Xu hướng kiểm toán và dịch vụ đảm bảo đối với lưu trữ dữ liệu trên đám mây và kinh nghiệm cho Việt Nam

ThS. Phùng Anh Thư*

Lưu trữ dữ liệu trên đám mây bao gồm việc sử dụng các trung tâm dữ liệu từ xa để lưu trữ dữ liệu người dùng mà người dùng thực sự không có quyền kiểm soát. Điều này đã đưa ra yêu cầu tạo điều kiện cho kiểm toán dịch vụ đối với lưu trữ đám mây ra đời, để người dùng có thể dựa vào Kiểm toán viên (KTV) để kiểm tra tính toàn vẹn của dữ liệu được lưu trữ trong đám mây. Tuy nhiên, KTV không nên đưa ra các mối đe dọa mới đối với sự riêng tư của dữ liệu người dùng và không nên tăng gánh nặng trực tuyến lên người dùng điện toán đám mây. Bài báo này tổng hợp các đề xuất từ các nghiên cứu về kế hoạch lưu trữ đám mây an toàn hỗ trợ bảo vệ sự riêng tư của loại hình kiểm toán dịch vụ này.

Từ khóa: Kiểm toán, lưu trữ đám mây.

Auditing trends and assurance for cloud datastore and experience for Vietnam

Cloud datastore includes the use of remote data centres to store user data that the user does not actually have control over. This has provided a requirement for service auditing upon cloudstore to be made, so that users can rely on the Auditor to verify the integrity of the data stored in the cloud. However, Auditor should not present new threats to the privacy of user data and should not expand the burden online on cloud computing users. This paper synthesizes recommendations from research into secure cloud hosting plans that support the protection of the privacy of this type of service audit.

Keywords: Audit cloudstore.

1.Giới thiệu

Điện toán đám mây (ĐTĐM) đã phát triển như là điều tốt nhất tiếp theo trong thế giới Internet, có thể cung cấp tất cả mọi thứ, từ khả năng tính toán không giới hạn đến không gian sẵn có của cơ sở hạ tầng máy tính, các ứng dụng, không gian lưu trữ, quy trình kinh doanh để hợp tác cá nhân như một dịch vụ cho người dùng bất cứ khi nào và bất cứ nơi nào người sử dụng muốn. ‘‘Cloud’’ ở đây có nghĩa là mạng máy tính, CPU, thiết bị lưu trữ, phần cứng, dịch vụ cộng tác để cung cấp toàn bộ gói tính toán như một dịch vụ. Cloud có thể mở rộng, nghĩa là nó có khả năng mở rộng và thu nhỏ để phù hợp với nhu cầu của các nguồn lực. Nó tạo điều kiện cho các giao diện lập trình ứng dụng (API) có sẵn được lập hóa đơn theo cách sử dụng (mô hình trả tiền khi bạn đi).

Điều mới mẻ mang tính đột phá của ĐTĐM không nằm ở bản chất công nghệ, mà là mô hình hướng dịch vụ, và mang lại sự thay đổi trong nhận thức về cách cung cấp dịch vụ (cho nhà cung cấp) và cách thuê bao sử dụng dịch vụ (cho người sử

*Trường Đại học Nguyễn Tất Thành

dụng). Tất cả được đưa đến người sử dụng (NSD) dưới hình thức dịch vụ, từ nguồn cung ứng điện toán hàng ngày, đơn giản giống như những nguồn cung ứng điện, nước.

Trong mô hình cung cầu các dịch vụ ĐTĐM, vai trò tham gia của các bên bao gồm NSD, Nhà cung ứng dịch vụ, Nhà hỗ trợ triển khai dịch vụ và Nhà quy hoạch chính sách.

NSD là các đối tượng trả tiền thuê bao để sử dụng dịch vụ ĐTĐM, phương thức trả tiền theo cách dùng bao nhiêu, trả bấy nhiêu (pay-per-use). NSD có thể là một cá nhân (ví dụ một NSD dịch vụ hòm thư điện tử của Google, hiện tại dịch vụ này đang được cung cấp miễn phí). NSD cũng có thể là một tổ chức, hoặc một doanh nghiệp (ví dụ một doanh nghiệp muốn sử dụng dịch vụ hệ thống thư điện tử của Microsoft, trong trường hợp này phí thuê bao tính theo đơn vị số hộp thư và theo từng tháng) muốn tận dụng dịch vụ được cung cấp sẵn bởi các nhà cung cấp dịch vụ ĐTĐM, thay vì họ phải tự đầu tư và vận hành những hệ thống IT trong nội bộ để có được những dịch vụ đó.

Nhà cung ứng dịch vụ là các doanh nghiệp, hãng tin học sở hữu và vận hành hệ thống hạ tầng cho ĐTĐM để cung cấp các dịch vụ khác nhau trên hạ tầng đó đến NSD. Microsoft, IBM, Google... là những ví dụ cho vai trò của nhà cung cấp dịch vụ ĐTĐM.

Nhà hỗ trợ triển khai dịch vụ là các công ty tin học cung cấp các giải pháp, các sản phẩm và/hoặc dịch vụ để thiết lập và hỗ trợ sự cung cấp các dịch vụ ĐTĐM. Cisco, Symantec, TrenMicro McAfee... là những ví dụ cho vai trò hỗ trợ triển khai dịch vụ ĐTĐM, khi họ cung cấp các giải pháp cho lộ trình hợp nhất và ảo hóa các trung tâm dữ liệu, các kiến trúc hạ tầng liên quan (Cisco), hay các giải pháp bảo mật thông tin cho những dịch vụ cung cấp qua Internet (Cisco, Symantec, Trendmicro). Nhà hỗ trợ triển khai dịch vụ ĐTĐM có thể là các công ty tin học cung cấp các sản phẩm phần mềm sẵn có để Nhà cung ứng dịch vụ đóng gói thành dịch vụ đưa đến NSD. Nhà hỗ trợ triển khai dịch vụ cũng có thể là các công ty cung cấp dịch vụ chuyển đổi cho một tổ chức doanh nghiệp muốn chuyển đổi hệ thống đang được chính họ vận hành sang nền tảng đám mây của các Nhà cung ứng dịch vụ.

Nhà quy hoạch chính sách là các cơ quan quản lý Chính phủ, hoặc các tổ chức chuyên ngành quốc tế. Với các điều luật nhất định, những cơ quan, tổ chức này sẽ cho phép hoặc không cho phép việc sử dụng các dịch vụ ĐTĐM. Ví dụ, khi một tổ chức

thuê bao dịch vụ ĐTĐM của nhà cung cấp dịch vụ, dữ liệu của họ sẽ được quản lý bởi nhà cung cấp dịch vụ. Nếu điều này không được chấp thuận bởi cơ quan quản lý chính sách thì tổ chức sẽ không được phép thuê bao dịch vụ ĐTĐM.

Xét trên yếu tố về đối tượng sử dụng, dịch vụ ĐTĐM có thể được phân loại thành dịch vụ Cộng đồng (Public) hay dịch vụ Riêng biệt (Private). Dịch vụ cộng đồng được cung cấp đến tất cả mọi đối tượng sử dụng Internet (Amazon Web Services là một ví dụ điển hình). Không giống như vậy, dịch vụ ĐTĐM riêng biệt chỉ được cung cấp cho một nhóm đối tượng nhất định và nhà cung cấp dịch vụ chỉ sử dụng những nguồn tài nguyên hạ tầng của riêng họ.

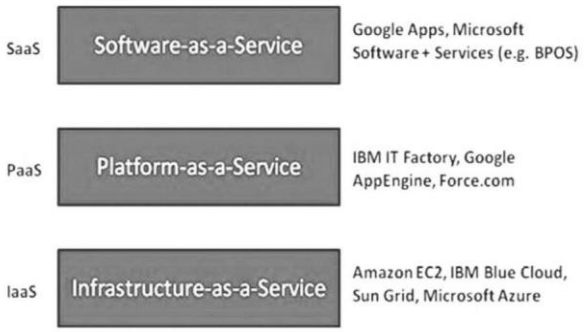
Từ quan điểm tính năng dịch vụ (với thành ngữ trong tiếng Anh: as-a-service), các sản phẩm ĐTĐM có thể được chia thành 3 loại hình chính là IaaS, PaaS và SaaS như được minh họa trong Hình 1 [3].

- *Dịch vụ cung cấp hạ tầng - Infrastructure as a Service (IaaS):* Dịch vụ này cung cấp cho NSD thuê các tài nguyên hạ tầng (ví dụ như các máy chủ ảo, dung lượng lưu trữ) theo nhu cầu sử dụng. Dịch vụ lưu trữ Amazon S3, hay tài nguyên điện toán Amazon EC2, IBM Blue Cloud là những ví dụ của IaaS.

- *Dịch vụ cung cấp nền tảng - Platform as a Service (PaaS):* Dịch vụ này cung cấp môi trường phát triển phần mềm đã có sẵn để NSD có thể thiết lập và tự phát triển trên nền tảng đó các ứng dụng hay các dịch vụ của mình. Microsoft Azure, Google App Engine, Amazon Relation Databse Services là những ví dụ của PaaS.

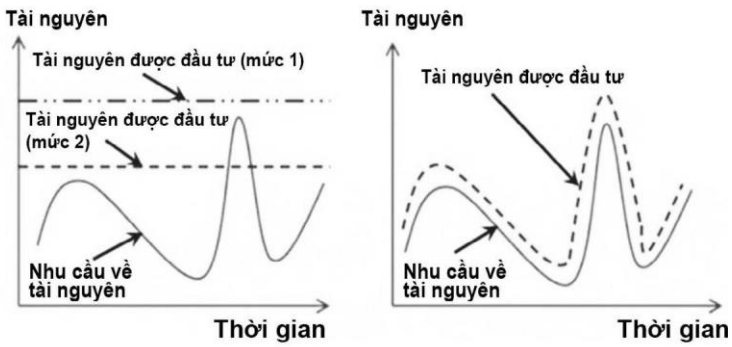
- *Dịch vụ cung cấp phần mềm - Software as a Service (SaaS):* Dịch vụ này cung cấp cho NSD các ứng dụng đã được cài đặt và cấu hình sẵn trên ĐTĐM. NSD chỉ việc dùng từ xa các ứng dụng, thay vì phải cài đặt, cấu hình trên các máy trạm của họ. Ví dụ cho loại hình này là các ứng dụng trên nền Web, hoặc các ứng dụng tại chỗ nhưng sử dụng tài nguyên (xử lý, lưu trữ) qua mạng Internet. Google Apps, Gmail, Facebook là một vài ví dụ điển hình của SaaS.

Hình 1. Các loại hình dịch vụ ĐTĐM



Với việc dùng các dịch vụ ĐTĐM do các nhà cung cấp dịch vụ mang lại, ưu điểm nổi trội là NSD sẽ trả (thuê bao) tài nguyên theo sát với nhu cầu thực sự (pay-as-you-go), tránh được sự cứng nhắc về tài nguyên và những lãng phí hoặc không đảm bảo chất lượng dịch vụ do sự cứng nhắc đó. Kiểm soát chi phí nhờ đó cũng sẽ trở nên linh hoạt và theo sát với nhu cầu của doanh nghiệp (Hình 2b).

Hình 2. Tương quan giữa mức tài nguyên được NSD đầu tư (hoặc trả tiền thuê bao) và nhu cầu sử dụng đầu tư



Bên trái (a): mô hình tự cung cấp dịch vụ bằng hệ thống riêng sẽ dẫn đến tình trạng phải đầu tư thừa tài nguyên (Mức 1) để đảm bảo chất lượng dịch vụ, hoặc đầu tư ít tài nguyên hơn (Mức 2) nhưng phải chấp nhận sẽ có sự suy giảm và không đảm bảo về chất lượng dịch vụ trong quá trình sử dụng. Bên phải (b): Sử dụng dịch vụ ĐTĐM sẽ tránh được sự cứng nhắc về đầu tư tài nguyên bằng cách chỉ trả thuê bao theo nhu cầu sử dụng thực tế (pay-as-you-go) mà vẫn đảm bảo chất lượng dịch vụ.

Tuy nhiên, việc gia công dữ liệu cho một Nhà cung cấp Dịch vụ Đám mây (CSP), một thực thể hành chính riêng biệt, vừa giải phóng kiểm soát

của người dùng qua dữ liệu của mình. Vì vậy, độ chính xác của dữ liệu trong đám mây là vấn đề. Một số rủi ro có thể được liệt kê dưới đây:

- Có rất nhiều điều có thể thúc đẩy CSP không hành xử trung thực với người dùng về tình trạng dữ liệu được thuê ngoài của mình.

- CSP không nên sử dụng dữ liệu của người dùng cho lợi ích của họ.

- Mặc dù kiến trúc lưu trữ đám mây an toàn hơn và mạnh mẽ hơn các máy tính cục bộ của người sử dụng nhưng bên cạnh đó cũng có các mối đe dọa từ bên ngoài và bên trong.

Việc sở hữu vật lý của dữ liệu được thuê ngoài không còn nữa. Việc tải xuống dữ liệu đã lưu trữ để kiểm tra tính toàn vẹn của nó có thể không phải là một giải pháp kinh tế và thực tế khả thi dựa trên chi phí đầu vào/đầu ra cao cũng như chi phí truyền tải qua mạng. Hơn nữa, các kích thước dữ liệu có thể lớn và truy cập vào toàn bộ tập tin từ các máy chủ từ xa có thể tốn kém chi phí I/O cho máy chủ lưu trữ. Truyền tệp trên mạng có thể tiêu tốn băng thông lớn. Về mặt lịch sử, tốc độ tăng dung lượng lưu trữ nhanh hơn tốc độ băng thông mạng. Hơn nữa, hoạt động của I/O để thiết lập độ chính xác của dữ liệu cũng sử dụng cùng một băng thông của máy chủ mà nếu không được sử dụng cho các hoạt động thường xuyên của lưu trữ và truy xuất dữ liệu.

Để tiết kiệm cho người dùng khỏi gánh nặng tải toàn bộ dữ liệu và kiểm tra tính toàn vẹn của nó, cần thận trọng khi cho phép kiểm tra các kho lưu trữ trong đám mây để người dùng có thể dựa vào một kiểm toán viên không phải là bên thứ ba để kiểm toán các nguồn dữ liệu bên ngoài khi cần thiết. Cũng như nó tiết kiệm cho các máy chủ đám mây khỏi các vấn đề băng thông và quan trọng nhất đảm bảo tính toàn vẹn dữ liệu.

Theo nghiên cứu của P. K. Deshmukh, V. R. Desale, R. A. Deshmukh (2013), trong thế giới ngày nay, cơ chế kiểm tra bên thứ ba (KTV) cho tính toàn vẹn dữ liệu ngày càng trở nên quan trọng và có thể sớm trở thành không thể tránh được để đảm bảo cho bảo vệ dữ liệu và độ tin cậy của dịch vụ. Kiểm toán viên bên thứ ba là một chuyên gia theo chiều dọc và có khả năng và khả năng cần thiết mà người dùng thông thường không có. Kiểm toán viên được giao nhiệm vụ đánh giá nguy cơ của các dịch vụ lưu trữ đám mây thay mặt người dùng. KTV sẽ yêu cầu CSP cung cấp bằng chứng rằng dữ liệu an toàn và chưa được sửa đổi.

Kiểm toán dịch vụ có nghĩa là cho phép một cơ quan bên ngoài, để đánh giá tính toàn vẹn của dữ liệu được thuê ngoài của người dùng. Tuy nhiên, theo H. Shacham and B. Waters (2008); Q. Wang, C. Wang, K. Ren, W. Lou, and J. Li (2011); C. Wang, K. Ren, W. Lou and J. Li, (2010) hầu hết các chương trình đều không bảo đảm sự riêng tư của dữ liệu người dùng và do đó dữ liệu được tiết lộ cho các kiểm toán viên bên thứ ba. Trong khi đó, M.A. Shah, M. Baker, J.C. Mogul, and R. Swaminathan (2007) M.A. Shah, R. Swaminathan, and M. Baker (2007) người dùng cũng muốn quá trình kiểm toán để giới thiệu các lỗ hổng mới về rò rỉ dữ liệu cho các kiểm toán viên bên thứ ba chỉ để kiểm tra tính toàn vẹn của dữ liệu thuê ngoài.

Nghiên cứu này nhằm giải quyết những vấn đề trên bằng cách sử dụng kỹ thuật xác thực tuyến tính chung dựa trên khóa công khai H. Shacham and B. Waters (2008); Q. Wang, C. Wang, K. Ren, W. Lou, and J. Li (2011); C. Wang, K. Ren, W. Lou and J. Li, (2010), cho phép KTV thực hiện kiểm toán công mà không yêu cầu dữ liệu thực tế. Nghiên cứu đã tích hợp HLA với sự che phủ ngẫu nhiên để đảm bảo rằng KTV không bao giờ có được bất kỳ kiến thức về dữ liệu được lưu trữ tại máy chủ dựa trên đám mây (CS) trong quá trình kiểm tra.

2. Công việc có liên quan

Công việc đầu tiên của kiểm toán công đã được thực hiện bởi Ateniese và cộng sự trong "khả năng lưu trữ dữ liệu có thể thực hiện được tại các cửa hàng không đáng tin cậy". Họ đề nghị lấy mẫu ngẫu nhiên các dữ liệu được thuê ngoài và sử dụng mô hình RSA với các bộ xác thực tuyến tính đồng bộ để kiểm tra dữ liệu được thuê ngoài. Vì đây là kế hoạch đầu tiên, bảo vệ sự riêng tư của dữ liệu đã không được xem xét bởi chúng do đó dữ liệu có thể truy cập được bởi kiểm toán viên bên ngoài cho mục đích kiểm toán.

M.A. Shah và cộng sự đã giới thiệu một KTV để kiểm tra tính trung thực của bộ lưu trữ trực tuyến bằng cách mã hoá tập tin dữ liệu đầu tiên được lưu trữ và sau đó một số kết hợp khóa đối xứng được đánh giá trước đối với tệp dữ liệu được mật mã sẽ được gửi tới kiểm toán viên. Vai trò của kiểm toán viên là xác định tính toàn vẹn tập tin dữ liệu và khóa giải mã được cam kết trước đó được tổ chức tại máy chủ. Điểm mấu chốt của kế hoạch này là KTV cần phải duy trì trạng thái và do đó bị hạn chế sử dụng, có thể gây gánh nặng thêm cho người tiêu dùng khi sử dụng tất cả các bảng cân đối đối xứng. Hơn nữa, chương trình này chỉ làm việc cho các tập tin dữ liệu được mã hóa. Các nhà nghiên cứu sử dụng thuật toán RSA để mã hóa và giải mã dữ liệu và thuật toán SHA 512 được sử dụng để kiểm tra tính xác thực và toàn vẹn của thông tin.

Govinda và các cộng sự sử dụng chữ ký số của RSA để cho phép KTV kiểm tra tính toàn vẹn của dữ liệu được thuê ngoài trong môi trường đám mây và bảo vệ sự riêng tư của nó. Thay mặt cho người dùng, KTV kiểm tra tính toàn vẹn của dữ liệu được thuê ngoài. Điều này tạo điều kiện cho khả năng xác minh công khai động lực dữ liệu để bảo mật lưu trữ trong đám mây và cũng tạo điều kiện kiểm toán về bảo mật tính riêng tư. Tuy nhiên, kế hoạch này không thể giúp khôi phục dữ liệu được thuê ngoài. Đó là bởi chủ yếu hai lý do được đề cập trong nghiên cứu của M.A. Shah, R. Swaminathan, and M. Baker (2007). Thứ nhất là sự không khớp giữa giá trị được lưu giữ và giá trị tính toán của checksum chỉ có thể xác định rằng một trong hai đã được sửa đổi nhưng không thể định rõ được, như trong nghiên cứu của Farzad Sabahi (2011) "Các mối đe dọa và phản ứng về bảo mật máy tính đám mây" và có thể tổng kiểm tra được lưu trữ được sửa đổi hoặc bị hỏng. Lý do thứ hai là các hàm băm (hash functions) miễn phí được sử dụng để tính giá trị kiểm tra và do đó dữ liệu không thể được thu hồi từ một giá trị kiểm tra nhất định.

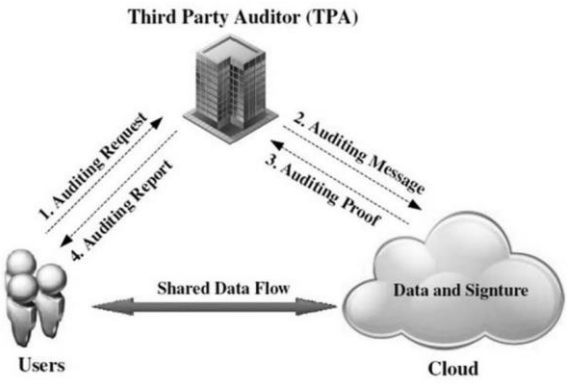
3. Vấn đề nghiên cứu

a. Mô hình hệ thống

Trong nghiên cứu này, chúng tôi đề cập đến ba thực thể - người sử dụng điện toán đám mây, máy

chủ đám mây và kiểm toán viên bên thứ ba. Người dùng Đám mây là người sử dụng máy chủ đám mây để lưu trữ số lượng lớn các tệp dữ liệu. Nhà cung cấp dịch vụ đám mây (CSP) cung cấp dịch vụ lưu trữ dữ liệu và có hầu hết các tài nguyên lưu trữ và tính toán không giới hạn, có thể mở rộng. Kiểm toán viên bên thứ ba (KTV) kiểm tra tính toàn vẹn của dữ liệu thay mặt cho người sử dụng điện toán đám mây sử dụng một kế hoạch kiểm toán công và sau đó KTV gửi báo cáo cho người dùng.

Hình 3. Cấu trúc mô hình hệ thống



Những lợi ích của mô hình hệ thống do người dùng chuyển dữ liệu sang đám mây - việc gia công dữ liệu ngoài việc giảm chi phí lưu trữ cũng giảm bớt sự bảo trì, giảm nguy cơ mất dữ liệu do sự cố phần cứng, dữ liệu có thể được truy cập từ bất cứ đâu trên thế giới. Để giảm chi phí tính toán của người dùng đám mây cũng như để tiết kiệm gánh nặng trực tuyến có thể được tạo ra khi người dùng kiểm tra tính toàn vẹn, người dùng sử dụng KTV để kiểm tra tính toàn vẹn của dữ liệu được lưu trữ.

b. Mô hình chỉ dẫn nguy cơ

Mối đe dọa về cơ bản là một sự kiện tiềm ẩn có thể là nguy hiểm hoặc ngẫu nhiên, ảnh hưởng đến tài nguyên đám mây.

Nguy cơ từ truy cập đối tượng dữ liệu data - Dữ liệu trong bộ nhớ đám mây có thể bị lạc do các vấn đề về phần cứng. Nhà cung cấp dịch vụ đám mây có thể xóa dữ liệu khi nó không được truy cập trong một thời gian dài.

Các cuộc tấn công khác có thể bao gồm - lỗi phần mềm, tin tặc, các vấn đề bảo mật trong đường

dẫn mạng... Đối với danh tiếng của họ, CSP có thể giấu những điều này từ người dùng.

Nguy cơ bảo mật - Có thể là dữ liệu được lưu trữ trên máy chủ đám mây có chứa thông tin bí mật về doanh nghiệp và bên ngoài có thể cố gắng truy cập vào nó bằng cách thao túng CSP. Cùng với dữ liệu này hoặc một phần của nó phải được giữ kín từ KTV trong quá trình kiểm tra.

c. Mục tiêu thiết kế

Giao thức của chúng tôi nhằm đạt được các tính chất sau đây:

- Kiểm toán dịch vụ - KTV có thể xác minh an toàn và hiệu quả dữ liệu mà không cần khôi phục bản sao của nó.

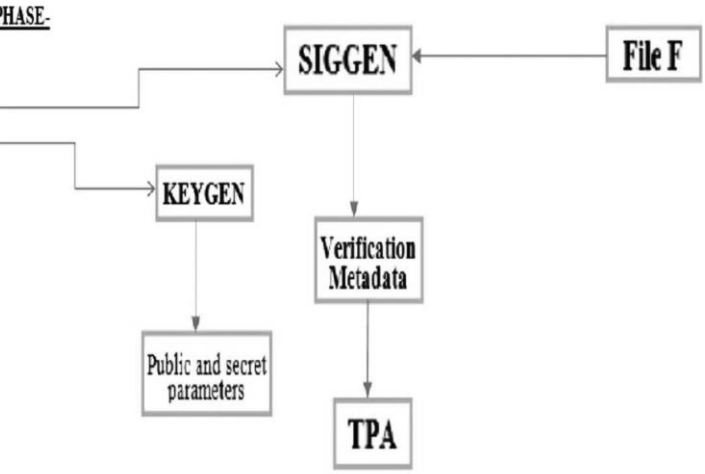
- Chính xác - Nếu có bất kỳ khối sửa đổi, sau đó KTV sẽ có thể phát hiện nó.

- Bảo mật - Bảo toàn - KTV không nên truy cập bất kỳ phần nào của dữ liệu trong quá trình kiểm toán.

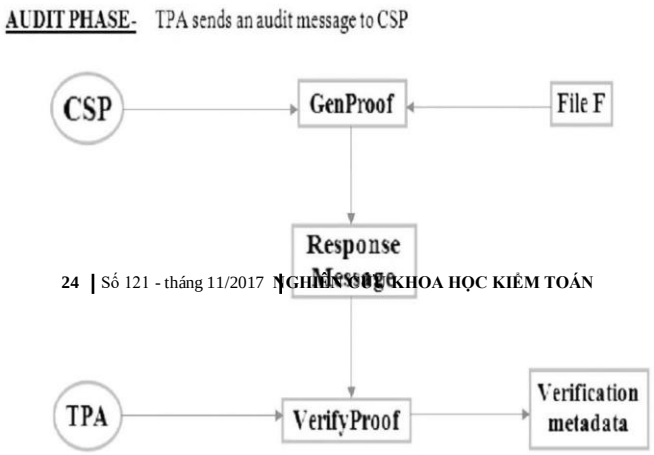
4. Đề xuất

Chúng tôi đã đề xuất một hệ thống sẽ sử dụng xác thực homomorphic dựa trên khóa công khai cùng với kỹ thuật masking ngẫu nhiên để tạo điều kiện bảo mật dữ liệu người dùng và cho phép kiểm tra dữ liệu của người dùng được lưu trữ trong đám mây. Chúng tôi đề xuất sử dụng bộ chứng thực homomorphic dựa trên khóa công khai thông qua đó KTV có thể thực hiện nhiệm vụ kiểm toán mà không yêu cầu sao chép dữ liệu của người dùng và sau đó tích hợp nó với kỹ thuật masking ngẫu nhiên, giao thức của chúng tôi hứa hẹn rằng KTV sẽ không có thông tin cần thiết để xây dựng lại chính xác Nhóm các phương trình tuyến tính và do đó không thể có bất kỳ kiến thức nào về dữ liệu của người dùng được lưu trữ trong máy chủ đám mây trong đề xuất rằng tệp tin phải được mã hóa ở phía người dùng và khóa được lưu trữ với người dùng trước khi tải tệp lên đám mây. Như vậy, quá trình trên sẽ trải qua hai giai đoạn như mô hình dưới đây:

Hình 4. Giai đoạn thiết lập Kế hoạch Kiểm toán



Hình 5. Giai đoạn thực hiện kế hoạch Kiểm toán



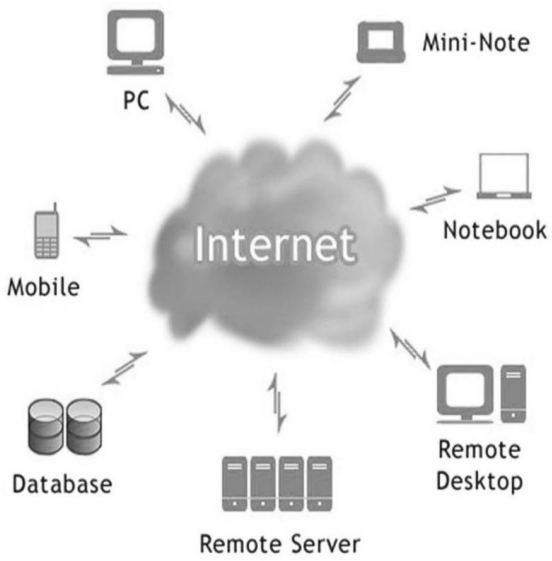
5. Xu hướng sử dụng điện toán đám mây và tiềm năng phát triển kiểm toán đám mây trên thị trường Việt Nam

Việt Nam đang dần tiếp cận các dịch vụ đám mây thông qua dự án của một số doanh nghiệp nước ngoài như Microsoft, Intel… cũng như từ những nhà phát triển, cung cấp trong nước như FPT, Biaki… IBM là doanh nghiệp tiên phong khai trương trung tâm điện toán đám mây tại Việt Nam vào tháng 9/2008 với khách hàng đầu tiên là Công ty Cổ phần Công nghệ và Truyền thông Việt Nam (VNTT). Có thể nói Việt Nam là một trong những nước đầu tiên ở ASEAN đưa vào sử dụng điện toán đám mây.

Công nghệ này được coi là giải pháp cho những vấn đề mà nhiều công ty đang gặp phải như thiếu

năng lực CNTT, chi phí đầu tư hạ tầng hạn chế... Hiện nay, nhiều công ty đang hoang phí tài nguyên như: không khai thác hết công suất của hệ thống máy chủ, đầu tư quá nhiều về mặt con người. Trong khi đó, về lý thuyết, đám mây (cloud computing) sẽ cho phép doanh nghiệp không cần tập trung quá nhiều cho cơ sở hạ tầng hoặc nâng cấp ứng dụng, không đòi hỏi nguồn nhân lực lớn và có thể dễ dàng thay đổi quy mô khi cần.

Mặc dù điện toán đám mây hiện đang được ứng dụng rộng rãi ở nhiều nước phát triển trên thế giới bởi lợi ích đáng kể mà nó đem lại, nhưng ở Việt Nam các doanh nghiệp vẫn chưa thực sự mặn mà với công nghệ này. Tuy nhiên, theo các chuyên gia nhận định, đây chính là giải pháp tối ưu để các doanh nghiệp nước ta giảm thiểu chi phí cũng như tăng hiệu suất làm việc ở mức tối đa. Mô hình sử dụng điện toán đám mây tại Việt Nam được khái quát hóa như hình 6.



Hình 6. Xu hướng sử dụng điện toán đám mây tại Việt Nam

Về thực trạng ứng dụng điện toán đám mây ở các doanh nghiệp Việt Nam, có thể rút ra kết luận như sau: Hiện nay, đã có một vài doanh nghiệp lớn tại Việt Nam đưa điện toán đám mây vào ứng dụng và hiệu suất kinh doanh được cải thiện đáng kể. Tuy nhiên, số lượng là khá ít. Phần lớn vẫn chỉ dừng ở mức quan tâm và tìm hiểu.

Tuy nhiên, theo khảo sát gần đây của Symantec, một công ty phần mềm hàng đầu thế giới, hiện có khoảng 46% doanh nghiệp và tổ chức Việt Nam đang triển khai ứng dụng công nghệ điện toán đám mây và các dự án ảo hóa khác.

Hãng bảo mật Symantec cũng cho rằng các doanh nghiệp Việt Nam có mối quan tâm đặc biệt đến việc ứng dụng điện toán đám mây và cơ hội mà công nghệ mới này đem tới. Kết quả từ cuộc khảo sát cho thấy 39% doanh nghiệp trong nước hiện đang sử dụng dịch vụ phần mềm ảo tư nhân (VPS), trong khi 21% đang ảo hóa máy chủ và cơ sở dữ liệu.

Một báo cáo gần đây của nhóm nghiên cứu Gartner nhấn mạnh tới sự phát triển của Điện toán đám mây trong bối cảnh toàn cầu hóa. Theo khảo sát, khoảng 50% doanh nghiệp và các tổ chức trên thế giới đang ứng dụng công nghệ hiện đại này với tốc độ tăng trưởng 17% mỗi năm. Năm 2011, doanh thu dịch vụ điện toán đám mây toàn cầu lên tới 2,4 tỷ USD. Gartner dự đoán con số này sẽ tăng gần gấp 4 lần trong năm 2012.

Việc ứng dụng công nghệ điện toán đám mây trong kinh doanh cũng như trong đời sống là một bước phát triển tất yếu với xu thế thời đại. Được dự đoán là làn sóng công nghệ mới, sẽ tạo ảnh hưởng đến thói quen, tư duy ứng dụng công nghệ hiện nay. Điều khó khăn là làm thế nào để các doanh nghiệp cũng như cá nhân chấp nhận xu thế đấy.

Đối với phần lớn các doanh nghiệp Việt Nam hiện nay (chủ yếu là doanh nghiệp vừa và nhỏ), rào cản ngôn ngữ là trở ngại lớn nhất trong quá trình tìm kiếm những công nghệ trợ giúp cho họ. Chính vì thế, các nhà cung cấp Việt Nam sẽ là cầu nối cho doanh nghiệp trong nước với xu thế công nghệ thế giới. Nó yêu cầu một trình độ nhất định về công nghệ, sự am hiểu thói quen, văn hóa của doanh nghiệp Việt Nam, và trên hết là khả năng đào tạo thị trường gắn với công nghệ. Nhà cung cấp Công nghệ Điện toán đám mây ở Việt Nam làm tốt cả 3 điều trên, thì thị trường Việt Nam sẽ không chỉ còn là thị trường tiềm năng nữa.

Công nghệ Điện toán đám mây là xu thế chung của thời đại, việc đưa ra ứng dụng, phát triển rộng rãi là điều tất yếu, nhất là trong bối cảnh toàn cầu

hóa. Nhưng để theo kịp xu thế, để thị trường phát triển mạnh thì còn nhiều điều cấp thiết phải làm. Thay đổi một tư duy làm việc, một thói quen hoạt động là điều mà các nhà cung cấp phải làm doanh nghiệp Việt Nam nhìn ra và chấp nhận.

Bài báo đã đề xuất một hệ thống kiểm toán bên thứ ba cho kho dữ liệu dựa trên đám mây đồng thời bảo vệ sự riêng tư của dữ liệu của người dùng. Hệ thống xác thực tuyến tính đơn vị và sự che phủ ngẫu nhiên đã được sử dụng để đảm bảo rằng KTV sẽ không thể truy cập vào các nội dung dữ liệu được lưu trữ trên máy chủ đám mây mà không ảnh hưởng đến hiệu quả của quy trình kiểm toán. Điều này loại bỏ gánh nặng của nhiệm vụ kiểm toán từ người sử dụng điện toán đám mây và cũng làm giảm nỗi lo sợ của người dùng rằng dữ liệu từ bên ngoài của họ có thể bị truy cập bởi một bên không tin tưởng. Vấn đề này mở ra cho các nghiên cứu ứng dụng và thực hiện kiểm toán đám mây – một mô hình dịch vụ khá mới đối với thị trường kiểm toán Việt Nam.

TÀI LIỆU THAM KHẢO

1. *G. Ateniese, R. Burns, R. Curtmola, J. Herring, L. Kissner, Z. Peterson, and D. Song, "Provable Data Possession at Untrusted Stores," in Proc. ACM CCS, 2007, pp. 598–610.*
2. *C. Wang, Q. Wang, K. Ren, and W. Lou, "Privacy-Preserving Public Auditing for Data Storage Security in Cloud Computing," in Proc. IEEE INFOCOM, 2010, pp. 525–533.*
3. *H. Shacham and B. Waters, "Compact Proofs of Retrievability," in Proc. Int'l Conf. Theory and Application of Cryptology and Information Security: Advances in Cryptology (Asiacrypt), vol. 5350, pp. 90-107, Dec. 2008.*
4. *B. Wang, B. Li, and H. Li, "Oruta: Privacy-Preserving Public Auditing for Shared Data in the Cloud" University of Toronto, Tech. Rep., pp. 295-302, 2011.*
5. *Q. Wang, C. Wang, K. Ren, W. Lou, and J. Li, "Enabling Public Auditability and Data Dynamics for Storage Security in Cloud Computing" IEEE Trans. Parallel and Distributed Systems, vol. 22, no. 5, pp. 847-859, May 2011.*
6. *S. Galbraith, "Supersingular curves in cryptography" (Asiacrypt) volume 2248 of Lecture Notes in Computer Science, SpringerVerlag , pages 495–513., 2001.*
7. *C. Wang, K. Ren, W. Lou and J. Li, "Towards Publicly Auditable Secure Cloud Data Storage Services" IEEE Network Magazine, vol. 24, no. 4, pp. 19-24, July/Aug. 2010.*
8. *M.A. Shah, M. Baker, J.C. Mogul, and R. Swaminathan, "Auditing to Keep Online Storage Services Honest," in Proc. 11th USENIX Workshop Hot Topics in Operating Systems (HotOS '07), pp. 1-6, 2007.*
9. *M.A. Shah, R. Swaminathan, and M. Baker, "Privacy-Preserving Audit and Extraction of Digital Contents," Cryptology ePrint Archive, Report 2008/186, 2008.*
10. *Govinda V, Gurunathaprasad and H Sathshkumar, "Third Party Auditing For Security Data Storage in cloud through digital signature using RSA" IJASATR, issue 2,vol-4, Issn 2249-9954, 2012.*
11. *Farzad Sabahi,"Cloud Computing Security Threats and Responses" IEEE conference, 978-1-61284-486-2/111, 2011.*
12. *D. Boneh, B. Lynn, and H. Shacham. "Short signatures from the Weil pairing," In Asiacrypt, volume 2248 of Lecture Notes in Computer Science, pp. 514+, 2001.*
13. *T. Okamoto and D. Pointcheval, "The gap-problems: A new class of problems for the security of cryptographic schemes," In Public Key Cryptography, LNCS 1992, pp. 104–118, 2001.*
14. *Ben Lynn, "On the implementation of pairing-based cryptosystems" Thesis, Stanford University, Unites States, 2007.*
15. *M. Armbrust, A. Fox, R. Griffith, A. D. Joseph, R. H. Katz, A. Konwinski, G. Lee, D. A. Patterson, A. Rabkin, I. Stoica, and M. Zaharia, "A View of Cloud Computing" Communications of the ACM, vol. 53, no. 4, pp. 50–58, April 2010.*
16. *Bhagat and R. K. Sahu, "Using Third Party Auditor for Cloud Data Security: A Review" International Journal of Advanced Research in Computer Science and Software Engineering 3(3), pp. 34-39, March – 2013.*
17. *P.K.Deshmukh,V.R.Desale,R.A.Deshmukh, "Investigation of KTV (Third Party Auditor Role) for Cloud Data Security", IJSER, vo. 4, no. 2,ISSN 2229-5518, Feb 2013.*