(12) BẢN MÔ TẢ SÁNG CHẾ THUỘC BẰNG ĐỘC QUYỀN SÁNG CHẾ
(19) **Cộng hòa xã hội chủ nghĩa Việt Nam (VN)**
CỤC SỞ HỮU TRÍ TUỆ
(11) **1-0041316**
(51)[2020.01] **G06F 21/57**; G06F 21/33
(13) **B**

(21) 1-2020-06841
(22) 26/11/2020
(30) 10-2020-0137893 22/10/2020 KR
(45) 25/10/2024 439
(43) 25/04/2022 409
(73) TATUM INC. (KR)
309, Mokdongdong-ro, Yangcheon-gu, Seoul, Republic of Korea
(72) Yang Hyuk-Jae (KR).
(74) Công ty TNHH Quốc tế D &N (D&N INTERNATIONAL CO.,LTD.)

(54) THIẾT BỊ QUÉT VÀ QUẢN LÝ VIỆC TUÂN THỦ BẢO MẬT ĐÁM MÂY

(57) Sáng chế đề cập đến thiết bị quét và quản lý việc tuân thủ các quy định bảo mật đám mây, và cụ thể hơn là bằng cách quét thông tin cài đặt bảo mật đám mây rồi so sánh và đánh giá xem các nguyên tắc bảo mật quốc tế có được tuân thủ hay không thông qua thông tin quét, các lỗi trong bảo mật cài đặt được phát hiện. Thiết bị quét và quản lý việc tuân thủ bảo mật đám mây theo sáng chế bao gồm: đơn vị kết nối đám mây để kết nối với đám mây của khách hàng bằng cách sử dụng khóa xác thực truy cập được cấp từ nhà cung cấp dịch vụ đám mây; đơn vị quét thông tin cài đặt bảo mật tài nguyên đám mây quét tuần tự thông tin cài đặt bảo mật đám mây của khách hàng theo đơn vị kết nối để tạo ra nhiều tập dữ liệu thông tin cài đặt bảo mật, và định dạng dữ liệu của tập dữ liệu thông tin cài đặt bảo mật ở các định dạng khác nhau được thay đổi và tích hợp; đơn vị quét quy định bảo mật đám mây để quét quy định bảo mật đám mây của khách hàng bằng cách so sánh và đánh giá hướng dẫn quy định về bảo mật đám mây được cung cấp và tập dữ liệu thông tin cài đặt tích hợp.

Lĩnh vực kỹ thuật được đề cập

Sáng chế đề cập đến thiết bị quét và quản lý việc tuân thủ các quy định bảo mật đám mây, và cụ thể hơn là thiết bị quét và quản lý việc tuân thủ các quy định bảo mật đám mây bằng cách quét thông tin cài đặt bảo mật đám mây rồi so sánh và đánh giá xem các nguyên tắc bảo mật quốc tế có được tuân thủ hay không thông qua thông tin quét, và sửa các lỗi trong cài đặt bảo mật được phát hiện.

Tình trạng kỹ thuật của sáng chế

Thông thường, khách hàng cá nhân vận hành đám mây bằng cách nhận các dịch vụ đám mây từ nhà cung cấp dịch vụ đám mây. Người quản lý quản lý bảo mật của khách hàng đặt cài đặt bảo mật cho từng tài nguyên trên đám mây trong khi vận hành dịch vụ đám mây của công ty do nhà cung cấp dịch vụ đám mây cung cấp. Đồng thời, các cài đặt bảo mật chính bao gồm quản lý người dùng bên ngoài, quản lý khóa, quản lý quyền hạn, tiếp xúc Internet, cài đặt mã hóa, cài đặt sao lưu, cài đặt ảnh chụp nhanh, và cài đặt sao lưu hình ảnh.

Mặt khác, các vấn đề liên quan đến bảo mật do người quản lý bảo mật đặt ra trong khi vận hành đám mây hầu hết là lỗi trong các giá trị cài đặt bảo mật được đặt bởi người quản lý bảo mật. Cụ thể, lỗi giá trị cài đặt bảo mật như vậy có thể làm lộ tài nguyên của đám mây trên Internet, và thông tin cá nhân có thể bị truy cập từ bên ngoài do lỗi thiết lập quyền hạn truy cập thông tin cá nhân.

Do đó, yêu cầu cấp thiết là cần phải phát triển thiết bị quản lý các cài đặt bảo mật được thiết lập nội bộ này các nguyên tắc bảo mật quốc tế.

Tài liệu kỹ thuật có liên quan

Tài liệu sáng chế

Sáng chế Hàn Quốc có số công bố 10-1544750,

Sáng chế Hàn Quốc có số công bố 10-2018-0015640,

Sáng chế Hàn Quốc có số công bố 10-1914416.

Bản chất kỹ thuật của sáng chế

Theo đó, sáng chế được thực hiện để khắc phục những hạn chế nêu trên, và mục tiêu của sáng chế là đề xuất thiết bị có thể đánh giá được mức độ rủi ro tổng thể liên quan đến bảo mật trong nháy mắt bằng cách phân tích xu hướng cho từng loại, đồng thời so sánh và đánh giá sự tuân thủ của khách hàng đối với các hướng dẫn về cài đặt bảo mật đám mây, và đánh giá rủi ro về cài đặt bảo mật đám mây theo thời gian, tài khoản, và tài nguyên.

Tuy nhiên, mục tiêu của sáng chế không chỉ giới hạn ở mục tiêu trên, và các mục tiêu khác không được đề cập vẫn được hiểu rõ bởi người có hiểu biết trung bình trong lĩnh vực này thông qua phần mô tả sau đây.

Để đạt được mục tiêu trên, sáng chế đề xuất thiết bị quét và quản lý việc tuân thủ bảo mật đám mây, thiết bị bao gồm: đơn vị kết nối đám mây để kết nối với đám mây của khách hàng sử dụng khóa xác thực truy cập được cấp từ nhà cung cấp dịch vụ đám mây, đơn vị quét thông tin cài đặt bảo mật tài nguyên đám mây quét tuần tự thông tin cài đặt bảo mật đám mây của khách hàng theo đơn vị kết nối để tạo ra nhiều tập dữ liệu thông tin cài đặt bảo mật, và định dạng dữ liệu của tập dữ liệu thông tin cài đặt bảo mật ở các định dạng khác nhau được thay đổi và tích hợp, đơn vị quét quy định bảo mật đám mây để quét quy định bảo mật đám mây của khách hàng bằng cách so

sánh và đánh giá hướng dẫn quy định về bảo mật đám mây được cung cấp và tập dữ liệu thông tin cài đặt tích hợp.

Ngoài ra, đơn vị quét thông tin cài đặt bảo mật tài nguyên đám mây bao gồm đơn vị yêu cầu thông tin cài đặt bảo mật tài nguyên đám mây yêu cầu tuần tự thông tin cài đặt bảo mật đám mây của máy khách theo đơn vị kết nối, đơn vị thu thập thông tin cài đặt bảo mật tài nguyên trên đám mây tiếp nhận tuần tự thông tin cài đặt bảo mật ở các định dạng khác nhau từ các đám mây riêng lẻ của máy khách được kết nối theo yêu cầu và tạo tập dữ liệu thông tin cài đặt bảo mật, đơn vị tích hợp định dạng dữ liệu tạo ra tập dữ liệu thông tin cài đặt tích hợp bằng cách thay đổi và tích hợp tuần tự định dạng của tập dữ liệu thông tin cài đặt bảo mật ở các định dạng khác nhau được nhập tuần tự.

Ngoài ra, thiết bị quét và quản lý việc tuân thủ bảo mật đám mây còn bao gồm thêm đơn vị lập danh sách kiểm tra quy định bảo mật bao gồm đơn vị kiểm tra tuân thủ quy định bảo mật kiểm tra xem các quy định bảo mật có được tuân thủ hay không theo đánh giá và quét các mục quy định bảo mật đám mây của khách hàng, và đơn vị phân tích nguyên nhân của mục không được tuân thủ để phân tích nguyên nhân của mục không được tuân thủ quy định bảo mật.

Hơn nữa, thiết bị quét và quản lý việc tuân thủ bảo mật đám mây cũng bao gồm đơn vị cung cấp phân tích xu hướng để phân tích và cung cấp các xu hướng thay đổi của các quy định bảo mật theo mỗi khoảng thời gian, mỗi tài khoản, và mỗi tài nguyên dựa trên tập dữ liệu quét quy định bảo mật được tạo bởi đơn vị lập danh sách kiểm tra quy định bảo mật.

Hơn nữa, thiết bị quét và quản lý việc tuân thủ bảo mật đám mây cũng bao gồm đơn vị hành động quy định bảo mật đám mây có nhiệm vụ cung cấp một URL tương ứng để sửa quy định bảo mật không tuân thủ theo phân tích nguyên nhân của đơn vị phân tích nguyên nhân của mục không được tuân thủ.

Theo sáng chế như được mô tả ở trên, mức độ rủi ro liên quan đến bảo mật tổng thể được đánh giá tức thì bằng cách so sánh và đánh giá sự tuân thủ của khách hàng đối với các nguyên tắc về cài đặt bảo mật đám mây, và phân tích rủi ro đối với cài đặt bảo mật đám mây theo thời gian, tài khoản, và tài nguyên.

Ngoài ra, thiết bị theo sáng chế có hiệu quả nhanh chóng thực hiện các biện pháp đối với các vi phạm nguyên tắc và rủi ro bằng cách phát hiện và đánh giá các rủi ro liên quan đến cài đặt bảo mật của tài nguyên đám mây theo thời gian thực.

Ngoài ra, rủi ro có thể được ngăn chặn bằng cách phát hiện, phản hồi, và dự đoán các yếu tố nguy cơ liên quan đến cài đặt bảo mật đám mây theo nguyên tắc hoặc chính sách bảo mật đám mây.

Mô tả vắn tắt các hình vẽ

Sáng chế sẽ được mô tả chi tiết thông qua các phương án thực hiện ưu tiên cùng với các hình vẽ kèm theo, tuy nhiên, các phương án thực hiện cùng các hình vẽ chỉ được mô tả nhằm mục đích minh họa để làm rõ sáng chế mà không giới hạn phạm vi của sáng chế. Trong đó:

Fig.1 là sơ đồ minh họa quy trình cấp khóa xác thực truy cập để truy cập vào đám mây máy khách theo phương án thực hiện của sáng chế;

Fig.2- Fig.4 là các sơ đồ minh họa cấu hình của thiết bị quét và quản lý việc tuân thủ các quy định về bảo mật đám mây theo phương án thực hiện của sáng chế;

Fig.5 là sơ đồ minh họa trình tự phương pháp quét và quản lý việc tuân thủ các quy định bảo mật đám mây theo phương án thực hiện của sáng chế.

Mô tả chi tiết sáng chế

Sau đây, phương án thực hiện được ưu tiên của sáng chế sẽ được mô tả có tham chiếu đến các hình vẽ. Các phương án thực hiện được mô tả dưới đây cũng như toàn bộ cấu hình được mô tả trong phương án thực hiện không giới hạn phạm vi của sáng. Những mô tả kỹ thuật có thể được hiểu dễ dàng bởi người có hiểu biết trung bình trong lĩnh vực này có thể bỏ qua, tuy nhiên những mô tả được bỏ qua đó vẫn thuộc phạm vi tinh thần kỹ thuật của sáng chế.

Thiết bị quét và quản lý xem các quy định bảo mật đám mây có được tuân thủ hay không theo phương án thực hiện của sáng chế sẽ quét rồi phân tích và quét các mục liên quan đến cài đặt bảo mật của máy khách, và kiểm tra các mục không tuân thủ quy định bảo mật rồi hiển thị kết quả phân tích xu hướng trên bảng điều khiển. Sáng chế đề xuất biện pháp đối phó để khách hàng có thể sửa chữa ngay lập tức các lỗi bảo mật không tuân thủ quy định. Sau đây, thiết bị để quét và quản lý việc tuân thủ các quy định bảo mật đám mây theo phương án thực hiện của sáng chế sẽ được mô tả chi tiết cùng với các hình vẽ kèm theo.

Tham khảo các Fig.1 và Fig.5, nhà cung cấp dịch vụ đám mây cung cấp dịch vụ đám mây cho người dùng dịch vụ đám mây (cụ thể là khách hàng). Khách hàng sử dụng dịch vụ đám mây được cung cấp, và khi sử dụng dịch vụ đám mây, khách hàng thực hiện cài đặt bảo mật cho tài nguyên đám mây để sử dụng dịch vụ đám mây. Tại thời điểm này, cài đặt bảo mật đám mây được khách hàng sử dụng là ví dụ, và sự cố bảo mật xảy ra do lỗi cài đặt của quản trị viên nội bộ. Do đó, cần thiết phải quét xem

khách hàng có tuân thủ các quy định bảo mật đối với cài đặt bảo mật đám mây hay không, và để quét xem các quy định bảo mật có được tuân thủ hay không, cần phải lấy khóa xác thực truy cập từ nhà cung cấp dịch vụ đám mây. Để phát hành khóa xác thực truy cập, trước tiên công ty sẽ kiểm tra và quản lý xem khách hàng có tuân thủ các quy định bảo mật hay không, hoặc đơn vị kiểm tra bảo mật đám mây 300 cấp khóa xác thực truy cập có thể quét cài đặt bảo mật đám mây tới khách hàng hoặc máy chủ của khách hàng 200. Khách hàng hoặc máy chủ của khách hàng 200 đã nhận được yêu cầu cấp khóa xác thực truy cập yêu cầu nhà cung cấp dịch vụ đám mây hoặc máy chủ của nhà cung cấp dịch vụ đám mây 110, 120 và 130 cấp lại khóa xác thực truy cập. Khi máy chủ của khách hàng 200 gửi yêu cầu cấp khóa xác thực truy cập đến các máy chủ của nhà cung cấp dịch vụ đám mây 110, 120 và 130, các máy chủ của nhà cung cấp dịch vụ đám mây 110, 120 và 130 sẽ cấp khóa xác thực truy cập và truyền đến máy chủ của khách hàng 200. Máy chủ của khách 200 truyền lại khóa xác thực truy cập cho đơn vị kiểm tra bảo mật đám mây 300. Khóa xác thực truy cập đã truyền được lưu trữ trong đơn vị kiểm tra bảo mật đám mây 300, qua đó đơn vị kiểm tra bảo mật đám mây 300 có thể truy cập vào đám mây của khách hàng. Lúc này, khóa xác thực truy cập do nhà cung cấp dịch vụ đám mây cấp là khóa xác thực truy cập tối thiểu có thể quét các cài đặt bảo mật đám mây.

Trong khi đó, trên Fig.1, khách hàng sử dụng dịch vụ đám mây được cung cấp bởi nhà cung cấp dịch vụ đám mây A, B và n, và khóa xác thực truy cập A, B và n để truy cập từng đám mây A, B và n được cấp. Theo đó, đơn vị kiểm tra bảo mật đám mây 300 có thể truy cập vào đám mây bằng cách sử dụng các khóa xác thực truy cập khác nhau.

Tham khảo Fig.2, đơn vị kiểm tra bảo mật đám mây 300 được cấp khóa xác thực truy cập từ mỗi nhà cung cấp dịch vụ đám mây 110, 120, 130, quét tuần tự các cài đặt bảo mật của mỗi đám mây. Với mục đích này, đơn vị kiểm tra bảo mật đám mây 300 bao gồm đơn vị quét thông tin cài đặt bảo mật tài nguyên đám mây (hoặc đơn vị phân tích cú pháp). Đơn vị quét thông tin cài đặt bảo mật tài nguyên đám mây bao gồm đơn vị nhận khóa xác thực truy cập đám mây 310, đơn vị kết nối đám mây 315, đơn vị yêu cầu thông tin cài đặt bảo mật tài nguyên đám mây 320, đơn vị thu thập thông tin cài đặt bảo mật tài nguyên đám mây 330, và đơn vị tích hợp định dạng dữ liệu 340.

Đơn vị nhận khóa xác thực truy cập đám mây 310 nhận các khóa xác thực truy cập A, B, n từ máy chủ của khách hàng 200 và lưu trữ chúng trong cơ sở dữ liệu. Khóa xác thực truy cập được lưu trữ là khóa xác thực cho phép khách hàng truy cập vào từng dịch vụ đám mây đang được sử dụng.

Đơn vị kết nối đám mây 315 sử dụng khóa xác thực truy cập được cấp từ nhà cung cấp dịch vụ đám mây để quét máy khách của khách hàng.

Như được minh họa trên Fig.3, đơn vị tích hợp định dạng dữ liệu 340 lần lượt thay đổi và tích hợp định dạng của tập dữ liệu thông tin cài đặt bảo mật A, B và n được tạo thành ở các định dạng khác nhau, lần lượt nhập tập dữ liệu thông tin định dạng tích hợp At, tạo tập dữ liệu thông tin cấu hình tích hợp Bt và tập dữ liệu thông tin cấu hình tích hợp nt. Cụ thể là, đơn vị tích hợp định dạng dữ liệu đám mây A 341 nhận tập dữ liệu thông tin cài đặt bảo mật A từ đơn vị thu thập thông tin cài đặt bảo mật tài nguyên đám mây A 331, và tích hợp At bằng cách thay đổi và tích hợp định dạng dữ liệu của mỗi tài nguyên có định dạng dữ liệu khác nhau. Tạo tập dữ liệu thông tin cài đặt (At =

{A1', A2', A3', A4'}). Đơn vị tích hợp định dạng dữ liệu đám mây B 342 nhận tập dữ liệu thông tin cài đặt bảo mật B từ đơn vị thu thập thông tin cài đặt bảo mật tài nguyên đám mây B 332, đồng thời thay đổi và tích hợp định dạng dữ liệu của mỗi tài nguyên có định dạng dữ liệu khác nhau để tích hợp thông tin cài đặt tích hợp Bt. Tạo tập dữ liệu (Bt = {B1', B2', B3', B4'}). n đơn vị tích hợp định dạng dữ liệu đám mây 343 nhận n tập dữ liệu thông tin cài đặt bảo mật từ n bộ thu thập thông tin cài đặt bảo mật tài nguyên đám mây 333, đồng thời thay đổi và tích hợp định dạng dữ liệu của từng tài nguyên với các định dạng dữ liệu khác nhau thành thông tin cài đặt tích hợp nt. Tạo tập dữ liệu (nt = {n1', n2', n3', n4'}).

Đồng thời, đơn vị tích hợp định dạng dữ liệu 340 được mô tả ở trên chuyển đổi và tích hợp các tập dữ liệu có định dạng khác nhau thành các tập dữ liệu có cùng định dạng. Chuyển đổi định dạng dữ liệu của tập dữ liệu thông tin cài đặt bảo mật là ví dụ về chuyển đổi tập dữ liệu thông tin cài đặt bảo mật (A1 là ví dụ) của mỗi tài nguyên đám mây bao gồm "Loại Jason" và "Loại lớp" thành "Loại tfstate" định dạng (A1 là ví dụ). Tuy nhiên, định dạng dữ liệu của "Loại tfstate" sẽ được chuyển đổi có thể được thay đổi khi cần thiết thành định dạng dữ liệu khác có thể tích hợp và khớp với tập dữ liệu thông tin cài đặt bảo mật của mỗi đám mây bao gồm các tập dữ liệu có định dạng khác nhau. Theo đó, tập dữ liệu đã thay đổi và tích hợp được thay đổi và tích hợp vào tập dữ liệu có khả năng tương thích vốn có cho phép quét các quy định bảo mật sẽ được mô tả sau này. Ngoài ra, việc tích hợp định dạng dữ liệu của tập dữ liệu thông tin cài đặt bảo mật có nghĩa là, ví dụ, tài nguyên đám mây của đám mây A được nhóm lại với nhau, tài nguyên đám mây của đám mây B được đóng gói và tích hợp, và tài nguyên đám mây của đám mây n được nhóm lại và tích hợp.

Đơn vị yêu cầu cài đặt thông tin bảo mật tài nguyên đám mây 320 được mô tả ở trên, đơn vị thu thập thông tin cài đặt bảo mật tài nguyên đám mây 330, và đơn vị tích hợp định dạng dữ liệu 340 tuần tự tiến hành yêu cầu -> thu thập -> tích hợp thông tin cài đặt bảo mật của từng đám mây và lặp lại chu trình. Tại thời điểm này, do thông tin cài đặt bảo mật cho các tài nguyên thu thập của mỗi đám mây được thu thập ngẫu nhiên, nên cần phải chuyển đổi và tích hợp định dạng tập dữ liệu như mô tả ở trên. Mặt khác, thông tin cài đặt bảo mật đám mây có thể là giá trị cài đặt được đặt để có thể truy cập từ mạng bên ngoài vào mạng nội bộ, hoặc giá trị cài đặt bảo mật đặt xem có mã hóa và lưu trữ dữ liệu khi lưu trữ dữ liệu khách hàng hay không trên đám mây. Do lỗi cài đặt bảo mật của trình quản lý bảo mật, đám mây của khách hàng trở nên dễ bị tổn thương bảo mật và theo phương án thực hiện của sáng chế, thông tin cài đặt bảo mật được quét để tìm và quản lý lỗi.

Như được minh họa trên Fig.3, đơn vị kiểm tra bảo mật đám mây 300 bao gồm đơn vị quét quy định bảo mật đám mây 350, đơn vị lập danh sách kiểm tra quy định bảo mật 360, đơn vị cung cấp phân tích xu hướng 370, đơn vị hành động quy định bảo mật đám mây 380, và đơn vị cung cấp hướng dẫn quy định bảo mật đám mây 351.

Đơn vị quét quy định bảo mật đám mây 350 quét và đánh giá quy định bảo mật đám mây của khách hàng bằng cách so sánh và đánh giá các mục của hướng dẫn quy định bảo mật đám mây được cung cấp và một tập dữ liệu thông tin cài đặt tích hợp bất kỳ. Đơn vị cung cấp hướng dẫn quy định bảo mật đám mây 351 cung cấp hướng dẫn cho các quy định về bảo mật đám mây, và các nguyên tắc này liên tục được cập nhật như các quy định về bảo mật đám mây được quốc tế chấp nhận, cũng như các nguyên tắc được sử dụng làm dự án quốc gia. Các nguyên tắc vận hành đám mây của cũng có thể được áp dụng và cập nhật.

Để đơn vị quét quy định bảo mật đám mây 350 so sánh và đánh giá các mục quy định bảo mật được cung cấp bởi đơn vị cung cấp hướng dẫn quy định bảo mật đám mây 351 và tập dữ liệu thông tin cài đặt tích hợp, như được mô tả ở trên, cần phải chuyển đổi và tích hợp tập dữ liệu thông tin cấu hình bảo mật thành tập dữ liệu thông tin cấu hình tích hợp có khả năng tương thích vốn có.

Ví dụ: bằng cách đối sánh "mục 1.1.1 liên quan đến máy chủ" trong hướng dẫn quy định bảo mật đám mây và tập dữ liệu thông tin cấu hình tích hợp liên quan đến máy chủ, so sánh và đánh giá chúng với nhau. Tập dữ liệu thông tin được đối sánh và đánh giá để so sánh.

Đơn vị lập danh sách kiểm tra quy định bảo mật 360 bao gồm đơn vị kiểm tra tuân thủ quy định bảo mật (không được minh họa) và đơn vị phân tích nguyên nhân mục không tuân thủ (không được minh họa).

Đơn vị kiểm tra tuân thủ quy định bảo mật kiểm tra xem các quy định bảo mật có được tuân thủ hay không theo đánh giá và quét các mục quy định bảo mật đám mây của khách hàng A, B, n của đơn vị quét quy định bảo mật đám mây 350, đồng thời lựa chọn và phân tách các quy định bảo mật không được tuân thủ. Ngoài ra, nếu cần thiết, bằng cách liên kết với đơn vị phân tích nguyên nhân mục không tuân thủ và đơn vị hành động quy định bảo mật đám mây 380, sẽ được mô tả sau, nếu có quy định bảo mật không được tuân thủ dễ bị tấn công hoặc đe dọa nhất, nó sẽ được chọn và thông báo kịp thời cho nhân viên quản lý bảo mật của khách hàng để có hành động kịp thời. Ngoài ra, nếu có sự thay đổi trong cài đặt bảo mật đám mây của khách hàng, Đơn vị kiểm tra sẽ phát hiện và kiểm tra xem có lỗi cài đặt hay không bằng cách phát hiện theo thời gian thực.

Đơn vị phân tích nguyên nhân của mục không được tuân thủ phân tích và đưa ra nguyên nhân của mục không được tuân thủ. Nói cách khác, nếu có mục không được tuân thủ đối với cài đặt bảo mật đám mây của khách hàng, phân tích chuyên sâu sẽ được cung cấp cho các nguyên nhân của các mục không tuân thủ.

Thông qua đơn vị kiểm tra tuân thủ bảo mật được mô tả ở trên và đơn vị phân tích nguyên nhân mục không tuân thủ, danh sách kiểm tra các mục cài đặt bảo mật được tạo để xem liệu cài đặt bảo mật đám mây của khách hàng có tuân thủ các nguyên tắc hay không và cài đặt bảo mật được thiết lập sai ở đâu. Ví dụ, đối với mỗi mục so sánh nguyên tắc, 1) kiểm tra xem các quy định bảo mật đã được tuân thủ hay chưa, và 2) cung cấp phân tích nguyên nhân tại sao nó không được tuân thủ (vì mã hóa bị tắt hoặc truy cập từ mạng bên ngoài vào mạng nội bộ là có thể vì nó được thiết lập).

Đơn vị hành động quy định bảo mật đám mây 380 cung cấp một URL tương ứng cho người quản lý bảo mật của khách hàng thông qua đơn vị cung cấp URL 381 để các quy định bảo mật không tuân thủ có thể được sửa chữa liên quan đến đơn vị lập danh sách kiểm tra quy định bảo mật 360. Đơn vị cung cấp URL 381 cung cấp URL phản hồi để sửa các quy định bảo mật không tuân thủ, và người quản lý bảo mật của khách hàng có thể nhấp vào URL phản hồi để phân tích nguyên nhân vi phạm và xác định các biện pháp có thể được thực hiện. Theo đó, cài đặt bảo mật đám mây của công ty có thể nhanh chóng được sửa chữa để phù hợp với các nguyên tắc. Trong trường hợp này, đơn vị hành động quy định bảo mật đám mây 380 trước tiên có thể chọn quy định bảo mật có cài đặt bảo mật dễ bị tấn công hoặc đe dọa nhất, đồng thời thông báo ngay cho người quản lý bảo mật về quy định bảo mật và thực hiện hành động được khuyến nghị để sửa nó.

Như được minh họa trên Fig.4, đơn vị cung cấp phân tích xu hướng 370 tính toán sự thay đổi của các quy định bảo mật theo khoảng thời gian, tài khoản, và tài nguyên dựa trên tập dữ liệu quét quy định bảo mật được tạo bởi đơn vị lập danh sách kiểm tra quy định bảo mật 360. Phân tích được cung cấp, và mục quy địch bảo mật không được tuân thủ dễ bị tấn công hoặc đe dọa nhất được xếp hạng và hiển thị. Ví dụ: đơn vị cung cấp phân tích xu hướng 370 cung cấp phân tích xu hướng về số lượng các mục tuân thủ nguyên tắc và số lượng các mục không tuân thủ cho mỗi khoảng thời gian của đám mây của khách hàng. Ngoài ra, đơn vị cung cấp phân tích xu hướng 370 cung cấp phân tích xu hướng về số lượng các mục tuân thủ nguyên tắc và các mục không tuân thủ cho mỗi tài nguyên của đám mây của khách hàng. Ngoài ra, đơn vị cung cấp phân tích xu hướng 370 cung cấp phân tích xu hướng về số lượng mục tuân thủ các nguyên tắc và số lượng mục không tuân thủ cho từng tài khoản của đám mây của khách hàng (trên mỗi tài khoản quản trị viên đám mây của khách hàng). Ngoài ra, có thể đưa ra phân tích xu hướng bằng cách chia cho rủi ro đồng thời phân tích xu hướng thay đổi theo thời gian, tài khoản, và tài nguyên. Theo đó, có thể nhanh chóng nắm bắt được sự tuân thủ của khách hàng đối với các nguyên tắc về cài đặt bảo mật đám mây, và rủi ro của cài đặt bảo mật đám mây có thể được xác định trong nháy mắt theo thời gian, tài khoản, và tài nguyên.

Mặt khác, nếu ngày được chọn theo phân tích xu hướng, trạng thái cài đặt bảo mật của tài nguyên đám mây vào ngày đó có thể được theo dõi, và mức độ nghiêm trọng của cài đặt bảo mật cho từng tài khoản có thể được cung cấp riêng theo mức độ tốt/cảnh báo/nguy hiểm, và các vi phạm có thể được phát hiện.

Trong khi mô tả sáng chế, những mô tả kỹ thuật có thể được hiểu dễ dàng bởi người có hiểu biết trung bình trong lĩnh vực này có thể bỏ qua, tuy nhiên những mô tả được bỏ qua đó vẫn thuộc phạm vi tinh thần kỹ thuật của sáng chế.

Các mô tả về cấu hình và chức năng của từng bộ phận đã được mô tả tách biệt với nhau để thuận tiện cho việc mô tả, và cấu hình cũng như chức năng bất kỳ có thể được thực hiện bằng cách tích hợp vào các thành phần khác, hoặc được chia nhỏ hơn khi cần thiết.

Sáng chế đã được mô tả chi tiết thông qua các phương án thực hiện cụ thể cùng với các hình vẽ kèm theo. Tuy nhiên, các phương án thực hiện được mô tả chỉ nhằm mục đích minh họa mà không giới hạn phạm vi của sáng chế. Người có hiểu biết trung bình trong lĩnh vực này có thể thực hiện sửa đổi, cải biến dựa trên các phương án thực hiện, nhưng những sửa đổi, cải biến được thực hiện vẫn thuộc phạm vi của sáng chế. Ngoài ra, những phần mô tả không cần thiết làm cho sáng chế khó hiểu hoặc nhầm lẫn sẽ được bỏ qua.

Danh mục các số tham chiếu

110: Máy chủ của nhà cung cấp dịch vụ đám mây A

120: Máy chủ của nhà cung cấp dịch vụ đám mây B

130: Máy chủ của nhà cung cấp dịch vụ đám mây n

200: Máy chủ của khách hàng

210: Đám mây A

220: Đám mây B

230: Đám mây n

300: Đơn vị kiểm tra bảo mật đám mây

310: Đơn vị nhận khóa xác thực truy cập đám mây

315: Đơn vị kết nối đám mây

320: Đơn vị yêu cầu thông tin cài đặt bảo mật tài nguyên đám mây

330: Đơn vị thu thập thông tin cài đặt bảo mật tài nguyên đám mây

331: Đơn vị thu thập thông tin cài đặt bảo mật tài nguyên đám mây A

332: Đơn vị thu thập thông tin cài đặt bảo mật tài nguyên đám mây B

333: Đơn vị thu thập thông tin cài đặt bảo mật tài nguyên đám mây n

340: Đơn vị tích hợp định dạng dữ liệu

341: Đơn vị tích hợp định dạng dữ liệu đám mây A

342: Đơn vị tích hợp định dạng dữ liệu đám mây B

343: Đơn vị tích hợp định dạng dữ liệu đám mây n

350: Đơn vị quét quy định bảo mật đám mây

351: Đơn vị cung cấp hướng dẫn quy định bảo mật đám mây

360: Đơn vị lập danh sách kiểm tra quy định bảo mật

370: Đơn vị cung cấp phân tích xu hướng

371: Đơn vị phân tích xu hướng theo khoảng thời gian

372: Đơn vị phân tích xu hướng theo tài nguyên

373: Đơn vị phân tích xu hướng cho từng tài khoản

380: Đơn vị hành động quy định bảo mật đám mây

381: Đơn vị cung cấp URL

390: Đơn vị hiển thị

YÊU CẦU BẢO HỘ

1. Thiết bị quét và quản lý việc tuân thủ bảo mật đám mây, thiết bị bao gồm:

đơn vị kết nối đám mây để kết nối với đám mây của khách hàng bằng cách sử dụng khóa xác thực truy cập được cấp từ nhà cung cấp dịch vụ đám mây,

đơn vị quét thông tin cài đặt bảo mật tài nguyên đám mây quét tuần tự thông tin cài đặt bảo mật đám mây của khách hàng theo đơn vị kết nối để tạo ra nhiều tập dữ liệu thông tin cài đặt bảo mật, và định dạng dữ liệu của tập dữ liệu thông tin cài đặt bảo mật ở các định dạng khác nhau được thay đổi và tích hợp,

đơn vị quét quy định bảo mật đám mây để quét quy định bảo mật đám mây của khách hàng bằng cách so sánh và đánh giá hướng dẫn quy định về bảo mật đám mây được cung cấp và tập dữ liệu thông tin cài đặt tích hợp.

2. Thiết bị theo điểm 1, trong đó đơn vị quét thông tin cài đặt bảo mật tài nguyên đám mây bao gồm:

đơn vị yêu cầu thông tin cài đặt bảo mật tài nguyên đám mây yêu cầu tuần tự thông tin cài đặt bảo mật đám mây của máy khách theo đơn vị kết nối,

đơn vị thu thập thông tin cài đặt bảo mật tài nguyên trên đám mây tiếp nhận tuần tự thông tin cài đặt bảo mật ở các định dạng khác nhau từ các đám mây riêng lẻ của máy khách được kết nối theo yêu cầu và tạo tập dữ liệu thông tin cài đặt bảo mật,

đơn vị tích hợp định dạng dữ liệu tạo ra tập dữ liệu thông tin cài đặt tích hợp bằng cách thay đổi và tích hợp tuần tự định dạng của tập dữ liệu thông tin cài đặt bảo mật ở các định dạng khác nhau được nhập tuần tự.

3. Thiết bị theo điểm 2, còn bao gồm thêm:

đơn vị lập danh sách kiểm tra quy định bảo mật bao gồm

đơn vị kiểm tra tuân thủ quy định bảo mật kiểm tra xem các quy định bảo mật có được tuân thủ hay không theo đánh giá và quét các mục quy định bảo mật đám mây của khách hàng, và

đơn vị phân tích nguyên nhân của mục không được tuân thủ để phân tích nguyên nhân của mục không được tuân thủ quy định bảo mật.

4. Thiết bị theo điểm 3, còn bao gồm thêm:

đơn vị cung cấp phân tích xu hướng để phân tích và cung cấp các xu hướng thay đổi của các quy định bảo mật theo mỗi khoảng thời gian, mỗi tài khoản, và mỗi tài nguyên dựa trên tập dữ liệu quét quy định bảo mật được tạo bởi đơn vị lập danh sách kiểm tra quy định bảo mật.

5. Thiết bị theo điểm 4, còn bao gồm thêm:

đơn vị hành động quy định bảo mật đám mây có nhiệm vụ cung cấp một URL tương ứng để sửa quy định bảo mật không tuân thủ theo phân tích nguyên nhân của đơn vị phân tích nguyên nhân của mục không được tuân thủ.

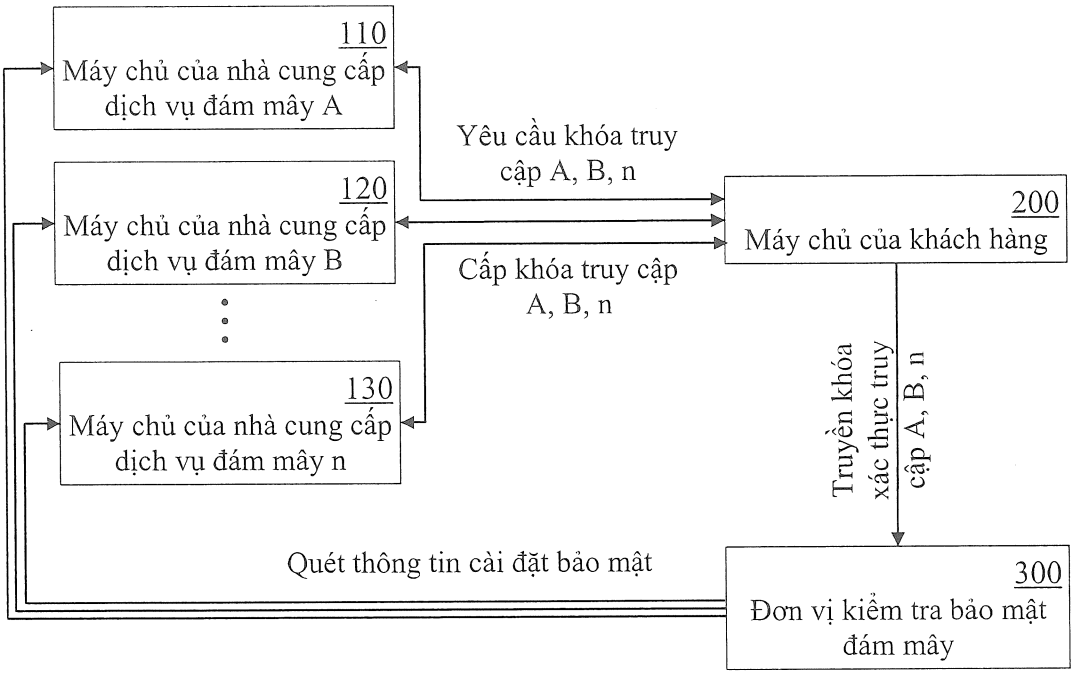
110
Máy chủ của nhà cung cấp dịch vụ đám mây A
120
Máy chủ của nhà cung cấp dịch vụ đám mây B
130
Máy chủ của nhà cung cấp dịch vụ đám mây n
Yêu cầu khóa truy cập A, B, n
Cấp khóa truy cập A, B, n
200
Máy chủ của khách hàng
Truyền khóa xác thực truy cập A, B, n
Quét thông tin cài đặt bảo mật
300
Đơn vị kiểm tra bảo mật đám mây

Fig.1

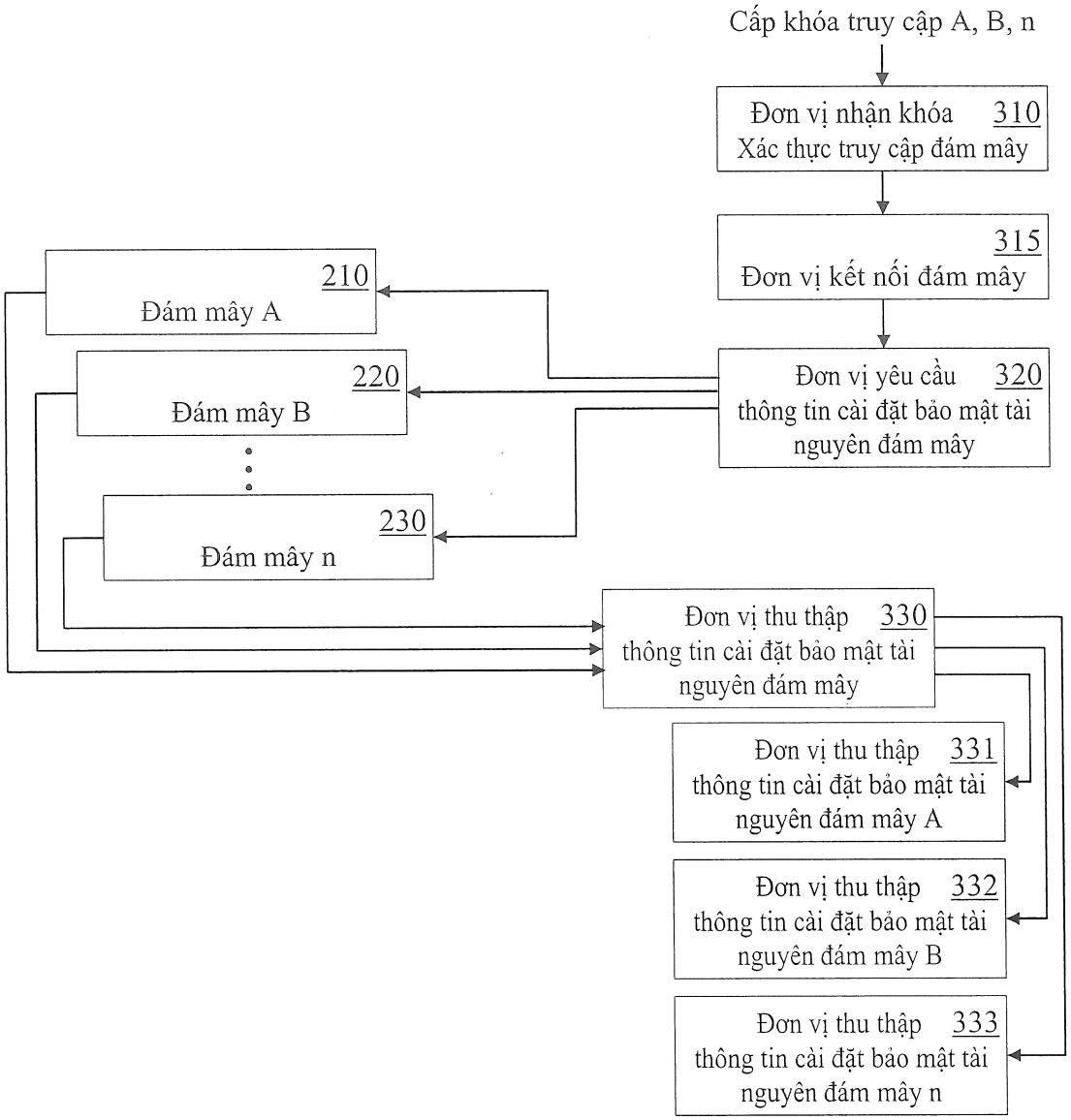
Cấp khóa truy cập A, B, n
Đơn vị nhận khóa 310
Xác thực truy cập đám mây
315
Đơn vị kết nối đám mây
210
Đám mây A
220
Đám mây B
230
Đám mây n
Đơn vị yêu cầu 320
thông tin cài đặt bảo mật tài
nguyên đám mây
Đơn vị thu thập 330
thông tin cài đặt bảo mật tài
nguyên đám mây
Đơn vị thu thập 331
thông tin cài đặt bảo mật tài
nguyên đám mây A
Đơn vị thu thập 332
thông tin cài đặt bảo mật tài
nguyên đám mây B
Đơn vị thu thập 333
thông tin cài đặt bảo mật tài
nguyên đám mây n

Fig.2

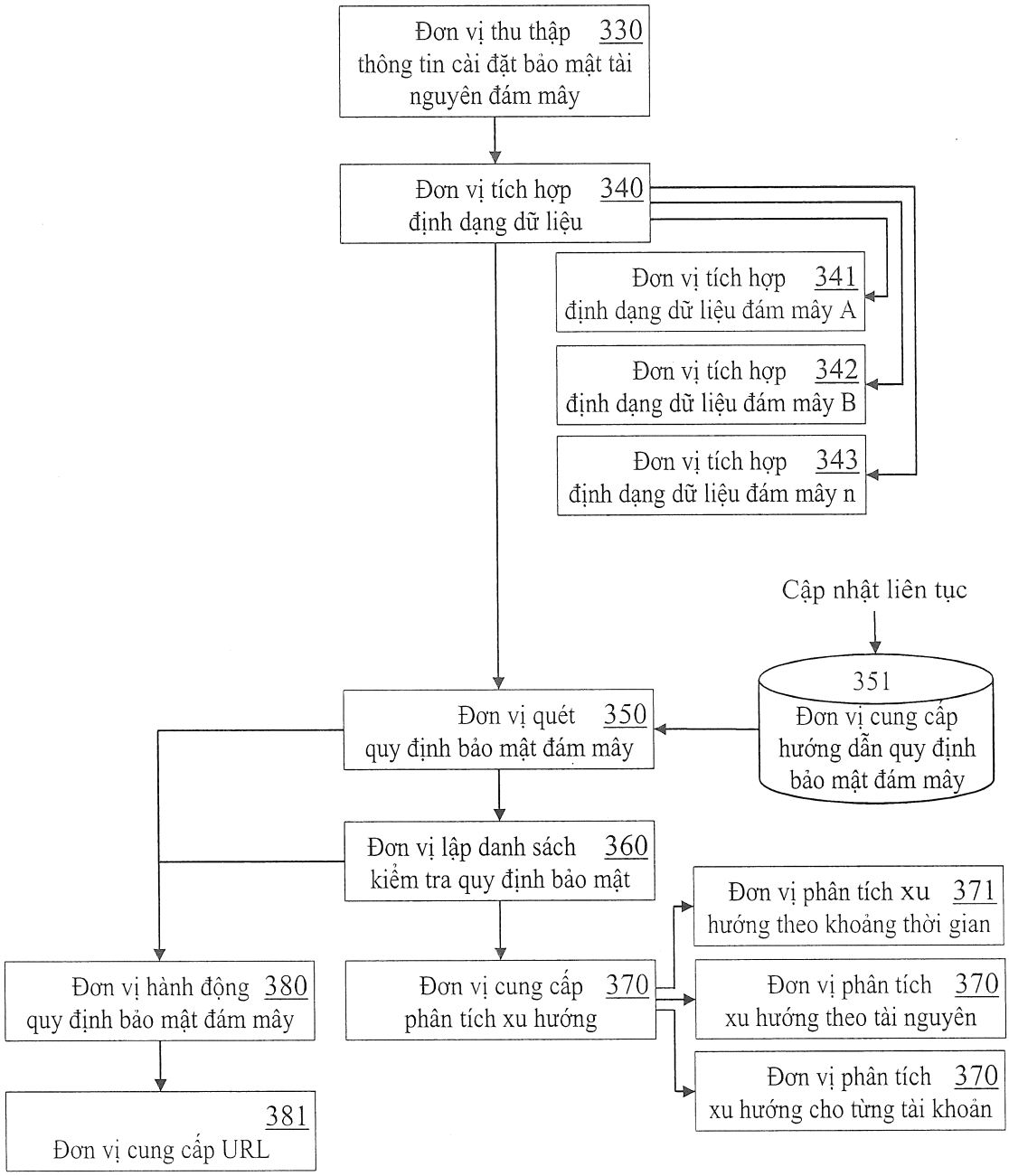
Đơn vị thu thập 330
thông tin cài đặt bảo mật tài nguyên đám mây
Đơn vị tích hợp 340
định dạng dữ liệu
Đơn vị tích hợp 341
định dạng dữ liệu đám mây A
Đơn vị tích hợp 342
định dạng dữ liệu đám mây B
Đơn vị tích hợp 343
định dạng dữ liệu đám mây n
Cập nhật liên tục
351
Đơn vị cung cấp hướng dẫn quy định bảo mật đám mây
Đơn vị quét 350
quy định bảo mật đám mây
Đơn vị lập danh sách 360
kiểm tra quy định bảo mật
Đơn vị phân tích xu 371
hướng theo khoảng thời gian
Đơn vị hành động 380
quy định bảo mật đám mây
Đơn vị cung cấp 370
phân tích xu hướng
Đơn vị phân tích 370
xu hướng theo tài nguyên
Đơn vị phân tích 370
xu hướng cho từng tài khoản
381
Đơn vị cung cấp URL

Fig.3

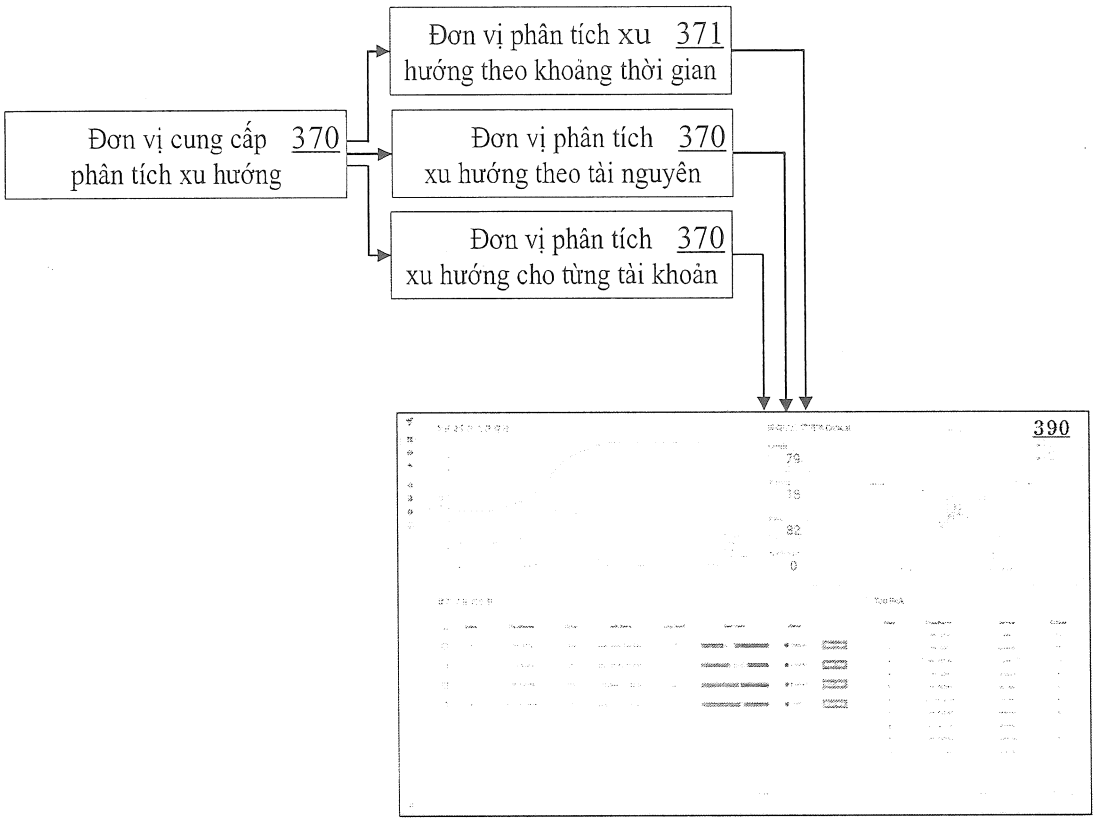
Đơn vị phân tích xu hướng theo khoảng thời gian 371
Đơn vị cung cấp phân tích xu hướng 370
Đơn vị phân tích xu hướng theo tài nguyên 370
Đơn vị phân tích xu hướng cho từng tài khoản 370
390

Fig.4

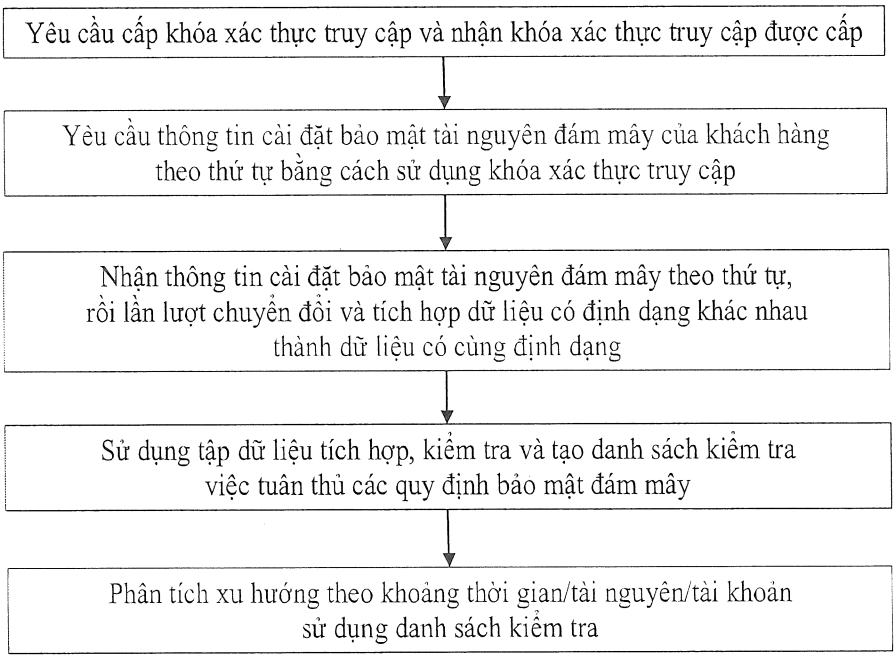
Yêu cầu cấp khóa xác thực truy cập và nhận khóa xác thực truy cập được cấp
Yêu cầu thông tin cài đặt bảo mật tài nguyên đám mây của khách hàng theo thứ tự bằng cách sử dụng khóa xác thực truy cập
Nhận thông tin cài đặt bảo mật tài nguyên đám mây theo thứ tự, rồi lần lượt chuyển đổi và tích hợp dữ liệu có định dạng khác nhau thành dữ liệu có cùng định dạng
Sử dụng tập dữ liệu tích hợp, kiểm tra và tạo danh sách kiểm tra việc tuân thủ các quy định bảo mật đám mây
Phân tích xu hướng theo khoảng thời gian/tài nguyên/tài khoản sử dụng danh sách kiểm tra

Fig.5