Tự điển mở Wikipedia 2 định nghĩa: "Điện toán đám mây là việc sử dụng các tài nguyên máy tính (phần cứng và phần mềm) có sẵn từ xa và truy cập được qua mạng (thường là Internet)". Hình 1 phát họa khái niệm về điện toán đám mây. Điện toán đám mây cung cấp các tiện ích để truy cập vào tài nguyên chia sẻ và cơ sở hạ tầng chung, cung cấp dịch vụ theo yêu cầu qua mạng để thực hiện các hoạt động đáp ứng nhu cầu tác nghiệp. Vị trí của nguồn lực vật chất và thiết bị được truy cập là trong suốt, không được biết (và cũng không cần biết) đối với người dùng cuối (end user). Nó cũng cung cấp phương tiện cho người sử dụng (hay khách hàng) để phát triển, triển khai và

quản lý các ứng dụng của họ trên các đám mây, kể cả ảo hóa các nguồn tài nguyên, tự bảo trì và quản lý các ứng dụng.

2.2 Các dịch vụ cơ bản của điện toán đám mây

Điện toán đám mây cung cấp 3 mô hình dịch vụ cơ bản: dịch vụ hạ tầng (IaaS), dịch vụ nền tảng (PaaS) và dịch vụ phần mềm (SaaS), với một số đặc trưng chính: thuê bao theo yêu cầu, nhiều thuê bao, dùng bao nhiêu trả bấy nhiêu. Về mặt kỹ thuật, đám mây là một tập hợp tài nguyên tính toán rộng lớn và cung cấp 3 dịch vụ nói trên.

Dịch vụ hạ tầng (IaaS - Infrastructure as a Service) nói đến khả năng cung cấp cho khách hàng tài nguyên phần cứng như khả năng tính toán, xử lí (tức là CPU), lưu trữ, mạng và các tài nguyên khác, để khách hàng có thể triển khai và chạy phần mềm tùy ý, trong đó có thể bao gồm các hệ điều hành và các ứng dụng. Khách hàng sẽ không quản lý hoặc kiểm soát các cơ sở hạ tầng điện toán đám mây nhưng có kiểm soát đối với các hệ điều hành, lưu trữ, ứng dụng triển khai và kiểm soát có hạn chế các thành phần mạng được cung cấp. IaaS gắn liền với việc ảo hóa tài nguyên phần cứng. Những Nhà cung cấp IaaS điển hình là Amazon EC2, GoGrid và HP [19]. Nhà cung cấp dịch vụ Iaas sẽ chịu trách nhiệm mọi công việc nặng nề về thiết lập hạ tầng, thiết lập chức năng để cung cấp hạ tầng và thu phí thuê bao hạ tầng. Khách hàng có thể tăng giảm một cách tự động, thuận tiện về tài nguyên họ cần. Một số lượng lớn tài nguyên có thể được cung cấp và sẵn dùng trong một thời gian ngắn sau khi được yêu cầu và quan trọng hơn là hành vi của hệ thống không thay đổi, không có lỗi tiềm tàng do chuyển đổi từ hệ thống nhỏ sang hệ thống lớn hơn hay ngược lại.

Dịch vụ nền tảng (PaaS- Platform as a Service): đó là khả năng cung cấp cho khách hàng nền tảng để triển khai trên cơ sở hạ tầng điện toán đám mây các ứng dụng do khách hàng tạo ra từ ngôn ngữ lập trình và các công cụ hỗ trợ của nhà cung cấp. Khách hàng không quản lý hoặc kiểm soát cơ sở hạ tầng điện toán đám mây cơ bản như mạng, máy chủ, hệ điều hành, thiết bị lưu trữ, nhưng có kiểm soát đối với các ứng dụng triển khai và có thể thực hiện cấu hình môi trường lưu trữ. Có thể coi dịch vụ này cung cấp các phần mềm hệ thống cần thiết như là ngôn ngữ lập trình, môi trường lập trình, môi trường thực thi, hệ điều hành để người dùng truy cập tài nguyên và tạo ra các ứng dụng của mình. Các nhà cung cấp dịch vụ này điển hình như Microsoft Windows Azure, Google App Engine.

Dịch vụ phần mềm (SaaS – Software as a Service) đó là khả năng cung cấp cho khách hàng sử dụng các ứng dụng (phần mềm) của nhà cung cấp đang chạy trên một cơ sở hạ tầng điện toán đám mây. Các ứng dụng có thể truy cập từ các thiết bị khác nhau thông qua một giao diện người dùng như một trình duyệt web. Khách hàng không quản lý hoặc kiểm soát các cơ sở hạ tầng cơ bản đám mây nhưng có thể thiết lập cấu hình cho ứng dụng phù hợp với mình. Nhiều người trong chúng ta chắc đã sử dụng phần mềm trên điện toán đám mây của Google như: Gmail, Google Docs, trình tìm kiếm của Google,... Đó là những ví dụ điển hình về SaaS. Dịch vụ phần mềm được cung cấp dựa theo cơ chế dịch vụ web (web service) và các cổng thông tin điện tử (portal).

2.3 Các mô hình triển khai điện toán đám mây

Có bốn mô hình chính để triển khai điện toán đám mây đó là:

Hình 2: Năm đặc trưng quan trọng của điện toán đám mây

Đám mây công cộng (Public Cloud): đám mây được thiết lập và cung cấp cho rộng rãi người dùng thông qua Internet. Nó còn được biết như là đám mây nhiều thuê bao với các đặc trưng cơ bản là hạ tầng thống nhất, chính sách chung, nguồn lực chia sẻ cho nhiều thuê bao, đa qui mô. Mô hình đám mây này thường ít an toàn hơn các mô hình khác và thường chỉ cung cấp các dịch vụ phần mềm chung nhất như bộ phần mềm văn phòng, chat, họp trực tuyến,…

Đám mây riêng (Private Cloud): đám mây được thiết lập chỉ cho một tổ chức tương tự như một mạng nội bộ. Nó có thể được quản lý bởi chính tổ chức đó hoặc một bên thứ ba và có thể tồn tại trên cơ sở hạ tầng trước đó đã có. Mô hình này còn được gọi là đám mây nội bộ và thường chỉ dành quyền truy cập vào tài nguyên của nó cho người dùng trong nội bộ tổ chức là chủ sở hữu đám mây. Đặc điểm cơ bản của đám mây riêng là hạ tầng không đồng nhất, chính sách "may đo" và tùy chỉnh, tài nguyên dành riêng, cơ sở hạ tầng "cây nhà lá vườn". Tuy nhiên do chỉ có các tổ chức và người dùng được phép mới có thể truy cập nên nó có thể được bảo vệ bởi các quy trình, quy chế bảo mật riêng, điều này làm cho nó khó bị tấn công hơn.

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,…

Đám mây hỗn hợp (Hybrid Cloud): hạ tầng của đám mây là một sự kết nối của nhiều mô hình triển khai đám mây (chung, riêng, cộng đồng)

2.4 Đặc trưng của điện toán đám mây và lợi ích của nó

Điện toán đám mây có 5 đặc trưng quan trọng (xem Hình 2):

Khả năng co giãn (scalability): đám mây có thể cung cấp tài nguyên tính toán theo yêu cầu. Việc cung cấp này trên nguyên tắc là động và nhiều thuê bao, vì vậy tránh lãng phí (dùng bao nhiêu trả bấy nhiêu).

– Khả năng quản trị và vận hành (manageability): đây là khả năng điều khiển, kiểm soát hệ thống và tính cước phí thuê bao.

– Khả năng truy cập (accessibility) và khả chuyển: truy cập mọi lúc mọi nơi một cách nhất quán và khả năng truy cập với các thiết bị nhỏ, yếu (thin client) như là điện thoại di động.

– Hiệu năng cao và tối ưu hóa (performance and Optimization): hạ tầng đám mây giải quyết và che dấu mọi vấn đề phức tạp trong tính toán song song, cân bằng tải, lập lịch để cung cấp khả năng tính toán hiệu năng cao và tối ưu hóa.

– Khả năng sẵn dùng với độ tin cậy cao (availability): hạ tầng đám mây cùng được cung cấp rộng rãi cho người dùng với khả năng chịu đựng lỗi cao, hệ thống tồn tại lâu dài và khả năng bảo mật tốt.

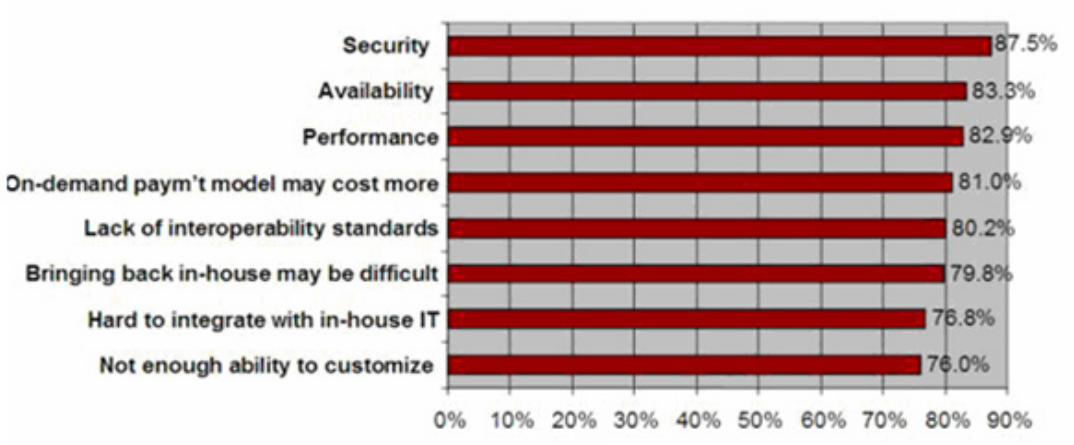
3 NGHIÊN CỨU CÓ LIÊN QUAN VỀ AN TOÀN TRÊN ĐIỆN TOÁN ĐÁM MÂY

Rõ ràng rằng có nhiều vấn đề cần bàn trong quyết định chấp nhận điện toán đám mây. Hình 3 cho một số vấn đề chính trên điện toán đám mây. Đây là những chủ đề luôn được quan tâm, theo nghiên cứu đã chỉ ra trong 5, vấn đề an toàn được đặt hàng đầu. Vấn đề thì khó nhưng lý do có vẻ thật đơn giản, bởi vì người ta đặt dữ liệu của mình (loại tài sản (rất) có giá trị) trên một máy tính ở "trên mây", dùng một phần mềm của ai đó (một nhà cung cấp) ở một nơi nào đó không biết rõ và chạy trên một máy ảo mà máy thật (tức là CPU vật lý) nằm ở đâu cũng không rõ nốt. Có rất nhiều nỗi lo lắng trong hoàn cảnh như vậy: mất dữ liệu, thông tin bị rò rỉ, bị theo dõi, bị lấy cắp, lừa đảo, nghẽn mạng,…

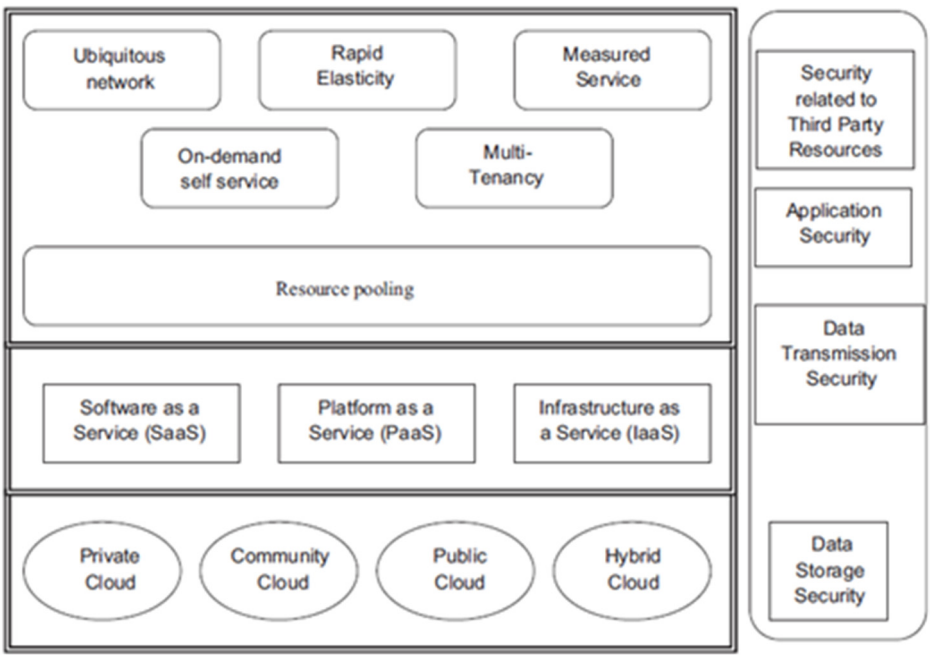
Nhiều nghiên cứu về vấn an toàn trên điện toán đám mây đã được thực hiện. Nhóm "Cloud Computing Use Cases" 6 thảo luận nhiều vấn đề liên quan tới mô hình điện toán đám mây trên các quan điểm của người dùng, nhà phát triển và kỹ sư bảo mật. Văn phòng an toàn thông tin và mạng Châu Âu (ENISA) 7 đưa ra các rủi ro, các ảnh hưởng, các điểm yếu của điện toán đám mây. Một nghiên cứu về an toàn được ràng buộc bằng hợp đồng 9 cố gắng đưa ra các đặc tả liên quan tới vị trí đặt dữ liệu, phân nhóm dữ liệu và phục hồi dữ liệu. Một số vấn đề chuyên biệt về an toàn trên điện toán đám mây như toàn vẹn dữ liệu, tính riêng tư và thông tin nhạy cảm được thảo luận trong 10. Vấn đề kỹ thuật tấn công, chẳng hạn kiểu tấn công XML (XML-attack) có thể tìm thấy trong 11, lỗ hổng bảo mật đám mây có thể tìm thấy trong 12. Các thách thức an toàn và bảo mật liên quan đến các mô hình dịch vụ của điện toán đám mây, đặc biệt là mô hình SaaS có thể tham khảo trong 13.

Vấn đề an toàn trên điện toán đám mây là rất phức tạp vì nó liên quan đến nhiều khía cạnh và chủ thể: kiến trúc, dịch vụ điện toán đám mây, đặc trưng của đám mây, thuê bao, chủ sở hữu, chính sách bảo

mật dữ liệu,… Hình 4 cho một hình ảnh rộng, khái quát về sự phức tạp của vấn đề này. Phần tiếp theo của bài viết sẽ đi vào tổng hợp về vấn đề an ninh trên điện toán đám mây từ góc độ kiến trúc, dịch vụ và một số đặc điểm chính của điện toán đám mây.



Hình 3: Các vấn đề quan tâm hàng đầu trong điện toán đám mây 5



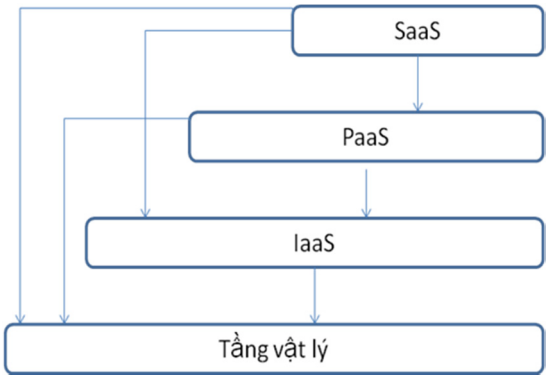
Hình 4: Sự phức tạp của vấn đề an toàn trên điện toán đám mây 13

4 MỘT SỐ VẤN ĐỀ ĐƯỢC QUAN TÂM VỀ AN TOÀN TRÊN ĐIỆN TOÁN ĐÁM MÂY

4.1 Vấn đề an toàn liên quan đến kiến trúc của điện toán đám mây

Một đám mây điện tử là một cụm máy tính kết nối nhau thông qua mạng cục bộ hoặc mạng diện rộng trên cơ sở ảo hóa tài nguyên phần cứng nhờ chức năng ảo hóa để cung cấp một cách trong suốt 3 dịch vụ cơ bản của điện toán đám mây là SaaS, PaaS và IaaS. Mô hình triển khai đám mây có thể là công cộng, đám mây riêng hoặc cộng đồng hay hỗn hợp như đã nói ở phần trên.

Các dịch vụ điện toán đám mây có kiến trúc phân tầng (layer), mỗi tầng cung cấp các dịch vụ và tiện ích (chức năng) riêng của nó trên cơ sở các dịch vụ và tiện ích của tầng thấp hơn (xem Hình 5). 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 1 dịch vụ hay tiện ích.



Hình 5: Kiến trúc phân tầng dịch vụ trong điện toán đám mây

4.1.1 An ninh ở mức hạ tầng

An ninh của các dịch vụ ở tầng thấp như tầng vật lý hay hạ tầng (IaaS) phụ thuộc vào nhà cung cấp, tức là chủ sở hữu của đám mây. Hiện tại, có một số nhà cung cấp dịch vụ IaaS nhưng chưa có chuẩn nào về an ninh cho các dịch vụ này. Về mặt nguyên tắc, khách hàng thuê bao dịch vụ IaaS có thể áp đặt các chính sách an ninh của mình bằng cách phát triển các dịch vụ hay tiện ích riêng thông qua các dịch vụ của tầng vật lý và các dịch vụ IaaS của nhà cung cấp. Chính sách về an toàn ở mức này là rất phức tạp vì nhiều chính sách khác nhau áp đặt lên cùng một môi trường phần cứng (vật lý).

Những mối đe dọa an toàn ở mức này có thể liên quan tới máy chủ ảo (Virtual Machine) như là vi-rút và các phần mềm độc hại khác. Nhà cung cấp dịch vụ chịu trách nhiệm chính về giải pháp cho vấn đề này. Khách hàng thuê bao cũng có thể thực hiện các giải pháp và chính sách an toàn riêng cho mình, từ đó làm gia tăng gánh nặng lên phần cứng và hiệu năng chung của hệ thống. Các máy chủ ảo vẫn có thể bị lây nhiễm hay bị kiểm soát bởi phần mềm độc hại. Trong trường hợp này, các chính sách an ninh của khách hàng có thể bị vô hiệu, như vậy nhà cung cấp dịch vụ phải là người có vai trò chính trong an ninh ở mức này. Ngoài ra, vì IaaS khai thác hạ tầng vật lý và chính sách chung như DNS Server, Switch, IP protocol,… Vì vậy, khả năng bị tấn công vào "khách hàng yếu nhất" sau đó "lây lan" cho các khách hàng khác. Vấn đề này hiện nay khách hàng thuê bao không thể can thiệp gì vì nhiều máy chủ ảo chia sẻ cùng tài nguyên vật lý như CPU, bộ nhớ, đĩa,… Mọi ánh xạ vật lý-máy ảo, máy ảo-vật lý đều thông qua một "bộ ảo hóa", nếu bộ này bị phần mềm độc hại kiểm soát thì toàn bộ khách hàng trong đám mây sẽ bị cùng một mối hiểm họa như nhau.

4.1.2 An ninh ở mức dịch vụ nền tảng

Ở mức trung gian, dịch vụ nền tảng (PaaS) dựa trên dịch vụ tầng dưới (IaaS) và cung cấp dịch vụ của mình cho tầng trên nó (SaaS). Ở mức này, các dịch vụ hay tiện ích về an toàn có thể được cài đặt thêm hoặc cấu hình các dịch vụ được cung cấp từ tầng dưới. Ở đây, người dùng có thể quản trị phần thuê bao của mình để tạo ra môi trường thực thi các ứng dụng. Hiện nay, dịch vụ PaaS của đám mây dựa trên mô hình kiến trúc hướng dịch vụ (SOA) vì vậy những nguy cơ về an toàn giống hệt như những nguy cơ an toàn của SOA như tấn công từ chối dịch vụ, tấn công XML và nhiều cách tấn công khác 1114.

Vì dịch vụ nền tảng là dịch vụ đa thuê bao, nhiều người dùng nên cơ chế xác thực, chứng thực là rất quan trọng. Trách nhiệm bảo mật và an toàn trong trường hợp này liên quan đến cả nhà cung cấp, người thuê bao và người dùng (user). Các dịch vụ PaaS phải cung cấp môi trường để phát triển ứng dụng bao gồm chức năng tác nghiệp, các chức năng an toàn và quản lí hệ thống. Nhà cung cấp cần có cơ chế bắt buộc chứng thực để truy cập các dịch vụ PaaS, người thuê bao có trách nhiệm phát triển hay cung cấp các chức năng bảo mật cần thiết thông qua cơ chế chứng thực chung và người dùng phải có trách nhiệm bảo vệ tài khoản đăng nhập cá nhân của mình.

4.1.3 An ninh ở mức dịch vụ phần mềm

Ở mức dịch vụ phần mềm (SaaS), các phần mềm được cung cấp như là dịch vụ trên mạng, sử dụng các chính sách bảo mật dữ liệu và tài nguyên khác từ các tầng bên dưới cung cấp. Một số dịch vụ phần mềm khá phổ biến hiện nay là Google Search Engine, Google mail… Khách hàng của các dịch vụ này không biết được dữ liệu của mình được quản lí và khai thác như thế nào và nó nằm ở đâu trên thế giới này. Vấn đề an ninh ở đây liên quan đến bảo mật dữ liệu, rò rỉ thông tin nhạy cảm và nguy cơ bị tấn công từ chối truy cập… Trách nhiệm về an toàn được chia sẻ cho nhà cung cấp hạ tầng đám mây và nhà cung cấp dịch vụ phần mềm. Người dùng đầu cuối (end user) chỉ là người dùng phần mềm với các lựa chọn cấu hình khác nhau được cung cấp bởi phần mềm nên không có nhiều vai trò trong an toàn hệ thống. Người dùng cuối chỉ biết tin vào nhà cung cấp phần mềm và các cam kết của nhà cung cấp về trách nhiệm bảo mật. Thông thường các cam kết này có thể là điều khoản trong hợp đồng thuê bao phần mềm, như là: an toàn thông tin và chất lượng dịch vụ. Chúng thường bao gồm: dung lượng dữ liệu, toàn vẹn dữ liệu, chính

sách về phân tán, sao lưu và phục hồi dữ liệu khi có sự cố, độ tin cậy, tính riêng tư và an toàn mạng cùng với các cam kết khác về chất lượng dịch vụ như dung lượng đường truyền, tính sẵn dùng 13.

Ở mức này, các phần mềm được cung cấp trên nền web (web-based application). Các web này thường được đặt ở máy chủ ảo trên đám mây, cho nên chúng phải được kiểm tra bằng cách quét các yếu điểm web nhờ vào một ứng dụng quét nào đó, ví dụ như các phần mềm có các chức năng như trong công bố 15. Các tường lửa có thể được dùng để ngăn chặn các tấn công vào điểm yếu đã biết của các phần mềm nền web. Những công việc này thuộc về nhà cung cấp phần mềm hoặc đám mây, người dùng cuối nhiều lắm là tham gia vào lựa chọn các cấu hình (option) khác nhau mà thôi. Tình hình này có thể dẫn đến những lộn xộn trong cấu hình an toàn chung của hệ thống do tính chất đa thuê bao, kéo theo những lỗ hổng trong an toàn hệ thống. Vì vậy, các nhà cung cấp phải có những chính sách chung bắt buộc và cách kiểm soát sao cho những cấu hình an toàn, bảo mật phải nhất quán, chặt chẽ và không có lỗ hổng.

4.2 Vấn đề quản lí an toàn hệ thống

Phần trên vừa trình bày cho thấy tính phức tạp trong "kỹ thuật" an toàn trên đám mây từ góc độ kiến trúc và dịch vụ của điện toán đám mây. Phần này xin đề cập đến một số khía cạnh về quản lí, vốn không thể tách rời với kỹ thuật nhằm đảm bảo cho sự áp dụng chính sách bảo mật đúng đắn, cộng tác và có trách nhiệm giữa các bên có liên quan trong điện toán đám mây. Nghiên cứu về quản lí an toàn trên đám mây là rất phức tạp vì nó liên quan đến số lượng lớn người có liên quan với các yêu cầu (requirement) khác nhau về an toàn. Việc quản lí an toàn liên quan tới việc xây dựng các yêu cầu về an toàn, đặc tả chính sách an toàn, cơ chế kiểm soát và các cấu hình khác nhau về an toàn tương ứng với các chính sách đặc thù. Việc quản lí này là động vì luôn phải đáp ứng các yêu cầu mới, các phản hồi từ môi trường và từ chính quá trình kiểm soát an toàn.

Điện toán đám mây cung cấp các dịch vụ trên cơ sở một hợp đồng trách nhiệm (SLA – Service Level Agreement), đây là pháp lý quan trọng trong các tranh chấp, bất đồng sau này. Hợp đồng thông thường bao gồm chất lượng dịch vụ, tính sẵn dùng, độ tin cậy và an toàn. Và như bao cam kết hợp đồng, nó có những điều khoản về trả phí dịch vụ xử phạt và bồi thường. Một đòi hỏi cao về an toàn thường dẫn đến một tiêu tốn nhiều nguồn lực và vì vậy mức giá dịch vụ sẽ cao lên tương ứng. Một mẫu (template) hướng dẫn về hợp đồng dịch vụ đám mây có thể tìm thấy tại 16. Độc giả quan tâm sâu phần này có thể xem thêm trong 17. Cần lưu ý rằng những đòi hỏi khắc khe về an toàn có thể ảnh hưởng đến hiệu năng chung của hệ thống (cồng kềnh hơn, chậm hơn,…). Vì vậy, cần có sự cân bằng giữa yêu cầu an toàn, chi phí và hiệu năng của hệ thống. Nhiều khía cạnh khác liên quan đến quản lí an toàn cũng như các cơ quan quản lí an toàn đám mây có thể tìm thấy trong công bố 18.

5 KẾT LUẬN

Mặc dù điện toán đám mây đang được coi là một cuộc cách mạng Internet làm thay đổi cách ứng dụng công nghệ thông tin, nhưng việc chấp nhận nó vẫn còn nhiều vấn đề và e ngại chung quanh câu hỏi an toàn, bảo mật thông tin. Lợi ích của điện toán đám mây là rõ ràng và vô cùng hấp dẫn, nó làm giảm nhẹ chi phí đầu tư và gánh nặng bảo trì phần cứng, phần mềm, tuy nhiên từ kiến trúc, dịch vụ và các đặc điểm của điện toán đám mây cho thấy vẫn còn nhiều câu hỏi đặt ra cho vấn đề an toàn và bảo mật. Các vấn đề bảo mật ở cấp càng thấp thì vai trò và trách nhiệm của nhà cung cấp càng lớn, nhưng khách hàng có thể cảm thấy bất an vì họ không nắm rõ. Điều này có thể khắc phục bằng các hợp đồng (SLA) rõ ràng, chặt chẽ và tin cậy. Vấn đề an toàn có thể liên quan tới máy chủ ảo, bộ ảo hóa cũng như là kiến trúc hướng dịch vụ SOA.

Mặt khác, vấn đề an toàn trên điện toán đám mây không chỉ là trách nhiệm của nhà cung cấp dịch vụ mà còn là trách nhiệm của tất cả các bên có liên quan trong đám mây: nhà cung cấp, khách hàng, người dùng cuối. Vấn đề này có lẽ vẫn còn phải cần một thời gian nữa để có thể có giải pháp thỏa đáng làm tăng độ an toàn của đám mây, nhất là đám mây công cộng (public).

Điện toán đám mây còn rất mới và còn tiềm năng phát triển và ứng dụng, vấn đề an toàn của đám mây cần được nghiên cứu tiếp tục để ngày càng trở nên an toàn hơn. Mặt khác, sử dụng đám mây như thế nào cho có lợi, cân bằng giữa lợi ích và tính an toàn là sự tính toán của các nhà quản lí công ty, doanh nghiệp và sự tư vấn sáng suốt của các chuyên gia công nghệ thông tin.

TÀI LIỆU THAM KHẢO

1. Peter Mell, Timothy Grance, The NIST Definition of Cloud Computing, National Institute of Standards and Technology, Special Publication 800-145, September 2011.

2. http://en.wikipedia.org/wiki/Cloud_computing
3. Frank Gens, Robert P Mahowald and Richard L Villars, IDC Cloud Computing 2010.
4. http://www.idc.com/prodserv/idc_cloud.jsp
5. Chang, L, Ti ; Chin L; Chang, A.Y.; Chun J, C;(2010), Information security issue of enterprises adopting the application of cloud computing, IEEE 2010 Sixth International Conference on Networked Computing and Advanced Information Management (NCM), pp.645, 16-18 Aug. 2010.
6. Cloud Computing Use Case Discussion Group, "Cloud Computing Use Cases Version 3.0," 2010.
7. ENISA, "Cloud computing: benefits, risks and recommendations for information security," 2009,
8. http://www.enisa.europa.eu/act/rm/files/deliverables/cloud-computingrisk-assessment
9. Balachandra Reddy Kandukuri, Ramakrishna Paturi and Atanu Rakshit, "Cloud Security Issues," in Proceedings of the 2009 IEEE International Conference on Services Computing, 2009, pp. 517-520.
10. Kresimir Popovic , Zeljko Hocenski, "Cloud computing security issues and challenges," in The Third International Conference on Advances in Human-oriented and Personalized Mechanisms, Technologies, and Services, 2010, pp. 344-349.
11. Meiko Jensen, Jörg Schwenk, Nils Gruschka and Luigi Lo Iacono, "On Technical Security Issues in Cloud Computing," in IEEE ICCC, Bangalore 2009, pp. 109-116.
12. Bernd Grobauer, Tobias Walloschek and Elmar Stöcker, "Understanding Cloud-Computing Vulnerabilities," IEEE Security and Privacy, vol. 99, 2010.
13. S. Subashini, ,Kavitha, V., "A survey on security issues in service delivery models of cloud computing," Journal of Network and Computer Applications, Vol. 34, 2011.
14. Z. Wenjun, "Integrated Security Framework for Secure Web Services," in IITSI 2010 , pp. 178-183.
15. F. Elizabeth, , Vadim, Okun, "Web Application Scanners: Definitions and Functions," in HICSS 2007, pp. 280b-280b.
16. http://www.ibm.com/developerworks/cloud/library/cl-slastandards/
17. Wieder, P.; Butler, J.M.; Theilmann, W.; Yahyapour, R. (Eds.), Service Level Agreements for Cloud Computing, Springer, XXII, 2011.
18. Mohamed Al Morsy, John Grundy and Ingo Müller, An Analysis of The Cloud Computing Security Problem, Proceedings of APSEC 2010 Cloud Workshop, Sydney, Australia, 2010.
19. http://www.clouds360.com/iaas.php