(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) **1-0025104**

(51)[7] **G06F 15/00**; G06Q 10/10

(13) **B**

(21) 1-2013-03581 (22) 13/11/2013

(30) 10-2013-0106170 04/09/2013 KR

(45) 25/08/2020 389 (43) 25/03/2015 324A

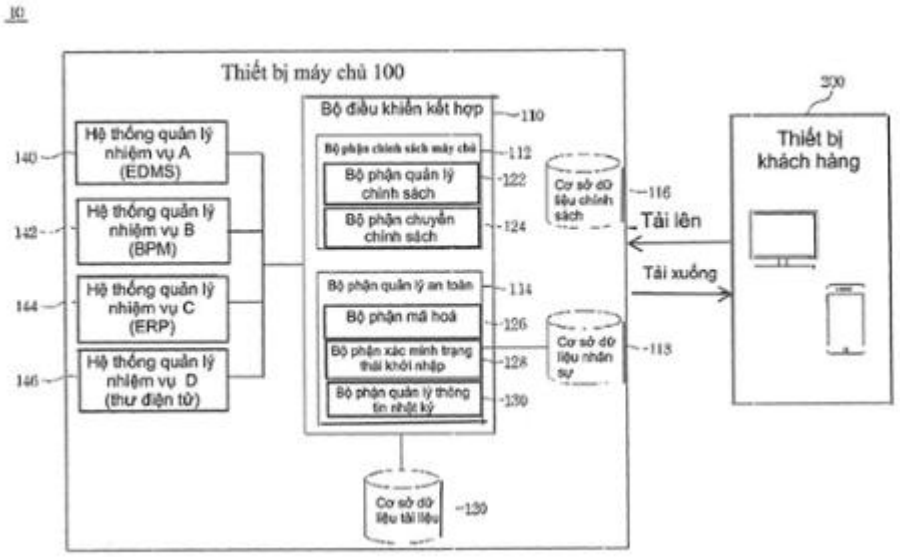
(73) MARKANY INC (KR)
10F, Ssanglim bldg, 151-11, Ssanglim-dong, Chung-gu, Seoul, Korea

(72) CHOI, Jong-Uk (KR); CHO, Joo Won (KR); Yusep Rosmansyah (ID).

(74) Công ty TNHH Sở hữu trí tuệ WINCO (WINCO CO., LTD.)

(54) HỆ THỐNG QUẢN LÝ TÀI LIỆU TÍCH HỢP

(57) Sáng chế đề cập tới hệ thống quản lý tài liệu tích hợp bao gồm máy chủ và thiết bị khách hàng, máy chủ bao gồm cơ sở dữ liệu tài liệu có trong máy chủ, cơ sở dữ liệu nhân sự, cơ sở dữ liệu quy tắc, và bộ điều khiển tích hợp được nối với các hệ thống quản lý nhiệm vụ, vì thế các hệ thống quản lý nhiệm vụ được thiết lập bởi các nhà cung cấp khác nhau có thể được kiểm soát theo cách tích hợp, trong đó các hệ thống quản lý nhiệm vụ dùng chung cơ sở dữ liệu nhân sự và cơ sở dữ liệu quy tắc bằng cách sử dụng bộ điều khiển tích hợp. Hơn nữa, thiết bị khách hàng bao gồm bộ phận giám sát, bộ điều khiển, bộ phận lưu trữ tài liệu, và bộ phận đảm bảo an toàn tài liệu được làm thích ứng để tìm kiếm một dữ liệu văn bản từ tệp tài liệu điện tử, tìm kiếm các từ liên quan tới thông tin kinh doanh từ dữ liệu văn bản tìm được, tính toán điểm số bộc lộ dựa trên số lần mà các từ liên quan tới thông tin kinh doanh được tìm kiếm và thông tin thiết lập cấp tài liệu, gán một cấp tài liệu cho tệp tài liệu điện tử dựa trên điểm số bộc lộ, và chèn một dấu mờ vào văn bản của tệp tài liệu điện tử cần hiển thị trên thiết bị khách hàng.



Lĩnh vực kỹ thuật được đề cập

Sáng chế đề cập tới hệ thống quản lý tài liệu tích hợp, và cụ thể hơn, sáng chế đề cập tới hệ thống quản lý tài liệu tích hợp có khả năng kiểm soát theo cách tích hợp nhiều hệ thống quản lý nhiệm vụ.

Tình trạng kỹ thuật của sáng chế

Hiện nay, nhờ cuộc cách mạng về công nghệ thông tin, thế giới số hoá đã trở nên phổ biến với chúng ta. Hơn nữa, liên quan tới một mô thức mới của sự phát triển xanh dựa trên ý tưởng thân thiện với môi trường, việc sử dụng giấy hiện đang giảm dần. Ngoài ra, trong khi hệ thống thực hiện nhiệm vụ đang chuyển thành môi trường làm việc thông minh, trong đó không tồn tại các giới hạn về thời gian và không gian, theo xu hướng số hóa và phát triển xanh, một nhiệm vụ có thể được thực hiện bằng cách truy nhập hệ thống ở thời điểm bất kỳ và ở bất cứ nơi đâu. Xu hướng chuyển dịch này hiện đang mở rộng trong các cơ quan chính phủ và các doanh nghiệp tư nhân tại các quốc gia đang phát triển cũng như các quốc gia phát triển.

Để cho phép đưa ra môi trường làm việc thông minh, tạo ra và quản lý các tài liệu điện tử, và thực hiện nhiệm vụ theo cách hiệu quả hơn nhờ sự hợp tác trong từng tổ chức, nhiều loại hệ thống quản lý nhiệm vụ khác nhau đang được sử dụng. Ví dụ, hệ thống quản lý tài liệu điện tử (EDMS) để cung cấp các dịch vụ: tạo ra, lưu trữ và tìm kiếm các tài liệu, và phần mềm làm việc nhóm (GW) nhằm mục đích hợp tác trong một công ty là những hệ thống quản lý nhiệm vụ tiêu biểu.

Một hiện tượng khác đang xảy ra trong ngành công nghiệp IT (công nghệ thông tin) là sự thay đổi trong các thiết bị khác nhau. Các hệ thống máy tính trước đây hiện đang được đưa vào các vi thiết bị khác nhau sau khi đưa

vào các thiết bị di động để tạo ra các sản phẩm như điện thoại thông minh, máy tính bảng, v.v.. Các vi thiết bị khác nhau bao gồm camêra cỡ nhỏ, máy ghi hình cỡ nhỏ, v.v., cũng như sản phẩm iWatch của Apple, sản phẩm Google Glasses của Google là các sản phẩm tiêu biểu đang được đưa vào thị trường. Tuy nhiên, bằng cách sử dụng với mục đích xấu các vi thiết bị này, sự rò rỉ thông tin kinh doanh của các cơ quan chính phủ và các doanh nghiệp tư nhân sẽ mở rộng, và do vậy, việc tăng cường an toàn trở thành một yêu cầu cấp thiết.

Việc số hóa thế giới, sự phát triển của các thiết bị khác nhau và thay đổi trong hệ thống thực hiện nhiệm vụ không chỉ đem lại tiện ích cho cuộc sống con người mà, không may là, còn đe doạ đến sự an toàn. Cụ thể là, do các kỹ thuật hackinh càng ngày càng phát triển, thông tin kinh doanh của các cơ quan chính phủ và các doanh nghiệp tư nhân có thể bị làm lộ, hoặc xảy ra các tổn thất lớn lao có thể đe doạ đến sự tồn vong của các công ty.

Theo sự phát triển của các kỹ thuật hackinh và ứng dụng của các vi thiết bị khác nhau, các cơ quan chính phủ và các doanh nghiệp tư nhân hiện đang xây dựng các hệ thống quản lý nhiệm vụ khác nhau cho công việc thông minh nội bộ cũng như các hệ thống an toàn để tăng cường độ an toàn. Tuy nhiên, khi xem xét rằng cấu trúc này được làm thích ứng sao cho từng hệ thống được thiết lập tách rời và được bổ sung trong cấu trúc hệ thống hiện có mỗi khi cần, chứ không phải trong một hệ thống tích hợp, chi phí cho việc xây dựng và tích hợp sẽ gia tăng và cơ sở dữ liệu không thể được dùng chung. Ví dụ, hãy giả sử rằng một công ty thiết lập và sử dụng riêng biệt một hệ thống an toàn quản lý bản quyền số (DRM) để tăng cường độ an toàn, trong khi sử dụng các hệ thống quản lý nhiệm vụ EDMS và GW. Trước hết, hệ thống EDMS, là một hệ thống quản lý tài liệu, đưa thông tin cá nhân người dùng (số ID (nhận dạng), thông tin PWD (in thư mục đang làm việc), bộ phận làm việc, vị trí làm việc, v.v.) và thông tin về sơ đồ tổ chức từ cơ sở dữ liệu nhân sự khi người dùng

đăng nhập, so sánh thông tin với cấp an toàn của các tài liệu, và tiếp đó chỉ cho người dùng xem các tài liệu được phép truy nhập. Trong GW, nhằm mục đích hợp tác, đối với một hệ thống phê chuẩn điện tử, máy chủ đưa ra thông tin cá nhân người dùng và thông tin về sơ đồ tổ chức từ cơ sở dữ liệu nhân sự, và giới hạn vị trí mà tài liệu tương ứng cần được truyền để phê chuẩn và giới hạn các thao tác 'đọc, ghi, soạn thảo', v.v., tài liệu theo khả năng truy nhập của người dùng. Hơn nữa, máy chủ DRM còn tạo ra thông tin kiểm soát khả năng truy nhập của người dùng để kiểm soát khả năng truy nhập của người dùng tới một tài liệu dựa trên thông tin cá nhân người dùng và thông tin tổ chức được đưa ra từ cơ sở dữ liệu nhân sự, và cấp an toàn của tài liệu tương ứng. Sau đó, thông tin kiểm soát khả năng truy nhập được tạo ra được chèn vào phần đầu tệp của tài liệu và được mã hoá với khoá mã hoá của người dùng để đảm bảo an toàn cho tài liệu. Nghĩa là, từng hệ thống lưu trữ cùng thông tin trong từng cơ sở dữ liệu nhân sự và đưa ra thông tin từ cơ sở dữ liệu nhân sự mỗi khi người dùng truy nhập. Cấu trúc hệ thống hiện có này có thể tạo ra nhiều vấn đề kể cả làm tăng chi phí cho việc xây dựng và tích hợp hệ thống như nêu trên.

Trong các cấu trúc hệ thống hiện có, vì từng hệ thống tồn tại riêng biệt, thông tin cá nhân người dùng (số ID (nhận dạng), thông tin PWD (in thư mục đang làm việc), bộ phận làm việc, vị trí làm việc, v.v.) và thông tin tổ chức được lưu trữ nhiều lần trong cơ sở dữ liệu nhân sự trong từng hệ thống máy chủ. Vì thế, ngoài vấn đề lãng phí bộ nhớ gây ra bởi dữ liệu được lưu trữ nhiều lần là vấn đề chính, còn tồn tại nhiều vấn đề phụ. Cơ sở dữ liệu không chỉ được sử dụng bởi một cá nhân duy nhất mà còn là vị trí mà nhiều người dùng truy nhập theo thời gian thực và sử dụng đồng thời, và trong đó các thay đổi liên tục, như thay mới, chèn, xóa, v.v. xảy ra. Do đó, nếu tồn tại nhiều cơ sở dữ liệu chứa cùng thông tin, khó có thể thực hiện việc quản lý một cách nhất quán tất cả các cơ sở dữ liệu này. Ví dụ, nếu các thay đổi trong thông tin

cá nhân người dùng chỉ được áp dụng cho cơ sở dữ liệu nhân sự trong máy chủ của hệ thống EDMS, trong hệ thống GW, người dùng không thể xác nhận một cách thích hợp các tài liệu có thể truy nhập được với cấp của người này và vẫn có thể dễ dàng truy nhập các tài liệu không được phép, điều này gây ra các vấn đề nghiêm trọng. Nghĩa là, nếu các thay đổi trong thông tin cá nhân người dùng không được phản ánh trong tất cả cơ sở dữ liệu nhân sự trong máy chủ, một lỗ hổng an toàn lớn có thể được tạo ra. Như vậy, có vấn đề là tất cả các yếu tố bao gồm tính bảo mật, tính toàn vẹn và đặc tính khả dụng, là ba yếu tố liên quan tới sự an toàn, đều có thể sụp đổ.

Ngoài ra, trong các cấu trúc hiện có trong đó từng máy chủ được vận hành riêng biệt, xảy ra lãng phí thời gian do hoạt động lặp lại. Mỗi khi người dùng truy nhập từng máy chủ, từng máy chủ cần tìm kiếm dữ liệu về thông tin cá nhân người dùng và thông tin về sơ đồ tổ chức vì từng máy chủ quản lý cơ sở dữ liệu nhân sự riêng. Ví dụ, trong các cấu trúc hệ thống hiện có, khi người dùng truy nhập máy chủ của hệ thống EDMS và tiếp đó là hệ thống GW, thông tin cá nhân người dùng, thông tin về sơ đồ tổ chức, v.v. được tìm kiếm nhiều lần, điều này làm giảm tốc độ hệ thống và làm giảm hiệu quả công việc. Nói cách khác, theo các giải pháp kỹ thuật đã biết, các hệ thống quản lý nhiệm vụ khác nhau được sử dụng để tìm kiếm sự hợp tác của công ty trong môi trường làm việc thông minh; tuy nhiên, từng hệ thống này không được tích hợp một cách hữu hiệu, điều này dẫn đến chi phí rất lớn và khó khăn trong việc thiết lập hệ thống, và gây ra vấn đề về sự an toàn do lặp lại dữ liệu trong cơ sở dữ liệu.

Ngoài ra, với các giải pháp kỹ thuật đã biết, độ an toàn đối với việc phổ biến hoá các vi thiết bị là không đủ, và môi trường thực hiện nhiệm vụ di động sẽ được khởi hoạt thêm trong tương lai cũng không thể được hỗ trợ đầy đủ. Theo các giải pháp kỹ thuật đã biết, phương pháp quản lý bản quyền số (DRM) hoặc phương pháp ngăn chặn tổn thất dữ liệu (DLP) chủ yếu được sử

dụng cho hệ thống an toàn của một công ty. Theo khía cạnh này, phương pháp DRM là phương pháp mã hoá một tài liệu cần được truyền và kiểm soát việc truy nhập tới một tài liệu đã giải mã theo khả năng truy nhập của người dùng. Tuy nhiên, phương pháp quản lý bản quyền số (DRM) có vấn đề là người dùng có thể truy nhập tới các tài liệu này có thể dễ dàng truy nhập các nội dung bất cứ lúc nào. Phương pháp DLP là phương pháp tìm kiếm một văn bản bằng cách tìm kiếm nội dung của tài liệu, xác định cấp an toàn của tài liệu này, và xử lý tương ứng tài liệu. Tuy nhiên, phương pháp DLP, để phát hiện sự rò rỉ của các nội dung bằng cách tìm kiếm nội dung, có các vấn đề bổ sung vì tài liệu được truyền ở dạng văn bản rõ ràng trong trường hợp có sự rò rỉ của các nội dung. Do các vấn đề nêu trên, phương pháp DRM và phương pháp DLP là các phương pháp tiêu biểu được áp dụng để đảm bảo an toàn trong các công ty theo các giải pháp kỹ thuật đã biết là chưa đủ để giải quyết các vấn đề về độ an toàn liên quan tới việc áp dụng rộng rãi các vi thiết bị.

Giải pháp kỹ thuật đã biết

Tài liệu patent 1: Công bố đơn yêu cầu cấp patent Hàn Quốc số 2008-0064164 (công bố ngày 8 tháng 7 năm 2008).

Bản chất kỹ thuật của sáng chế

Để giải quyết các vấn đề nêu trên, sáng chế đề xuất phương pháp và thiết bị để hỗ trợ hệ thống quản lý nhiệm vụ dạng số kiểu tích hợp và định hướng người dùng dựa trên sự trợ giúp của giải pháp bảo vệ thông tin của công ty để quản lý theo cách tích hợp nhiều hệ thống thực hiện nhiệm vụ khác nhau trong môi trường làm việc thông minh bằng cách sử dụng một hệ thống kiểm soát quản lý tích hợp, cũng như để tăng cường an toàn của công ty bằng cách giảm tới mức tối thiểu sự rò rỉ của thông tin kinh doanh dựa trên việc tích hợp hệ thống với các công nghệ tìm kiếm nội dung theo phương pháp DRM và phương pháp DLP đã biết nhờ áp dụng kỹ thuật mã hoá và kiểm soát khả năng

truy nhập. Nhằm mục đích này, sáng chế đề xuất hệ thống đăng nhập tích hợp bằng cách sử dụng hệ thống kiểm soát quản lý tích hợp (IMCS) dựa trên thông tin cá nhân người dùng và thông tin về sơ đồ tổ chức, và quản lý theo cách tích hợp nhiều hệ thống thực hiện nhiệm vụ khác nhau.

Ngoài ra, liên quan tới việc các tài liệu điện tử trong công ty có chứa các nội dung mật hay không, sáng chế áp dụng các kỹ thuật tìm kiếm và xác nhận nội dung của các tài liệu điện tử, xác định hệ số quan trọng của các tài liệu điện tử dựa trên các kỹ thuật này, thiết lập cấp của các tài liệu, và gán cấp có thể truy nhập cho từng người dùng, và tạo ra việc kiểm soát truy nhập. Ngoài ra, sáng chế cho phép mã hóa các tài liệu điện tử và chèn các dấu mờ văn bản phân biệt dựa trên thông tin cá nhân người dùng để cho phép dò sau đó trong trường hợp các tài liệu bị làm lộ, và vì thế có mục tiêu khác là tăng cường biện pháp đảm bảo an toàn sau cũng như biện pháp đảm bảo an toàn trước nhờ phương pháp DRM và phương pháp DLP.

Một mục đích khác của sáng chế là tăng cường độ an toàn trong môi trường thực hiện nhiệm vụ di động bằng cách sử dụng các thiết bị và các thiết bị thông minh khác nhau nhờ cấu trúc của hệ thống an toàn dựa trên các thiết bị người dùng. Vì một đầu cuối người dùng, chứ không phải hệ thống an toàn đã biết trong máy chủ, tạo ra biện pháp đảm bảo an toàn trước bằng cách tìm kiếm nội dung và thiết lập cấp của các tài liệu và biện pháp đảm bảo an toàn sau bằng cách chèn dấu mờ văn bản, sáng chế cho phép tạo ra hệ thống an toàn hiệu quả phù hợp với sự chuyển đổi sang môi trường thực hiện nhiệm vụ di động.

Để đạt được mục đích như nêu trên, sáng chế đề xuất hệ thống quản lý tài liệu tích hợp bao gồm máy chủ và thiết bị khách hàng, máy chủ có khả năng kiểm soát theo cách tích hợp nhiều hệ thống quản lý nhiệm vụ bao gồm các hệ thống quản lý nhiệm vụ được thiết lập bởi các nhà cung cấp khác nhau; cơ sở dữ liệu tài liệu để lưu trữ các tài liệu điện tử có thông tin kinh doanh; cơ

sở dữ liệu nhân sự để lưu trữ sơ đồ tổ chức và thông tin người dùng; cơ sở dữ liệu quy tắc để lưu trữ tệp quy tắc liên quan tới quy tắc về an toàn thông tin kinh doanh; và bộ điều khiển tích hợp được nối với các hệ thống quản lý nhiệm vụ, trong đó các hệ thống quản lý nhiệm vụ dùng chung cơ sở dữ liệu nhân sự và cơ sở dữ liệu quy tắc bằng cách sử dụng bộ điều khiển tích hợp. Bộ điều khiển tích hợp bao gồm bộ phận quy tắc máy chủ được nối với cơ sở dữ liệu quy tắc và bao gồm bộ phận quản lý quy tắc để quản lý tệp quy tắc được lưu trữ trong cơ sở dữ liệu quy tắc và bộ phận truyền quy tắc để truyền tệp quy tắc tới thiết bị khách hàng, và bộ phận quản lý an toàn bao gồm bộ phận mã hoá để mã hoá tệp tài liệu điện tử cần truyền từ cơ sở dữ liệu tài liệu tới thiết bị khách hàng, bộ phận xác minh thông tin đăng nhập để xác minh thông tin đăng nhập của người dùng của thiết bị khách hàng bằng cách so sánh với thông tin người dùng được lưu trữ trong cơ sở dữ liệu nhân sự, và bộ phận quản lý thông tin nhật ký để quản lý thông tin nhật ký nhận được từ thiết bị khách hàng.

Tiếp theo, thiết bị khách hàng có thể bao gồm bộ phận giám sát để giám sát việc tạo ra tệp tài liệu điện tử và các thay đổi trên tệp tài liệu điện tử này; bộ điều khiển để thu nhận tệp quy tắc từ cơ sở dữ liệu quy tắc trong máy chủ, tệp quy tắc có thông tin thiết lập cấp tài liệu và quy tắc về xử lý an toàn; bộ phận đảm bảo an toàn tài liệu; và bộ phận lưu trữ tài liệu. Bộ phận đảm bảo an toàn tài liệu có thể được làm thích ứng để tìm kiếm một dữ liệu văn bản từ tệp tài liệu điện tử, tìm kiếm các từ liên quan tới thông tin kinh doanh từ dữ liệu văn bản tìm được, tính toán điểm số bộc lộ đối với tệp tài liệu điện tử dựa trên số lần mà các từ liên quan tới thông tin kinh doanh được tìm kiếm và thông tin thiết lập cấp tài liệu, gán một cấp tài liệu liên quan tới khả năng truy nhập của người dùng cho tệp tài liệu điện tử dựa trên điểm số bộc lộ, và chèn một dấu mờ vào văn bản của tệp tài liệu điện tử cần hiển thị trên thiết bị khách hàng dựa trên thông tin cá nhân người dùng nhận được từ máy chủ. Hơn nữa, bộ

phận lưu trữ tài liệu có thể được làm thích ứng để tải lên tệp tài liệu điện tử được tạo ra trong bộ phận đảm bảo an toàn tài liệu tới cơ sở dữ liệu tài liệu hoặc tải xuống tệp tài liệu điện tử đã mã hóa từ bộ phận mã hoá.

Theo một phương án khác, các hệ thống quản lý nhiệm vụ bao gồm ít nhất một trong số: hệ thống quản lý tài liệu điện tử (EDMS), phần mềm làm việc nhóm (GW), hệ thống quản lý quy trình kinh doanh (BPM), hệ thống hoạch định tài nguyên doanh nghiệp (ERP) và hệ thống thư điện tử.

Hiệu quả của sáng chế

Nhờ hệ thống quản lý tài liệu tích hợp theo sáng chế, các hệ thống quản lý nhiệm vụ khác nhau được tích hợp với hệ thống kiểm soát quản lý tích hợp (IMCS) là trung tâm dựa trên hệ thống quản lý tài liệu đã biết, các hệ thống quản lý nhiệm vụ dạng số khác nhau, như hệ thống phê chuẩn điện tử, v.v.. Cụ thể hơn, sáng chế đề xuất một hệ thống tích hợp của thông tin cá nhân người dùng và thông tin về sơ đồ tổ chức trong một cơ sở dữ liệu nhân sự với hệ thống IMCS là trung tâm chứ không phải chỉ tích hợp đơn giản các hệ thống quản lý nhiệm vụ dạng số và các hệ thống quản lý nhiệm vụ khác nhau. Nhờ đó, sáng chế cho phép giảm bớt đáng kể chi phí bổ sung cần thiết cho việc xây dựng và tích hợp hệ thống bổ sung. Hơn nữa, vì các hệ thống quản lý nhiệm vụ khác nhau trong máy chủ dùng chung một cơ sở dữ liệu nhân sự, sáng chế cho phép ngăn chặn lãng phí thời gian gây ra bởi việc tìm kiếm lặp lại người dùng nhân sự thông tin và thông tin về sơ đồ tổ chức mỗi khi người dùng truy nhập máy chủ, và làm tăng hiệu quả trong việc xử lý nhiệm vụ. Ngoài ra, sáng chế cho phép giải quyết vấn đề về độ an toàn có thể gặp phải do sự không nhất quán trong thông tin do lặp lại dữ liệu, và dễ dàng tích hợp các hệ thống thực hiện nhiệm vụ khác nhau trong tương lai để có thể tạo ra môi trường thực hiện nhiệm vụ nhất quán.

Ngoài ra, theo một phương án khác của sáng chế, bằng cách dùng chung

các tài liệu bên trong công ty giữa các thiết bị khách hàng sử dụng máy chủ, các thiết bị khách hàng bổ sung các chức năng tìm kiếm nội dung của phương pháp DLP vào phương pháp DRM bằng cách sử dụng khả năng mã hoá và kiểm soát truy nhập đã biết để cho phép thực hiện quy tắc về an toàn đối với các tài liệu được tạo ra trong các thiết bị người dùng, các tài liệu được truyền qua web, và các tài liệu được lưu trữ trong một phương tiện bộ nhớ, theo cấp an toàn của chúng, và vì thế nguy cơ xảy ra sự rò rỉ của các tài liệu được duy trì mức thấp. Do đó, sáng chế cho phép tăng cường biện pháp đảm bảo an toàn trước.

Ngoài ra, sáng chế sử dụng kỹ thuật tạo dấu mờ văn bản để phân biệt từng người dùng với cỡ phông chữ và khoảng cách từ, điều này cho phép dò đường dẫn làm lộ bí mật khi một tài liệu bị làm lộ, và nhờ đó có thể tăng cường biện pháp đảm bảo an toàn sau cũng như biện pháp đảm bảo an toàn trước. Nghĩa là, sáng chế cho phép tích hợp các hệ thống khác nhau với hệ thống IMCS trong máy chủ là trung tâm, và tăng cường biện pháp đảm bảo an toàn trước nhờ phương pháp DRM và phương pháp DLP và biện pháp đảm bảo an toàn sau bằng cách dò dấu mờ văn bản.

Ngoài ra, cấu trúc của hệ thống an toàn dựa trên các thiết bị người dùng cho phép tăng cường an toàn trong môi trường thực hiện nhiệm vụ di động nhờ các thiết bị và các thiết bị thông minh khác nhau. Theo sáng chế, vì chính đầu cuối người dùng chứ không phải hệ thống an toàn đã biết trong máy chủ tạo ra biện pháp đảm bảo an toàn trước bằng cách tìm kiếm nội dung và thiết lập cấp của các tài liệu và biện pháp đảm bảo an toàn sau bằng cách chèn dấu mờ văn bản, sáng chế cho phép tạo ra hệ thống an toàn và hiệu quả phù hợp với sự chuyển đổi sang môi trường thực hiện nhiệm vụ di động.

Mô tả vắn tắt các hình vẽ

Các mục đích, ưu điểm và khía cạnh khác nữa của sáng chế sẽ trở nên rõ

ràng hơn qua phần mô tả chi tiết dưới đây có dựa vào các hình vẽ kèm theo, trong đó:

Fig.1 là hình vẽ dạng sơ đồ thể hiện hệ thống quản lý tài liệu tích hợp bao gồm máy chủ và thiết bị khách hàng có khả năng kiểm soát theo cách tích hợp nhiều hệ thống quản lý nhiệm vụ;

Fig.2 là hình vẽ dạng sơ đồ thể hiện thiết bị khách hàng theo một phương án của sáng chế;

Fig.3 là lưu đồ thể hiện quy trình để tạo ra tệp tài liệu điện tử trong thiết bị khách hàng để tăng cường độ an toàn thông tin kinh doanh theo một phương án của sáng chế;

Fig.4 là lưu đồ thể hiện quy trình dùng chung các tài liệu công ty giữa các thiết bị khách hàng sử dụng máy chủ;

Fig.5 thể hiện tệp quy tắc theo một phương án của sáng chế;

Fig.6 thể hiện một ví dụ về thông tin thiết lập cấp tài liệu được sử dụng theo sáng chế;

Fig.7 là hình vẽ dạng sơ đồ thể hiện bộ phận tìm kiếm theo một phương án của sáng chế;

Fig.8 là hình vẽ dạng sơ đồ thể hiện bộ phận xác định cấp theo một phương án của sáng chế; và

Fig.9 thể hiện một phương án chèn dấu mờ bằng cách điều chỉnh cỡ phông chữ và độ đậm nhạt của phông chữ.

Mô tả chi tiết sáng chế

Tiếp theo sẽ mô tả chi tiết về các phương án thực hiện sáng chế, các ví dụ của chúng được minh hoạ trên các hình vẽ kèm theo.

Liên quan tới các phương án thực hiện sáng chế được mô tả chi tiết ở đây, phần giải thích cấu trúc hoặc chức năng cụ thể chỉ là ví dụ minh hoạ nhằm mục đích giải thích các phương án này của sáng chế. Ngoài ra, các

phương án thực hiện sáng chế có thể được thực hiện theo nhiều hình thức khác nhau, và sáng chế không bị hạn chế ở các phương án được giải thích chi tiết ở đây.

Các phương án cải biến khác nhau có thể được thực hiện theo sáng chế, và sáng chế có thể có nhiều hình thức khác nhau. Như vậy, các phương án cụ thể sẽ được minh hoạ trên các hình vẽ và được giải thích chi tiết trong phần Mô tả chi tiết sáng chế. Tuy nhiên, các phương án cụ thể này không nhằm giới hạn sáng chế, và cần phải hiểu rằng sáng chế bao hàm tất cả các cải biến, thay đổi tương đương hoặc thay thế thích hợp trong phạm vi sáng tạo và phạm vi kỹ thuật của sáng chế.

Trừ khi được xác định khác đi, tất cả thuật ngữ được sử dụng ở đây kể cả các thuật ngữ kỹ thuật hoặc khoa học đều có nội hàm giống như các thuật ngữ được hiểu bởi các chuyên gia trong lĩnh vực kỹ thuật mà sáng chế liên quan. Các thuật ngữ như các thuật ngữ được xác định trong từ điển sử dụng thông thường cần phải được diễn dịch với nội hàm phù hợp với ngữ cảnh của lĩnh vực kỹ thuật liên quan, và không được diễn dịch ở trường hợp lý tưởng hoặc vượt quá cách hiểu chính thức trừ khi được xác định là hiển nhiên theo sáng chế.

Sau đây, các phương án ưu tiên của sáng chế sẽ được giải thích chi tiết hơn có dựa vào các hình vẽ kèm theo. Cần lưu ý rằng cùng số chỉ dẫn được sử dụng để biểu thị các chi tiết giống nhau trên các hình vẽ, và phần giải thích về các chi tiết giống nhau này sẽ được lược bỏ.

Fig.1 là hình vẽ dạng sơ đồ thể hiện hệ thống quản lý tài liệu tích hợp 10 bao gồm máy chủ 100 và thiết bị khách hàng 200, hệ thống này có khả năng kiểm soát theo cách tích hợp nhiều hệ thống quản lý nhiệm vụ. Máy chủ 100 có thể bao gồm bộ điều khiển tích hợp 110, cơ sở dữ liệu quy tắc 116, cơ sở dữ liệu nhân sự 118, cơ sở dữ liệu tài liệu 120 và các hệ thống quản lý nhiệm vụ 140, 142, 144, 146. Hệ thống kiểm soát quản lý tích hợp (IMCS)

theo sáng chế có thể được bổ sung vào bộ điều khiển tích hợp 110 trong máy chủ.

Bộ điều khiển tích hợp 110 có thể được nối với cơ sở dữ liệu tài liệu 120 và có thể bao gồm bộ phận quy tắc máy chủ 112 được nối với cơ sở dữ liệu quy tắc 116 và bộ phận quản lý an toàn 114 được nối với cơ sở dữ liệu nhân sự. Bộ phận quy tắc máy chủ 112 có thể bao gồm bộ phận quản lý quy tắc 122 và bộ phận truyền quy tắc 124. Bộ phận quản lý quy tắc 122 thực hiện việc quản lý các tệp quy tắc bao gồm các quy tắc để thiết lập cấp của các tài liệu dựa trên điểm số bộc lộ của thông tin kinh doanh đối với các tài liệu tương ứng, và cấp khả năng truy nhập của người dùng, v.v., và được lưu trữ trong cơ sở dữ liệu quy tắc, các thao tác quản lý như lưu, cập nhật, xóa, v.v., các tệp quy tắc. Bộ phận truyền quy tắc 124 có thể giữ vai trò truyền tệp quy tắc được lưu trữ trong cơ sở dữ liệu quy tắc tới thiết bị khách hàng, nếu cần. Bộ phận quản lý an toàn 114 trong máy chủ thực hiện việc xác minh thông tin đăng nhập của người dùng, phát hiện thông tin nhật ký, và hỗ trợ việc mã hoá một tài liệu. Cụ thể là, bộ phận quản lý an toàn 114 có thể bao gồm bộ phận mã hoá 126 để mã hoá một tài liệu điện tử trước khi truyền tài liệu điện tử này tới thiết bị khách hàng, bộ phận xác minh thông tin đăng nhập 128 để xác minh quyền đăng nhập đối với từng người dùng dựa trên thông tin người dùng và thông tin về sơ đồ tổ chức được lưu trữ trong cơ sở dữ liệu nhân sự trong máy chủ khi người dùng đăng nhập, và bộ phận quản lý thông tin nhật ký 130 quản lý thông tin liên quan tới việc xử lý an toàn theo các kết quả phát hiện ở dạng dữ liệu nhật ký nhận được từ thiết bị khách hàng trong trường hợp thông tin kinh doanh được phát hiện trong thiết bị khách hàng.

Như được thể hiện trên Fig.1, cơ sở dữ liệu quy tắc 116 được nối với bộ phận quy tắc máy chủ 112 và lưu trữ các tệp quy tắc có thông tin liên quan tới quy tắc về an toàn đối với thông tin kinh doanh. Fig.5 thể hiện một ví dụ về tệp quy tắc được sử dụng theo sáng chế. Cơ sở dữ liệu nhân sự 118 được nối

với bộ phận quản lý an toàn 114 của máy chủ, và có thể lưu trữ thông tin của ban lãnh đạo và nhân viên của công ty, nghĩa là thông tin của những người dùng có thể đọc các tài liệu chứa thông tin kinh doanh, thông tin về sơ đồ tổ chức của công ty, v.v.. Nếu thiết bị khách hàng được nối với máy chủ yêu cầu đăng nhập, bộ phận xác minh thông tin đăng nhập 128 trong máy chủ có thể xác minh thông tin đăng nhập bằng cách hỏi tin về sơ đồ tổ chức và thông tin người dùng, v.v. được lưu trữ trong cơ sở dữ liệu nhân sự. Cơ sở dữ liệu tài liệu 120 mà các tệp tài liệu điện tử chứa thông tin kinh doanh được lưu trữ trong đó có thể được nối với bộ điều khiển tích hợp và có thể lưu trữ tệp tài liệu điện tử được tải lên từ thiết bị khách hàng. Nếu thiết bị khách hàng yêu cầu tải xuống, máy chủ hỏi tin về tệp tài liệu điện tử từ cơ sở dữ liệu tài liệu, mã hóa tệp tài liệu tương ứng bằng cách sử dụng bộ phận mã hoá trong bộ điều khiển tích hợp, và truyền tệp tài liệu điện tử đã mã hóa tới thiết bị khách hàng.

Máy chủ 100 có thể còn bao gồm các hệ thống quản lý nhiệm vụ 140, 142, 144, 146. Các hệ thống quản lý nhiệm vụ này có thể là các hệ thống quản lý tài liệu điện tử bất kỳ trong công ty để xử lý các tài liệu nội bộ, như phê chuẩn, dùng chung, hiệu chỉnh, lưu trữ, truyền, v.v. các tài liệu, chẳng hạn hệ thống quản lý tài liệu điện tử (EDMS), phần mềm làm việc nhóm (GW), hệ thống quản lý quy trình kinh doanh (BPM), hệ thống hoạch định tài nguyên doanh nghiệp (ERP), hệ thống thư điện tử, v.v.. Các hệ thống này có thể là các hệ thống được thiết lập bởi các nhà cung cấp dịch vụ khác nhau.

Các hệ thống quản lý nhiệm vụ được cài đặt trong máy chủ theo sáng chế không có cơ sở dữ liệu nhân sự và/hoặc cơ sở dữ liệu quy tắc trong từng hệ thống mà tích hợp các hệ thống quản lý nhiệm vụ khác nhau với hệ thống kiểm soát quản lý tích hợp (IMCS) được tích hợp vào bộ điều khiển tích hợp, nghĩa là dùng chung cơ sở dữ liệu nhân sự có thông tin cá nhân người dùng và thông tin về sơ đồ tổ chức và/hoặc cơ sở dữ liệu quy tắc. Bằng cách đưa ra hệ

thống kiểm soát quản lý tích hợp đối với các hệ thống quản lý nhiệm vụ khác nhau, có thể giảm bớt đáng kể chi phí bổ sung cần thiết cho việc xây dựng và tích hợp hệ thống mỗi khi từng hệ thống quản lý nhiệm vụ được bổ sung. Ngoài ra, vì các hệ thống quản lý nhiệm vụ khác nhau sử dụng một cơ sở dữ liệu nhân sự và/hoặc cơ sở dữ liệu quy tắc tích hợp trong máy chủ, có thể ngăn chặn lãng phí thời gian dùng cho việc tìm kiếm thông tin cá nhân người dùng và thông tin về sơ đồ tổ chức là công việc được thực hiện lặp lại mỗi khi nối với máy chủ, và cải thiện hiệu quả công việc. Ngoài ra, có thể giải quyết vấn đề về độ an toàn có thể gặp phải do sự không nhất quán trong thông tin do lặp lại dữ liệu, và dễ dàng tích hợp các hệ thống thực hiện nhiệm vụ khác nhau trong tương lai để cho phép tạo ra môi trường thực hiện nhiệm vụ nhất quán.

Như được thể hiện trên Fig.1, máy chủ 100 có thể được nối với thiết bị khách hàng qua mạng, và có thể được nối đồng thời với nhiều thiết bị khách hàng. Thiết bị khách hàng được nối với máy chủ có thể tải lên tệp tài liệu điện tử trong máy chủ và tải xuống tệp tài liệu điện tử từ máy chủ. Một ví dụ cụ thể về cấu trúc của thiết bị khách hàng có thể nối với máy chủ được thể hiện trên Fig.2.

Như được thể hiện trên Fig.2, thiết bị khách hàng 200 có thể bao gồm bộ điều khiển 201, bộ phận giám sát 202 và bộ phận quản lý tài liệu khách hàng 203. Trong trường hợp này, bộ phận quản lý tài liệu khách hàng 203 có thể bao gồm bộ phận đảm bảo an toàn tài liệu 204 và bộ phận lưu trữ tài liệu 205.

Bộ phận đảm bảo an toàn tài liệu cần được khởi hoạt nhờ một bộ phận khởi hoạt vì các tham số thiết lập có thể thay đổi liên tục do các lần cập nhật thường xuyên hoặc các thay đổi tham số thiết lập của người dùng, v.v.. Như vậy, bộ điều khiển 201 có thể được làm thích ứng để tạo ra chức năng khởi hoạt để khởi hoạt bộ phận đảm bảo an toàn tài liệu 204 trong bộ phận quản lý tài liệu khách hàng 203; thu nhận các tệp quy tắc từ máy chủ; mở hoặc đóng

các tệp quy tắc thu nhận được; và đọc, ghi và xoá các mục cụ thể trong các tệp quy tắc, v.v.. Bộ điều khiển 201 còn có thể chỉ thị bộ phận đảm bảo an toàn tài liệu kiểm tra tệp tài liệu được tải xuống thiết bị khách hàng.

Bộ phận giám sát 202 có thể bao gồm bộ phận lọc quy trình để thông báo thông tin quy trình nếu bộ phận giám sát phát hiện được việc tạo ra tệp tài liệu điện tử trong quá trình xử lý tệp tài liệu của thiết bị khách hàng hoặc các thay đổi trong đó bằng cách giám sát theo thời gian thực quá trình xử lý tệp tài liệu; bộ phận lọc tệp thực hiện giám sát theo thời gian thực các tệp dựa trên tên tệp, phần mở rộng, v.v., và thông báo thay đổi nếu thay đổi được phát hiện trong tệp; và bộ phận thiết lập ánh xạ danh sách tệp có khả năng làm tăng hiệu quả phát hiện bằng cách quản lý danh sách bao gồm các tệp được phát hiện một lần để được loại trừ trong lần phát hiện tiếp theo.

Tiếp theo sẽ mô tả chi tiết hơn về bộ phận đảm bảo an toàn tài liệu 204 tạo thành bộ phận quản lý tài liệu khách hàng 203, bộ phận đảm bảo an toàn tài liệu này có thể bao gồm bộ phận giao diện 210, bộ phát hiện tệp mã hoá/không mã hoá 220, bộ phận tìm kiếm 230, bộ phận xác định cấp 240, bộ phận tạo dấu mờ 250, bộ phận xử lý an toàn 260 và bộ phận tạo ra tệp 270.

Bộ phận giao diện 210 thu nhận một thông báo về thay đổi trong tài liệu từ bộ phận giám sát 202, thu nhận lệnh tìm kiếm nhờ bộ điều khiển 201, và thu nhận tài liệu tải xuống được từ máy chủ nhờ bộ phận lưu trữ tài liệu 205. Tệp tài liệu điện tử đã tải xuống được từ máy chủ, tệp tài liệu này nhận được từ bộ phận giao diện 210, được truyền tới bộ phận phát hiện tệp mã hoá/không mã hoá 220 để được xác định xem tài liệu này có được mã hoá hay không. Nếu đã được mã hoá, tài liệu này có thể được giải mã và được lưu trữ tạm thời trong trong một bộ nhớ. Tệp tài liệu điện tử không được mã hoá hoặc đã giải mã được truyền tới bộ phận tìm kiếm 230 trong bộ phận đảm bảo an toàn tài liệu để được tìm kiếm xem tệp tài liệu tương ứng này có chứa thông tin kinh doanh hay không. Bộ phận tìm kiếm 230 sẽ được giải thích chi tiết hơn có dựa

vào Fig.7. Bộ phận xác định cấp 240 xác định cấp của một tài liệu và cấp khả năng truy nhập của người dùng dựa trên các kết quả tìm kiếm văn bản tài liệu và các tệp quy tắc nhận được từ máy chủ. Bộ phận xác định cấp 240 sẽ được giải thích chi tiết hơn có dựa vào Fig.8. Bộ phận tạo dấu mờ 250 thu nhận thông tin cá nhân người dùng từ máy chủ và chèn một dấu mờ văn bản để phân biệt tài liệu thiết lập cấp cần hiển thị dựa trên thông tin cá nhân người dùng thu nhận được. Các phương án trong đó một dấu mờ văn bản được chèn được thể hiện trên Fig.9. Sau đó, bộ phận xử lý an toàn 260 thực hiện xử lý an toàn bao gồm các thao tác: xoá, cách ly, v.v. tệp tài liệu điện tử đã được tạo dấu mờ, và bộ phận tạo ra tệp 270 tạo ra tệp cuối cùng trong đó thông tin về khả năng truy nhập được chèn vào phần đầu tệp của tệp.

Fig.3 là lưu đồ thể hiện quy trình tạo ra tệp tài liệu điện tử trong thiết bị khách hàng để tăng cường độ an toàn thông tin kinh doanh theo một phương án của sáng chế. Như được thể hiện trên Fig.3, quy trình được khởi hoạt bằng cách tải xuống hoặc tạo ra tệp tài liệu điện tử trong thiết bị khách hàng (bước S300). Bộ phận giám sát trong thiết bị khách hàng giám sát việc tạo ra tệp tài liệu điện tử trong thiết bị khách hàng và/hoặc các thay đổi trong tệp tài liệu điện tử được tải xuống từ máy chủ (bước S302). Thiết bị khách hàng còn có thể thu nhận các tệp quy tắc có thông tin thiết lập cấp tài liệu và quy tắc về xử lý an toàn từ máy chủ (bước S304). Thông tin thiết lập cấp tài liệu có thể có thông tin về hệ số quan trọng trong từng từ liên quan tới thông tin kinh doanh, quy tắc về cấp tài liệu xác định cấp tài liệu theo điểm số bộc lộ và quy tắc về khả năng truy nhập của người dùng xác định khả năng truy nhập của người dùng tới các tài liệu theo cấp tài liệu đã gán. Như được thể hiện trên Fig.5, tệp quy tắc có thể còn chứa các biểu thức chính quy và các từ khoá. Bước này có thể được thực hiện khi việc tạo ra và/hoặc các thay đổi của tệp tài liệu điện tử được giám sát trong thiết bị khách hàng, hoặc còn có thể được thực hiện thường xuyên vô điều kiện.

Bộ phận tìm kiếm 230 trong thiết bị khách hàng có thể tìm kiếm một dữ liệu văn bản từ tệp tài liệu điện tử được giám sát (bước S306) và tìm kiếm các từ liên quan tới thông tin kinh doanh từ dữ liệu văn bản tìm được (bước S308). Bộ phận xác định cấp 240 trong thiết bị khách hàng có thể tính toán số lần mà các từ liên quan tới thông tin kinh doanh được tìm kiếm và tính toán điểm số bộc lộ của tệp tài liệu điện tử dựa trên số lần tìm được đối với các từ liên quan tới thông tin kinh doanh và thông tin thiết lập cấp tài liệu có trong tệp quy tắc (bước S310).

Bộ phận xác định cấp 240 trong thiết bị khách hàng gán một cấp tài liệu liên quan tới khả năng truy nhập của người dùng cho tệp tài liệu điện tử dựa trên quy tắc về khả năng truy nhập của người dùng có trong tệp quy tắc theo điểm số bộc lộ tính toán được (bước S312). Bộ phận tạo dấu mờ 250 trong thiết bị khách hàng thu nhận thông tin cá nhân người dùng của thiết bị khách hàng từ máy chủ, và chèn dấu mờ vào văn bản của tệp tài liệu điện tử cần hiển thị trong thiết bị khách hàng dựa trên thông tin cá nhân người dùng thu nhận được (bước S314). Dấu mờ có thể được chèn bằng cách thực hiện ít nhất một thao tác trong số: điều chỉnh cỡ phông chữ của văn bản và điều chỉnh độ đậm nhạt của phông chữ của văn bản theo thông tin cá nhân người dùng.

Sau đó, bộ phận xử lý an toàn 260 trong thiết bị khách hàng có thể thực hiện thao tác bất kỳ trong số các thao tác: xoá hoàn toàn, cách ly, mã hoá hoặc thông báo tệp tài liệu điện tử có cấp an toàn được xác định và dấu mờ đã được chèn vào đó dựa trên quy tắc về xử lý an toàn đối với từng cấp, và bộ phận tạo ra tệp 270 có thể tạo ra một tệp có phần đầu tệp trong đó thông tin liên quan tới độ an toàn được chèn vào (bước S316).

Fig.4 là lưu đồ thể hiện quy trình dùng chung các tài liệu công ty giữa các thiết bị khách hàng sử dụng máy chủ có khả năng kiểm soát theo cách tích hợp nhiều hệ thống quản lý nhiệm vụ theo một phương án của sáng chế. Trước hết, thiết bị khách hàng thứ nhất có thể tạo ra tệp tài liệu điện tử và tải lên tệp

tài liệu trong cơ sở dữ liệu tài liệu của máy chủ (bước S400).

Sau đó, thiết bị khách hàng thứ hai có thể yêu cầu tải tệp tài liệu điện tử được lưu trữ trong cơ sở dữ liệu tài liệu xuống máy chủ. Trạng thái tải lên từ thiết bị khách hàng thứ nhất và yêu cầu tải xuống của thiết bị khách hàng thứ hai có thể được thực hiện liên tục hoặc không liên tục. Thiết bị khách hàng thứ nhất và thiết bị khách hàng thứ hai có thể là các đầu cuối của cùng người dùng hoặc các đầu cuối của những người dùng khác nhau.

Theo yêu cầu tải xuống của thiết bị khách hàng thứ hai, máy chủ thu nhận yêu cầu tải xuống tệp tài liệu điện tử từ thiết bị khách hàng thứ hai (bước S410), và vì thế, xác minh thông tin đăng nhập của người dùng của thiết bị khách hàng thứ hai trong bộ phận xác minh thông tin đăng nhập 128 trong máy chủ dựa trên sơ đồ tổ chức và thông tin của người dùng được lưu trữ trong cơ sở dữ liệu nhân sự (bước S420). Tiếp theo, máy chủ truyền tệp tài liệu điện tử mà thiết bị khách hàng thứ hai yêu cầu tải xuống từ cơ sở dữ liệu tài liệu tới bộ phận mã hoá 126, mã hóa tài liệu trong bộ phận mã hoá và tạo ra tệp tài liệu điện tử đã mã hóa (bước S430).

Máy chủ truyền tệp tài liệu điện tử đã mã hóa tới thiết bị khách hàng thứ hai, và do đó, thiết bị khách hàng thứ hai tải xuống tệp tài liệu điện tử đã mã hóa (bước S440). Theo quy trình như nêu trên liên quan tới Fig.3, nếu việc tạo ra và các thay đổi của tệp tài liệu điện tử được phát hiện trong thiết bị khách hàng thứ hai nhờ trạng thái tải xuống tệp tài liệu điện tử này từ máy chủ, thiết bị khách hàng thứ hai tìm kiếm một dữ liệu văn bản từ tệp tài liệu điện tử, tìm kiếm các từ liên quan tới thông tin kinh doanh từ dữ liệu văn bản tìm được, tính toán điểm số bộc lộ, gán một cấp tài liệu dựa trên thông tin thiết lập cấp tài liệu có trong tệp quy tắc nhận được từ máy chủ, và chèn một dấu mờ dựa trên thông tin cá nhân người dùng (bước S450). Sau đó, dựa trên tài liệu khả năng truy nhập theo cấp an toàn của tệp tài liệu tương ứng điện tử của người dùng của thiết bị khách hàng thứ hai, tệp tài liệu điện tử trong đó dấu mờ đã

được chèn được hiển thị trong thiết bị khách hàng thứ hai (bước S460).

Như được thể hiện trên Fig.4, quy trình dùng chung các tài liệu công ty giữa các thiết bị khách hàng theo sáng chế không thực hiện xử lý an toàn trong máy chủ, nghĩa là khác với các giải pháp kỹ thuật đã biết, và tạo ra biện pháp đảm bảo an toàn trước bằng cách tìm kiếm nội dung và thiết lập cấp trong chính đầu cuối của người dùng và biện pháp đảm bảo an toàn sau bằng cách chèn một dấu mờ văn bản để cho phép hệ thống an toàn hiệu quả hơn và chắc chắn hơn phù hợp với các thay đổi của môi trường thực hiện nhiệm vụ di động.

Fig.5 thể hiện tệp quy tắc được quản lý trong máy chủ và được truyền từ máy chủ tới thiết bị khách hàng theo một phương án của sáng chế. Tệp quy tắc 500 chứa các biểu thức chính quy 510, các từ khoá 520, quy tắc về an toàn 530 và thông tin thiết lập cấp tài liệu 540. Theo phương án này của sáng chế, tệp quy tắc 500 có thể được cập nhật thường xuyên nhờ máy chủ.

Các biểu thức chính quy 510 biểu thị tất cả thông tin có thể thu được bằng cách nhận dạng hoặc suy ra từ thông tin kinh doanh ở dạng biểu thức chính quy. Các biểu thức chính quy được làm thích ứng cho việc tìm kiếm và thế các chuỗi ký tự trong các bộ soạn thảo văn bản và các ngôn ngữ lập trình khác nhau. Các từ khoá 520 xác định các từ liên quan tới thông tin kinh doanh, và có thể có các cụm từ: "thông tin mật, trạng thái bảo vệ thông tin, công bố hạn chế, thông tin tối mật, thông tin mật cấp hai, thông tin đặc quyền", v.v..

Quy tắc về xử lý an toàn 530 nghĩa là quy tắc nội bộ được thiết lập trước của công ty mà theo đó loại đảm bảo an toàn áp dụng cho các tài liệu theo các cấp nhất định. Thông tin thiết lập cấp tài liệu 540 có thể bao gồm quy tắc thiết lập cấp tệp 541 và quy tắc về khả năng truy nhập của người dùng 542. Thông tin thiết lập cấp tài liệu có thể có thông tin liên quan tới việc thiết lập cấp của các tài liệu kinh doanh, chẳng hạn thông tin về hệ số quan trọng trong

đó các từ liên quan tới thông tin kinh doanh được xếp hạng để thiết lập cấp của các tài liệu kinh doanh, thông tin của giai đoạn đọc theo từng cấp của tài liệu, v.v..

Fig.6 thể hiện một ví dụ về các tệp quy tắc có thể được sử dụng theo sáng chế. Fig.6 (a) thể hiện thông tin về hệ số quan trọng đối với từng từ liên quan tới thông tin kinh doanh. Ví dụ, các từ: "năm vào công ty" có hệ số quan trọng là 1 điểm, và các từ: "số đăng ký chính thức của ban lãnh đạo và nhân viên" có hệ số quan trọng là 5 điểm.

Fig.6 (b) thể hiện cấp người dùng theo vị trí trong công ty. Ví dụ, người dùng của thiết bị khách hàng có vị trí làm việc chỉ là nhân viên có cấp người dùng là '5'; người dùng là trợ lý bộ phận có cấp người dùng là '4'; người dùng là trưởng bộ phận có cấp người dùng là '3'; người dùng là trưởng nhóm hoặc phó phòng có cấp người dùng là '2'; người dùng là lãnh đạo công ty có cấp người dùng là '1'. Nói chung, cấp người dùng càng cao thì khả năng truy nhập của người dùng tới các tài liệu càng rộng.

Fig.7 thể hiện chi tiết hơn bộ phận tìm kiếm 230 có thể có trong bộ phận tìm kiếm trong thiết bị khách hàng theo một phương án của sáng chế. Bộ phận tìm kiếm 230 có thể bao gồm bộ phận giao diện 710, bộ phận lọc 730 và bộ phận phát hiện 750. Bộ phận giao diện 710 thu nhận lệnh để phát hiện các tài liệu từ bộ điều khiển 201, và thu nhận tệp tài liệu điện tử không được mã hoá hoặc đã giải mã để phát hiện từ bộ phát hiện tệp mã hoá/không mã hoá 220.

Bộ phận lọc 730 bao gồm một vài bộ lọc thực hiện chức năng tìm kiếm riêng các văn bản đối với một tài liệu điện tử nhất định để tìm kiếm thông tin văn bản có trong các tài liệu điện tử khác nhau. Bộ phận lọc 730 thực hiện việc phát hiện khuôn tài liệu, xác minh lỗi tài liệu, tìm kiếm thông tin tài liệu, và tìm kiếm văn bản. Cụ thể hơn, bộ phận lọc 730 có thể bao gồm bộ lọc văn bản tệp thông thường 732, bộ lọc văn bản nhớ 734, bộ lọc khuôn tệp 736, bộ lọc tệp nén 738, và bộ lọc trang nhất định 740.

Bộ lọc văn bản tệp thông thường 732 duyệt thông tin của một tệp nhất định và tìm kiếm văn bản của tệp tương ứng. Bộ lọc văn bản nhớ 734 duyệt thông tin địa chỉ của một bộ nhớ nhất định trong đó dữ liệu được lưu trữ và tìm kiếm văn bản của bộ nhớ tương ứng. Bộ lọc khuôn tệp 736 phát hiện xem phần mở rộng của tệp tương ứng cần tìm kiếm có bị giả mạo hay không. Bộ lọc tệp nén 738 có thể chỉ tìm kiếm thông tin tệp (tên tệp, thông tin khuôn tệp, v.v.) trong tệp nén tương ứng trong trường hợp tệp nén này cần được tìm kiếm, hoặc lọc duy nhất một tệp nhất định. Bộ lọc trang nhất định 740 thực hiện lọc riêng thông tin văn bản đối với các trang nhất định trong toàn bộ tệp.

Thông tin văn bản được tìm kiếm từ bộ phận lọc 730 được cấp tới bộ phận phát hiện 750, và bộ phận phát hiện 750 so sánh thông tin văn bản được tìm kiếm với các biểu thức chính quy và các từ khoá về thông tin kinh doanh có trong tệp quy tắc nhận được từ máy chủ để phát hiện xem các từ liên quan tới thông tin kinh doanh có chứa trong tệp tài liệu tương ứng hay không. Bộ phận phát hiện 750 có thể tải tệp quy tắc chứa các biểu thức chính quy và các từ khoá nhận được từ máy chủ nhờ bộ điều khiển 201 hoặc lưu trữ tệp quy tắc tải được trong một bộ nhớ riêng biệt.

Fig.8 thể hiện chi tiết hơn bộ phận xác định cấp 240 có thể có trong bộ phận đảm bảo an toàn tài liệu trong thiết bị khách hàng theo một phương án của sáng chế. Bộ phận xác định cấp 240 này có thể bao gồm bộ phận giao diện 810, bộ phận đếm 820, bộ phận tính toán số điểm 830 và bộ phận gán cấp 840.

Bộ phận giao diện 810 thu nhận các kết quả phát hiện thông tin văn bản từ bộ phận phát hiện 750 trong bộ phận tìm kiếm 230 cùng với lệnh khởi hoạt việc phát hiện cấp. Bộ phận đếm 820 đếm số lần mà các từ liên quan tới thông tin kinh doanh được tìm kiếm từ bộ phận phát hiện. Bộ phận tính toán số điểm 830 tính toán điểm số bộc lộ của thông tin kinh doanh nhờ công thức sau: tổng của (số lần mà các từ liên quan tới thông tin kinh doanh được tìm kiếm nhân với hệ số quan trọng đối với thông tin kinh doanh) = điểm số bộc lộ. Ví dụ,

nếu giả sử cụm từ "số đăng ký chính thức" được tìm thấy hai lần và cụm từ "năm vào công ty" được tìm thấy một lần từ văn bản, dựa vào hệ số quan trọng của từng từ được thể hiện trên Fig.6 (a), có thể hiểu rằng "số đăng ký chính thức" có hệ số quan trọng là 5, và "năm vào công ty" có hệ số quan trọng là 1. Như vậy, trong trường hợp này, điểm số bộc lộ của tài liệu tương ứng là 5 x 2 (hệ số quan trọng của "số đăng ký chính thức" nhân với số lần được tìm kiếm) + 1 x 1 (hệ số quan trọng của "năm vào công ty" nhân với số lần được tìm kiếm) = 11 theo công thức nêu trên.

Bộ phận gán cấp 840 gán cấp cho tài liệu dựa trên điểm số bộc lộ tính toán được trong bộ phận tính toán số điểm, vì thế khả năng truy nhập của người dùng đối với từng tài liệu có thể được kiểm soát theo thông tin thiết lập cấp tài liệu có trong tệp quy tắc. Theo khía cạnh này, Fig.6 (c) thể hiện một phương án của quy tắc về cấp tài liệu gán cấp cho tài liệu theo điểm số bộc lộ. Theo phương án này, ví dụ, trong trường hợp điểm số bộc lộ nằm trong khoảng từ 0 tới 5, tài liệu được gán cấp 5; trong trường hợp điểm số bộc lộ nằm trong khoảng từ 6 tới 9, tài liệu được gán cấp 4; trong trường hợp điểm số bộc lộ nằm trong khoảng từ 10 tới 14, tài liệu được gán cấp 3; trong trường hợp điểm số bộc lộ nằm trong khoảng từ 15 tới 19, tài liệu được gán cấp 2; và trong trường hợp điểm số bộc lộ lớn hơn hoặc bằng 20, tài liệu được gán cấp 1. Như đã giải thích trên đây, tệp quy tắc nhận được từ máy chủ còn có quy tắc về khả năng truy nhập của người dùng. Theo Fig.6 (c), ví dụ, trong trường hợp một tài liệu được gán cấp 1, nếu cấp người dùng của thiết bị khách hàng là cấp 1 hoặc cao hơn, người dùng có thể có khả năng truy nhập tài liệu bao gồm các thao tác: đọc, lưu trữ, in, và hiệu chỉnh tài liệu. Theo phương án này, trong trường hợp một tài liệu được gán cấp 1, người dùng có cấp khác cấp 1 không thể đọc, lưu trữ, in và hiệu chỉnh tài liệu. Hơn nữa, theo phương án này, trong trường hợp một tài liệu được gán cấp 2; người dùng có cấp là cấp 2 hoặc cao hơn có thể đọc, lưu trữ, in và hiệu chỉnh tài liệu; người dùng có cấp là cấp 3

có thể đọc và in tài liệu nhưng không thể lưu trữ và hiệu chỉnh tài liệu; người dùng có cấp là cấp 4 chỉ có thể đọc tài liệu; và người dùng có cấp là cấp 5 không thể được phép thực hiện thao tác bất kỳ trong số: đọc, lưu trữ, in và hiệu chỉnh tài liệu. Khả năng truy nhập của người dùng theo cấp của người này có thể được thay đổi và được cập nhật tới máy chủ bất kỳ lúc nào theo quy tắc về an toàn của công ty.

Fig.9 thể hiện một phương án chèn dấu mờ vào tài liệu văn bản trong bộ phận tạo dấu mờ có thể có trong bộ phận đảm bảo an toàn tài liệu trong thiết bị khách hàng theo một phương án của sáng chế. Fig.9 (a) và Fig.9 (b) thể hiện phương pháp chèn dấu mờ theo cách sao cho cỡ phông chữ của một văn bản nhất định bị thu nhỏ. Văn bản trong đó dấu mờ đã được chèn được thể hiện trên Fig.9 (a). Giả sử tài liệu tương ứng có cỡ phông chữ cơ bản là 12 pt, và người dùng của tài liệu có khoá người dùng là "10011". Theo phương án này, từng dòng văn bản của văn bản được thể hiện trên Fig.9 (a) có thể lần lượt tương ứng với từng giá trị bit của khoá người dùng. Do đó, dòng thứ nhất trong văn bản tương ứng với bit thứ nhất của khoá người dùng là “1”; dòng thứ hai trong văn bản tương ứng với bit thứ hai của khoá người dùng là “0”; dòng thứ ba trong văn bản tương ứng với bit thứ ba của khoá người dùng là “0”; dòng thứ tư trong văn bản tương ứng với bit thứ tư của khoá người dùng là “1”; và dòng thứ năm trong văn bản tương ứng với bit thứ năm của khoá người dùng là “1”. Tiếp đó, bộ phận tạo dấu mờ 250 có thể thu nhỏ hoặc phóng to cỡ phông chữ của văn bản trong từng dòng lớn bằng kích thước xác định. Ví dụ, các văn bản được gán bit “1” có thể được thu nhỏ bằng 1 pt. Cụ thể hơn, như được thể hiện trên Fig.9 (b), văn bản trong các dòng thứ nhất, thứ tư và thứ năm tương ứng với bit “1” có thể được điều chỉnh sao cho có cỡ phông chữ là 11 pt, nghĩa là được giảm bớt 1 pt so với cỡ phông chữ cơ bản. Trong trường hợp này, cỡ phông chữ của dòng thứ hai và dòng thứ ba, tương ứng với bit “0”, sẽ được duy trì là 12 pt. Trong trường hợp số bit của khoá

người dùng được cố định bằng 5 bit, nếu giá trị khoá người dùng được áp dụng lặp lại trong một nhóm bao gồm 5 dòng một tính từ dòng thứ nhất của văn bản, khoảng cách giữa các dòng văn bản bao gồm 5 dòng một được điều chỉnh. Trong trường hợp này, một dấu mờ có thể được dễ dàng phát hiện sau đó. Cùng lúc này, kích thước văn bản có thể được thu nhỏ hoặc được mở rộng ở giá trị bit "1" hoặc "0", nhưng nói chung việc thu nhỏ cỡ phông chữ được ưu tiên để tránh vấn đề tràn bộ nhớ hệ thống.

Tiếp theo, Fig.9 (c) và Fig.9 (d) thể hiện phương pháp chèn dấu mờ bằng cách thay đổi độ đậm nhạt của phông chữ của một văn bản nhất định. Văn bản trong đó một dấu mờ được chèn vào được thể hiện trên Fig.9 (c). Theo một phương án của sáng chế, các phụ âm hoặc các nguyên âm được dùng nhiều nhất trong văn bản được phát hiện, các bit của khoá người dùng lần lượt được tạo ra lặp lại tương ứng với các văn bản có các phụ âm hoặc các nguyên âm này, và độ đậm nhạt của phông chữ được thay đổi sao cho mảnh hơn hoặc dày hơn bằng cách thay đổi đường bao của các văn bản. Việc xử lý đường bao phông chữ làm thay đổi độ đậm nhạt của phông chữ theo khoá người dùng có thể được thực hiện trong toàn bộ văn bản. Ví dụ, nếu giả sử khoá người dùng là "10011" và phụ âm được phát hiện nhiều nhất là 'ㄱ', 1, 0, 0, 1, 1 có thể tương ứng với "가", "각", "각," 과", và "과" có phụ âm 'ㄱ', theo thứ tự, như được thể hiện trên Fig.9 (d), và độ đậm nhạt của phông chữ của văn bản tương ứng với bit "1" có thể được điều chỉnh sao cho mảnh hơn hoặc dày hơn. Nếu tài liệu trong đó một dấu mờ được chèn theo cách sao cho bị làm lộ bởi thao tác in hoặc chụp ảnh của một bên thứ ba, giá trị khoá người dùng có thể được dò lại với riêng độ đậm nhạt của phông chữ. Như vậy, có thể dễ dàng dò ra đường dẫn làm lộ bí mật, và nhờ đó biện pháp đảm bảo an toàn sau được tăng cường.

Máy chủ có khả năng kiểm soát theo cách tích hợp nhiều hệ thống quản lý nhiệm vụ trong hệ thống quản lý tài liệu tích hợp theo sáng chế tích hợp hệ

thống kiểm soát quản lý tích hợp (IMCS) với bộ điều khiển tích hợp để cho phép tạo ra cơ sở dữ liệu nhân sự tích hợp, v.v. đối với các hệ thống quản lý nhiệm vụ. Như vậy, sáng chế cho phép giảm bớt đáng kể chi phí bổ sung cần thiết cho việc xây dựng và tích hợp hệ thống khi xây dựng bổ sung các hệ thống quản lý nhiệm vụ dạng số và các hệ thống an toàn khác nhau. Hơn nữa, sáng chế có thể ngăn chặn lãng phí thời gian dùng cho việc tìm kiếm thông tin cá nhân người dùng và thông tin tổ chức được thực hiện lặp lại mỗi khi người dùng truy nhập máy chủ, và cải thiện hiệu quả trong việc xử lý nhiệm vụ vì các hệ thống quản lý nhiệm vụ khác nhau được sử dụng trên cơ sở dữ liệu nhân sự trong máy chủ. Ngoài ra, sáng chế có thể giải quyết vấn đề về độ an toàn có thể gặp phải do sự không nhất quán trong thông tin do dữ liệu lặp lại, và có thể dễ dàng tích hợp các hệ thống thực hiện nhiệm vụ khác nhau khác và tạo ra môi trường thực hiện nhiệm vụ nhất quán.

Ngoài ra, khi xử lý một tệp tài liệu điện tử có thông tin kinh doanh trong thiết bị khách hàng, sáng chế cho phép tìm kiếm xem các tài liệu điện tử có trong công ty có chứa thông tin kinh doanh mật hay không, tính toán điểm số bộc lộ dựa trên mức độ bộc lộ để xác định cấp an toàn của tài liệu tương ứng, và kiểm soát khả năng truy nhập của người dùng đối với từng cấp tài liệu, nghĩa là giải quyết các vấn đề mà phương pháp DRM và phương pháp DLP theo kỹ thuật đã biết gặp phải, để cho phép kiểm soát khả năng truy nhập tới các tài liệu đối với từng người dùng, và áp dụng quy tắc về an toàn thích hợp cho từng tài liệu nhằm tạo ra biện pháp đảm bảo an toàn trước được tăng cường để ngăn chặn từ sớm sự rò rỉ của thông tin kinh doanh ra bên ngoài.

Ngoài ra, sáng chế còn cho phép chèn một dấu mờ vào tài liệu tương ứng dựa trên một giá trị đặc biệt có thể phân biệt từng người dùng để tạo ra dấu hiệu phân biệt cho tài liệu cần hiển thị, và nhờ đó cho phép dò ra đường dẫn rò rỉ nếu tài liệu tương ứng bị làm lộ bởi hành vi chụp ảnh, v.v., của một bên thứ ba. Như vậy, sáng chế cho phép tạo ra biện pháp đảm bảo an toàn sau

cho công ty nhằm đối phó với sự phát triển của các vi thiết bị khác nhau.

Ngoài ra, sáng chế cho phép thiết bị khách hàng, chứ không phải máy chủ, có thể tạo ra một tệp tài liệu điện tử trong đó an toàn kinh doanh được tăng cường để cho phép tạo ra độ an toàn thông tin kinh doanh hiệu quả và chắc chắn hơn nhằm đối phó với việc sử dụng các vi thiết bị và việc mở rộng của môi trường thực hiện nhiệm vụ di động.

Mặc dù sáng chế đã được mô tả chi tiết liên quan tới các phương án ưu tiên của nó, người có hiểu biết trung bình trong lĩnh vực kỹ thuật này cần phải hiểu rằng các thay đổi khác nhau có thể được thực hiện mà không nằm ngoài phạm vi của sáng chế.

YÊU CẦU BẢO HỘ

1. Hệ thống quản lý tài liệu tích hợp bao gồm máy chủ và thiết bị khách hàng, máy chủ bao gồm:

các hệ thống quản lý nhiệm vụ được thiết lập bởi các nhà cung cấp khác nhau;

cơ sở dữ liệu tài liệu để lưu trữ các tài liệu điện tử có thông tin kinh doanh;

cơ sở dữ liệu nhân sự để lưu trữ sơ đồ tổ chức và thông tin người dùng;

cơ sở dữ liệu quy tắc để lưu trữ tệp quy tắc liên quan tới quy tắc về an toàn thông tin kinh doanh, tệp quy tắc này có thông tin thiết lập cấp tài liệu và quy tắc an toàn; và

bộ điều khiển tích hợp được nối với các hệ thống quản lý nhiệm vụ,

trong đó các hệ thống quản lý nhiệm vụ dùng chung cơ sở dữ liệu nhân sự và cơ sở dữ liệu quy tắc bằng cách sử dụng bộ điều khiển tích hợp,

bộ điều khiển tích hợp bao gồm:

bộ phận quy tắc máy chủ được nối với cơ sở dữ liệu quy tắc và bao gồm bộ phận quản lý quy tắc để quản lý tệp quy tắc được lưu trữ trong cơ sở dữ liệu quy tắc và bộ phận truyền quy tắc để truyền tệp quy tắc tới thiết bị khách hàng; và

bộ phận quản lý an toàn bao gồm bộ phận xác minh thông tin đăng nhập để xác minh thông tin đăng nhập của người dùng bằng cách so sánh với thông tin người dùng được lưu trữ trong cơ sở dữ liệu nhân sự, bộ phận mã hoá để mã hoá tệp tài liệu điện tử cần truyền từ cơ sở dữ liệu tài liệu tới thiết bị khách hàng, và bộ phận quản lý thông tin nhật ký để quản lý thông tin nhật ký nhận được từ thiết bị khách hàng, và

thiết bị khách hàng bao gồm:

bộ phận giám sát để giám sát việc tạo ra tệp tài liệu điện tử và các thay đổi trên tệp tài liệu điện tử này;

bộ điều khiển để thu nhận tệp quy tắc từ cơ sở dữ liệu quy tắc trong máy chủ;

bộ phận đảm bảo an toàn tài liệu để thực hiện xử lý an toàn đối với tài liệu điện tử được làm thích ứng để:

tìm kiếm một dữ liệu văn bản từ tệp tài liệu điện tử;

tìm kiếm các từ liên quan tới thông tin kinh doanh từ dữ liệu văn bản tìm được, trong đó thông tin thiết lập cấp tài liệu của tệp quy tắc được lưu trữ trong cơ sở dữ liệu quy tắc chứa hệ số quan trọng của từng từ liên quan tới thông tin kinh doanh;

đối với từng từ, đếm số lần mà từ liên quan tới thông tin kinh doanh được sử dụng trong tệp tài liệu điện tử;

tính toán điểm số bộc lộ của tệp tài liệu điện tử dựa trên các từ được tìm kiếm liên quan tới thông tin kinh doanh, trong đó điểm số bộc lộ là tổng của tích, đối với từng từ liên quan tới thông tin kinh doanh, giữa số lần đếm được mà từ liên quan tới thông tin kinh doanh được tìm kiếm nhân với hệ số quan trọng của từ;

dựa trên điểm số bộc lộ tính toán được, tự động gán một cấp tài liệu cho tệp tài liệu điện tử theo thông tin thiết lập cấp tài liệu, trong đó khả năng truy nhập của người dùng đối với cấp tài liệu được xác định trong thông tin thiết lập cấp tài liệu của cơ sở dữ liệu quy tắc trong máy chủ;

chèn một dấu mờ vào văn bản của tệp tài liệu điện tử cần hiển thị trên thiết bị khách hàng dựa trên khóa người dùng tương ứng với thông tin cá nhân người dùng của người dùng của thiết bị khách hàng và nhận được từ máy chủ, trong đó việc chèn dấu mờ được thực hiện bằng cách

thay đổi cỡ phông chữ hoặc độ dày phông chữ của văn bản theo khóa người dùng; và

thực hiện xử lý an toàn đối với tệp tài liệu điện tử mà dấu mờ đã được chèn vào theo quy tắc về an toàn, việc xử lý an toàn này là thực hiện một trong số các thao tác: xóa, cách ly, mã hoá và thông báo; và

bộ phận lưu trữ tài liệu để tải lên tệp tài liệu điện tử được tạo ra trong bộ phận đảm bảo an toàn tài liệu hoặc tải xuống tệp tài liệu điện tử đã mã hóa từ bộ phận mã hoá.

2. Hệ thống theo điểm 1, trong đó các hệ thống quản lý nhiệm vụ bao gồm ít nhất một trong số: hệ thống quản lý tài liệu điện tử (EDMS), phần mềm làm việc nhóm (GW), hệ thống quản lý quy trình kinh doanh (BPM), hệ thống hoạch định tài nguyên doanh nghiệp (ERP) và hệ thống thư điện tử.

Fig.1

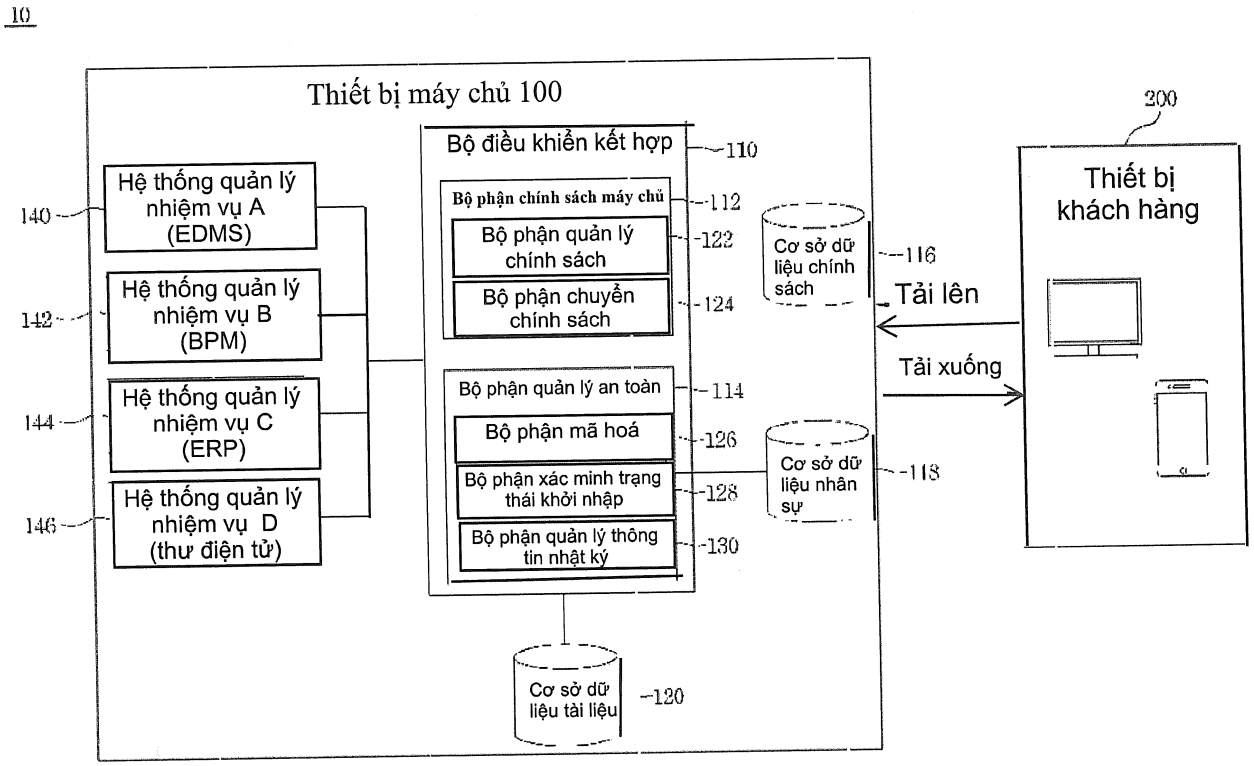

10
Thiết bị máy chủ 100
Bộ điều khiển kết hợp
110
Bộ phận chính sách máy chủ
112
Bộ phận quản lý chính sách
122
Bộ phận chuyển chính sách
124
Bộ phận quản lý an toàn
114
Bộ phận mã hoá
126
Bộ phận xác minh trạng thái khởi nhập
128
Bộ phận quản lý thông tin nhật ký
130
Hệ thống quản lý nhiệm vụ A (EDMS)
140
Hệ thống quản lý nhiệm vụ B (BPM)
142
Hệ thống quản lý nhiệm vụ C (ERP)
144
Hệ thống quản lý nhiệm vụ D (thư điện tử)
146
Cơ sở dữ liệu chính sách
116
Cơ sở dữ liệu nhân sự
118
Cơ sở dữ liệu tài liệu
120
Tải lên
Tải xuống
200
Thiết bị khách hàng

Fig.2

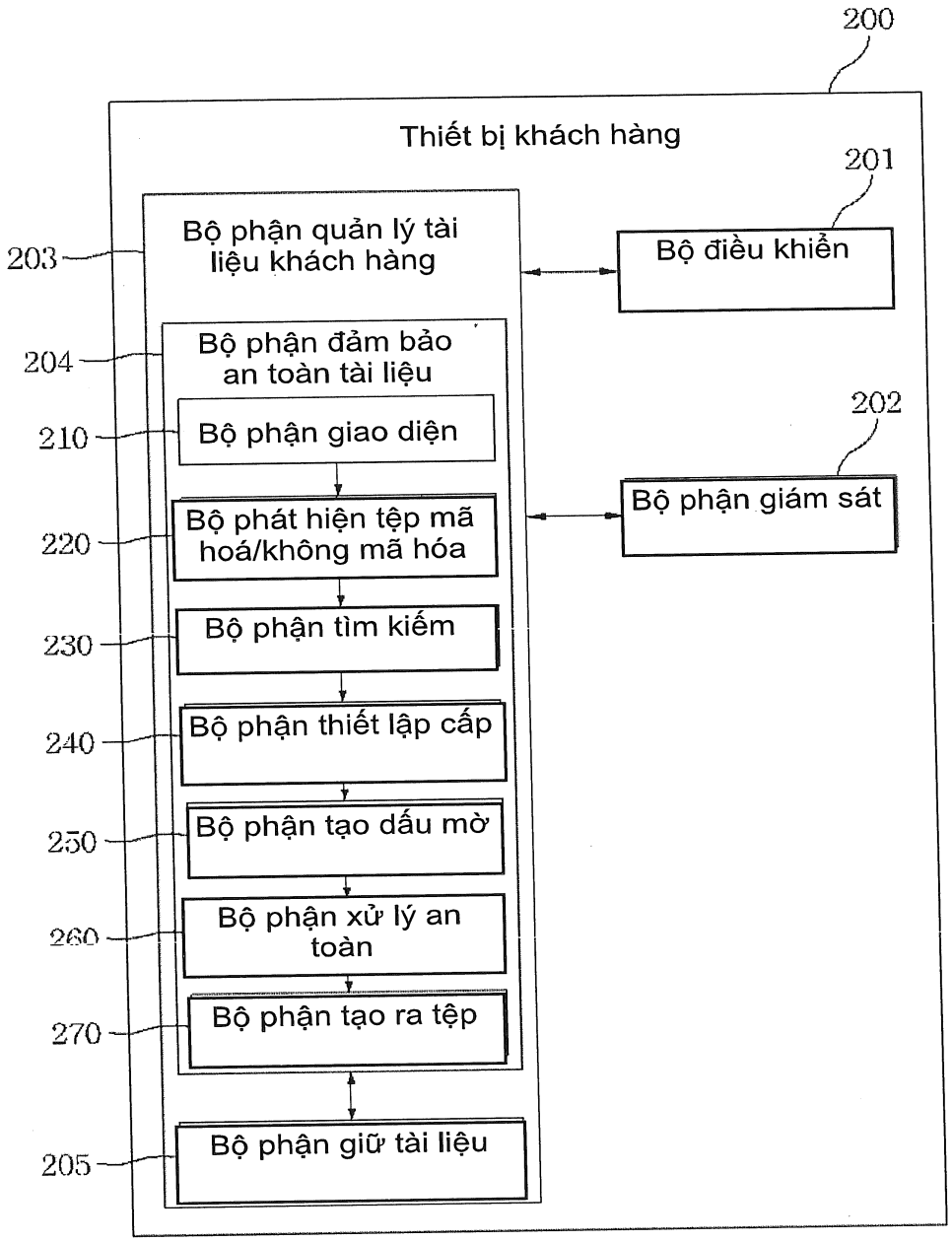

200
Thiết bị khách hàng
201
Bộ điều khiển
203
Bộ phận quản lý tài liệu khách hàng
204
Bộ phận đảm bảo an toàn tài liệu
210
Bộ phận giao diện
202
Bộ phận giám sát
220
Bộ phát hiện tệp mã hoá/không mã hóa
230
Bộ phận tìm kiếm
240
Bộ phận thiết lập cấp
250
Bộ phận tạo dấu mờ
260
Bộ phận xử lý an toàn
270
Bộ phận tạo ra tệp
205
Bộ phận giữ tài liệu

Fig.3

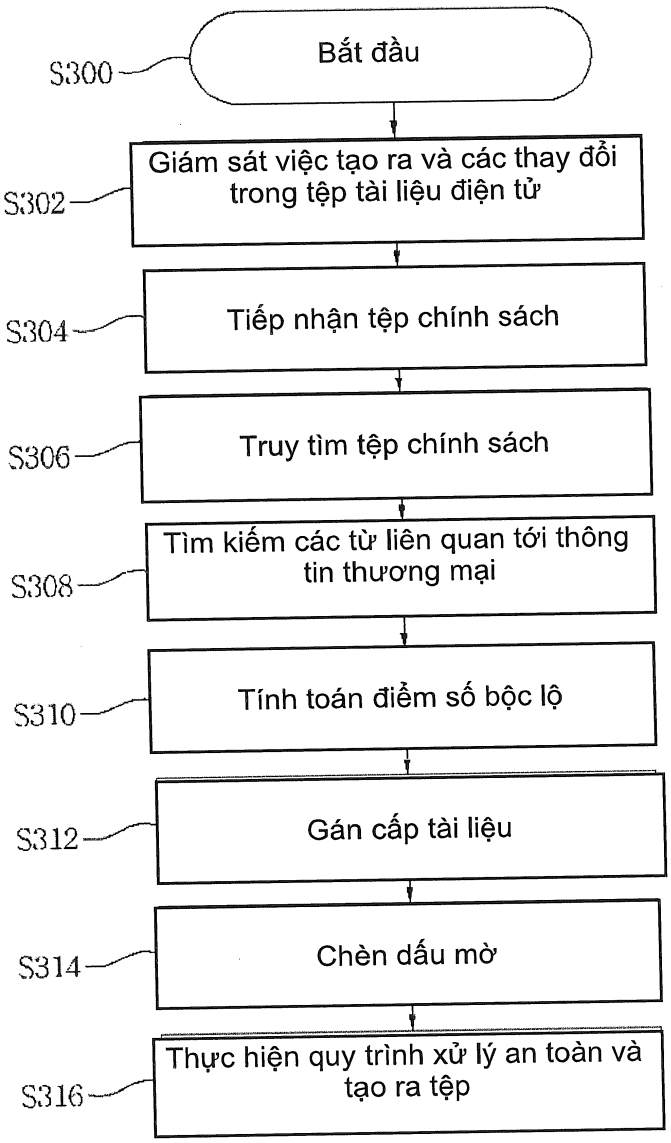

S300
Bắt đầu
S302
Giám sát việc tạo ra và các thay đổi trong tệp tài liệu điện tử
S304
Tiếp nhận tệp chính sách
S306
Truy tìm tệp chính sách
S308
Tìm kiếm các từ liên quan tới thông tin thương mại
S310
Tính toán điểm số bộc lộ
S312
Gán cấp tài liệu
S314
Chèn dấu mờ
S316
Thực hiện quy trình xử lý an toàn và tạo ra tệp

Fig.4

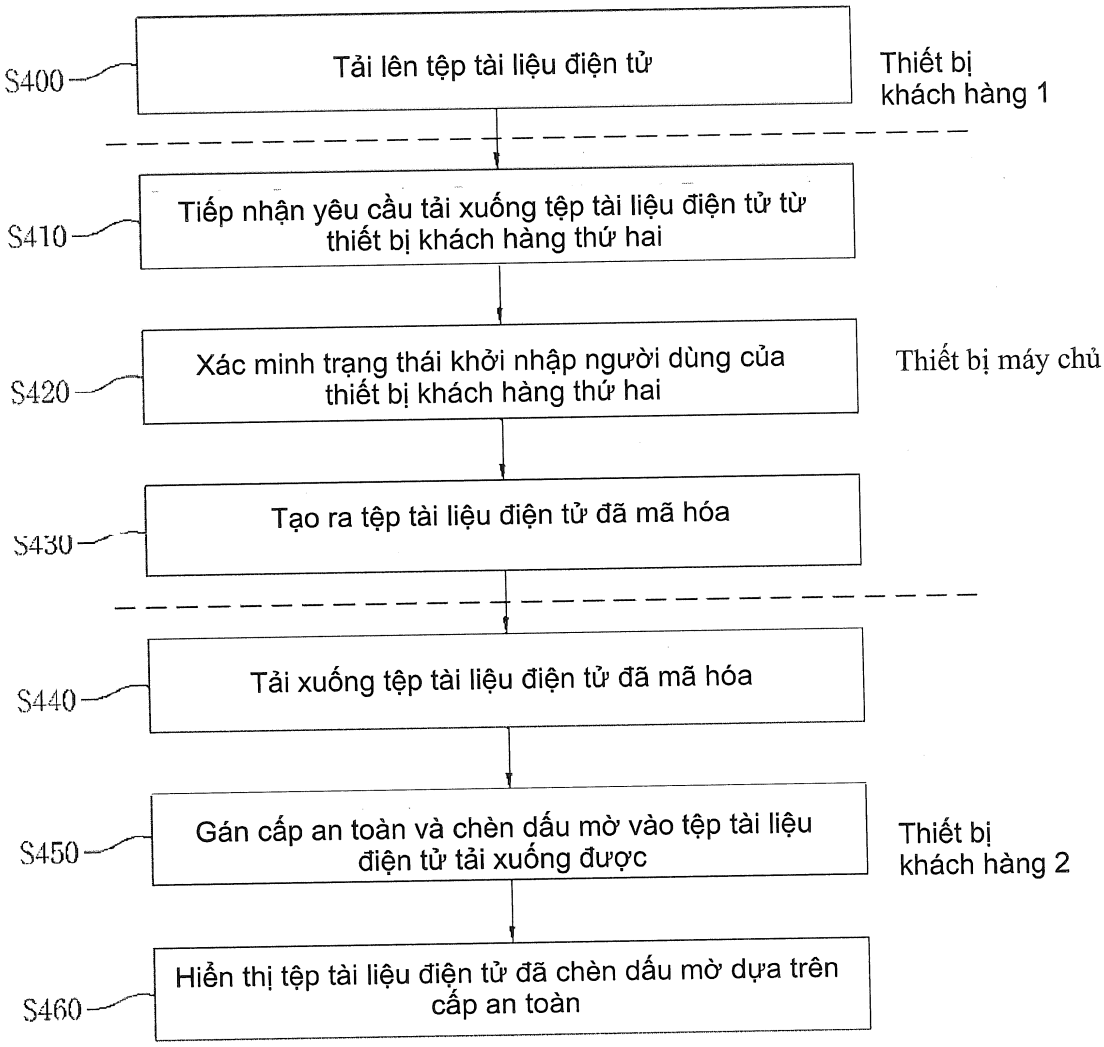

S400
Tải lên tệp tài liệu điện tử
Thiết bị khách hàng 1
S410
Tiếp nhận yêu cầu tải xuống tệp tài liệu điện tử từ thiết bị khách hàng thứ hai
S420
Xác minh trạng thái khởi nhập người dùng của thiết bị khách hàng thứ hai
Thiết bị máy chủ
S430
Tạo ra tệp tài liệu điện tử đã mã hóa
S440
Tải xuống tệp tài liệu điện tử đã mã hóa
S450
Gán cấp an toàn và chèn dấu mờ vào tệp tài liệu điện tử tải xuống được
Thiết bị khách hàng 2
S460
Hiển thị tệp tài liệu điện tử đã chèn dấu mờ dựa trên cấp an toàn

Fig.5

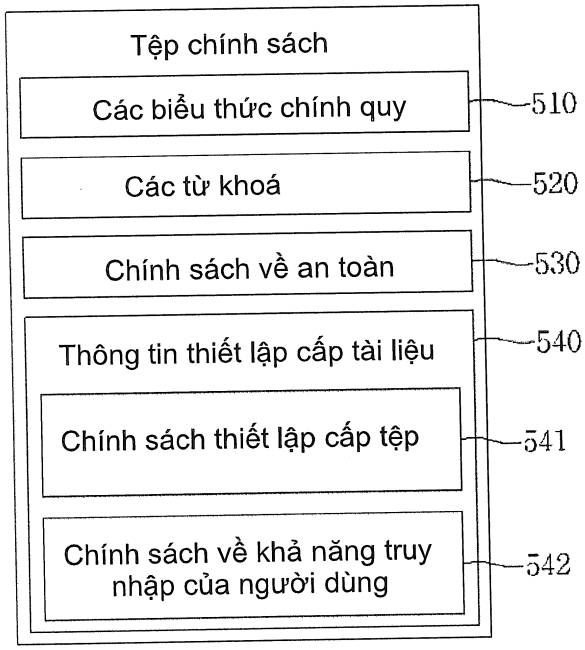

Tệp chính sách
Các biểu thức chính quy
510
Các từ khoá
520
Chính sách về an toàn
530
Thông tin thiết lập cấp tài liệu
540
Chính sách thiết lập cấp tệp
541
Chính sách về khả năng truy nhập của người dùng
542

Fig.6

Hệ số quan trọng	Các từ
1	"năm vào công ty"...
2	
3	.....
4	.....
5	"số ID của ban lãnh đạo và nhân viên"

(a)

Cấp người dùng	Vị trí làm việc
1	Ban lãnh đạo
2	Trưởng nhóm hoặc phó phòng
3	
4	Trưởng bộ phận
5	Nhân viên

(b)

Điểm số bộc lộ	Cấp	Khả năng truy nhập
Lớn hơn hoặc bằng 20	1	Cấp người dùng 1 hoặc thấp hơn: đọc (0), lưu (0), in (0), soạn thảo (0) Cấp người dùng 2: đọc (X), lưu (X), in (X), soạn thảo (X) Cấp người dùng 3: đọc (X), lưu (X), in (X), soạn thảo (X) Cấp người dùng 4: đọc (X), lưu (X), in (X), soạn thảo (X) Cấp người dùng 5: đọc (X), lưu (X), in (X), soạn thảo (X)
15-19	2	Cấp người dùng 2 hoặc thấp hơn: đọc (0), lưu (0), in (0), soạn thảo (0) Cấp người dùng 3: đọc (0), lưu (X), in (0), soạn thảo (X) Cấp người dùng 4: đọc (0), lưu (X), in (X), soạn thảo (X) Cấp người dùng 5: đọc (X), lưu (X), in (X), soạn thảo (X)
10-14	3	Cấp người dùng 3 hoặc thấp hơn: đọc (0), lưu (0), in (0), soạn thảo (0) Cấp người dùng 4: đọc (0), lưu (X), in (0), soạn thảo (0) Cấp người dùng 5: đọc (0), lưu (X), in (0), soạn thảo (X)
6-9	4	Cấp người dùng 4 hoặc thấp hơn: đọc (0), lưu (0), in (0), soạn thảo (0) Cấp người dùng 5: đọc (0), lưu (X), in (0), soạn thảo (0)
0-5	5	Cấp người dùng 5 hoặc thấp hơn: đọc (0), lưu (0), in (0), soạn thảo (0)

(c)

Fig.7

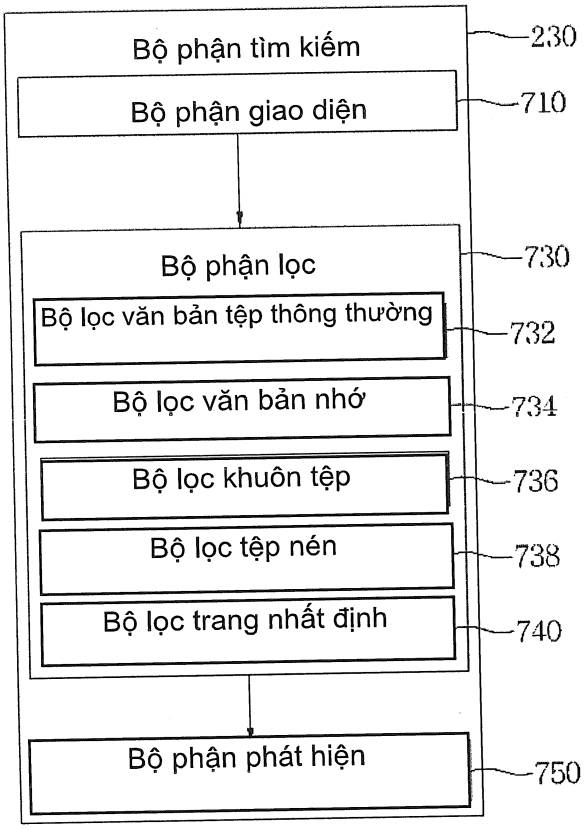

Bộ phận tìm kiếm
230
Bộ phận giao diện
710
Bộ phận lọc
730
Bộ lọc văn bản tệp thông thường
732
Bộ lọc văn bản nhớ
734
Bộ lọc khuôn tệp
736
Bộ lọc tệp nén
738
Bộ lọc trang nhất định
740
Bộ phận phát hiện
750

Fig.8

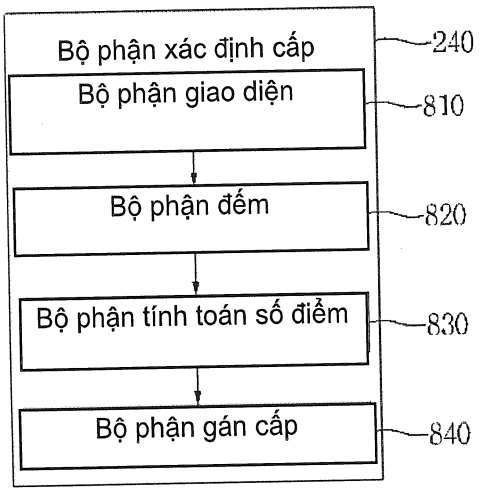
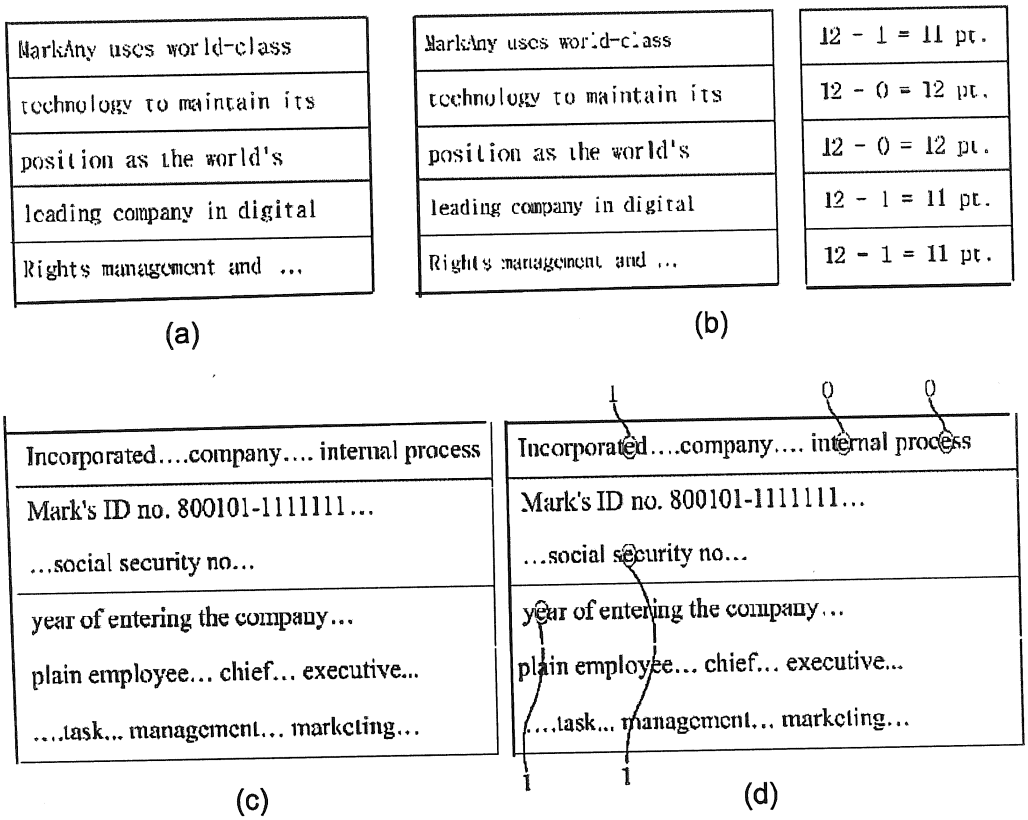

Bộ phận xác định cấp
240
Bộ phận giao diện
810
Bộ phận đếm
820
Bộ phận tính toán số điểm
830
Bộ phận gán cấp
840

Fig.9


MarkAny uses world-class
technology to maintain its
position as the world's
leading company in digital
Rights management and ...
(a)
MarkAny uses world-class
technology to maintain its
position as the world's
leading company in digital
Rights management and ...
12 - 1 = 11 pt.
12 - 0 = 12 pt.
12 - 0 = 12 pt.
12 - 1 = 11 pt.
12 - 1 = 11 pt.
(b)
Incorporated....company.... internal process
Mark's ID no. 800101-1111111...
...social security no...
year of entering the company...
plain employee... chief... executive...
....task... management... marketing...
(c)
1
0
0
Incorporated....company.... internal process
Mark's ID no. 800101-1111111...
...social security no...
year of entering the company...
plain employee... chief... executive...
....task... management... marketing...
1
1
(d)