



(12) BẢN MÔ TẢ SÁNG CHẾ THUỘC BẰNG ĐỘC QUYỀN SÁNG CHẾ

(19) Cộng hòa xã hội chủ nghĩa Việt Nam (VN) (11)
CỤC SỞ HỮU TRÍ TUỆ



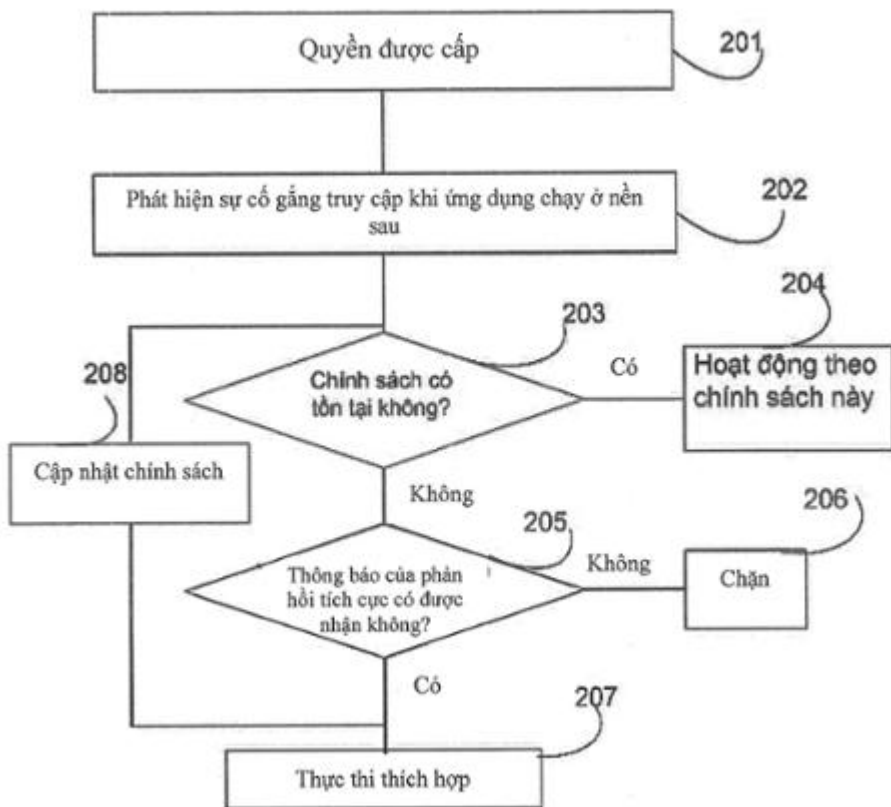
1-0040202

(51)^{2020.01} G06F 21/50; G06F 21/82; G06F 21/62 (13) B

-
- (21) 1-2020-02169 (22) 11/10/2018
(86) PCT/CN2018/109853 11/10/2018 (87) WO 2019/080713 02/05/2019
(30) 15/795,101 26/10/2017 US
(45) 25/06/2024 435 (43) 27/07/2020 388
(73) HUAWEI TECHNOLOGIES CO., LTD. (CN)
Huawei Administration Building, Bantian, Longgang District, Shenzhen, Guangdong
518129, China
(72) HUANG, Paihan (US); CHEN, Maoter (TW); YANG, I-Hsuan (US).
(74) Công ty TNHH Tầm nhìn và Liên danh (VISION & ASSOCIATES CO.LTD.)
-

(54) PHƯƠNG PHÁP QUẢN LÝ VIỆC TRUY CẬP TÀI NGUYÊN PHẦN CỨNG
TRÊN THIẾT BỊ DI ĐỘNG, THIẾT BỊ DI ĐỘNG VÀ VẬT GHI LƯU TRỮ
CHƯƠNG TRÌNH MÁY TÍNH

(57) Sáng chế đề cập đến các phương pháp quản lý việc truy cập tài nguyên phần cứng trên thiết bị di động bao gồm các bước: phát hiện sự cố gắng truy cập tài nguyên phần cứng thứ nhất bởi ứng dụng thứ nhất khi ứng dụng này đang thực thi ở nền sau và xác định rằng không có chính sách dùng cho ứng dụng thứ nhất để truy cập phần cứng thứ nhất, tạo ra thông báo yêu cầu đầu vào người dùng của nó và thêm chính sách mới vào theo đó. Ngoài ra, các phương án đề xuất các thiết bị điện tử di động và vật ghi lưu trữ lưu trữ chương trình máy tính.



Lĩnh vực kỹ thuật được đề cập

Nói chung, sáng chế đề cập đến việc vận hành các thiết bị điện tử, và cụ thể hơn là, phương pháp quản lý việc truy cập tài nguyên phần cứng trên thiết bị di động, thiết bị di động và vật ghi lưu trữ chương trình máy tính.

Tình trạng kỹ thuật của sáng chế

Các thiết bị điện tử di động khả dụng hiện nay chẳng hạn như điện thoại thông minh, máy tính dạng bảng và đồng hồ thông minh mang lại trải nghiệm phong phú và dễ chịu cho những người dùng cuối có các khả năng truyền thông phong phú cũng như các ứng dụng phần mềm có tính năng phong phú được cung cấp bởi các thiết bị này. Tuy nhiên, một số thiết bị di động có thể bị nhiễm phần mềm độc (“malware”) thực hiện các hoạt động mà người dùng không hay biết. Việc phát hiện phần mềm độc có thể khó khăn do tính chất hoạt động bí mật của phần mềm này.

Bản chất kỹ thuật của sáng chế

Một phương án làm ví dụ bao gồm phương pháp quản lý việc truy cập tài nguyên phần cứng trên thiết bị di động bao gồm các bước: nhận đầu vào người dùng thứ nhất cấp quyền cho ứng dụng thứ nhất trên thiết bị di động truy cập tài nguyên phần cứng thứ nhất của thiết bị di động và, dựa vào đó, cấp quyền cho ứng dụng thứ nhất để truy cập tài nguyên phần cứng thứ nhất; sau khi cấp quyền cho ứng dụng thứ nhất để truy cập tài nguyên phần cứng thứ nhất, thì phát hiện sự cố gắng truy cập tài nguyên phần cứng thứ nhất bởi ứng dụng thứ nhất khi ứng dụng này đang thực thi ở nền sau và dựa vào đó: thu chế độ hoạt động thứ nhất của thiết bị di động trong đó chế độ hoạt động thứ nhất này bao gồm thông tin chỉ báo về việc thiết bị di động ở trạng thái khoá hay trạng thái mở khoá; xác định rằng không có chính sách nào trong số các chính sách mà cấp quyền cho ứng dụng thứ nhất để truy cập phần cứng thứ nhất trong chế độ hoạt động thứ nhất; dựa vào bước xác định, tạo ra thông báo yêu cầu đầu vào người dùng để cấp hoặc từ chối truy cập vào tài nguyên phần cứng thứ nhất bởi ứng dụng thứ nhất; nhận đầu vào người dùng thứ hai đáp lại thông báo này; và thêm, vào các chính sách, chính sách mới để cấp hoặc từ chối truy cập vào các chính sách đối với tài nguyên phần cứng thứ nhất bởi ứng dụng thứ nhất trong chế độ hoạt động thứ nhất theo đầu vào người dùng thứ hai.

Tùy chọn, theo phương án bất kỳ trong số các phương án nêu trên, trong đó đầu vào người dùng thứ hai cấp quyền truy cập vào tài nguyên phần cứng thứ nhất, phương

pháp này còn bao gồm bước cấp quyền truy cập vào ứng dụng thứ nhất để truy cập tài nguyên phần cứng thứ nhất.

Tùy chọn, theo phương án bất kỳ trong số các phương án nêu trên, trong đó đầu vào người dùng thứ hai từ chối truy cập vào tài nguyên phần cứng thứ nhất, phương pháp này còn bao gồm bước từ chối truy cập vào ứng dụng thứ nhất để truy cập tài nguyên phần cứng thứ nhất.

Tùy chọn, theo phương án bất kỳ trong số các phương án nêu trên, trong đó đầu vào người dùng thứ hai từ chối truy cập vào tài nguyên phần cứng thứ nhất, phương pháp này còn bao gồm bước từ chối truy cập vào ứng dụng thứ nhất để truy cập tài nguyên phần cứng thứ nhất.

Tùy chọn, theo phương án bất kỳ trong số các phương án nêu trên, trong đó tài nguyên phần cứng thứ nhất bao gồm đầu vào micrô, đầu vào camera, đầu vào màn hình cảm ứng, đầu vào bàn phím, đầu ra hiển thị, đầu ra xúc giác, thông tin vị trí thiết bị di động hoặc giá trị chỉ thị cảm biến tiệm cận.

Tùy chọn, theo phương án bất kỳ trong số các phương án nêu trên, trong đó đầu vào camera là từ camera hồng ngoại.

Tùy chọn, theo phương án bất kỳ trong số các phương án nêu trên, phương pháp này còn bao gồm bước nhận các chính sách từ máy chủ và gửi chính sách mới này đến máy chủ.

Tùy chọn, theo phương án bất kỳ trong số các phương án nêu trên, phương pháp trong đó bước tạo ra thông báo yêu cầu đầu vào người dùng để cấp hoặc từ chối truy cập bao gồm bước tạo ra giao diện người dùng đồ họa trên màn hiển thị của thiết bị di động hoặc tạo ra thông điệp ngôn ngữ tự nhiên bằng cách sử dụng đầu ra âm thanh của thiết bị di động.

Tùy chọn, theo phương án bất kỳ trong số các phương án nêu trên, trong đó chế độ hoạt động còn bao gồm một hoặc nhiều chỉ báo về một hoặc nhiều ứng dụng khác mà được cài đặt trên thiết bị di động, chỉ báo về một hoặc nhiều ứng dụng khác mà hiện đang thực thi trên thiết bị di động, hoặc vị trí hiện tại của thiết bị di động.

Tùy chọn, theo phương án bất kỳ trong số các phương án nêu trên, phương pháp này còn bao gồm bước xác định rằng khoảng thời gian đã trôi qua kể từ khi thêm chính sách mới vào các chính sách và, dựa vào đó, loại bỏ chính sách mới này khỏi các chính sách.

Theo một phương án khác, hệ thống điều khiển truy cập được sử dụng để quản lý các tài nguyên phần cứng truy cập trong thiết bị di động. Hệ thống điều khiển truy

cập này bao gồm: phần tử giới hạn chức năng để cấp quyền cho ứng dụng thứ nhất để truy cập tài nguyên phần cứng thứ nhất, trong đó tài nguyên phần cứng thứ nhất là camera của thiết bị di động hoặc micrô của thiết bị di động; và phần tử phát hiện để phát hiện sự cố gắng truy cập tài nguyên phần cứng thứ nhất bởi ứng dụng thứ nhất khi ứng dụng thứ nhất đang thực thi ở nền sau. Phần tử giới hạn chức năng có thể từ chối truy cập vào tài nguyên thứ nhất bởi ứng dụng thứ nhất theo sự phát hiện sự cố gắng truy cập tài nguyên phần cứng thứ nhất bởi ứng dụng thứ nhất khi ứng dụng thứ nhất đang thực thi ở nền sau.

Một phương án khác bao gồm thiết bị điện tử di động bao gồm: màn hình để hiển thị thông tin đồ họa; bộ nhớ lưu trữ các lệnh; và một hoặc nhiều bộ xử lý truyền thông với bộ nhớ và màn hình, trong đó một hoặc nhiều bộ xử lý được tạo cấu hình để thực thi các lệnh để: nhận đầu vào người dùng thứ nhất cấp quyền cho ứng dụng thứ nhất trên thiết bị di động để truy cập tài nguyên phần cứng thứ nhất của thiết bị di động và, dựa vào đó, cấp quyền cho ứng dụng thứ nhất để truy cập tài nguyên phần cứng thứ nhất; sau khi cấp quyền cho ứng dụng thứ nhất để truy cập tài nguyên phần cứng thứ nhất, thì phát hiện sự cố gắng truy cập tài nguyên phần cứng thứ nhất bởi ứng dụng thứ nhất khi ứng dụng này đang thực thi ở nền sau và dựa vào đó: thu chế độ hoạt động thứ nhất của thiết bị di động trong đó chế độ hoạt động thứ nhất này bao gồm chỉ báo về việc thiết bị di động ở trạng thái khoá hay trạng thái mở khoá; xác định rằng không có chính sách nào trong số các chính sách mà cấp quyền cho ứng dụng thứ nhất để truy cập phần cứng thứ nhất ở chế độ hoạt động thứ nhất; dựa vào bước xác định này, tạo ra thông báo yêu cầu đầu vào người dùng để cấp hoặc từ chối truy cập vào tài nguyên phần cứng thứ nhất bởi ứng dụng thứ nhất; nhận đầu vào người dùng thứ hai đáp lại thông báo này; và thêm, vào các chính sách, chính sách mới để cấp hoặc từ chối truy cập vào các chính sách đối với tài nguyên phần cứng thứ nhất bởi ứng dụng thứ nhất ở chế độ hoạt động thứ nhất theo đầu vào người dùng thứ hai.

Tùy chọn, theo phương án bất kỳ trong số các phương án nêu trên, sáng chế đề xuất thiết bị điện tử di động trong đó đầu vào người dùng thứ hai cấp quyền truy cập vào tài nguyên phần cứng thứ nhất, một hoặc nhiều bộ xử lý được tạo cấu hình để cấp quyền truy cập cho ứng dụng thứ nhất để truy cập tài nguyên phần cứng thứ nhất.

Tùy chọn, theo phương án bất kỳ trong số các phương án nêu trên, sáng chế đề xuất thiết bị điện tử di động trong đó đầu vào người dùng thứ hai từ chối truy cập vào tài nguyên phần cứng thứ nhất, một hoặc nhiều bộ xử lý được tạo cấu hình để từ chối truy cập vào ứng dụng thứ nhất để truy cập tài nguyên phần cứng thứ nhất.

Tùy chọn, theo phương án bất kỳ trong số các phương án nêu trên, sáng chế đề xuất thiết bị điện tử di động trong đó tài nguyên phần cứng thứ nhất bao gồm đầu vào

micro, đầu vào camera, đầu vào màn hình cảm ứng, đầu ra hiển thị, đầu ra xúc giác, thông tin vị trí thiết bị di động hoặc giá trị chỉ thị cảm biến tiệm cận.

Tùy chọn, theo phương án bất kỳ trong số các phương án nêu trên, sáng chế đề xuất thiết bị điện tử di động trong đó đầu vào camera là từ một camera hồng ngoại.

Tùy chọn, theo phương án bất kỳ trong số các phương án nêu trên, thiết bị điện tử di động còn bao gồm một hoặc nhiều bộ xử lý được tạo cấu hình để nhận các chính sách từ máy chủ và gửi chính sách mới đến máy chủ này.

Tùy chọn, theo phương án bất kỳ trong số các phương án nêu trên, sáng chế đề xuất thiết bị điện tử di động trong đó bước tạo ra thông báo yêu cầu đầu vào người dùng để cấp hoặc từ chối truy cập bao gồm bước tạo ra giao diện người dùng đồ họa trên màn hình hiển thị của thiết bị di động hoặc tạo ra thông điệp ngôn ngữ tự nhiên bằng cách sử dụng đầu ra âm thanh của thiết bị di động này.

Tùy chọn, theo phương án bất kỳ trong số các phương án nêu trên, sáng chế đề xuất thiết bị điện tử di động trong đó chế độ hoạt động còn bao gồm một hoặc nhiều chỉ báo về một hoặc nhiều ứng dụng khác mà được cài đặt trên thiết bị di động, chỉ báo về một hoặc nhiều ứng dụng khác mà hiện đang thực thi trên thiết bị di động hoặc vị trí hiện tại của thiết bị di động.

Tùy chọn, theo phương án bất kỳ trong số các phương án nêu trên, thiết bị điện tử di động còn bao gồm một hoặc nhiều bộ xử lý được tạo cấu hình để xác định rằng khoảng thời gian đã trôi qua kể từ khi thêm chính sách mới vào các chính sách và, dựa vào đó, loại bỏ chính sách mới này ra khỏi các chính sách.

Tùy chọn, theo phương án bất kỳ trong số các phương án nêu trên, sáng chế đề xuất thiết bị điện tử di động.

Mô tả vắn tắt các hình vẽ

Fig.1 là hình vẽ minh họa các ví dụ về thiết bị tính toán di động 100 ở các chế độ hoạt động khác nhau;

Fig.2 là lưu đồ minh họa kỹ thuật được thực hiện bằng máy tính để truy cập tài nguyên phân cứng của thiết bị điện tử di động theo một phương án của sáng chế;

Fig.3 là hình vẽ minh họa hệ thống để quản lý tài nguyên theo một phương án của sáng chế;

Fig.4 là lưu đồ làm ví dụ minh họa kỹ thuật được thực hiện bằng máy tính để truy cập tài nguyên phân cứng của thiết bị điện tử di động theo một phương án của sáng chế; và

Fig.5 là sơ đồ khối minh họa các thành phần của thiết bị điện tử di động 500 theo

một phương án của sáng chế.

Mô tả chi tiết sáng chế

Phần tham khảo hiện sẽ được thực hiện một cách chi tiết đối với các phương án của sáng chế, các ví dụ về các phương án này được minh họa trên các hình vẽ kèm theo. Trong phần mô tả chi tiết sau đây, nhiều chi tiết cụ thể được đưa ra để cung cấp sự hiểu biết thấu đáo sáng chế. Tuy nhiên, người có hiểu biết trung bình trong lĩnh vực kỹ thuật sẽ thấy rõ ràng rằng các phương án có thể được thực hiện mà không có các chi tiết cụ thể này hoặc các thay đổi và thay thế khác nhau có thể được thực hiện đối với các phương án này mà không lệch khỏi mục đích và phạm vi của sáng chế. Trong các ví dụ khác, các phương pháp, thủ tục, thành phần và mạch đã được biết đến đã không được mô tả một cách chi tiết để không gây khó hiểu một cách không cần thiết khía cạnh của phương án này.

(“Ứng dụng”) phần mềm ứng dụng hoặc chương trình ứng dụng là chương trình máy tính được thiết kế để thực hiện nhóm gồm các chức năng, tác vụ hoặc các hoạt động vì lợi ích của người dùng. Các ví dụ về các ứng dụng bao gồm xử lý văn bản, bảng tính, phần mềm kế toán, trình duyệt web, trình phát đa phương tiện, trò chơi điện tử hoặc các trình chỉnh sửa ảnh chẳng hạn. Điều này trái ngược với phần mềm hệ thống, như thống điều hành chẳng hạn, mà quản lý việc thực thi các ứng dụng trên thiết bị tính toán.

Phần mềm theo dõi không đồng thuận như phần mềm độc hại có thể được cài đặt trên thiết bị tính toán theo một số cách. Ví dụ, phần mềm theo dõi này có thể được cài đặt trên thiết bị tính toán dưới dạng sản phẩm phụ để cài đặt ứng dụng khác trên thiết bị tính toán. Phần mềm theo dõi thường chạy trong nền sau và giám sát một hoặc nhiều tài nguyên phần cứng của thiết bị tính toán. Ngay cả khi nhà sản xuất thiết bị tính toán có mức độ bảo mật cao, vẫn có các cách khác để cài đặt phần mềm độc hại này. Ví dụ, phần mềm độc có thể tránh các biện pháp bảo mật của phần mềm hệ thống để cài đặt chương trình theo dõi ẩn chạy trong nền sau. Các ứng dụng phần mềm độc hại có thể theo dõi các hoạt động của người dùng mà người dùng không hay biết bằng cách truy cập các tài nguyên phần cứng của thiết bị tính toán của người dùng như điện thoại thông minh, đồng hồ thông minh, máy tính dạng bảng hoặc máy tính xách tay.

Một tài nguyên phần cứng là thành phần phần cứng vật lý của thiết bị tính toán; nhập vào hoặc kết xuất khỏi (I/O), một hoặc nhiều phần cứng vật lý của các thành phần này; hoặc dữ liệu thu được từ I/O của các thành phần phần cứng vật lý. Bằng cách minh họa, thành phần phần cứng vật lý có thể là micrô, bộ cảm biến tiệm cận, bộ cảm biến hình ảnh, màn hình cảm ứng, nút vật lý, bộ thu hệ thống định vị toàn cầu (global positioning system, GPS), vô tuyến di động, vô tuyến Wi-Fi hoặc bộ thu-phát Bluetooth. Các ví dụ về các thành phần phần cứng I/O bao gồm đầu vào micrô, đầu vào bộ cảm

biển hình ảnh (ví dụ, camera), đầu vào màn hình cảm ứng, đầu vào bàn phím, đầu ra hiển thị, đầu ra xúc giác hoặc giá trị chỉ thị cảm biến tiệm cận, v.v.. Một ví dụ về dữ liệu thu được từ I/O của các thành phần phần cứng vật lý là vị trí địa lý (“geolocation”) của thiết bị tính toán mà dựa vào thông tin nhận được bởi bộ thu GPS và vô tuyến Wi-Fi chẳng hạn. Có thể có các kiểu tài nguyên phần cứng khác.

Thiết bị tính toán có các chế độ hoạt động khác nhau. Nói chung, chế độ hoạt động là biểu thức Boolean mà biểu diễn trạng thái của thiết bị tính toán khi thiết bị tính toán này được bật lên. Trạng thái của thiết bị tính toán bao gồm một hoặc nhiều yếu tố trong số các yếu tố sau: xem ứng dụng được chỉ định đang thực thi ở nền trước hay nền sau, xem thiết bị được khoá hay được mở khoá; xem thiết bị ở chế độ máy bay hay không; chỉ báo về các ứng dụng mà đang thực thi trên thiết bị; và vị trí địa lý hiện tại của thiết bị. Nghĩa là, chế độ hoạt động là biểu thức Boolean của các yếu tố này. Khi thiết bị tính toán ở chế độ máy bay, thì thiết bị tính toán có thể tạm dừng việc truyền dẫn tín hiệu tần số vô tuyến (ví dụ, truyền dẫn di động, Wi-Fi và Bluetooth). Khi thiết bị tính toán không ở chế độ máy bay, thì thiết bị tính toán có thể hoạt động theo cách thông thường, như nhận và truyền các tín hiệu sử dụng các truyền dẫn di động, Wi-Fi và Bluetooth. Trạng thái khoá có thể được sử dụng để ngăn ngừa hoạt động vô ý của việc hiển thị màn hình cảm ứng, ví dụ, trong khi thiết bị ở trong túi hoặc ví của người dùng hoặc khi vật khác được đặt đè lên thiết bị. Trạng thái khoá cũng có thể được sử dụng để ngăn ngừa người không có thẩm quyền không sử dụng thiết bị. Nói chung, thiết bị được lập trình để vào trạng thái khoá khi người dùng ấn vào nút cụ thể hoặc một loạt nút hoặc khi thiết bị không hoạt động trong khoảng thời gian nhất định. Khi người dùng muốn sử dụng thiết bị mà ở trạng thái khoá, thì người dùng có thể được yêu cầu ra lệnh, kéo thanh trượt, ấn vào nút cụ thể hoặc một loạt nút (ví dụ, để nhập mật khẩu) để mở khoá thiết bị.

Fig.1 là hình vẽ minh hoạ các ví dụ về thiết bị tính toán di động 100 ở các chế độ hoạt động khác nhau. Thiết bị tính toán di động 100, ví dụ, thiết bị tính toán như điện thoại thông minh, đồng hồ thông minh hoặc thiết bị máy tính dạng bảng, được thể hiện ở chế độ hoạt động trạng thái mở khoá 101 với màn hiển thị 104 để tạo ra giao diện người dùng đồ hoạ (graphical user interface, GUI), trong đó các ứng dụng trên thiết bị tính toán di động được biểu diễn bởi các biểu tượng lựa chọn được bởi người dùng trong GUI. Ở chế độ hoạt động trạng thái khoá 102, màn hiển thị 104 của thiết bị tính toán di động có thể được tắt nguồn. Nhiều chức năng có thể bị treo khi thiết bị tính toán di động 100 ở trạng thái khoá. Ở chế độ hoạt động 103 khác, thông báo người dùng 106 được hiển thị trên màn hiển thị 104. Thông báo này có thể được hiển thị khi thiết bị tính toán 100 ở trạng thái khoá hoặc mở khoá để thu hút sự chú ý của người dùng thiết bị tính toán 100. Theo một số phương án thực hiện, thông báo được tạo ra cho người dùng thiết

bị tính toán 100 để yêu cầu đầu vào để cấp hoặc từ chối ứng dụng truy cập vào tài nguyên phần cứng. Theo cách khác hoặc ngoài ra, thông báo này có thể là thông điệp bằng giọng nói, âm thanh hoặc phản hồi xúc giác chẳng hạn. Màn hiển thị của thiết bị điện tử di động có thể được kích hoạt để thể hiện thông điệp thông báo như được thể hiện ở 103. Chính thông điệp thông báo này có thể được thể hiện ở cùng thời điểm.

Sáng chế đề xuất các phương án khác nhau để quản lý việc truy cập tài nguyên phần cứng trên thiết bị di động bằng cách sử dụng các chính sách để truy cập vào các tài nguyên phần cứng có thể được điều khiển theo cách an toàn cũng như theo cách thuận tiện cho người dùng.

Một phương án của sáng chế đề xuất rằng thiết bị được tạo cấu hình có các chính sách điều khiển việc truy cập vào các tài nguyên phần cứng. Chính sách là quy tắc mà biểu thị xem ứng dụng đã chỉ định được cấp hay bị từ chối truy cập vào tài nguyên phần cứng đã chỉ định trên thiết bị tính toán trong chế độ hoạt động đã chỉ định của thiết bị tính toán. Chính sách này có thể được lưu trữ trong tệp tin, ví dụ, tệp tin XML, hoặc văn bản hoặc tệp tin tương tự. Dạng chung của chính sách là: < mã nhận dạng ứng dụng, mã nhận dạng tài nguyên phần cứng, biểu thức Boolean chế độ hoạt động, cấp/từ chối > trong đó mã nhận dạng ứng dụng xác định ứng dụng, mã nhận dạng tài nguyên phần cứng xác định tài nguyên phần cứng (ví dụ, micrô, camera, v.v.), và chế độ hoạt động là biểu thức Boolean của một hoặc nhiều trong số các yếu tố được mô tả ở trên. Chính sách có thể bao gồm các bản ghi, và mỗi bản ghi này có thể bao gồm dạng chính sách như được mô tả ở trên. Chính sách được kích hoạt khi ID ứng dụng, ID tài nguyên phần cứng khớp với các ID tương ứng và khi biểu thức chế độ hoạt động đánh giá là ĐÚNG. Khi chính sách được kích hoạt, thì việc truy cập vào tài nguyên phần cứng đã xác định bởi ứng dụng đã xác định được cấp hoặc bị từ chối dựa vào trường cấp/từ chối của chính sách này. Một cách tùy chọn, các chính sách có thể có các thời gian hết hạn sau đó các chính sách này không còn hoạt động nữa.

Bằng cách minh họa, Bảng 1 liệt kê các chính sách làm ví dụ.

Bảng 1

Chính sách #	ID ứng dụng	ID tài nguyên phần cứng	Chế độ hoạt động	Cấp/Từ chối
1	App 1	Micrô	App 1 thực thi ở nền sau VÀ App camera hiện đang thực thi	Từ chối
2	App 1	Các dịch vụ vị trí	App 1 thực thi ở nền sau và (Chế độ khoá HOẶC Chế độ máy bay)	Từ chối
3	App 1	Micrô	App 1 thực thi ở nền sau VÀ KHÔNG bị khoá	Cấp
4	App 2	Các dịch vụ vị trí	App 2 thực thi ở nền sau	Từ chối
5	App 2	Các dịch vụ vị trí	App 2 thực thi ở nền trước	Cấp
6	App 3	Camera	Trạng thái khoá	Từ chối
7	App 3	Camera	App 3 thực thi ở nền trước	Cấp

Mỗi dòng trên Bảng 1 có thể là chính sách làm ví dụ, và chính sách này có thể được thể hiện dưới dạng một hoặc nhiều bản ghi. Ví dụ, liên quan đến ứng dụng thứ nhất (App 1) trên Bảng 1, khi App 1 thực thi ở nền sau, và App camera hiện đang thực thi, App 1 dự định bắt đầu hoạt động hoặc truy cập vào micrô, và dự định hoặc truy cập như vậy sẽ bị từ chối theo chính sách thứ nhất trên Bảng 1, Dòng 1. chính sách liên quan đến App 3, ví dụ, khi App 3 đang thực thi ở nền trước, và App 3 dự định bắt đầu hoạt động hoặc truy cập vào camera, dự định hoặc truy cập như vậy sẽ được cấp theo chính sách thứ hai trên Bảng 1, Dòng 7.

Khi ứng dụng cố gắng truy cập tài nguyên phần cứng của thiết bị, thì thiết bị này xác định nếu có một hoặc nhiều chính sách cấp quyền cho ứng dụng để truy cập tài nguyên phần cứng. Ví dụ, khi quyền truy cập không được cấp bởi chính sách, hoặc quyền truy cập của ứng dụng vào tài nguyên phần cứng bị từ chối hoặc thông báo được tạo ra cho người dùng thiết bị yêu cầu rằng người dùng cấp hoặc từ chối truy cập vào tài nguyên phần cứng đối với ứng dụng này. Như được lưu ý ở trên, thông báo như vậy có thể là thông điệp trong GUI của thiết bị tính toán hoặc lời nhắc bằng giọng nói. Trong trường hợp trong đó thông báo được tạo ra, phản hồi của người dùng đối với thông báo được sử dụng để tạo ra chính sách mới. Chính sách mới này chỉ định ứng dụng, tài nguyên phần cứng mà ứng dụng này cố gắng truy cập, biểu thức Boolean biểu diễn chế độ hoạt động của thiết bị tính toán khi ứng dụng cố gắng truy cập, và chỉ báo về việc người dùng đã cấp hay từ chối truy cập. Khi ứng dụng cố gắng truy cập vào cùng tài nguyên phần cứng trong cùng chế độ hoạt động, chính sách sẽ tự động cấp quyền cho ứng dụng này mà không cần thu đầu vào người dùng.

Fig.2 là lưu đồ minh hoạ kỹ thuật được thực hiện bằng máy tính để truy cập tài nguyên phần cứng của thiết bị điện tử di động theo một phương án của sáng chế.

Ở bước 201, quyền để ứng dụng thứ nhất truy cập tài nguyên phần cứng thứ nhất của thiết bị 100 nhận được khi cài đặt ứng dụng thứ nhất. Ứng dụng thứ nhất này có thể được cung cấp bởi thiết bị 100 hoặc nhà sản xuất hệ điều hành hoặc bên thứ ba. Dựa vào đó, ở bước 202, ứng dụng thứ nhất cố gắng truy cập tài nguyên phần cứng thứ nhất khi ứng dụng thứ nhất đang thực thi ở nền sau được phát hiện. Và dựa vào đó, chế độ hoạt động thứ nhất của thiết bị di động 100 thu được, trong đó chế độ hoạt động thứ nhất có thể bao gồm chỉ báo về việc thiết bị di động ở trạng thái khoá hay trạng thái mở khoá; ở bước 203, xác định rằng nếu có chính sách trong các chính sách mà cấp quyền cho ứng dụng thứ nhất để truy cập tài nguyên phần cứng thứ nhất trong chế độ hoạt động thứ nhất; ở bước 204, nếu chính sách thích hợp tồn tại và hoạt động dựa vào chính sách này có thể được thực thi theo đó; nếu không có chính sách như vậy tồn tại, thì thông báo được tạo ra để yêu cầu đầu vào người dùng cấp hoặc từ chối truy cập vào tài nguyên phần cứng thứ nhất bởi ứng dụng thứ nhất; ở bước 205, đầu vào người dùng phản hồi thông báo nhận được; khi phản hồi đối với thông báo này là quyền truy cập không được phép, thì việc cố gắng truy cập bởi ứng dụng thứ nhất bị chặn ở bước 206; mặt khác, ở bước 207, việc thực thi thích hợp được thực hiện đối với ứng dụng thứ nhất; sau đó ở bước 208, chính sách mới được thêm vào các chính sách, để cấp hoặc từ chối truy cập vào các chính sách đối với tài nguyên phần cứng thứ nhất bởi ứng dụng thứ nhất trong chế độ hoạt động thứ nhất theo đầu vào người dùng.

Fig.3 là hình vẽ minh hoạ hệ thống quản lý tài nguyên bao gồm một hoặc nhiều thiết bị di động 301, 304, 305 tương tác với mạng 302 theo một phương án của sáng chế. Mạng 302 có thể là máy chủ đám mây chẳng hạn. Các phương án khác nhau của sáng chế có thể được áp dụng bởi các tương tác của các thiết bị di động 301, 304, 305 với mạng 302.

Chính sách SP1 có thể được tải vào thiết bị di động 301 từ mạng 302. SP1 có thể là chính sách mà hầu hết mọi người đã công nhận, hoặc chính sách mà đã được tính toán thông qua thuật toán hiện có về các lựa chọn tối ưu của tiện ích của ứng dụng chẳng hạn. Hệ thống nghiên cứu kịch bản đáng ngờ đã chỉ định (specified suspicious scenario, SSS) 303 có thể được tạo ra để tính toán chính sách SP1. Hệ thống nghiên cứu SSS 303 có thể tạo ra chính sách được cập nhật một cách định kỳ cho mạng 302. Hệ thống nghiên cứu SSS 303 nhận dữ liệu người dùng về các sở thích hoặc các kết quả sử dụng ứng dụng từ các thiết bị khác nhau, ví dụ, 301, 304, 305. Hệ thống nghiên cứu SSS 303 có thể là phần tử trong mạng 302 hoặc được tạo cấu hình độc lập với mạng 302. Cơ sở dữ liệu 306 có thể được tạo cấu hình để lưu trữ dữ liệu phản hồi của người dùng.

Việc tính toán chính sách SP1 có thể là quy trình phân tích các hình mẫu của các sở thích từ dữ liệu lớn mà đã được thu thập từ các thiết bị 301, 304 và 305 khác nhau, chẳng hạn như tìm ra chính sách tối ưu ngoài dữ liệu lớn. Việc phân tích có thể dựa vào các sở thích của các người dùng, kiến thức phần mềm an toàn và không an toàn được nghiên cứu bởi nhóm kỹ sư, cách hiệu quả nhất để trình bày cho người dùng v.v.. Tất cả các tệp tin chính sách SSS có thể được lưu trữ trong một tệp tin xml hoặc các tệp tin xml trong cơ sở dữ liệu 306.

Thiết bị di động 301, 304, 305 có thể tải lên chính sách gần đây nhất SP2 của nó một cách định kỳ lên mạng 302 hoặc hệ thống nghiên cứu 303. Chu kỳ tải lên có thể là hàng ngày hoặc vài ngày một lần hoặc có thể được tạo cấu hình bởi thiết bị di động 301, 304, 305.

Chính sách có thể bao gồm một hoặc nhiều tệp tin chính sách. Chính sách hoặc tệp tin chính sách có thể bao gồm một hoặc nhiều bản ghi thể hiện chính sách nào dưới trường hợp nhất định. Mạng 302 có thể cập nhật tệp tin chính sách SSS mặc định, dựa vào các bản ghi khác nhau của SSS được thu thập từ các thiết bị 301, 304, 305 khác nhau; sau đó phân bố tệp tin chính sách SSS mặc định đã cập nhật đến các thiết bị 301, 304, 305 khác nhau. Tệp tin chính sách SSS mặc định này có thể là chính sách SP1 như được bộc lộ ở trên. Sau đây, tệp tin chính sách SSS mặc định đã cập nhật có thể được xác định dưới dạng chính sách SP3. Máy chủ đám mây 303 có thể tải chính sách SP3 lên các thiết bị 301, 304, 305 khác nhau. Mỗi khi các thiết bị 301, 304, 305 khác nhau này nhận chính sách SP3, chính sách trên thiết bị SP1 có thể được thay thế bằng SP3.

Tệp tin chính sách có thể được đọc hoặc phát hiện bởi trình phát hiện của các thiết bị 301, 304, 305 khác nhau, hoặc chương trình trên các thiết bị 301, 304, 305 khác nhau. Trình phát hiện 311 có thể được ghép nối với giao diện chương trình ứng dụng (Application Programming Interface, API). Trình phát hiện 311 này có thể truyền thông qua API đến trình thực thi 313 của các thiết bị 301, 304 và 305 khác nhau để thực hiện các thực thi theo tệp tin chính sách. Trình phát hiện 311 và trình thực thi 313 có thể là một chương trình duy nhất hoặc các chương trình riêng biệt chạy trên thiết bị 301, 304, 305.

Trình phát hiện 311 hoặc chương trình để phát hiện tệp tin chính sách SSS có thể được xác định dưới dạng chương trình máy tính mà chạy dưới dạng quy trình nền sau, hoặc chương trình dưới sự điều khiển trực tiếp của người dùng tương tác. Tên gọi có thể được xác định cho chương trình này trong môi trường khác nhau, ví dụ daemon, quy trình daemon, chương trình daemon (daemon program, DP), công việc ma, dịch vụ, tác vụ bắt đầu hoặc dạng tương tự.

Quy trình cha của daemon thường, nhưng có thể không phải luôn luôn, là quy

trình khởi tạo (init). Daemon thường được tạo ra bởi quy trình phân nhánh quy trình con và sau đó thoát ra ngay lập tức, do đó khiến init chấp nhận quy trình con này, hoặc được khởi chạy bởi quy trình init một cách trực tiếp. Ngoài ra, daemon được khởi chạy bằng cách phân nhánh và thoát ra thường có thể thực hiện các hoạt động khác, chẳng hạn như tách quy trình ra khỏi thiết bị đầu cuối điều khiển bất kỳ. Các thủ tục này thường được thực hiện theo các thường trình thuận tiện khác nhau chẳng hạn như daemon trong UNIX®.

Các hệ thống thường bắt đầu các daemon ở thời gian khởi động mà sẽ đáp lại các yêu cầu mạng, các hoạt động tài nguyên phần cứng hoặc các chương trình khác. Các daemon này có thể còn thực hiện các tác vụ đã xác định ở các thời gian đã lập lịch.

Chương trình daemon (DP) có thể là chương trình luôn chạy, mà có thể không cần gọi hệ điều hành nhất định, ví dụ, Android®, IOS®, để hỗ trợ. Tuy nhiên, chương trình daemon có thể cần gọi hệ điều hành nhất định để thực thi các chương trình khác trên hệ điều hành này. Các chương trình khác này có thể bật lên hộp thoại trên màn hình của thiết bị, và cho phép các người dùng xác định xem có cấp quyền chạy quy trình theo chính sách SSS đã xác định hay không. Hộp thoại này có thể là thông báo mà xuất hiện ở vùng trong màn hình của thiết bị di động như người dùng đã biết nhưng không chiếm phần lớn diện tích màn hình. Ví dụ, thay vì là thông điệp bật lên khó chịu, biểu tượng pin có thể nhấp nháy màu đỏ trong giây lát hoặc dạng tương tự.

Chương trình daemon có thể giám sát tất cả các tài nguyên của thiết bị, ví dụ, micro, camera, màn hình v.v.. Chương trình daemon này có thể là một phần của giao diện người dùng (user interface, UI).

Chương trình daemon có thể là trình phát hiện chủ động, mà có thể không cần kích hoạt đặc biệt bởi các chương trình khác của hệ điều hành. Trình phát hiện đã phản ứng, trái ngược với trình phát hiện chủ động, có thể giữ trạng thái ngủ hoặc chờ và cần được kích hoạt để hoạt động bởi sự kiện hoặc chương trình hoặc dạng tương tự.

Một phương án của sáng chế đề xuất thiết bị điện tử di động mà minh họa các phương pháp quản lý việc truy cập tài nguyên phần cứng như được mô tả ở trên. Trình phát hiện của thiết bị được tạo cấu hình để tải tệp tin chính sách SSS thứ nhất (SP1) lên thiết bị; lắng nghe các hoạt động của thành phần phần mềm và/hoặc phần cứng. SP1 có thể được xác định trước bởi nhà sản xuất thiết bị di động, hoặc sóng mang chạy mạng di động, hoặc trình chạy hệ điều hành, hoặc SP1 có thể được tải từ máy chủ đám mây. Tệp tin chính sách SSS thứ hai (SP2) có thể là chính sách SSS cục bộ, mà có thể tạo ra các bản ghi để chọn các sở thích được tạo ra bởi người dùng bằng thiết bị này. Thiết bị di động có thể được tạo cấu hình dưới dạng cấu hình người dùng được ưu tiên, chẳng hạn như SP2 được ưu tiên so với SP1.

Như được bộc lộ ở trên, trình phát hiện có thể là chương trình thứ nhất, chẳng hạn như chương trình daemon (DP). Khi sự thay đổi của hoạt động hệ thống xảy ra, thì DP có thể phát hiện và xác định xem có sự điều khiển chính sách SSS bất kỳ được tìm thấy hay không. Ví dụ, nếu đó là thời gian thực thi như được tạo cấu hình, và sự thay đổi là gì. Nếu không có chính sách SSS được tìm thấy, thì DP có thể không làm gì cả. Nếu có chính sách SSS bất kỳ được tìm thấy, thì DP có thể tiến hành truy vấn đối với chương trình thứ hai. Chương trình thứ hai này có thể là chương trình apk là chương trình được viết trong hệ điều hành android, hoặc theo định dạng java, hoặc định dạng khác bất kỳ mà có thể hoạt động cho mục đích tương tự.

Fig.4 là lưu đồ làm ví dụ minh họa kỹ thuật được thực hiện bằng máy tính để truy cập tài nguyên phần cứng của thiết bị điện tử di động theo một phương án của sáng chế.

Ở bước 401, ứng dụng cố gắng truy cập các tài nguyên hệ thống, chẳng hạn như tài nguyên phần cứng.

Ở bước 402, DP hỏi apk để đăng thông điệp uỷ quyền trên màn hình của thiết bị di động;

Ở bước 402', xác định xem có cấp quyền chạy quy trình theo chính sách SSS đã xác định (SP1) hay không.

Ở bước 403, khi không có chính sách SSS được tìm thấy, thì DP có thể không làm bất kỳ điều gì. Hoặc khi quyền chạy không được cấp, thì ứng dụng bị cấm thực thi.

Ở bước 404, nếu quyền chạy được cấp, thì sự kết hợp “app + tìm thấy chính sách SSS” này được đưa vào danh sách trắng dưới dạng bản ghi đối với chính sách SSS, chính sách này có thể được lưu trữ với ngày hết hạn (expiration date, ED). Danh sách trắng có thể là danh sách mà cung cấp đặc quyền, dịch vụ, tính di động, truy cập hoặc công nhận cụ thể. Các hoạt động trên danh sách sẽ được chấp nhận, phê duyệt và/hoặc công nhận. Danh sách trắng có thể là sự đảo ngược của danh sách đen. Các hoạt động trên danh sách đen có thể bị từ chối, không được công nhận hoặc bị tẩy chay.

Ở bước 405, bản ghi trong một chính sách SP2 có thể được tạo ra bao gồm dữ liệu chẳng hạn như sau:

S40, App + phần cứng → chính sách SSS

S41, Thiết lập hạn → hệ thống nghiên cứu

Các kết hợp như vậy giống như S40 hoặc S41, có thể được gọi là sự kết hợp được cho phép bởi người dùng (user permitted combination, UPC) hoặc sự kết hợp người dùng (user combination, UC) mà có thể được xác định dưới dạng một ví dụ được thể hiện dưới dạng “app + tìm thấy chính sách SSS” hoặc dạng tương tự; mọi UPC có thể

đã được tạo cấu hình có ngày hết hạn (ED).

Khi UPC hết hạn, thì DP có thể bật lên hộp thoại hoặc thông điệp hoặc dạng tương tự để hỏi người dùng cấp quyền lại cho UPC; DP có thể kích hoạt âm thanh hoặc dạng tương tự để đẩy thông điệp cảnh báo đến người dùng. Nếu được cấp một lần nữa, thì ED có thể cũng được cập nhật. Thời lượng cấp quyền (permission duration, PD) có thể được tăng lên kể từ khi nó được xác nhận lần thứ hai. PD có thể được xác định dưới dạng chu kỳ cấp quyền, ví dụ, một tuần, một tháng, mãi mãi v.v.. Nếu không được cấp, UPC này có thể bị thu hồi.

Ở bước 405', khi SP2 hiện có được phát hiện, thì cập nhật SP2 bằng bản ghi như được mô tả ở bước 404.

Sở thích của người dùng có thể được thu thập mỗi lần với sự lựa chọn bởi người dùng.

Ở bước 406, SP1 có thể được cập nhật với sự kết hợp có trong danh sách trắng như được mô tả ở bước 404.

Thiết bị điện tử di động được sản xuất để minh họa các giải pháp như được mô tả theo các phương án của sáng chế.

Fig.5 là sơ đồ khối minh họa các thành phần của thiết bị điện tử di động 500 theo một phương án của sáng chế. Thiết bị 500 này được tạo cấu hình để thực hiện các phương án như được mô tả ở trên. Thiết bị 500 bao gồm bộ nhớ 501, bộ xử lý 502, giao diện ngoại vi 503, bộ điều khiển bộ nhớ 504, bộ phận xử lý đồ họa (graphics processing unit, GPU) 505, một hoặc nhiều bộ cảm biến 506. Bộ xử lý cũng có thể được ghép nối với môđun giới hạn chức năng 507, môđun kích hoạt 508 và bộ phận xử lý trung tâm (central processing unit, CPU) 509. CPU cũng có thể được ghép nối với giao diện ngoại vi 503. Thiết bị này có thể còn bao gồm hệ mạch tần số vô tuyến (Radio Frequency, RF) 521 mà có thể bao gồm giao diện wi-fi và/hoặc giao diện Bluetooth. Thiết bị 500 có thể còn bao gồm một hoặc nhiều cổng bên ngoài 522, hệ mạch âm thanh 523 mà có thể còn được kết nối với một hoặc nhiều loa 525 và/hoặc micrô 526. Thiết bị này có thể còn bao gồm màn hình 524 mà có thể được ghép nối với giao diện ngoại vi 503. Các thành phần này truyền thông qua một hoặc nhiều bus truyền thông hoặc đường tín hiệu. Ví dụ, thiết bị điện tử di động 500 có thể là máy tính cầm tay, máy tính bảng, điện thoại di động, máy phát đa phương tiện hoặc thiết bị kỹ thuật số hỗ trợ cá nhân (personal digital assistant, PDA). Các thành phần khác nhau được thể hiện trên Fig.5 có thể được thực hiện trong tài nguyên phần cứng hoặc sự kết hợp của tài nguyên phần cứng và tài nguyên phần mềm, bao gồm một hoặc nhiều mạch tích hợp xử lý tín hiệu và/hoặc cho ứng dụng cụ thể.

Theo các phương án khác của của sáng chế, bộ nhớ 501 có thể bao gồm bộ lưu trữ được bố trí cách xa với thiết bị điện tử di động 500 chẳng hạn như mạng Internet, (các) mạng intranet, mạng vùng cục bộ (Local Area Network, LAN), mạng vùng cục bộ rộng (Wide Local Area Network, WLAN), mạng vùng lưu trữ (Storage Area Network, SAN) và mạng tương tự, hoặc sự kết hợp thích hợp bất kỳ của các mạng này.

Giao diện ngoại vi 503 ghép nối các thiết bị ngoại vi đầu vào và đầu ra của thiết bị 500 với CPU 509, GPU 505 và bộ nhớ 501. CPU 509 chạy các chương trình phần mềm khác nhau và/hoặc thiết lập các lệnh được lưu trữ trong bộ nhớ 501 để thực hiện các chức năng khác nhau đối với thiết bị điện tử di động 500 và để xử lý dữ liệu. GPU 505 xử lý các chức năng xử lý đồ họa đối với màn hình 524. Theo một số phương án, các chức năng xử lý đồ họa được xử lý bởi CPU 509, vì vậy GPU 505 có thể được lưu trữ.

Cổng bên ngoài 522 được làm thích ứng để ghép nối với các thiết bị khác theo cách trực tiếp hoặc từ xa qua một mạng. Ví dụ, cổng bên ngoài 522 có thể bao gồm bus nối tiếp đa năng (Universal Serial Bus, USB), FireWire, khe nhớ để nhận vật ghi lưu trữ bên ngoài, v.v..

Hệ mạch tần số vô tuyến (radio frequency, RF) 521 nhận và gửi các tín hiệu RF, mà có thể còn được gọi là các tín hiệu điện từ. Mạch RF 521 chuyển đổi các tín hiệu điện thành/từ các tín hiệu điện từ và truyền thông với các mạng truyền thông và các thiết bị truyền thông khác thông qua các tín hiệu điện từ này. Mạch RF 521 này có thể bao gồm hệ mạch đã biết để thực hiện các chức năng này, bao gồm nhưng không bị giới hạn ở hệ thống ăngten, bộ thu-phát RF, một hoặc nhiều bộ khuếch đại, bộ điều hướng, một hoặc nhiều bộ dao động, bộ xử lý tín hiệu số, bộ chip CODEC, thẻ môđun nhận dạng thuê bao (subscriber identity module, SIM), bộ nhớ v.v.. Hệ mạch RF 521 có thể truyền thông với các mạng, chẳng hạn như Internet, mạng intranet và/hoặc mạng không dây, chẳng hạn như mạng điện thoại tế bào, mạng vùng cục bộ không dây (LAN) và/hoặc mạng vùng đô thị (metropolitan area network, MAN), và các thiết bị khác bằng cách truyền thông không dây. Các mạng truyền thông không dây có thể sử dụng bất kỳ trong số các tiêu chuẩn truyền thông, các giao thức và các công nghệ, bao gồm nhưng không bị giới hạn ở hệ thống truyền thông di động toàn cầu (Global System for Mobile Communications, GSM), môi trường GSM dữ liệu nâng cao (Enhanced Data GSM Environment, EDGE), truy cập gói đường xuống tốc độ cao (high-speed downlink packet access, HSDPA), truy cập gói đường lên tốc độ cao (high-speed uplink packet access, HSUPA), đa truy cập phân chia theo mã băng rộng (wideband code division multiple access, W-CDMA), đa truy cập phân chia theo mã (code division multiple access, CDMA), đa truy cập phân chia theo thời gian (time division multiple access,

TDMA), Bluetooth, hệ thống truy cập internet không dây sử dụng sóng vô tuyến (Wireless Fidelity, Wi-Fi) (ví dụ, IEEE 802.11a, IEEE 802.11b, IEEE 802.11g và/hoặc IEEE 802.11n), truyền thoại qua giao thức Internet (voice over Internet Protocol, VoIP), Wi-MAX hoặc giao thức truyền thông thích hợp khác bất kỳ.

Hệ mạch âm thanh 523 kết nối với một hoặc nhiều loa 525 và micrô 526. Cùng với các thành phần này tạo ra giao diện âm thanh giữa người dùng và thiết bị điện tử di động 500. Hệ mạch âm thanh 523 này nhận dữ liệu âm thanh từ giao diện ngoại vi 503, chuyển đổi dữ liệu âm thanh thành tín hiệu điện, và truyền tín hiệu điện này đến (các) loa 525. (Các) loa 525 chuyển đổi tín hiệu điện thành các sóng âm thanh mà con người có thể nghe được. Hệ mạch âm thanh 190 còn nhận tín hiệu điện được chuyển đổi bởi micrô 526 từ các sóng âm thanh. Hệ mạch âm thanh 523 chuyển đổi tín hiệu điện thành dữ liệu âm thanh và truyền dữ liệu âm thanh này đến giao diện ngoại vi 503 để xử lý. Dữ liệu âm thanh có thể được truy xuất từ và/hoặc được truyền đến bộ nhớ 501 và/hoặc hệ mạch RF 521 bởi giao diện ngoại vi 503.

Màn hình 524 có thể là màn hình cảm ứng hoặc màn hình gập được và tạo ra cả giao diện đầu ra và giao diện đầu vào giữa thiết bị và người dùng. Màn hình 524 này hiển thị đầu ra trực quan cho người dùng mà có thể bao gồm văn bản, đồ họa, video và sự kết hợp bất kỳ của chúng. Một số hoặc tất cả các đầu ra trực quan có thể tương ứng với các đối tượng giao diện người dùng, các chi tiết khác về chúng được mô tả dưới đây. Màn hình 524 có thể sử dụng công nghệ màn hình thị tinh thể lỏng (liquid crystal display, LCD), hoặc các công nghệ hiển thị đã biết khác. Màn hình 524 còn chấp nhận đầu vào từ người dùng dựa vào xúc giác và/hoặc tiếp xúc thuộc xúc giác.

Hệ điều hành 510 được lưu trữ trong bộ nhớ 501 (ví dụ, Android, RTXC, Linux, UNIX®, Apple OS® X, Microsoft Windows® hoặc hệ điều hành nhúng chẳng hạn như VxWorks®) có thể bao gồm các thành phần phần mềm khác nhau và/hoặc các trình điều khiển để điều khiển và quản lý các tác vụ hệ thống chung (ví dụ, quản lý bộ nhớ, điều khiển thiết bị lưu trữ, quản lý nguồn điện, v.v.) và tạo điều kiện thuận lợi để truyền thông giữa các thành phần phần cứng và phần mềm khác nhau. Mặc dù nhiều loại hệ điều hành có thể được áp dụng, nhưng phần mô tả sau sẽ sử dụng Android làm một ví dụ để mô tả các phương án của sáng chế. Các ứng dụng khác nhau có thể được cài đặt trên hệ điều hành 510.

Chính sách SSS có thể bao gồm một hoặc nhiều ứng dụng mà có thể được truyền thông với bộ xử lý của thiết bị điện tử di động bởi API của thiết bị điện tử di động này. Chính sách SSS có thể được tạo cấu hình trước hoặc tinh chỉnh trong quá trình hoạt động từ lần này qua lần khác.

Trong lập trình máy tính, API là tập hợp gồm các định nghĩa, giao thức và công

cụ về đoạn chương trình con để xây dựng phần mềm ứng dụng. Theo các điều khoản chung, đây là tập hợp gồm các phương pháp truyền thông đã xác định rõ ràng giữa các thành phần phần mềm khác nhau. API có thể dùng cho hệ thống dựa trên web, hệ điều hành, hệ thống cơ sở dữ liệu và phần cứng máy tính hoặc thư viện phần mềm. Đặc tả API có thể có nhiều dạng, nhưng thường bao gồm các đặc tả đối với các đoạn chương trình, cấu trúc dữ liệu, lớp đối tượng, biến hoặc cuộc gọi từ xa. POSIX, Microsoft Windows API, C++ Standard Template Library và Java API là các ví dụ về các dạng khác nhau của các API. Tài liệu về API thường được cung cấp để tạo điều kiện thuận lợi cho việc sử dụng.

Ví dụ, tập hợp API trong thư viện đồ họa xác định cách các con trỏ được vẽ và có thể được hiển thị trên thiết bị đầu ra đồ họa. Khi ứng dụng cần chức năng con trỏ, nó có thể được chuyển đến để liên kết với tập hợp API này.

API có thể chỉ định giao diện giữa ứng dụng và hệ điều hành. Ví dụ, POSIX chỉ định tập hợp API chung mà nhằm cho phép ứng dụng được ghi cho hệ điều hành tương thích với POSIX cần được biên dịch cho hệ điều hành tương thích với POSIX khác. Phân phối phần mềm Linux và Berkeley là các ví dụ về hệ điều hành mà triển khai các POSIX API.

Các API từ xa cho phép các nhà phát triển kiểm soát các tài nguyên từ xa thông qua các giao thức, các tiêu chuẩn cụ thể để truyền thông mà cho phép các công nghệ khác nhau hoạt động cùng nhau, bất kể ngôn ngữ hoặc nền tảng. Ví dụ, API kết nối cơ sở dữ liệu Java cho phép các nhà phát triển truy vấn nhiều kiểu cơ sở dữ liệu khác nhau với cùng tập hợp chức năng, trong khi API gọi phương thức từ xa Java sử dụng giao thức phương thức từ xa Java để cho phép gọi các chức năng hoạt động từ xa, nhưng xuất hiện cục bộ đối với nhà phát triển. Do đó, các API từ xa hữu ích trong việc duy trì tính trừu tượng của đối tượng trong lập trình định hướng đối tượng; cuộc gọi phương pháp, được thực thi cục bộ trên đối tượng uỷ quyền, gọi ra phương pháp tương ứng trên đối tượng từ xa này, bằng cách sử dụng giao thức từ xa, và thu được kết quả cần được sử dụng cục bộ làm giá trị trả về. Cải biến đối với đối tượng uỷ quyền cũng sẽ dẫn đến cải biến tương ứng đối với đối tượng từ xa.

Các API web là các giao diện đã xác định thông qua đó các tương tác xảy ra giữa doanh nghiệp và các ứng dụng mà sử dụng các tài sản của họ. Cách tiếp cận API là cách tiếp cận kiến trúc mà xoay quanh việc cung cấp các giao diện lập trình được cho tập hợp dịch vụ đối với các ứng dụng khác nhau phục vụ các kiểu khách hàng khác nhau. Khi được sử dụng trong ngữ cảnh phát triển web, API thường được xác định dưới dạng tập hợp thông điệp yêu cầu giao thức truyền siêu văn bản (Hypertext Transfer Protocol, HTTP), cùng với việc định nghĩa cấu trúc của các thông điệp phản hồi, mà thường là

theo định dạng ngôn ngữ đánh dấu mở rộng được (Extensible Markup Language, XML) hoặc ký hiệu đối tượng JavaScript (JavaScript Object Notation, JSON). Một ví dụ có thể là API của công ty vận chuyển mà có thể được thêm vào trang web tập trung vào thương mại điện tử, để tạo điều kiện thuận lợi cho việc đặt dịch vụ vận chuyển và tự động bao gồm phí vận chuyển hiện tại mà nhà phát triển trang web không cần phải nhập bảng phí của người gửi hàng vào cơ sở dữ liệu web. Trong khi "API web" trong lịch sử gần như đồng nghĩa với dịch vụ web, nhưng xu hướng gần đây (được gọi là Web 2.0) đã chuyển từ các dịch vụ web dựa trên giao thức truy cập đối tượng đơn giản (Simple Object Access Protocol, SOAP) và kiến trúc định hướng dịch vụ (service-oriented architecture, SOA) sang các tài nguyên web kiểu chuyển trạng thái đại diện (representational state transfer, REST) trực tiếp hơn và kiến trúc định hướng tài nguyên (resource-oriented architecture, ROA). Một phần của xu hướng này có liên quan đến phong trào Web ngữ nghĩa hướng tới khung mô tả tài nguyên (Resource Description Framework, RDF), khái niệm để thúc đẩy các công nghệ kỹ thuật bản thể học dựa trên web. Các API web cho phép kết hợp nhiều API vào các ứng dụng mới được gọi là các bản kết hợp (mash-up). Trong không gian đa phương tiện xã hội, các API web đã cho phép các cộng đồng web tạo điều kiện thuận lợi cho việc chia sẻ nội dung và dữ liệu giữa các cộng đồng và ứng dụng. Theo cách này, nội dung mà được tạo ra ở một địa điểm có thể được đăng và cập nhật động ở nhiều vị trí trên web.

Mặc dù sáng chế đã được mô tả dựa vào các dấu hiệu cụ thể và các phương án của sáng chế, nhưng cần hiểu rằng các thay đổi và thay thế khác nhau có thể được thực hiện mà không lệch khỏi mục đích và phạm vi của sáng chế như được xác định bởi các điểm yêu cầu bảo hộ sau.

YÊU CẦU BẢO HỘ

1. Phương pháp quản lý việc truy cập tài nguyên phần cứng trên thiết bị di động, phương pháp này bao gồm các bước:

nhận đầu vào người dùng thứ nhất cấp quyền cho ứng dụng thứ nhất trên thiết bị di động để truy cập tài nguyên phần cứng thứ nhất của thiết bị di động và, dựa vào đó, cấp quyền cho ứng dụng thứ nhất để truy cập tài nguyên phần cứng thứ nhất;

sau khi cấp quyền cho ứng dụng thứ nhất để truy cập tài nguyên phần cứng thứ nhất, thì phát hiện sự cố gắng thứ nhất bởi ứng dụng thứ nhất để truy cập tài nguyên phần cứng thứ nhất khi ứng dụng này đang thực thi ở nền sau và dựa vào đó:

thu chế độ hoạt động thứ nhất của thiết bị di động;

nếu chính sách mà cấp quyền cho ứng dụng thứ nhất đang thực thi ở nền sau để truy cập tài nguyên phần cứng thứ nhất trong chế độ hoạt động thứ nhất của thiết bị di động không tồn tại, thì tạo ra thông báo yêu cầu đầu vào người dùng cấp hoặc từ chối truy cập vào tài nguyên phần cứng thứ nhất bởi ứng dụng thứ nhất;

nhận đầu vào người dùng thứ hai đáp lại thông báo này; và

nếu đầu vào người dùng thứ hai đáp lại thông báo rằng không cho phép truy cập, thì chặn sự cố gắng thứ nhất bởi ứng dụng thứ nhất đang thực thi ở nền sau, để truy cập tài nguyên phần cứng thứ nhất.

2. Phương pháp theo điểm 1, trong đó phương pháp này còn bao gồm bước:

đáp lại bước phát hiện sự cố gắng thứ nhất bởi ứng dụng thứ nhất để truy cập tài nguyên phần cứng thứ nhất, thì xác định xem ứng dụng thứ nhất có đang thực thi ở nền sau của thiết bị di động hay không.

3. Phương pháp theo điểm 1 hoặc điểm 2, trong đó phương pháp này còn bao gồm bước:

nếu đầu vào người dùng thứ hai đáp lại thông báo rằng cho phép truy cập, thì thêm, vào các chính sách của thiết bị di động, chính sách mới để cấp quyền truy cập vào tài nguyên phần cứng thứ nhất bởi ứng dụng thứ nhất đang thực thi ở nền sau trong chế độ hoạt động thứ nhất theo đầu vào người dùng thứ hai.

4. Phương pháp theo điểm 3, trong đó phương pháp này còn bao gồm bước nhận các chính sách từ máy chủ và gửi chính sách mới đến máy chủ.

5. Phương pháp theo điểm 3 hoặc điểm 4, trong đó phương pháp này còn bao gồm bước:

xác định rằng khoảng thời gian đã trôi qua kể từ khi thêm chính sách mới vào các chính sách của thiết bị di động và, dựa vào đó, loại bỏ chính sách mới này khỏi các chính sách.

6. Phương pháp theo điểm bất kỳ trong số các điểm từ 1 đến 5, trong đó tài nguyên phần cứng thứ nhất bao gồm đầu vào micrô, đầu vào camera, đầu vào màn hình cảm ứng, đầu vào bàn phím, đầu ra hiển thị, đầu ra xúc giác, thông tin vị trí thiết bị di động, các dịch vụ vị trí hoặc giá trị chỉ thị cảm biến tiệm cận.

7. Phương pháp theo điểm 6, trong đó đầu vào camera là từ camera hồng ngoại.

8. Phương pháp theo điểm bất kỳ trong số các điểm từ 1 đến 7, trong đó bước tạo ra thông báo yêu cầu đầu vào người dùng cấp hoặc từ chối truy cập bao gồm bước tạo ra giao diện người dùng đồ hoạ trên màn hiển thị của thiết bị di động hoặc tạo ra thông điệp ngôn ngữ tự nhiên sử dụng đầu ra âm thanh của thiết bị di động.

9. Phương pháp theo điểm bất kỳ trong số các điểm từ 1 đến 8, trong đó chế độ hoạt động bao gồm một hoặc nhiều trong số chỉ báo về việc thiết bị di động là ở trạng thái khoá hay trạng thái mở khoá, chỉ báo về một hoặc nhiều ứng dụng khác mà được cài đặt trên thiết bị di động, chỉ báo về một hoặc nhiều ứng dụng khác mà hiện đang thực thi trên thiết bị di động hoặc vị trí hiện tại của thiết bị di động.

10. Thiết bị di động, thiết bị này bao gồm:

màn hình để hiển thị thông tin đồ hoạ;

bộ nhớ lưu trữ các lệnh; và

một hoặc nhiều bộ xử lý truyền thông với bộ nhớ và màn hình, trong đó một hoặc nhiều bộ xử lý này được tạo cấu hình để thực thi các lệnh để:

nhận đầu vào người dùng thứ nhất cấp quyền cho ứng dụng thứ nhất trên thiết bị di động truy cập tài nguyên phần cứng thứ nhất của thiết bị di động và, dựa vào đó, cấp quyền cho ứng dụng thứ nhất để truy cập tài nguyên phần cứng thứ nhất;

sau khi cấp quyền cho ứng dụng thứ nhất để truy cập tài nguyên phần cứng thứ nhất, thì phát hiện sự cố gắng thứ nhất bởi ứng dụng thứ nhất để truy cập tài nguyên phần cứng thứ nhất khi ứng dụng này đang thực thi ở nền sau và dựa vào đó:

thu chế độ hoạt động thứ nhất của thiết bị di động;

nếu chính sách mà cấp quyền cho ứng dụng thứ nhất đang thực thi ở nền sau để truy cập phần cứng thứ nhất trong chế độ hoạt động thứ nhất của thiết bị di động không tồn tại, thì tạo ra thông báo yêu cầu đầu vào người dùng cấp hoặc từ chối truy cập vào tài nguyên phần cứng thứ nhất bởi ứng dụng thứ nhất;

nhận đầu vào người dùng thứ hai đáp lại thông báo; và

nếu đầu vào người dùng thứ hai đáp lại thông báo rằng không cho

phép truy cập, thì chặn sự cố gắng bởi ứng dụng thứ nhất đang thực thi ở nền sau, để truy cập tài nguyên phần cứng thứ nhất.

11. Thiết bị theo điểm 10, trong đó đáp lại bước phát hiện sự cố gắng thứ nhất bởi ứng dụng thứ nhất để truy cập tài nguyên phần cứng thứ nhất, một hoặc nhiều bộ xử lý thực thi lệnh để:

xác định xem ứng dụng thứ nhất có đang thực thi ở nền sau của thiết bị di động hay không.

12. Thiết bị theo điểm 10 hoặc điểm 11, trong đó một hoặc nhiều bộ xử lý được tạo cấu hình để thực thi tiếp:

nếu đầu vào người dùng thứ hai đáp lại thông báo rằng cho phép truy cập, thì thêm, vào các chính sách của thiết bị di động, chính sách mới để cấp quyền truy cập vào tài nguyên phần cứng thứ nhất bởi ứng dụng thứ nhất đang thực thi ở nền sau trong chế độ hoạt động thứ nhất theo đầu vào người dùng thứ hai.

13. Thiết bị theo điểm 12, trong đó thiết bị này còn bao gồm một hoặc nhiều bộ xử lý được tạo cấu hình để nhận các chính sách từ máy chủ và gửi chính sách mới đến máy chủ.

14. Thiết bị theo điểm 12 hoặc điểm 13, trong đó thiết bị này còn bao gồm một hoặc nhiều bộ xử lý được tạo cấu hình để xác định rằng khoảng thời gian đã trôi qua kể từ khi thêm chính sách mới vào các chính sách của thiết bị di động và, dựa vào đó, loại bỏ chính sách mới này khỏi các chính sách.

15. Thiết bị theo điểm bất kỳ trong số các điểm từ 10 đến 14, trong đó tài nguyên phần cứng thứ nhất bao gồm đầu vào micrô, đầu vào camera, đầu vào màn hình cảm ứng, đầu ra hiển thị, đầu ra xúc giác, thông tin vị trí thiết bị di động, các dịch vụ vị trí hoặc giá trị chỉ thị cảm biến tiệm cận.

16. Thiết bị theo điểm 15, trong đó đầu vào camera là từ camera hồng ngoại.

17. Thiết bị theo điểm bất kỳ trong số các điểm từ 10 đến 16, trong đó bước tạo ra thông báo yêu cầu đầu vào người dùng cấp hoặc từ chối truy cập bao gồm bước tạo ra giao diện người dùng đồ họa trên màn hiển thị của thiết bị di động hoặc tạo ra thông điệp ngôn ngữ tự nhiên sử dụng đầu ra âm thanh của thiết bị di động.

18. Thiết bị theo điểm bất kỳ trong số các điểm từ 10 đến 17, trong đó chế độ hoạt động bao gồm một hoặc nhiều trong số chỉ báo về việc thiết bị di động là ở trạng thái khoá hay trạng thái mở khoá, chỉ báo về một hoặc nhiều ứng dụng khác mà được cài đặt trên thiết bị di động, chỉ báo về một hoặc nhiều ứng dụng khác mà hiện đang thực thi trên thiết bị di động hoặc vị trí hiện tại của thiết bị di động.

19. Thiết bị di động, thiết bị này bao gồm:

màn hình để hiển thị thông tin đồ họa;

bộ nhớ lưu trữ các lệnh; và

một hoặc nhiều bộ xử lý truyền thông với bộ nhớ và màn hình, trong đó một hoặc nhiều bộ xử lý này được tạo cấu hình để thực thi các lệnh để thực hiện phương pháp theo điểm bất kỳ trong số các điểm từ 1 đến 9.

20. Vật ghi lưu trữ lưu trữ chương trình máy tính bao gồm lệnh, trong đó khi lệnh này chạy trên máy tính, thì máy tính được cho phép thực hiện phương pháp theo điểm bất kỳ trong số các điểm từ 1 đến 9.

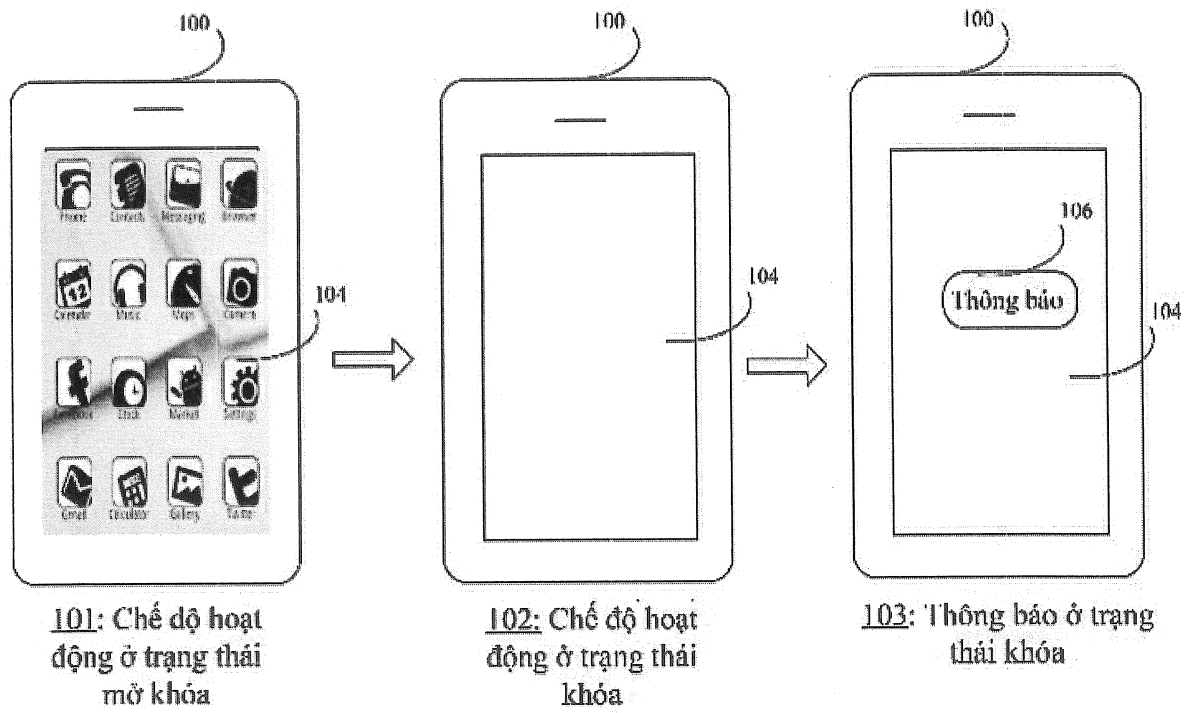


FIG.1

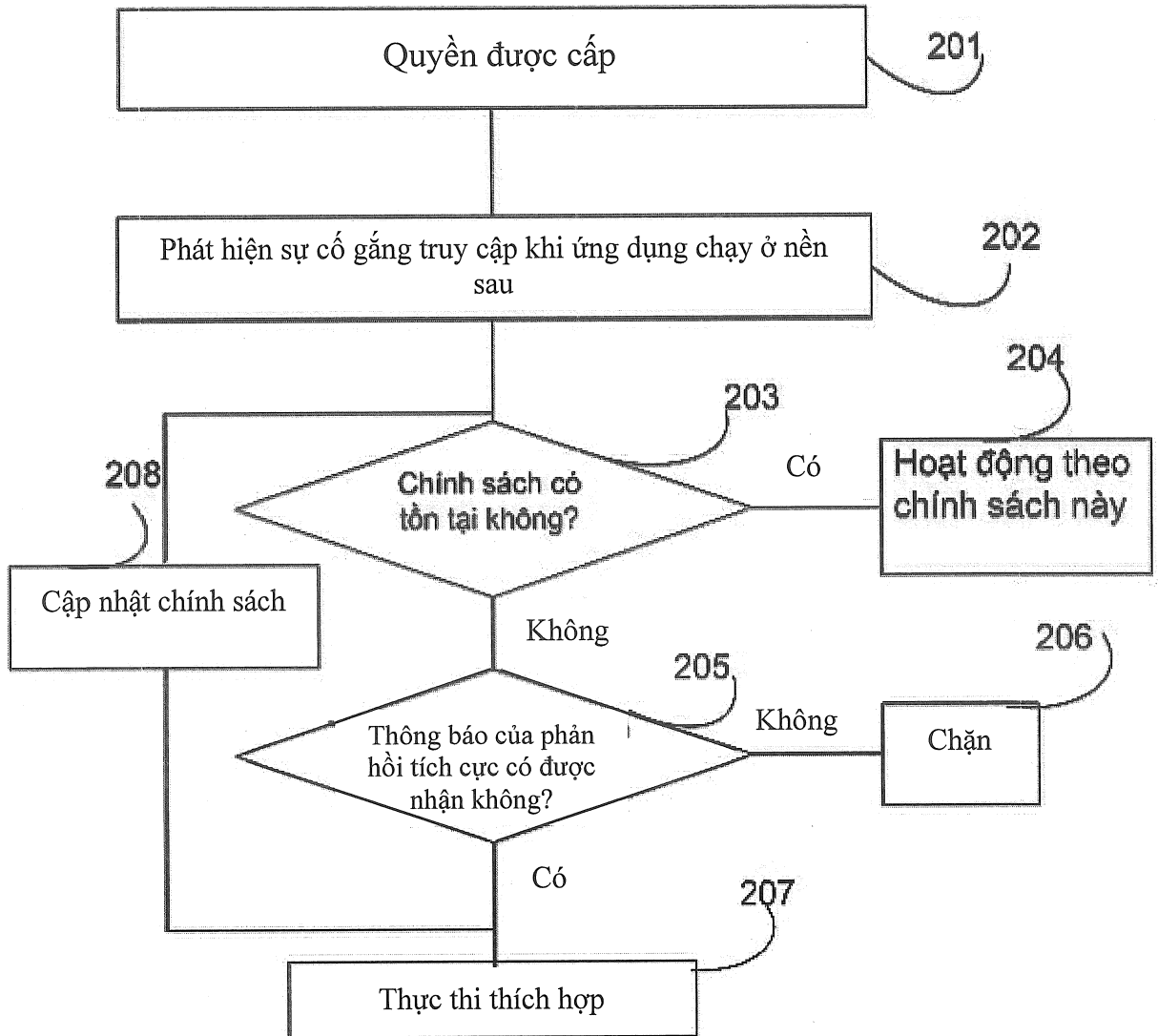


FIG.2

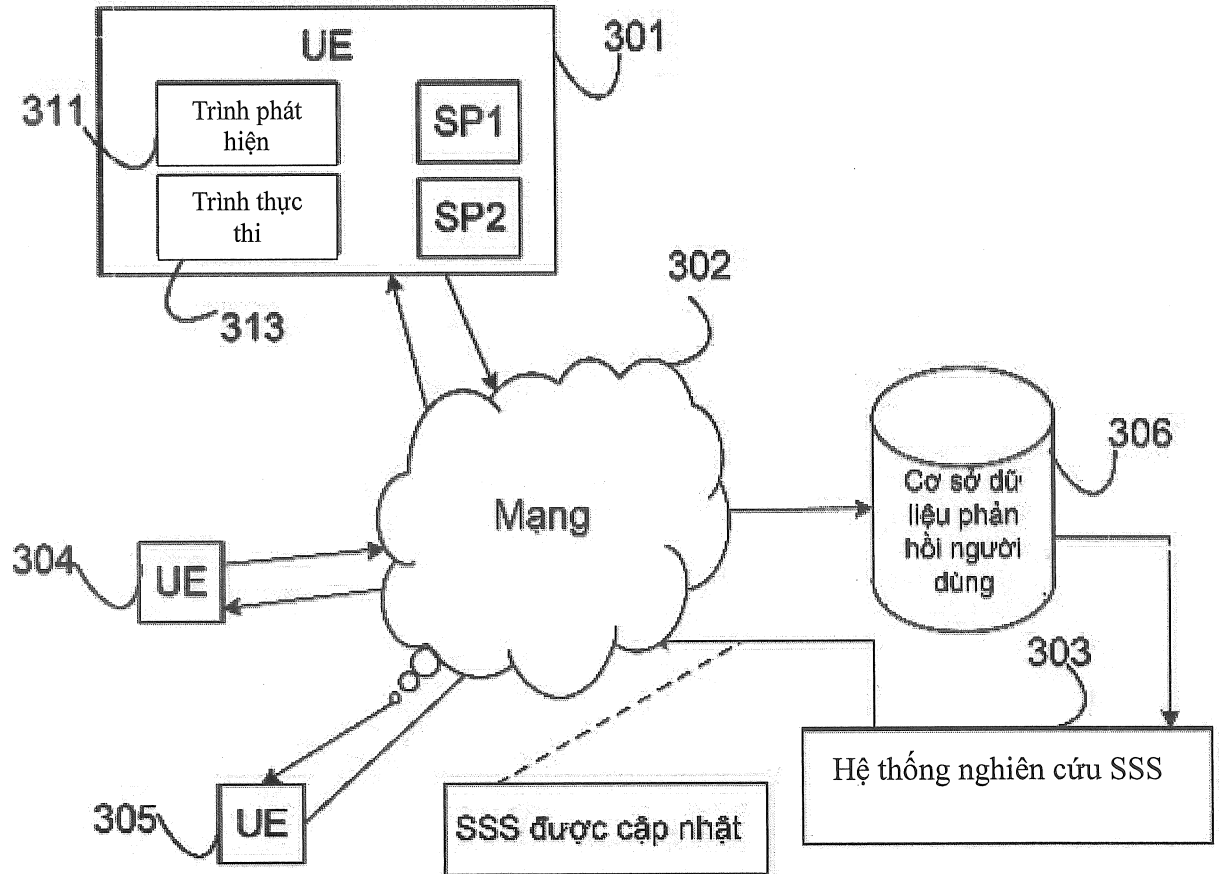


FIG.3

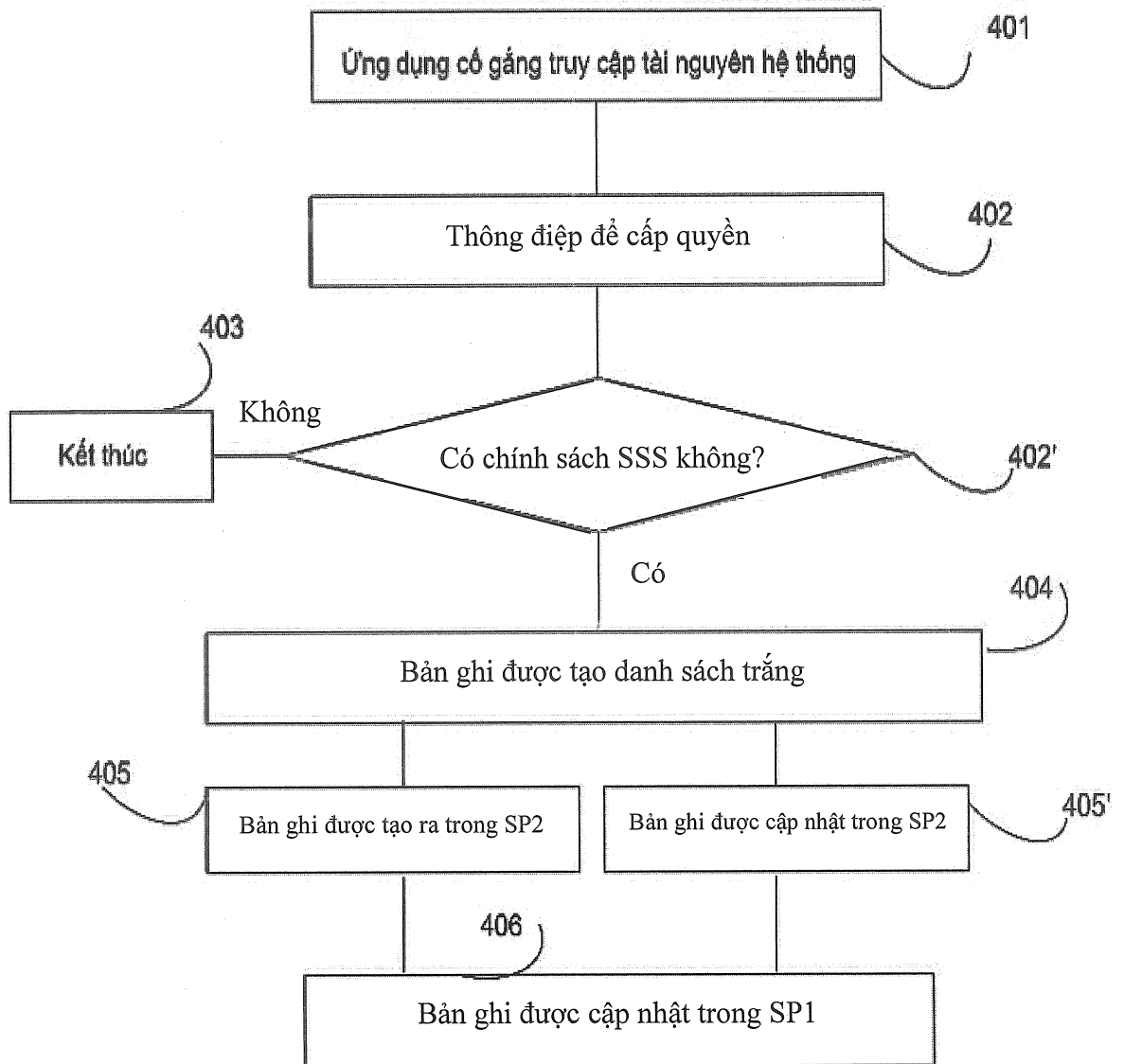


FIG.4

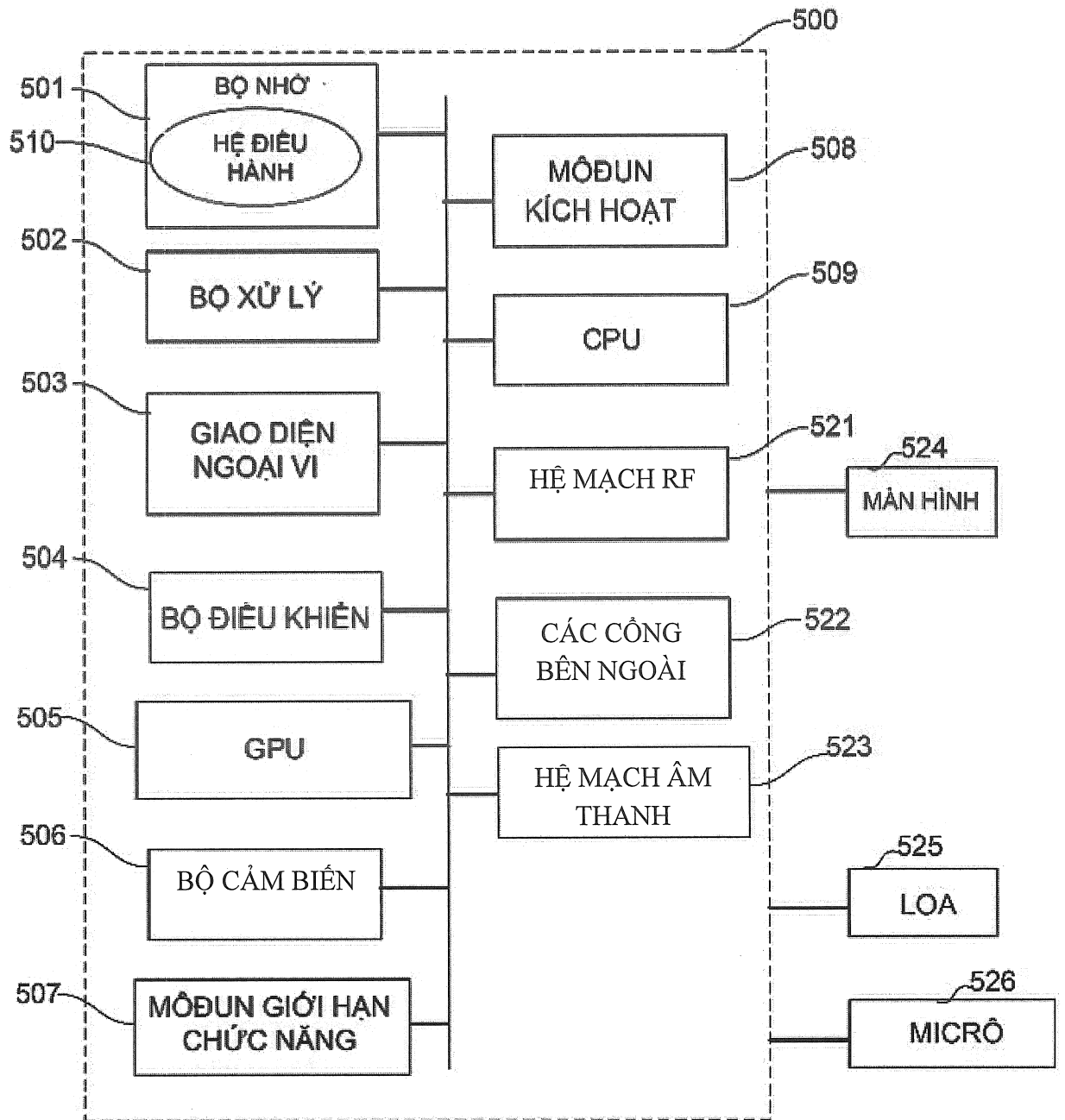


FIG.5