(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) **1-0023055**

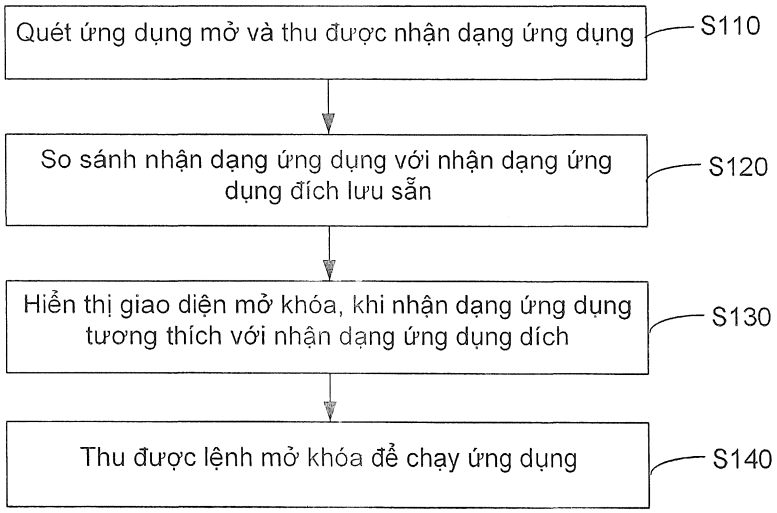
(51)[7] **G06F 21/10**

(13) **B**

(21) 1-2015-00477
(22) 10.07.2013
(86) PCT/CN2013/079131 10.07.2013
(87) WO2014/012448A1 23.01.2014
(30) 201210245772.2 16.07.2012 CN
(45) 25.02.2020 383
(43) 27.04.2015 325
(73) TENCENT TECHNOLOGY (SHENZHEN) COMPANY LIMITED (CN)
Room 403, East Block 2, SEG Park, Zhenxing Road, Futian, Shenzhen, Guangdong 518000, China
(72) ZHENG, Xiaosheng (CN)
(74) Công ty TNHH một thành viên Sở hữu trí tuệ VCCI (VCCI-IP CO.,LTD)

(54) PHƯƠNG PHÁP VÀ HỆ THỐNG KIỂM SOÁT VIỆC TRUY CẬP VÀO CÁC ỨNG DỤNG TRÊN THIẾT BỊ ĐẦU CUỐI DI ĐỘNG

(57) Sáng chế đề xuất phương pháp và hệ thống để kiểm soát việc truy cập vào các ứng dụng trên thiết bị đầu cuối di động. Trong phương pháp ví dụ, ứng dụng mở có thể được quét và nhận dạng ứng dụng có thể thu được. Nhận dạng ứng dụng có thể được so sánh với nhận dạng ứng dụng đích lưu sẵn. Khi nhận dạng ứng dụng được so sánh tương thích với nhận dạng ứng dụng đích lưu sẵn, giao diện mở khóa có thể được hiển thị. Lệnh mở khóa có thể thu được để chạy ứng dụng trên thiết bị đầu cuối di động. Hệ thống ví dụ để kiểm soát việc truy cập vào ứng dụng trên thiết bị đầu cuối di động có thể bao gồm môđun quét, môđun so sánh, môđun hiển thị và môđun thực hiện.



Lĩnh vực kỹ thuật được đề cập

Sáng chế đề cập đến lĩnh vực sự bảo mật của các thiết bị đầu cuối di động, và cụ thể là đề cập đến các phương pháp và các hệ thống kiểm soát việc truy cập vào các ứng dụng trên thiết bị đầu cuối di động.

Tình trạng kỹ thuật của sáng chế

Với sự phát triển của công nghệ máy tính, các thiết bị đầu cuối di động đang trở nên ngày càng phổ biến. Để đáp ứng các yêu cầu về trải nghiệm của người dùng, các ứng dụng khác nhau được cài đặt trên thiết bị đầu cuối di động. Các ứng dụng này có thể chứa thông tin cá nhân của người dùng. Thông tin cá nhân này là bí mật và không nhằm để những người khác biết. Do đó, sự bảo mật truy cập các ứng dụng trên thiết bị đầu cuối di động ngày càng trở nên quan trọng.

Ví dụ, các ứng dụng khác nhau có thể được cài đặt trên điện thoại di động trên cơ sở hệ điều hành Android. Các ứng dụng này có thể được sử dụng để kiểm tra các bản ghi cuộc gọi và/hoặc các bản ghi thông tin cá nhân, để kiểm tra các tài nguyên đa phương tiện, để xem tập (album), v.v.. Trong nhiều trường hợp, các ứng dụng này có thể được truy cập một cách dễ dàng. Khi điện thoại bị mất nhưng được tìm thấy bởi người khác hoặc được mượn bởi người khác, thông tin cá nhân/hồ sơ của chủ sở hữu có thể bị người khác xem. Nói cách khác, thông tin cá nhân hoặc hồ sơ của chủ sở hữu không được bảo vệ một cách hữu hiệu.

Do đó, mong muốn đề xuất các phương pháp và các hệ thống kiểm soát việc truy cập vào các ứng dụng trên thiết bị đầu cuối di động để đảm bảo sự bảo mật của các ứng dụng trên thiết bị đầu cuối di động.

Bản chất kỹ thuật của sáng chế

Theo các phương án khác nhau, phương pháp kiểm soát việc truy cập vào ứng dụng trên thiết bị đầu cuối di động được đề xuất. Trong phương pháp này, ứng dụng mở có thể được quét và nhận dạng ứng dụng có thể thu được. Nhận dạng ứng dụng có thể được so sánh với nhận dạng ứng dụng đích lưu sẵn. Giao diện mở khóa có thể được hiển thị, khi nhận dạng ứng dụng được so sánh là tương thích với nhận dạng ứng dụng đích lưu sẵn. Lệnh mở khóa có thể thu được để chạy ứng dụng trên thiết bị đầu cuối di động.

Theo các phương án khác nhau, hệ thống kiểm soát việc truy cập vào ứng dụng trên thiết bị đầu cuối di động được đề xuất. Hệ thống có thể gồm môđun quét, môđun so sánh, môđun hiển thị và môđun thực hiện. Môđun quét có thể được tạo cấu hình để quét ứng dụng mở và để thu được nhận dạng ứng dụng. Môđun so sánh có thể được tạo cấu hình để so sánh nhận dạng ứng dụng với nhận dạng ứng dụng đích lưu sẵn. Môđun hiển thị có thể được tạo cấu hình để hiển thị giao diện mở khóa, khi nhận dạng ứng dụng được so sánh là tương thích với nhận dạng ứng dụng đích lưu sẵn. Môđun thực hiện có thể được tạo cấu hình để thu được lệnh mở khóa để chạy ứng dụng.

Theo cách này, các phương pháp và các hệ thống kiểm soát việc truy cập vào các ứng dụng trên thiết bị đầu cuối di động được bộc lộ có thể so sánh nhận dạng ứng dụng sau khi quét với nhận dạng ứng dụng đích lưu sẵn. Khi nhận dạng ứng dụng đã quét tương thích với hoặc phù hợp với ứng dụng đích lưu sẵn, thì giao diện mở khóa có thể được hiển thị. Sau khi được mở khóa bằng cách thu lệnh mở khóa trên giao diện mở khóa, các ứng dụng tương ứng sau đó có thể được chạy trên giao diện mở khóa. Sự bảo mật truy cập các ứng dụng có thể được cải thiện. Sự bảo mật dữ liệu của thiết bị đầu cuối di động có thể được đảm bảo.

Các khía cạnh hoặc các phương án khác của sáng chế có thể được hiểu bởi người có trình độ trung bình trong lĩnh vực dựa vào phần mô tả, các yêu cầu bảo

hộ và các hình vẽ của sáng chế.

Mô tả vắn tắt các hình vẽ

Các hình vẽ sau đây chỉ đơn thuần là các ví dụ nhằm mục đích minh họa các phương án bộc lộ khác nhau và không nhằm mục đích giới hạn phạm vi của sáng chế.

Fig.1 minh họa phương pháp kiểm soát việc truy cập vào ứng dụng trên thiết bị đầu cuối di động ví dụ theo các phương án khác nhau của sáng chế;

Fig.2 minh họa phương pháp ví dụ để thiết đặt mẫu trượt để mở khóa ứng dụng trên thiết bị đầu cuối di động ví dụ theo các phương án khác nhau của sáng chế;

Fig.3 minh họa giao diện mở khóa ví dụ có mẫu trượt theo các phương án khác nhau của sáng chế;

Fig.4 minh họa hệ thống ví dụ để kiểm soát việc truy cập vào ứng dụng trên thiết bị đầu cuối di động theo các phương án khác nhau của sáng chế;

Fig.5 minh họa môđun quét ví dụ theo các phương án khác nhau của sáng chế;

Fig.6 minh họa môđun quét ví dụ khác theo các phương án khác nhau của sáng chế; và

Fig.7 thể hiện sơ đồ khối của hệ thống máy tính ví dụ có thể thực hiện thiết bị đầu cuối di động theo các phương án khác nhau của sáng chế.

Mô tả chi tiết sáng chế

Sáng chế sau đây được mô tả chi tiết dựa vào các phương án ví dụ, mà được minh họa trên các hình vẽ kèm theo. Các số chỉ dẫn giống nhau sẽ được sử dụng xuyên suốt các hình vẽ để chỉ các bộ phận giống nhau hoặc tương tự.

Fig.1 minh họa phương pháp ví dụ để kiểm soát việc truy cập vào ứng dụng trên thiết bị đầu cuối di động theo các phương án khác nhau của sáng chế. Trong

bước S110, ứng dụng mở có thể được quét và nhận dạng ứng dụng có thể thu được. Ví dụ, các phương pháp khác nhau có thể được sử dụng để quét ứng dụng đang chạy để thu được nhận dạng của ứng dụng đang chạy.

Trong phương pháp ví dụ để quét ứng dụng mở hoặc đang chạy, đầu chồng của chồng giao diện quan sát có thể được quét tại thời điểm dự kiến (ví dụ, theo chu kỳ hoặc thường xuyên) và nhận dạng của ứng dụng mở có thể thu được. Ví dụ, khoảng thời gian để quét tại thời điểm dự kiến có thể được đặt nếu cần. Ví dụ như, khoảng thời gian để quét có thể là khoảng 0,1 giây hoặc khoảng 0,5 giây hoặc khoảng thời gian phù hợp bất kỳ khác. Để thực hiện việc quét tại thời điểm dự kiến, khi hệ thống thiết bị chẳng hạn như hệ thống Android khởi động, thì luồng có thể được mở ở giai đoạn sau. Sử dụng vòng luồng, đầu chồng của chồng giao diện quan sát có thể được quét liên tục trong khoảng thời gian ngắn.

Ví dụ, quản lý hoạt động (ActivityManager) (ví dụ, công cụ quản lý việc xem) có thể được sử dụng để thu được hoạt động diễn ra nhiều nhất (topActivity) (ví dụ, giao diện quan sát hiện hành) của các chương tình/nhiệm vụ chạy hiện hành, ví dụ, sử dụng các nhiệm vụ chạy các ứng dụng (getRunningTasks) (ví dụ, công cụ để thu tuyển tập ứng dụng). Nhận dạng của ứng dụng được mở (hoặc nhận dạng ứng dụng) và tên của hoạt động (Activity) (hoặc tên hoạt động) sau đó có thể thu được qua hoạt động diễn ra nhiều nhất. Nhận dạng ứng dụng, ví dụ, có thể bao gồm tên ứng dụng, ID ứng dụng (nghĩa là, mã nhận dạng), và/hoặc sự kết hợp của chúng. Theo một phương án, tên hoạt động có thể là tên của giao diện ứng dụng. Mỗi trong số các ứng dụng có thể có nhiều giao diện và mỗi giao diện có thể tương ứng với hoạt động (ví dụ, giao diện quan sát).

Phương pháp ví dụ khác để quét ứng dụng mở hoặc đang chạy có thể bao gồm giám sát các nhật ký (log); phân tích cú pháp (hoặc biên dịch) thông tin của các mục khởi động trong các log, và thu nhận dạng của ứng dụng mở. Ví dụ, khi hệ thống Android khởi động, các log liên quan đến quản lý hoạt động có thể được tạo ra. Log có thể chứa lệnh đang khởi động hoặc KHỞI ĐỘNG (ví dụ,

bao gồm các mục khởi động), nhận dạng của ứng dụng mở (hoặc nhận dạng ứng dụng), và tên hoạt động.

Do đó, luồng có thể được mở ở giai đoạn sau để giám sát công cụ dòng lệnh để ghi nhật ký các thông báo hệ thống (logcat) và phát hiện log mà chỉ báo ứng dụng bắt đầu. Khi logcat được phát hiện, mỗi đường thông tin trong logcat có thể được phân tích cú pháp (hoặc biên dịch), vị trí "cmp" ở lần xuất hiện thứ nhất trong logcat có thể được định vị. Chuỗi ký tự bị chặn từ vị trí định vị có thể gồm nhận dạng ứng dụng và/hoặc tên hoạt động hiển thị hiện hành. Thông tin về các mục khởi động có thể gồm nhận dạng ứng dụng khởi động, tên hoạt động, v.v..

Trong bước S120, nhận dạng ứng dụng được so sánh với nhận dạng ứng dụng đích lưu sẵn.

Ví dụ, nhận dạng ứng dụng đích lưu sẵn gọi là nhận dạng ứng dụng được chọn mà cần sự bảo mật và bí mật ứng dụng. Nhận dạng ứng dụng đích có thể gồm tên của ứng dụng đích, ID ứng dụng đích, và/hoặc sự kết hợp của chúng. Nhận dạng ứng dụng (quét) có thể chứa nội dung giống như hoặc theo cách khác tương thích với các nội dung được chứa trong nhận dạng ứng dụng đích lưu sẵn. Do đó, nếu ứng dụng đích chứa tên của ứng dụng đích, thì nhận dạng ứng dụng có thể chứa tên của ứng dụng để so sánh.

Trong bước S130, khi nhận dạng ứng dụng được so sánh tương thích với nhận dạng ứng dụng đích, giao diện mở khóa được hiển thị.

Ví dụ, nhận dạng ứng dụng và nhận dạng ứng dụng đích có thể được so sánh với nhau. Nếu chúng tương thích với nhau, giao diện mở khóa có thể được hiển thị. Theo một phương án, nhận dạng ứng dụng có thể chứa tên ứng dụng, và tên ứng dụng có thể gồm chuỗi ký tự. Các tên của các ứng dụng đích lưu sẵn có thể được chứa trong danh sách bộ nhớ. Chuỗi ký tự của tên của ứng dụng quét có thể được so sánh từng cái với các chuỗi ký tự của các tên của các ứng dụng đích trong danh sách bộ nhớ. Nếu chúng tương thích với nhau, giao diện mở

khóa có thể được hiển thị.

Ngoài ra, theo các phương án khác, nhận dạng ứng dụng có thể gồm ID ứng dụng, và các ID ứng dụng đích có thể được chứa trong danh sách bộ nhớ. ID ứng dụng có thể được so sánh từng ID ứng dụng một với các ID ứng dụng đích chứa trong danh sách bộ nhớ. Khi chúng tương thích với nhau, giao diện mở khóa có thể được hiển thị. Theo cách khác, nhận dạng ứng dụng có thể gồm ID ứng dụng và tên ứng dụng, và các ID ứng dụng đích và các tên của ứng dụng đích cùng nhau được lưu giữ trong danh sách bộ nhớ. ID và tên ứng dụng có thể được so sánh từng cái với các ID đích và tên của ứng dụng chứa trong danh sách bộ nhớ. Nếu ID ứng dụng và ID ứng dụng đích tương thích với nhau và tên ứng dụng quét tương thích với tên ứng dụng đích, giao diện mở khóa có thể được hiển thị.

Giao diện mở khóa có thể gồm giao diện mở khóa để nhập mật khẩu và/hoặc giao diện mở khóa để trượt mẫu trên giao diện mở khóa. Giao diện mở khóa để nhập mật khẩu có thể hiển thị hộp nhập ký tự, các số, các chữ, các khóa, v.v.. Ví dụ, mật khẩu có thể là các số, các chữ, hoặc kết hợp của các số và các chữ. Theo phương án ví dụ, mật khẩu có thể được tạo ra bằng cách kết hợp từ 1 đến 16 ký tự mà không giới hạn. Mặt khác, giao diện mở khóa để trượt mẫu trên giao diện mở khóa có thể sử dụng mẫu ngầm định để mở khóa ứng dụng.

Fig.2 minh họa phương pháp ví dụ để mở khóa mật khẩu bằng cách trượt mẫu trên giao diện mở khóa. Như được thể hiện trong ví dụ trên Fig.2, bộ mẫu để trượt (hoặc mẫu trượt) có thể là bộ mẫu mở khóa theo mẫu có dạng hình chữ "Z" để trượt trên đó để mở khóa ứng dụng. Mẫu trượt để mở khóa ứng dụng này có thể được ghi. Ngoài ra, việc kiểm soát "Vẽ lại" và kiểm soát thông báo “Tiếp theo” có thể cũng được thể hiện trên giao diện mở khóa mẫu được thể hiện trên Fig.2.

Fig.3 minh họa giao diện mở khóa ví dụ khác có mẫu để trượt (hoặc mẫu trượt). Trên giao diện mở khóa mẫu, thông báo “Vẽ mẫu mở khóa" và kiểm soát

"Quên mật khẩu" có thể được đặt. Nếu mẫu vẽ di động là chính xác, mật khẩu có thể bị mở khóa và ứng dụng có thể bị truy cập.

Trở lại Fig.1, trong bước S140, lệnh mở khóa có thể thu được để chạy ứng dụng. Ví dụ, lệnh mở khóa có thể được tạo ra bằng cách nhập mật khẩu trên giao diện mở khóa (hoặc giao diện mật khẩu); trong khi lệnh mở khóa cũng có thể được tạo ra bởi mẫu vẽ di động được nhập vào bằng cách trượt mẫu trên giao diện mở khóa.

Ngoài ra, theo một phương án, phương pháp kiểm soát việc truy cập vào ứng dụng trên thiết bị đầu cuối di động có thể còn bao gồm các bước: dừng quét các ứng dụng khi phát hiện ra rằng màn hình của điện thoại di động tắt hoặc điện thoại di động ở chế độ chờ (standby). Ví dụ, trong suốt quá trình quét khi phát hiện ra rằng màn hình của thiết bị đầu cuối di động tắt hoặc điện thoại di động ở chế độ chờ, nghĩa là, không có các ứng dụng mới được mở, việc quét ứng dụng có thể bị dừng tại thời điểm này. Việc này có thể tiết kiệm năng lượng sử dụng để quét các ứng dụng trên điện thoại di động.

Fig.4 minh họa hệ thống ví dụ để kiểm soát việc truy cập vào ứng dụng trên thiết bị đầu cuối di động. Hệ thống ví dụ có thể bao gồm môđun quét 10, môđun so sánh 20, môđun hiển thị 30, và/hoặc môđun thực hiện 40.

Môđun quét 10 có thể được tạo cấu hình để quét ứng dụng mở hoặc ứng dụng đang chạy để thu được nhận dạng ứng dụng.

Như được thể hiện trên Fig.5, môđun quét 10 gồm môđun quét đầu chồng 501. Môđun quét đầu chồng 501 có thể được sử dụng để quét, tại thời điểm dự kiến (ví dụ, theo chu kỳ hoặc thường xuyên), đầu chồng của chồng giao diện quan sát để thu được nhận dạng của ứng dụng mở. Khoảng thời gian để quét tại thời điểm dự kiến có thể được đặt nếu cần. Theo ví dụ, khoảng thời gian để quét có thể là khoảng 0,1 giây hoặc khoảng 0,5 giây hoặc khoảng thời gian phù hợp bất kỳ khác. Để thực hiện việc quét tại thời điểm dự kiến, khi hệ thống thiết bị như hệ thống Android khởi động, luồng có thể được mở ra ở trạng thái ngược.

Sử dụng vòng luồn chương trình đang chạy, đầu chồng của chồng giao diện quan sát có thể được quét liên tục trong khoảng thời gian ngắn.

Ví dụ, quản lý hoạt động (ví dụ, công cụ quản lý việc xem) có thể được sử dụng để thu được hoạt động diễn ra nhiều nhất (ví dụ, giao diện quan sát hiện hành của các chương trình/nhiệm vụ chạy hiện hành, ví dụ, sử dụng các nhiệm vụ chạy các ứng dụng (ví dụ, công cụ để thu thập nhiệm vụ). Nhận dạng của ứng dụng mở (hoặc nhận dạng ứng dụng) và tên của hoạt động (hoặc tên hoạt động) sau đó có thể thu được qua hoạt động diễn ra nhiều nhất. Nhận dạng ứng dụng ví dụ có thể gồm tên ứng dụng, ID ứng dụng (nghĩa là, mã nhận dạng), và/hoặc sự kết hợp của chúng. Theo một phương án, tên hoạt động có thể là tên của giao diện ứng dụng. Mỗi ứng dụng có thể có nhiều giao diện và mỗi giao diện có thể tương ứng với hoạt động (ví dụ, giao diện quan sát).

Trên Fig.6, theo một phương án, môđun quét 10 bao gồm gồm môđun giám sát log 602 và môđun phân tích cú pháp 604. Môđun giám sát log 602 có thể được sử dụng để giám sát log. Môđun phân tích cú pháp 604 có thể được sử dụng để phân tích cú pháp (hoặc biên dịch) thông tin về các mục khởi động trong các log, và để thu được nhận dạng của ứng dụng mở. Ví dụ, khi hệ thống Android khởi động, thì các log liên quan đến việc quản lý hoạt động có thể được tạo ra. Log có thể chứa lệnh đang khởi động hoặc KHỞI ĐỘNG (ví dụ, gồm việc khởi động các mục), nhận dạng của ứng dụng mở (hoặc nhận dạng ứng dụng), và tên hoạt động.

Do đó, luồng có thể được mở ở giai đoạn sau để giám sát logcat và phát hiện log mà chỉ ra ứng dụng khởi động. Môđun giám sát log 602 có thể là luồng sử dụng để giám sát logcat. Môđun giám sát log 602 có thể phát hiện logcat, trong lúc môđun phân tích cú pháp 604 có thể phân tích cú pháp (hoặc biên dịch) mỗi dòng thông tin về logcat và vị trí định vị của thời gian thứ nhất "cmp" xuất hiện. Chuỗi bị chắn từ vị trí định vị có thể được nhận dạng ứng dụng và tên hoạt động hiển thị hiện hành. Thông tin về các mục khởi động có thể gồm nhận dạng ứng dụng khởi động, tên hoạt động, v.v.. Chuỗi ký tự bị chắn từ vị trí định

vị có thể gồm nhận dạng ứng dụng và/hoặc tên hoạt động hiển thị hiện hành. Thông tin về các mục khởi động có thể gồm nhận dạng ứng dụng khởi động, tên hoạt động, v.v..

Môđun so sánh 20 có thể được tạo cấu hình để so sánh nhận dạng ứng dụng với nhận dạng ứng dụng đích lưu sẵn.

Ví dụ, nhận dạng ứng dụng đích lưu sẵn gọi là nhận dạng ứng dụng được chọn cần sự bảo mật và bí mật ứng dụng. Nhận dạng ứng dụng đích có thể gồm tên của ứng dụng đích, ID ứng dụng đích, và/hoặc sự kết hợp của chúng. Nhận dạng ứng dụng (đã quét) có thể chứa nội dung giống như hoặc theo cách khác tương thích với các nội dung được chứa trong nhận dạng ứng dụng đích lưu sẵn. Do đó, nếu ứng dụng đích chứa tên của ứng dụng đích, nhận dạng ứng dụng có thể chứa tên của ứng dụng để so sánh.

Môđun hiển thị 30 có thể được tạo cấu hình để hiển thị giao diện mở khóa, khi nhận dạng ứng dụng tương thích với nhận dạng ứng dụng đích.

Theo một phương án, nhận dạng ứng dụng có thể chứa tên ứng dụng, và tên ứng dụng có thể gồm chuỗi ký tự. Các tên của các ứng dụng đích lưu sẵn có thể được chứa trong danh sách bộ nhớ. Môđun so sánh 20 có thể được tạo cấu hình để so sánh chuỗi ký tự của tên ứng dụng từng cái với các chuỗi ký tự của các tên của các ứng dụng đích trong danh sách bộ nhớ. Nếu chúng tương thích với nhau, môđun hiển thị 30 có thể được tạo cấu hình để hiển thị giao diện mở khóa.

Ngoài ra, theo các phương án khác, nhận dạng ứng dụng có thể gồm ID ứng dụng, và các ID ứng dụng đích có thể được chứa trong danh sách bộ nhớ. ID ứng dụng có thể được so sánh từng ID một với các ID ứng dụng đích chứa trong danh sách bộ nhớ. Khi các ID này tương thích với nhau, giao diện mở khóa có thể được hiển thị. Theo cách khác, nhận dạng ứng dụng có thể gồm ID ứng dụng và tên ứng dụng, và các ID và tên ứng dụng đích cùng được lưu trữ trong danh sách bộ nhớ. ID và tên ứng dụng có thể được so sánh từng ID và tên ứng dụng một với các ID và tên ứng dụng đích được chứa trong danh sách bộ nhớ. Nếu ID

ứng dụng và ID ứng dụng đích tương thích với nhau và tên ứng dụng quét phù hợp với tên ứng dụng đích, giao diện mở khóa có thể được hiển thị.

Giao diện mở khóa có thể gồm giao diện mở khóa để nhập mật khẩu và/hoặc giao diện mở khóa để trượt mẫu trên giao diện mở khóa. Giao diện mở khóa để nhập mật khẩu có thể hiển thị hộp nhập ký tự, các số, các chữ, các khóa, v.v.. Ví dụ, mật khẩu có thể là các số, các chữ, hoặc kết hợp của các số và các chữ. Theo phương án ví dụ, mật khẩu có thể được tạo ra bằng cách kết hợp khoảng từ 1 đến 16 ký tự không có giới hạn. Mặt khác, giao diện mở khóa để trượt mẫu trên giao diện mở khóa có thể sử dụng mẫu ngầm định để mở khóa ứng dụng, Ví dụ, như được minh họa trên các hình từ Fig.2 đến Fig.3.

Môđun thực hiện 40 được tạo cấu hình để thu được lệnh mở khóa để chạy ứng dụng. Ví dụ, lệnh mở khóa có thể được tạo ra bằng cách nhập mật khẩu trên giao diện mở khóa (hoặc giao diện mật khẩu); trong lúc lệnh mở khóa có thể cũng có thể được tạo ra bởi mẫu vẽ di động được nhập bằng cách trượt mẫu trên giao diện mở khóa.

Ngoài ra, theo một phương án, ứng dụng quét có thể bị dừng, khi môđun quét 10 phát hiện rằng màn hình của điện thoại di động tắt hoặc điện thoại di động ở chế độ chờ. Ví dụ, trong suốt quá trình quét khi phát hiện ra rằng màn hình của thiết bị đầu cuối di động tắt hoặc điện thoại di động ở chế độ chờ, nghĩa là, không có các ứng dụng mới được mở hoặc chạy, ứng dụng quét có thể bị dừng tại thời điểm này. Điều này có thể tiết kiệm điện sử dụng dung để quét các ứng dụng trên điện thoại di động.

Các phương pháp và các hệ thống kiểm soát việc truy cập vào ứng dụng trên thiết bị đầu cuối di động đã bộc lộ có thể so sánh nhận dạng ứng dụng với nhận dạng ứng dụng đích lưu sẵn. Khi nhận dạng ứng dụng tương thích với ứng dụng đích lưu sẵn, giao diện mở khóa có thể được hiển thị. Chỉ sau khi lệnh mở khóa thu được để mở khóa mật khẩu trên giao diện mở khóa, ứng dụng tương ứng có thể được truy cập. Sự bảo mật truy cập các ứng dụng có thể được nâng

cao. Sự bảo mật dữ liệu bên trong thiết bị đầu cuối di động có thể được đảm bảo.

Hơn nữa, so sánh với việc kiểm tra liên tục đầu chồng của ứng dụng nhận dạng, việc quét log có thể tiết kiệm điện và kéo dài thời gian sử dụng của thiết bị đầu cuối di động. Việc quét ứng dụng có thể bị dừng để tiết kiệm điện dung để quét, khi màn hình của thiết bị đầu cuối di động tắt hoặc khi thiết bị đầu cuối di động ở chế độ chờ. Điều này là thân thiện đối với người dùng để tạo ra các lựa chọn khác nhau cho người dùng chọn, ví dụ, bằng cách tạo ra giao diện mở khóa để nhập mật khẩu và bằng cách tạo ra giao diện mở khóa để trượt mẫu trên đó.

Theo các phương án khác nhau, thiết bị đầu cuối di động có thể được thực hiện trên hệ điều hành máy tính phù hợp. Fig.7 thể hiện sơ đồ khối của hệ thống máy tính ví dụ 700 có thể thực hiện thiết bị đầu cuối di động. Hệ thống máy tính 700 có thể bao gồm bộ xử lý 702, phương tiện lưu trữ 704, bộ giám sát 706, môđun truyền thông 708, cơ sở dữ liệu 710, và các thiết bị ngoại vi 712. Các thiết bị nhất định có thể được bỏ qua và có thể có các thiết bị khác.

Bộ xử lý 702 có thể gồm bộ xử lý hoặc các bộ xử lý thích hợp bất kỳ. Ngoài ra, bộ xử lý 702 có thể bao gồm nhiều lõi cho nhiều luồng hoặc xử lý song song. Phương tiện lưu trữ 704 có thể bao gồm các môđun bộ nhớ, chẳng hạn như ROM, RAM, và các mô đun bộ nhớ tia chớp, và các lưu giữ khối, chẳng hạn như CD-ROM, đĩa hình chữ U, đĩa cứng, v.v.. Phương tiện lưu trữ 704 có thể lưu trữ các chương trình máy tính để thực hiện các quy trình khác nhau, khi được xử lý bởi bộ xử lý 702.

Ngoài ra, các thiết bị ngoại vi 712 có thể bao gồm các thiết bị I/O chẳng hạn như bàn phím và chuột, và môđun truyền thông 708 có thể gồm các thiết bị mạng để thiết lập các kết nối qua mạng truyền thông vô tuyến và hữu tuyến. Cơ sở dữ liệu 710 có thể gồm một hoặc nhiều cơ sở dữ liệu để lưu trữ dữ liệu nhất định và để thực hiện thao tác nhất định trên dữ liệu được lưu trữ, như tìm kiếm cơ sở dữ liệu.

Trong các phương án khác nhau, các môđun được bộc lộ cho hệ thống ví

dụ được minh họa ở trên có thể được tạo cấu hình trong một thiết bị hoặc được tạo cấu hình trong nhiều thiết bị như mong muốn. Các môđun được bộc lộ ở đây có thể được tích hợp trong một môđun hoặc trong nhiều môđun để xử lý các thông báo. Mỗi trong số các môđun được bộc lộ ở đây có thể được chia thành một hoặc nhiều môđun con, mà có thể được tái kết cấu theo cách bất kỳ.

Các phương án đã bộc lộ chỉ đơn thuần là các ví dụ. Người có trình độ trung bình trong lĩnh vực cần hiểu rằng, phần mềm và/hoặc phần cứng phù hợp (ví dụ, hệ điều hành phần cứng vạn năng) có thể được bao gồm và được sử dụng để thực hiện các phương pháp đã được bộc lộ. Ví dụ, các phương án đã bộc lộ có thể được thực hiện chỉ bằng phần cứng, hoặc theo cách khác, phương án này có thể được thực hiện chỉ bằng các sản phẩm phần mềm. Các sản phẩm phần mềm có thể được lưu trữ trong phương tiện lưu trữ. Các sản phẩm phần mầm có thể bao gồm các lệnh thích hợp để cho phép thiết bị khách hàng bất kỳ (ví dụ, bao gồm điện thoại di động, máy tính cá nhân, máy chủ, hoặc thiết bị mạng, v.v.) thực hiện các phương án đã bộc lộ.

Các ứng dụng, các lợi ích, các thay đổi, các cải biến khác hoặc tương đương với các phương án đã bộc lộ là hiển nhiên đối với chuyên gia trong lĩnh vực và dự định nằm trong phạm vi của sáng chế.

Khả năng ứng dụng trong công nghiệp

Các phương án được nêu trên chỉ nhằm mục đích minh họa mà không nhằm giới hạn phạm vi của yêu cầu bảo hộ và/hoặc phần mô tả bất kỳ, các ví dụ về khả năng áp dụng công nghiệp và các ưu điểm nhất định. Các thay đổi, các cải biến hoặc tương đương với các giải pháp kỹ thuật của các phương án đã bộc lộ có thể là hiển nhiên đối với người có trình độ trung bình trong lĩnh vực và có thể được bao gồm trong phần mô tả này.

Các phương pháp và các hệ thống kiểm soát việc truy cập vào các ứng dụng trên thiết bị đầu cuối di động được bộc lộ có thể so sánh nhận dạng ứng dụng sau khi quét, với nhận dạng ứng dụng đích lưu sẵn. Khi nhận dạng ứng

dụng đã quét tương thích với hoặc phù hợp với ứng dụng đích lưu sẵn, giao diện mở khóa có thể được hiển thị. Sau khi được mở khóa bằng cách thu lệnh mở khóa trên giao diện mở khóa, các ứng dụng tương ứng sau đó có thể được chạy trên giao diện mở khóa. Sự bảo mật truy cập vào các ứng dụng có thể được nâng cao. Sự bảo mật dữ liệu của thiết bị đầu cuối di động có thể được đảm bảo.

Trong phương pháp kiểm soát việc truy cập vào ứng dụng trên thiết bị đầu cuối di động ví dụ, ứng dụng mở có thể được quét và nhận dạng ứng dụng có thể thu được. Nhận dạng ứng dụng có thể được so sánh với nhận dạng ứng dụng đích lưu sẵn. Giao diện mở khóa có thể được hiển thị, khi nhận dạng ứng dụng được so sánh tương thích với nhận dạng ứng dụng đích lưu sẵn. Lệnh mở khóa có thể thu được để chạy ứng dụng trên thiết bị đầu cuối di động.

Hệ thống kiểm soát việc truy cập vào ứng dụng trên thiết bị đầu cuối di động ví dụ có thể gồm môđun quét, môđun so sánh, môđun hiển thị, và môđun thực hiện. Môđun quét có thể được tạo cấu hình để quét ứng dụng mở và để thu được nhận dạng ứng dụng. Môđun so sánh có thể được tạo cấu hình để so sánh nhận dạng ứng dụng với nhận dạng ứng dụng đích lưu sẵn. Môđun hiển thị có thể được tạo cấu hình để hiển thị giao diện mở khóa, khi nhận dạng ứng dụng được so sánh là tương thích với nhận dạng ứng dụng đích lưu sẵn. Môđun thực hiện có thể được tạo cấu hình để thu được lệnh mở khóa để chạy ứng dụng.

Danh mục các số chỉ dẫn

YÊU CẦU BẢO HỘ

1. Phương pháp kiểm soát việc truy cập vào ứng dụng trên thiết bị đầu cuối di động, bao gồm các bước:

mở luồng ở giai đoạn sau bởi bộ xử lý của thiết bị đầu cuối di động khi thiết bị đầu cuối di động khởi động;

quét liên tục ứng dụng mở hiện hành và thu được nhận dạng ứng dụng của ứng dụng mở hiện hành tại khoảng thời gian dự kiến bằng việc lặp luồng như hoạt động giai đoạn sau, trong đó ứng dụng mở hiện hành được liên kết với một hoặc nhiều giao diện quan sát bao gồm giao diện quan sát hiện hành, và luồng được tạo cấu hình để quét đầu chồng của chồng các giao diện quan sát trên thiết bị đầu cuối di động để thu được giao diện quan sát hiện hành, và để thu được nhận dạng ứng dụng từ giao diện quan sát hiện hành;

so sánh nhận dạng ứng dụng với nhận dạng ứng dụng đích lưu sẵn, trong đó nhận dạng ứng dụng đích lưu sẵn được lưu trữ trong danh sách bộ nhớ trong thiết bị đầu cuối di động;

hiển thị giao diện mở khóa để nhập hành động mở khóa, khi nhận dạng ứng dụng được so sánh là tương thích với nhận dạng ứng dụng đích lưu sẵn; và

thu được lệnh mở khóa để truy cập ứng dụng mở hiện hành trên thiết bị đầu cuối di động, trong đó lệnh mở khóa được tạo ra khi hành động mở khóa được chấp nhận.

2. Phương pháp theo điểm 1, trong đó việc quét ứng dụng mở và việc thu được nhận dạng ứng dụng bao gồm các bước:

giám sát các nhật ký (log);

phân tích cú pháp thông tin của các mục khởi động trong các log, bao gồm định vị lần xuất hiện thứ nhất của vị trí của phần giữ chỗ bộ phận, và chặn chuỗi ký tự từ vị trí định vị; và

thu được nhận dạng ứng dụng.

3. Phương pháp theo điểm 1, trong đó giao diện mở khóa bao gồm giao diện mở khóa để nhập mật khẩu, giao diện mở khóa để trượt mẫu trên giao diện mở khóa, và sự kết hợp của chúng.

4. Phương pháp theo điểm 2, ngoài ra còn bao gồm bước:

dừng quét ứng dụng mở hiện hành trên thiết bị đầu cuối di động, khi màn hình của thiết bị đầu cuối di động tắt hoặc thiết bị đầu cuối di động ở chế độ chờ.

5. Phương pháp theo điểm 2, trong đó:

thiết bị đầu cuối di động chạy hệ điều hành ANDROID;

giám sát các log bao gồm mở luồng ở giai đoạn sau để giám sát công cụ dòng lệnh để ghi nhật ký các thông báo hệ thống (logcat); và

phần giữ chỗ bộ phận là cmp.

6. Phương pháp theo điểm 1, trong đó việc so sánh nhận dạng ứng dụng với nhận dạng ứng dụng đích lưu sẵn bao gồm bước:

so sánh mã nhận dạng (ID) ứng dụng và chuỗi ký tự của tên của nhận dạng ứng dụng từng cái với các ID ứng dụng và các chuỗi ký tự của các tên của các ứng dụng đích trong danh sách bộ nhớ.

7. Hệ thống kiểm soát việc truy cập vào ứng dụng trên thiết bị đầu cuối di động, bao gồm:

một hoặc nhiều bộ xử lý trong thiết bị đầu cuối di động;

bộ nhớ trong thiết bị đầu cuối di động; và

một hoặc nhiều môđun chương trình được lưu trữ trong bộ nhớ và cần được thực hiện bởi một hoặc nhiều bộ xử lý, một hoặc nhiều môđun chương trình bao gồm:

môđun quét, được tạo cấu hình để mở luồng ở giai đoạn sau khi thiết bị đầu cuối di động khởi động, để quét liên tục ứng dụng mở hiện hành và thu được nhận dạng ứng dụng của ứng dụng mở hiện hành tại khoảng thời gian dự kiến bằng việc lặp luồng như hoạt động giai đoạn sau, trong đó ứng dụng mở hiện hành được liên kết với một hoặc nhiều giao diện quan sát bao gồm giao diện quan sát hiện hành, và luồng được tạo cấu hình để quét đầu chồng của chồng các giao diện quan sát trên thiết bị đầu cuối di động để thu được giao diện quan sát hiện hành, và để thu được nhận dạng ứng dụng từ giao diện quan sát hiện hành;

môđun so sánh, được tạo cấu hình để so sánh nhận dạng ứng dụng với nhận dạng ứng dụng đích lưu sẵn, trong đó nhận dạng ứng dụng đích lưu sẵn được lưu trữ trong danh sách bộ nhớ trong thiết bị đầu cuối di động;

môđun hiển thị, được tạo cấu hình để hiển thị giao diện mở khóa để nhập hành động mở khóa, khi nhận dạng ứng dụng được so sánh là tương thích với nhận dạng ứng dụng đích lưu sẵn; và

môđun thực hiện, được tạo cấu hình để thu được lệnh mở khóa để truy cập ứng dụng mở hiện hành, trong đó lệnh mở khóa được tạo ra khi hành động mở khóa được chấp nhận.

8. Hệ thống theo điểm 7, trong đó môđun quét bao gồm:

môđun giám sát log, được tạo cấu hình để giám sát các log; và

môđun phân tích cú pháp, được tạo cấu hình để phân tích cú pháp thông tin của các mục khởi động trong các log và để thu được nhận dạng ứng dụng;

trong đó việc phân tích cú pháp thông tin của các mục khởi động trong các log bao gồm định vị lần xuất hiện thứ nhất của vị trí của phần giữ chỗ bộ phận, và chặn chuỗi ký tự từ vị trí định vị.

9. Hệ thống theo điểm 8, trong đó giao diện mở khóa bao gồm giao diện mở khóa để nhập mật khẩu, giao diện mở khóa để trượt mẫu trên giao diện mở khóa, và sự kết hợp của chúng.

10. Hệ thống theo điểm 7, trong đó môđun quét được tạo cấu hình để dừng quét ứng dụng trên thiết bị đầu cuối di động, khi màn hình của thiết bị đầu cuối di động tắt hoặc thiết bị đầu cuối di động ở chế độ chờ.

11. Hệ thống theo điểm 7, trong đó môđun so sánh được tạo cấu hình để:

so sánh ID ứng dụng và chuỗi ký tự của tên của nhận dạng ứng dụng từng cái với các ID ứng dụng và các chuỗi ký tự của các tên của các ứng dụng đích trong danh sách bộ nhớ.

Fig. 1

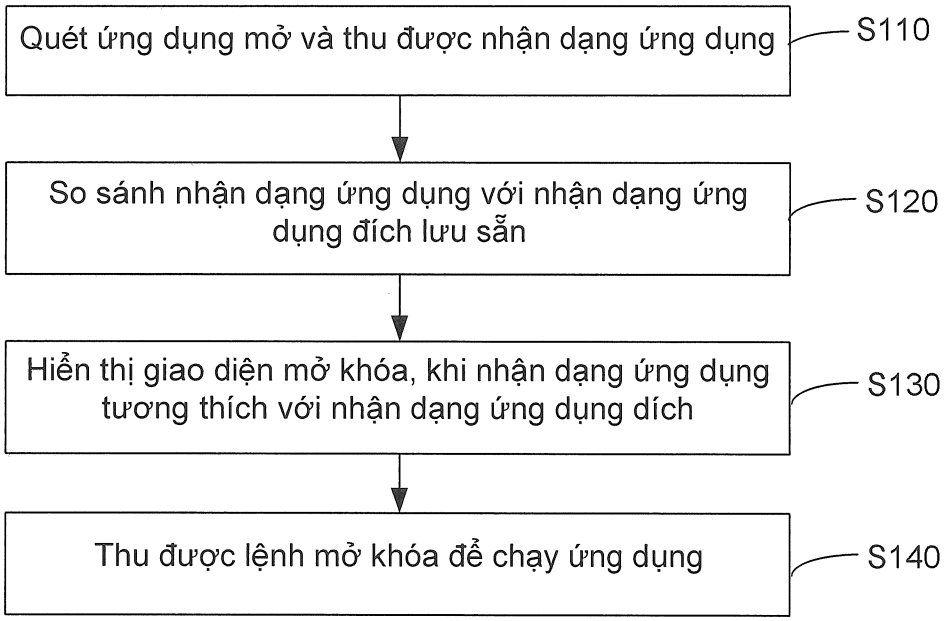

Quét ứng dụng mở và thu được nhận dạng ứng dụng
S110
So sánh nhận dạng ứng dụng với nhận dạng ứng dụng đích lưu sẵn
S120
Hiển thị giao diện mở khóa, khi nhận dạng ứng dụng tương thích với nhận dạng ứng dụng đích
S130
Thu được lệnh mở khóa để chạy ứng dụng
S140

Fig. 2

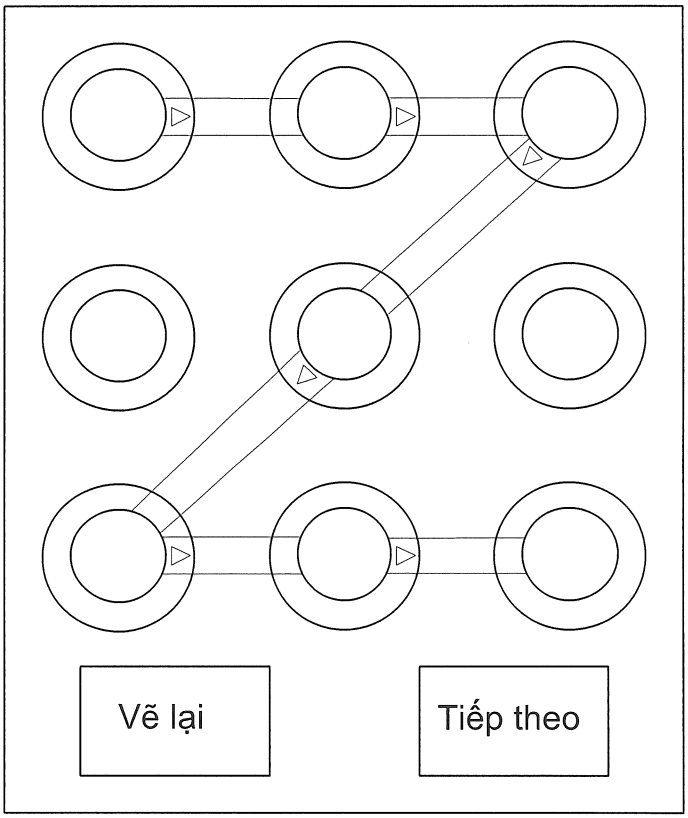


Fig. 3

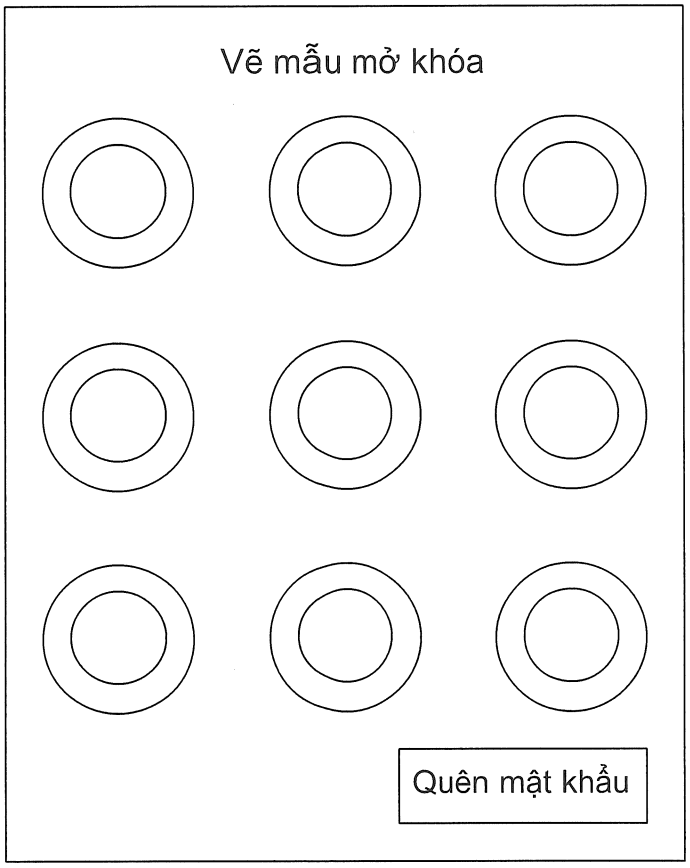


Fig. 4

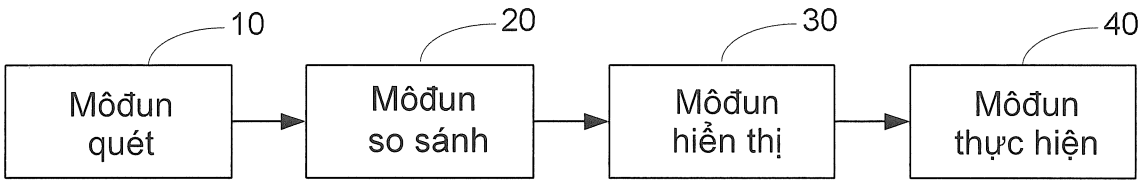


Fig. 5

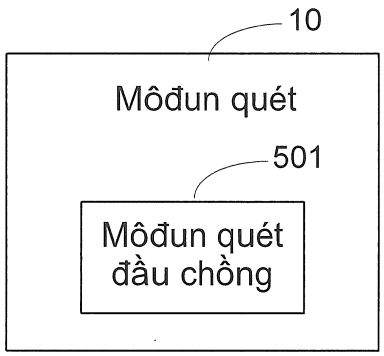


Fig. 6

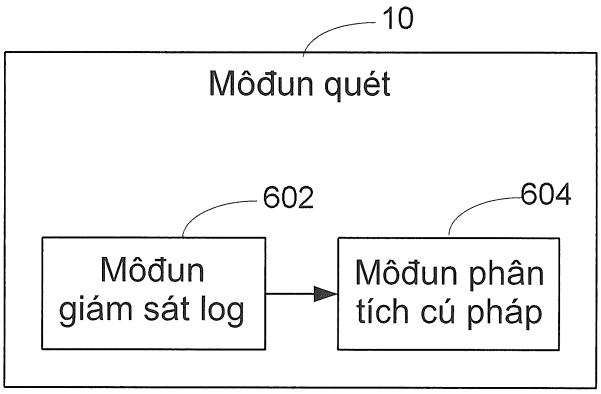
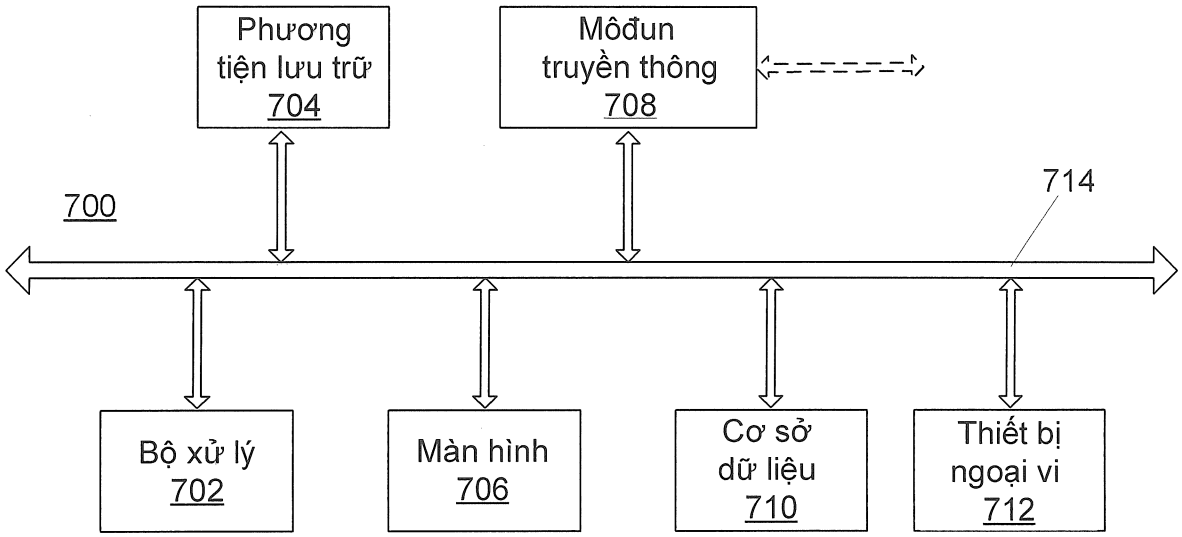


Fig. 7


Phương tiện lưu trữ 704
Môđun truyền thông 708
700
714
Bộ xử lý 702
Màn hình 706
Cơ sở dữ liệu 710
Thiết bị ngoại vi 712