(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) **1-0043441**

(51)[8] **G06F 21/62**

(13) **B**

(21) 1-2018-02834
(22) 09/11/2016
(86) PCT/CN2016/105159 09/11/2016
(87) WO 2017/092553 08/06/2017
(30) 201510859719.5 30/11/2015 CN
(45) 25/02/2025 443
(43) 27/08/2018 365A
(73) HUAWEI TECHNOLOGIES CO., LTD. (CN)
Huawei Administration Building, Bantian, Longgang District Shenzhen, Guangdong 518129, China
(72) YAO, Dongdong (CN).
(74) Công ty TNHH một thành viên Sở hữu trí tuệ VCCI (VCCI-IP CO.,LTD)

(54) PHƯƠNG PHÁP CHUYỂN ĐỔI GIAO DIỆN NGƯỜI DÙNG VÀ THIẾT BỊ ĐẦU CUỐI

(21) 1-2018-02834

(57) Sáng chế đề cập đến phương pháp chuyển đổi giao diện người dùng và thiết bị đầu cuối. Sau khi thiết bị đầu cuối kích hoạt yêu cầu hiển thị giao diện người dùng tin cậy (TUI-Trusted user interface) của ứng dụng máy khách (CA-Client application) theo hoạt động thứ nhất trên giao diện ứng dụng máy khách (CA) bởi người dùng, thiết bị đầu cuối chuyển đổi môi trường hiển thị của ứng dụng máy khách (CA) từ môi trường thực thi đầy đủ (REE-Rich execution environment) thành môi trường thực thi tin cậy (TEE-Trusted execution environment) theo yêu cầu hiển thị TUI, và sau đó hiển thị giao diện ứng dụng tin cậy (TA-Trusted application) mà của ứng dụng máy khách (CA) và nằm trong TEE. Trong trường hợp này, người dùng có thể thực hiện hoạt động nhập thông tin nhạy cảm trên giao diện ứng dụng tin cậy (TA), và chương trình độc hại mà chạy trong REE không thể truy nhập thiết bị phần cứng để thu nhận hoạt động nhập liệu trong TEE bởi người dùng. Do đó, khi hoạt động nhập liệu bởi người dùng được thực hiện bằng cách sử dụng phương pháp nêu trên, khả năng mà thông tin nhạy cảm của người dùng bị đánh cắp được ngăn ngừa, nhờ đó nâng cao một cách hiệu quả tính bảo mật của hoạt động nhập liệu bởi người dùng.

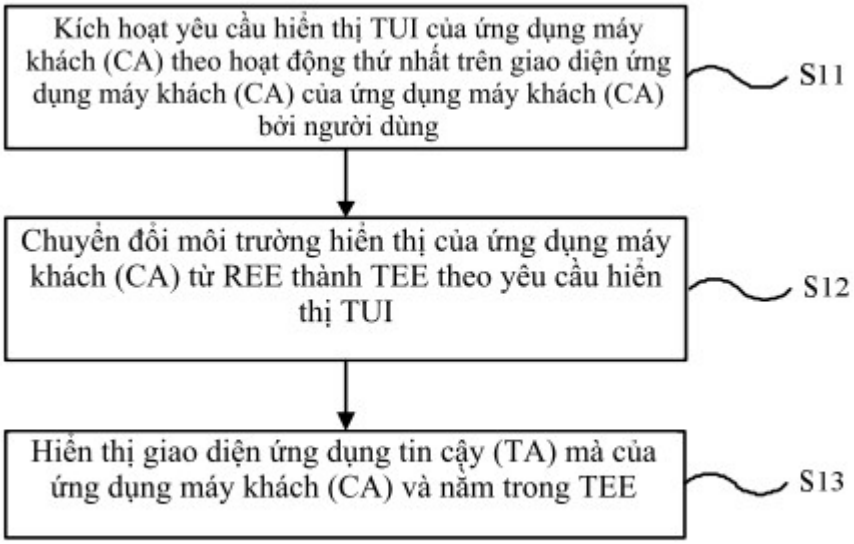

FIG. 2

Lĩnh vực kỹ thuật được đề cập

Sáng chế đề cập đến các kỹ thuật truyền thông, và cụ thể, đề cập đến phương pháp chuyển đổi giao diện người dùng và thiết bị đầu cuối.

Tình trạng kỹ thuật của sáng chế

Do các thiết bị đầu cuối thông minh như các điện thoại di động trở nên phổ biến, số lượng người dùng mua hàng trực tuyến bằng cách sử dụng trực tiếp các điện thoại di động tăng lên. Do đó, các vấn đề bảo mật trở nên khắt khe hơn. Hiện nay, trong các hệ điều hành chính như Android, các chương trình ứng dụng được cài đặt mà không có sự điều khiển và quản lý nghiêm ngặt. Một khi người dùng không cố ý cài đặt chương trình độc hại trên điện thoại di động, tính bảo mật của phần mềm như Alipay trên điện thoại di động có thể bị đe dọa.

Đối với phần mềm trả phí như Alipay trên điện thoại di động, các cơ chế để xác thực mật khẩu và mã hóa mật dữ liệu được cung cấp nội tại để đảm bảo tính bảo mật của việc truyền dữ liệu. Tuy nhiên, các bước quan trọng như việc nhập mật khẩu người dùng và việc nhập tài khoản người dùng chắc chắn bị bộc lộ trong môi trường phần mềm của hệ điều hành. Một khi các hoạt động nhập liệu này bị chặn bởi chương trình độc hại, thông tin nhạy cảm như mật khẩu người dùng và tài khoản người dùng có thể bị lấy cắp.

Giải pháp hiện tại để ngăn chương trình độc hại khỏi việc chặn hoạt động nhập liệu bởi người dùng là thiết lập bàn phím ngẫu nhiên. Cụ thể, khi người dùng thực hiện hoạt động nhập liệu, các phím của bàn phím được trộn ngẫu nhiên (tức là, các phím của bàn phím được bố trí ngẫu nhiên mỗi khi người dùng thực hiện hoạt động nhập liệu), để ngăn chương trình độc hại lấy cắp thông tin nhạy cảm như mật khẩu người dùng và tài khoản người dùng.

Tuy nhiên, giải pháp thiết lập bàn phím ngẫu nhiên này chỉ làm cho khó lấy cắp thông tin nhạy cảm hơn như mật khẩu người dùng và tài khoản người dùng. Chương trình độc hại có thể vẫn đọc bàn phím ngẫu nhiên và hoạt động nhập liệu bởi người. Do đó, tính bảo mật của giải pháp này cần được nâng cao.

Bản chất kỹ thuật của sáng chế

Đề giải quyết nhược điểm trong kỹ thuật đã biết, sáng chế đề xuất phương pháp chuyển đổi giao diện người dùng và thiết bị đầu cuối, để nâng cao tính bảo mật của việc nhập liệu bởi người dùng.

Theo khía cạnh thứ nhất của sáng chế, phương án của sáng chế đề xuất phương pháp chuyển đổi giao diện người dùng, trong đó phương pháp được sử dụng cho thiết bị đầu cuối, ứng dụng máy khách (CA) chạy trên thiết bị đầu cuối, môi trường thực thi đầy đủ và môi trường thực thi tin cậy được thiết lập trên thiết bị đầu cuối, và phương pháp này bao gồm: kích hoạt, bởi thiết bị đầu cuối, yêu cầu hiển thị giao diện người dùng tin cậy (TUI) của ứng dụng máy khách (CA) theo hoạt động thứ nhất trên giao diện ứng dụng máy khách (CA) của ứng dụng máy khách (CA) bởi người dùng; sau đó chuyển đổi môi trường hiển thị của ứng dụng máy khách (CA) từ môi trường thực thi đầy đủ thành môi trường thực thi tin cậy theo yêu cầu hiển thị TUI; và hiển thị giao diện ứng dụng tin cậy (TA) mà là của ứng dụng máy khách (CA) và nằm trong môi trường thực thi tin cậy, sao cho người dùng thực hiện hoạt động nhập thông tin nhảy cảm trên giao diện ứng dụng tin cậy (TA). Trong trường hợp này, chương trình độc hại mà chạy trong REE không thể truy nhập thiết bị phần cứng để đạt được hoạt động nhập liệu trong TEE bởi người dùng. Do đó, khi hoạt động nhập liệu bởi người dùng được thực hiện bằng cách sử dụng phương pháp nêu trên, khả năng mà thông tin nhạy cảm của người dùng bị đánh cắp được ngăn ngừa, nhờ đó nâng cao một cách hiệu quả tính bảo mật của hoạt động nhập liệu bởi người dùng.

Viện dẫn tới khía cạnh thứ nhất, theo cách thức thực hiện có thể thứ nhất của khía cạnh thứ nhất, thiết bị đầu cuối bao gồm thiết bị phần cứng liên

quan đến hiển thị, thiết bị phần cứng liên quan đến hiển thị này có cấu trúc để hiển thị giao diện ứng dụng máy khách (CA) và giao diện ứng dụng tin cậy (TA), và bước chuyển đổi môi trường hiển thị của ứng dụng máy khách (CA) từ môi trường thực thi đầy đủ thành môi trường thực thi tin cậy theo yêu cầu hiển thị TUI bao gồm:

điều khiển, theo yêu cầu hiển thị TUI của ứng dụng máy khách (CA) bằng cách sử dụng trình điều khiển mà của thiết bị phần cứng và nằm trong môi trường thực thi đầy đủ, thiết bị phần cứng để thoát khỏi chế độ không bảo mật hiện tại, trong đó chế độ không bảo mật này là chế độ đang chạy mà tương ứng với thiết bị phần cứng và nằm trong môi trường thực thi đầy đủ; và

điều khiển, theo thông tin chuyển đổi thứ nhất bằng cách sử dụng trình điều khiển mà của thiết bị phần cứng và nằm trong môi trường thực thi tin cậy, thiết bị phần cứng để đi vào chế độ bảo mật, trong đó thông tin chuyển đổi thứ nhất được sử dụng để chỉ báo rằng thiết bị phần cứng đã thoát khỏi chế độ không bảo mật, và chế độ bảo mật là chế độ đang chạy mà tương ứng với thiết bị phần cứng và nằm trong môi trường thực thi tin cậy.

Viện dẫn tới cách thức thực hiện có thể thứ nhất của khía cạnh thứ nhất, theo cách thức thực hiện có thể thứ hai của khía cạnh thứ nhất, bước hiển thị giao diện ứng dụng tin cậy (TA) mà của ứng dụng máy khách (CA) và nằm trong môi trường thực thi tin cậy bao gồm:

chạy, trong môi trường thực thi tin cậy, TA tương ứng với CA; và

hiển thị, trong môi trường thực thi tin cậy, giao diện ứng dụng tin cậy (TA) bằng cách viện dẫn tới thiết bị phần cứng trong chế độ bảo mật.

Viện dẫn tới khía cạnh thứ nhất, theo cách thức thực hiện có thể thứ ba của khía cạnh thứ nhất, phương pháp này còn bao gồm: chuyển đổi từ giao diện ứng dụng tin cậy (TA) hiện tại thành giao diện phản hồi của sự kiện thứ nhất trong môi trường thực thi đầy đủ theo bản tin phản hồi sự kiện không bảo mật, trong đó bản tin phản hồi sự kiện không bảo mật được kích hoạt bởi sự kiện thứ nhất trong môi trường thực thi đầy đủ; và

hiển thị giao diện ứng dụng tin cậy (TA) lần nữa theo bản tin hồi đáp

phản hồi, trong đó bản tin hồi đáp phản hồi chỉ báo rằng người dùng của thiết bị đầu cuối hoàn thành xử lý của sự kiện thứ nhất bằng cách sử dụng giao diện phản hồi. Phương pháp này có thể xử lý, trong xử lý hiển thị TUI, sự kiện không bảo mật đúng thời gian, và có tính linh hoạt cao.

Viện dẫn tới cách thức thực hiện có thể thứ ba của khía cạnh thứ nhất, theo cách thức thực hiện có thể thứ tư của khía cạnh thứ nhất, thiết bị đầu cuối bao gồm thiết bị phần cứng liên quan đến hiển thị, thiết bị phần cứng liên quan đến hiển thị có cấu trúc để hiển thị giao diện ứng dụng máy khách (CA) và giao diện ứng dụng tin cậy (TA), và bước chuyển đổi từ giao diện ứng dụng tin cậy (TA) hiện tại thành giao diện phản hồi của sự kiện thứ nhất trong môi trường thực thi đầy đủ theo bản tin phản hồi sự kiện không bảo mật một cách cụ thể bao gồm:

kích hoạt yêu cầu tạm dừng hiển thị TUI theo bản tin phản hồi sự kiện không bảo mật;

điều khiển, theo yêu cầu tạm dừng hiển thị TUI bằng cách sử dụng trình điều khiển mà của thiết bị phần cứng và nằm trong môi trường thực thi tin cậy, thiết bị phần cứng để thoát khỏi chế độ bảo mật hiện tại, trong đó chế độ bảo mật này là chế độ đang chạy mà tương ứng với thiết bị phần cứng và nằm trong môi trường thực thi tin cậy;

điều khiển, theo thông tin chuyển đổi thứ hai bằng cách sử dụng trình điều khiển mà của thiết bị phần cứng và nằm trong môi trường thực thi đầy đủ, thiết bị phần cứng để đi vào chế độ không bảo mật, trong đó thông tin chuyển đổi thứ hai được sử dụng để chỉ báo rằng thiết bị phần cứng đã thoát khỏi chế độ bảo mật, và chế độ không bảo mật là chế độ đang chạy mà tương ứng với thiết bị phần cứng và nằm trong môi trường thực thi đầy đủ; và

hiển thị giao diện phản hồi của sự kiện thứ nhất trong môi trường thực thi đầy đủ bằng cách viện dẫn tới thiết bị phần cứng mà đã chuyển đổi thành chế độ không bảo mật.

Viện dẫn tới bất kỳ trong số khía cạnh thứ nhất, hoặc các cách thức thực hiện có thể thứ nhất đến thứ tư của khía cạnh thứ nhất, theo cách thức thực

hiện có thể thứ năm của khía cạnh thứ nhất, phương pháp này còn bao gồm:

chuyển đổi từ giao diện ứng dụng tin cậy (TA) hiện tại thành giao diện ứng dụng máy khách (CA) theo yêu cầu thoát khỏi hiển thị TUI, trong đó yêu cầu thoát khỏi hiển thị TUI được kích hoạt bởi hoạt động thứ hai trên giao diện ứng dụng tin cậy (TA) bởi người dùng. Phương pháp này thực hiện việc chuyển đổi từ hiển thị bảo mật thành hiển thị không bảo mật, và hỗ trợ người dùng thực hiện hoạt động tiếp theo trên giao diện không bảo mật.

Viện dẫn tới cách thức thực hiện có thể thứ năm của khía cạnh thứ nhất, theo cách thức thực hiện có thể thứ sáu của khía cạnh thứ nhất, thiết bị đầu cuối bao gồm thiết bị phần cứng liên quan đến hiển thị, và bước chuyển đổi từ giao diện ứng dụng tin cậy (TA) hiện tại thành giao diện ứng dụng máy khách (CA) theo yêu cầu thoát khỏi hiển thị TUI một cách cụ thể bao gồm:

điều khiển, theo yêu cầu thoát khỏi hiển thị TUI bằng cách sử dụng trình điều khiển mà của thiết bị phần cứng và nằm trong môi trường thực thi tin cậy, thiết bị phần cứng để thoát khỏi chế độ bảo mật hiện tại, trong đó chế độ bảo mật này là chế độ đang chạy mà tương ứng với thiết bị phần cứng và nằm trong môi trường thực thi tin cậy;

điều khiển, theo thông tin chuyển đổi thứ ba bằng cách sử dụng trình điều khiển mà của thiết bị phần cứng và nằm trong môi trường thực thi đầy đủ, thiết bị phần cứng để đi vào chế độ không bảo mật, trong đó thông tin chuyển đổi thứ ba được sử dụng để chỉ báo rằng thiết bị phần cứng đã thoát khỏi chế độ bảo mật, và chế độ không bảo mật là chế độ đang chạy mà tương ứng với thiết bị phần cứng và nằm trong môi trường thực thi đầy đủ; và

hiển thị, trong môi trường thực thi đầy đủ, giao diện ứng dụng máy khách (CA) bằng cách viện dẫn tới thiết bị phần cứng mà đã chuyển đổi thành chế độ không bảo mật.

Theo khía cạnh thứ hai, phương án của sáng chế đề xuất thiết bị đầu cuối, trong đó ứng dụng máy khách (CA) chạy trên thiết bị đầu cuối, môi trường thực thi đầy đủ và môi trường thực thi tin cậy được thiết lập trên thiết bị đầu cuối, và thiết bị đầu cuối bao gồm:

môđun kích hoạt, có cấu trúc để kích hoạt yêu cầu hiển thị giao diện người dùng tin cậy (TUI) của ứng dụng máy khách (CA) theo hoạt động thứ nhất trên giao diện ứng dụng máy khách (CA) của ứng dụng máy khách (CA) bởi người dùng, trong đó giao diện ứng dụng máy khách (CA) là giao diện người dùng mà của ứng dụng máy khách (CA) và nằm trong môi trường thực thi đầy đủ;

môđun chuyển đổi, có cấu trúc để chuyển đổi môi trường hiển thị của ứng dụng máy khách (CA) từ môi trường thực thi đầy đủ thành môi trường thực thi tin cậy theo yêu cầu hiển thị TUI; và

môđun hiển thị, có cấu trúc để hiển thị giao diện ứng dụng tin cậy (TA) mà của ứng dụng máy khách (CA) và nằm trong môi trường thực thi tin cậy, trong đó giao diện ứng dụng tin cậy (TA) được sử dụng bởi người dùng của thiết bị đầu cuối để nhập vào thông tin cá nhân.

Viện dẫn tới khía cạnh thứ hai, theo cách thức thực hiện có thể khác của khía cạnh thứ hai, các nguyên tắc hoạt động của các môđun trong thiết bị đầu cuối là tương tự như các cách thức thực hiện của khía cạnh thứ nhất. Chi tiết có thể viện dẫn tới cách thức thực hiện có thể thứ nhất đến thứ sáu của khía cạnh thứ nhất.

Theo khía cạnh thứ ba, phương án của sáng chế đề xuất thiết bị đầu cuối, trong đó ứng dụng máy khách (CA) chạy trên thiết bị đầu cuối, môi trường thực thi đầy đủ và môi trường thực thi tin cậy được thiết lập trên thiết bị đầu cuối, và thiết bị đầu cuối bao gồm: bộ xử lý, bộ nhớ, và thiết bị phần cứng có cấu trúc để hiển thị giao diện của thiết bị đầu cuối, trong đó bộ nhớ lưu trữ chương trình hoặc chỉ dẫn, và bộ xử lý viện dẫn chương trình hoặc chỉ dẫn mà được lưu trữ trong bộ nhớ, để:

kích hoạt yêu cầu hiển thị giao diện người dùng tin cậy (TUI) của ứng dụng máy khách (CA) theo hoạt động thứ nhất trên giao diện ứng dụng máy khách (CA) của ứng dụng máy khách (CA) bởi người dùng, trong đó giao diện ứng dụng máy khách (CA) là giao diện người dùng mà của ứng dụng máy khách (CA) và nằm trong môi trường thực thi đầy đủ;

chuyển đổi môi trường hiển thị của ứng dụng máy khách (CA) từ môi trường thực thi đầy đủ thành môi trường thực thi tin cậy theo yêu cầu hiển thị TUI; và

điều khiển thiết bị phần cứng để hiển thị giao diện ứng dụng tin cậy (TA) mà của ứng dụng máy khách (CA) và nằm trong môi trường thực thi tin cậy, trong đó giao diện ứng dụng tin cậy (TA) được sử dụng bởi người dùng của thiết bị đầu cuối để nhập vào thông tin cá nhân.

Viện dẫn tới khía cạnh thứ ba, theo cách thức thực hiện có thể khác của khía cạnh thứ ba, nguyên tắc hoạt động của bộ xử lý trong thiết bị đầu cuối là tương tự như các cách thức thực hiện của khía cạnh thứ nhất. Chi tiết có thể viện dẫn tới cách thức thực hiện có thể thứ nhất đến thứ sáu của khía cạnh thứ nhất.

Bằng phương pháp chuyển đổi giao diện người dùng và thiết bị đầu cuối mà được đề xuất trong các phương án của sáng chế, sau khi thiết bị đầu cuối kích hoạt yêu cầu hiển thị TUI của ứng dụng máy khách (CA) theo hoạt động thứ nhất trên giao diện ứng dụng máy khách (CA) bởi người dùng, thiết bị đầu cuối chuyển đổi môi trường hiển thị của ứng dụng máy khách (CA) từ REE thành TEE theo yêu cầu hiển thị TUI, và sau đó hiển thị giao diện ứng dụng tin cậy (TA) mà của ứng dụng máy khách (CA) và nằm trong TEE. Trong trường hợp này, người dùng có thể thực hiện hoạt động nhập thông tin nhạy cảm trên giao diện ứng dụng tin cậy (TA), và chương trình độc hại mà chạy trong REE không thể truy nhập thiết bị phần cứng để thu nhận hoạt động nhập liệu trong TEE bởi người dùng. Do đó, khi hoạt động nhập liệu bởi người dùng được thực hiện bằng cách sử dụng phương pháp nêu trên, khả năng mà thông tin nhạy cảm của người dùng bị đánh cắp được ngăn ngừa, nhờ đó nâng cao một cách hiệu quả tính bảo mật của hoạt động nhập liệu bởi người dùng.

Mô tả vắn tắt các hình vẽ

FIG.1 là sơ đồ cấu trúc giản lược về cấu trúc khung của REE và TEE;

FIG.2 là lưu đồ giản lược của phương pháp chuyển đổi giao diện người dùng theo Phương án 1 của sáng chế;

FIG.3 là sơ đồ giản lược của việc chuyển đổi giao diện người dùng của thiết bị đầu cuối theo sáng chế;

FIG.4 là lưu đồ giản lược của phương pháp chuyển đổi giao diện người dùng theo Phương án 2 của sáng chế;

FIG.5 là lưu đồ giản lược của phương pháp chuyển đổi giao diện người dùng theo Phương án 3 của sáng chế;

FIG.6 là lưu đồ giản lược của phương pháp chuyển đổi giao diện người dùng theo Phương án 4 của sáng chế;

FIG.7 là lưu đồ giản lược của phương pháp chuyển đổi giao diện người dùng theo Phương án 5 của sáng chế;

FIG.8 là lưu đồ giản lược của phương pháp chuyển đổi giao diện người dùng theo Phương án 6 của sáng chế;

FIG.9 là sơ đồ cấu trúc giản lược của thiết bị đầu cuối theo phương án 1 của sáng chế;

FIG.10 là sơ đồ cấu trúc giản lược của thiết bị đầu cuối theo phương án 2 của sáng chế; và

FIG.11 là sơ đồ cấu trúc giản lược của thiết bị đầu cuối theo phương án 3 của sáng chế.

Mô tả chi tiết sáng chế

Để làm cho các mục đích, các giải pháp kỹ thuật, và các hiệu quả của các phương án của sáng chế rõ ràng hơn, phần sau đây mô tả rõ ràng các giải pháp kỹ thuật trong các phương án của sáng chế viện dẫn tới các hình vẽ kèm theo trong các phương án của sáng chế. Rõ ràng, các phương án được mô tả là một vài phương án của sáng chế mà không phải tất cả các phương án của sáng chế. Tất cả các phương án khác được thực hiện bởi người có hiểu biết trung bình trong lĩnh vực kỹ thuật dựa trên các phương án của sáng chế mà không cần cố gắng sáng tạo sẽ nằm trong phạm vi bảo hộ của sáng chế.

Thiết bị đầu cuối được mô tả trong các phương án của sáng chế có thể là thiết bị thông minh khác như điện thoại di động, thiết bị hỗ trợ cá nhân số

(PDA), hoặc máy tính bảng. Môi trường chạy không bảo mật và môi trường chạy bảo mật có thể được thiết lập trên thiết bị đầu cuối. Môi trường chạy không bảo mật là môi trường thực thi đầy đủ (REE) trên thiết bị đầu cuối, và hệ điều hành như Android, iOS, hoặc Windows Phone chạy trong môi trường chạy không bảo mật. Môi trường chạy bảo mật là môi trường thực thi tin cậy (TEE), và hệ điều hành bảo mật chạy trong môi trường chạy bảo mật. Các tài nguyên phần mềm và phần cứng được truy nhập trong TEE được tách biệt với REE. Các tài nguyên phần mềm và phần cứng trong thiết bị đầu cuối có thể được đánh dấu bởi hai trạng thái môi trường thực thi. Các tài nguyên phần mềm và phần cứng mà được đánh dấu bởi trạng thái thực thi bảo mật có thể được truy nhập chỉ trong TEE, và các tài nguyên phần mềm và phần cứng mà được đánh dấu bởi trạng thái thực thi không bảo mật có thể được truy nhập trong hai môi trường thực thi. Môi trường chạy bảo mật tách biệt với REE được xây dựng trong TEE, và có thể cấp môi trường thực thi bảo mật tới phần mềm tin cậy được cho phép.

Phương pháp chuyển đổi giao diện đối với thiết bị đầu cuối và thiết bị đầu cuối mà được đề xuất trong các phương án của sáng chế nhằm mục đích giải quyết vấn đề kỹ thuật trong kỹ thuật đã biết rằng tính bảo mật là thấp khi bàn phím ngẫu nhiên có cấu trúc để ngăn chương trình độc hại khỏi việc chặn hoạt động nhập liệu bởi người dùng.

FIG.1 là sơ đồ cấu trúc giản lược về cấu trúc khung của REE và TEE. Như được thể hiện trên FIG.1, trong REE, các ứng dụng máy khách (CA) khác nhau được cài đặt, và môđun điều khiển REE và môđun trình điều khiển được thiết lập. Trong TEE, các ứng dụng tin cậy (TA) khác nhau được cài đặt, và môđun điều khiển TEE và môđun trình điều khiển được thiết lập. Các môđun trình điều khiển trong cả REE và TEE có thể truy nhập các thiết bị phần cứng tương ứng. CA có thể là phần mềm ứng dụng cụ thể khác liên quan đến việc nhập thông tin nhạy cảm như tài khoản và mật khẩu, ví dụ, Alipay (hoặc Apple pay hoặc Huawei pay) và khách hàng ngân hàng. TA là ứng dụng bảo mật tương ứng với CA, và có cấu trúc để thực hiện hoạt động nhập thông tin nhạy cảm nằm trong CA. CA có thể truy nhập TA bằng cách sử dụng môđun điều khiển REE và

môđun điều khiển TEE, để thực hiện hoạt động bảo mật tương ứng. Cụ thể, môđun điều khiển REE có thể viện dẫn môđun trình điều khiển trên phía của REE theo yêu cầu truy nhập của ứng dụng máy khách (CA), để làm cho thiết bị phần cứng thoát khỏi chế độ hoạt động không bảo mật. Sau khi thiết bị phần cứng thoát khỏi chế độ hoạt động không bảo mật, môđun điều khiển TEE có thể viện dẫn môđun trình điều khiển trên phía của TEE theo bản tin được gửi bởi môđun điều khiển REE, để làm cho thiết bị phần cứng chuyển đổi thành môđun hoạt động, để thực hiện việc tách biệt phần cứng với REE, và sau đó có thể viện dẫn tới TA tương ứng để thực hiện việc truy nhập tới TA bởi CA. Tất cả các chức năng cụ thể của môđun điều khiển REE, môđun điều khiển TEE, và các môđun trình điều khiển trong hai môi trường chạy có thể được thực hiện bằng cách sử dụng bộ xử lý trong thiết bị đầu cuối.

Phần sau đây mô tả các giải pháp kỹ thuật của sáng chế một cách chi tiết bằng cách sử dụng các phương án cụ thể. Các phương án cụ thể sau đây có thể được kết hợp với nhau, và các khái niệm hoặc các xử lý trùng hoặc tương tự có thể không được mô tả lại trong một vài phương án.

FIG.2 là lưu đồ giản lược của phương pháp chuyển đổi giao diện người dùng theo Phương án 1 của sáng chế. Phương pháp này có thể được thực hiện bởi thiết bị đầu cuối.Trên thiết bị đầu cuối, ứng dụng máy khách (CA) chạy, và REE và TEE được thiết lập. Như được thể hiện trên FIG.2, phương pháp được đề xuất trong phương án này bao gồm các bước sau đây.

Bước S11: Kích hoạt yêu cầu hiển thị TUI của ứng dụng máy khách (CA) theo hoạt động thứ nhất trên giao diện ứng dụng máy khách (CA) của ứng dụng máy khách (CA) bởi người dùng.

Cụ thể, giao diện ứng dụng máy khách (CA) là giao diện người dùng mà của ứng dụng máy khách (CA) và nằm trong REE. Khi người dùng thực hiện hoạt động thứ nhất trên giao diện ứng dụng máy khách (CA) (ví dụ, người dùng ấn vào vị trí nhập thông tin nhạy cảm), để đi vào giao diện nhập thông tin nhạy cảm (ví dụ, bàn phím ảo) trong bước tiếp theo, CA được kích hoạt để tạo ra yêu cầu hiển thị giao diện người dùng tin cậy (TUI). Hoạt động thứ nhất có thể là

hoạt động ấn trên màn chạm bởi người dùng, hoặc có thể hoạt động ấn trên bàn phím cơ học bởi người dùng.

Bước S12: Chuyển đổi môi trường hiển thị của ứng dụng máy khách (CA) từ REE thành TEE theo yêu cầu hiển thị TUI.

Cụ thể, TEE là môi trường chạy bảo mật, và thiết bị đầu cuối chuyển đổi môi trường hiển thị của ứng dụng máy khách (CA) từ REE thành TEE theo yêu cầu hiển thị TUI. Trong trường hợp này, phần mềm ứng dụng khác nhau (bao gồm một vài phần mềm không độc hại và phần mềm độc hại) trong REE không thể truy nhập thiết bị phần cứng để thu nhận hoạt động trong TEE. Do đó, chức năng hoạt động bảo mật như hiển thị TUI có thể được thực hiện. Cụ thể, môi trường hiển thị có thể là môi trường chạy nền của ứng dụng máy khách (CA), hoặc có thể viện dẫn tới môi trường phần mềm để hiển thị CA. Nói cách khác, CA có thể chỉ chuyển đổi thành môi trường phần mềm để hiển thị CA, và môi trường chạy nền không thay đổi. Khi môi trường hiển thị của ứng dụng máy khách (CA) được chuyển đổi từ REE thành TEE, chỉ môi trường phần mềm mà nằm trên thiết bị đầu cuối và có cấu trúc để hiển thị giao diện ứng dụng máy khách (CA) có thể được chuyển đổi từ REE thành TEE, hoặc môi trường chạy hệ thống mà trong đó CA được bố trí trên thiết bị đầu cuối có thể được chuyển đổi từ REE thành TEE.

Bước S13: Hiển thị giao diện ứng dụng tin cậy (TA) mà của ứng dụng máy khách (CA) và nằm trong TEE.

Cụ thể, giao diện ứng dụng tin cậy (TA) được sử dụng bởi người dùng của thiết bị đầu cuối để nhập thông tin cá nhân, và TA được thiết lập trong TEE. Khi CA được thiết lập trong REE, TA tương ứng với CA có thể được thiết lập trong TEE, để thực hiện chức năng hoạt động bảo mật.

Sau khi thiết bị đầu cuối chuyển đổi môi trường hiển thị của ứng dụng máy khách (CA) từ REE thành TEE theo yêu cầu hiển thị TUI, môi trường thực thi bảo mật được cấp tới các hoạt động tiếp theo. Thiết bị đầu cuối có thể sau đó viện dẫn tới TA để hiển thị, trong TEE, giao diện ứng dụng tin cậy (TA), sao cho người dùng có thể thực hiện hoạt động nhập thông tin nhạy cảm trên giao diện

ứng dụng tin cậy (TA). Trong trường hợp này, hoạt động nhập thông tin nhạy cảm bởi người dùng được thực hiện trong TEE bảo mật, và ứng dụng không bảo mật (ví dụ, phần mềm độc hại mà bao gồm chương trình độc hại) trong REE không thể thu nhận hoạt động nhập liệu trên giao diện ứng dụng tin cậy (TA) bởi người dùng, nhờ đó ngăn ngừa thông tin nhạy cảm của người dùng bị đánh cắp bởi chương trình độc hại, và nâng cao tính bảo mật của hoạt động nhập liệu bởi người dùng. Cụ thể, môđun xử lý như môđun điều khiển REE trong thiết bị đầu cuối có thể thu nhận, tại cùng thời điểm khi thu nhận yêu cầu hiển thị TUI được gửi bởi CA, ký hiệu nhận dạng của TA tương ứng với CA mà trên đó người dùng thực hiện hoạt động thứ nhất , ví dụ, ID của TA. Thiết bị đầu cuối có thể viện dẫn tới TA tương ứng theo ký hiệu nhận dạng của TA.

Để mô tả giải pháp kỹ thuật trong phương án này một cách rõ ràng hơn, phần mô tả đưa ra phần mô tả minh họa bằng cách sử dụng sơ đồ giản lược của việc chuyển đổi giao diện cụ thể.

FIG.3 là sơ đồ giản lược của việc chuyển đổi giao diện người dùng của thiết bị đầu cuối theo sáng chế. Như được thể hiện trên FIG.3, người dùng thực hiện, bằng cách sử dụng ứng dụng trả phí (tức là, CA), hoạt động chuyển tiền tới số điện thoại. Khi người dùng ấn "Tiếp theo (Next)" (tức là, hoạt động thứ nhất) trên giao diện ứng dụng máy khách (CA) trong REE để thực hiện hoạt động nhập mật khẩu, thiết bị đầu cuối chuyển đổi môi trường hiển thị từ REE thành TEE theo hoạt động thứ nhất, và hiển thị, trong TEE, giao diện ứng dụng (tức là, giao diện ứng dụng tin cậy (TA)) mà bao gồm bàn phím ảo. Người dùng xác nhận thông tin chuyển tiền và sau đó thực hiện hoạt động nhập mật khẩu trên giao diện ứng dụng tin cậy (TA). Trong trường hợp này, hoạt động nhập mật khẩu bởi người dùng nằm trong môi trường chạy bảo mật (tức là, TEE), và ứng dụng trong môi trường chạy không bảo mật (tức là, REE) không thể lấy cắp mật khẩu được nhập bởi người dùng trong TEE, nhờ đó đảm bảo tính bảo mật của hoạt động nhập mật khẩu bởi người dùng.

Bằng phương pháp chuyển đổi giao diện người dùng được đề xuất trong phương án này, sau khi thiết bị đầu cuối kích hoạt yêu cầu hiển thị TUI

của ứng dụng máy khách (CA) theo hoạt động thứ nhất trên giao diện ứng dụng máy khách (CA) bởi người dùng, thiết bị đầu cuối chuyển đổi môi trường hiển thị của ứng dụng máy khách (CA) từ REE thành TEE theo yêu cầu hiển thị TUI, và sau đó hiển thị giao diện ứng dụng tin cậy (TA) mà của ứng dụng máy khách (CA) và nằm trong TEE. Trong trường hợp này, người dùng có thể thực hiện hoạt động nhập thông tin nhạy cảm trên giao diện ứng dụng tin cậy (TA), và chương trình độc hại mà chạy trong REE không thể truy nhập thiết bị phần cứng để thu nhận hoạt động nhập liệu trong TEE bởi người dùng. Do đó, khi hoạt động nhập liệu bởi người dùng được thực hiện bằng cách sử dụng phương pháp nêu trên, khả năng mà thông tin nhạy cảm của người dùng bị đánh cắp được ngăn ngừa, nhờ đó nâng cao một cách hiệu quả tính bảo mật của hoạt động nhập liệu bởi người dùng.

FIG.4 là lưu đồ giản lược của phương pháp chuyển đổi giao diện người dùng theo Phương án 2 của sáng chế. Phương án này là cách thức thực hiện cụ thể của bước S12 và bước S13 trong phương án được thể hiện trên FIG.2. Trong phương án này, thiết bị đầu cuối bao gồm thiết bị phần cứng liên quan đến hiển thị, và thiết bị phần cứng có cấu trúc để hiển thị giao diện ứng dụng máy khách (CA) và giao diện ứng dụng tin cậy (TA). Dựa trên phương án được thể hiện trên FIG.2, như được thể hiện trên FIG.4, bước chuyển đổi môi trường hiển thị của ứng dụng máy khách (CA) từ REE thành TEE theo yêu cầu hiển thị TUI trong bước 12 một cách cụ thể bao gồm các bước sau đây.

Bước S121: Điều khiển, theo yêu cầu hiển thị TUI của ứng dụng máy khách (CA) bằng cách sử dụng trình điều khiển mà của thiết bị phần cứng và nằm trong REE, thiết bị phần cứng để thoát khỏi chế độ không bảo mật hiện tại.

Cụ thể, thiết bị phần cứng liên quan đến hiển thị có thể bao gồm bộ nhớ hiển thị, thiết bị hiển thị, và màn chạm hoặc bàn phím cơ học, và có thể còn bao gồm thiết bị vân tay, thiết bị truyền thông trường gần (NFC), phần tử bảo mật (SE), và loại tương tự. Bằng cách sử dụng kỹ thuật mở rộng bảo mật liên quan (ví dụ, kỹ thuật vùng bảo mật-Vùng tin cậy (Trust Zone) được đề xuất trong chip ARM), các chế độ truy nhập của các thiết bị này có thể được cấu hình

thành hai chế độ hoạt động: chế độ bảo mật và chế độ không bảo mật. Chế độ bảo mật là chế độ đang chạy mà tương ứng với thiết bị phần cứng và nằm trong TEE, và chế độ không bảo mật là chế độ đang chạy mà tương ứng với thiết bị phần cứng và nằm trong REE.

Trình điều khiển (tức là, môđun trình điều khiển trên phía của REE trên FIG.1) của thiết bị phần cứng liên quan đến hiển thị được thiết lập trong REE cho thiết bị đầu cuối. Môđun điều khiển REE trong thiết bị đầu cuối có thể làm cho, bằng cách sử dụng trình điều khiển trong REE, thiết bị phần cứng liên quan đến hiển thị thoát khỏi cấu hình chế độ không bảo mật. Cụ thể, môđun điều khiển REE trong thiết bị đầu cuối có thể gửi bản tin báo hiệu tới trình điều khiển trong REE, để chỉ dẫn trình điều khiển làm cho thiết bị phần cứng thoát khỏi cấu hình chế độ không bảo mật. Sau khi thiết bị phần cứng thoát khỏi cấu hình chế độ không bảo mật, trình điều khiển có thể phản hồi báo hiệu hoàn thành việc thoát khỏi cấu hình chế độ không bảo mật tới môđun điều khiển REE.

Bước S122: Điều khiển, theo thông tin chuyển đổi thứ nhất bằng cách sử dụng trình điều khiển mà của thiết bị phần cứng và nằm trong TEE, thiết bị phần cứng để đi vào chế độ bảo mật.

Cụ thể, sau khi thiết bị phần cứng thoát khỏi cấu hình chế độ không bảo mật, môđun điều khiển REE trong thiết bị đầu cuối có thể gửi thông tin chuyển đổi thứ nhất tới môđun điều khiển TEE, để chỉ báo rằng thiết bị phần cứng đã thoát khỏi chế độ không bảo mật. Trình điều khiển (tức là, môđun trình điều khiển trên phía của TEE trên FIG.1) của thiết bị phần cứng liên quan đến hiển thị cũng được thiết lập trong TEE đối với thiết bị đầu cuối. Sau khi thu thông tin chuyển đổi thứ nhất, môđun điều khiển TEE có thể làm cho, bằng cách sử dụng trình điều khiển trong TEE, thiết bị phần cứng liên quan đến hiển thị đi vào cấu hình chế độ bảo mật. Tương tự bước S121, môđun điều khiển TEE có thể gửi bản tin báo hiệu tới trình điều khiển trong TEE, để chỉ dẫn trình điều khiển làm cho thiết bị phần cứng đi vào cấu hình chế độ bảo mật. Sau khi thiết bị phần cứng đi vào cấu hình chế độ bảo mật, trình điều khiển có thể phản hồi báo hiệu hoàn thành việc đi vào cấu hình chế độ bảo mật tới môđun điều khiển

TEE. Trong trường hợp này, môi trường hiển thị của ứng dụng máy khách (CA) cũng được chuyển đổi từ REE thành TEE.

Đối với các trình điều khiển nêu trên, thiết bị phần cứng liên quan đến hiển thị này bao gồm bộ nhớ hiển thị, thiết bị hiển thị, và màn chạm được sử dụng như là ví dụ. Trình điều khiển hiển thị, trình điều khiển xuất/nhập mục đích chung (GPIO), và trình điều khiển màn chạm được thiết lập trong cả REE và TEE. Trình điều khiển hiển thị có cấu trúc để điều khiển việc chuyển đổi của chế độ hoạt động của bộ nhớ hiển thị và thiết bị hiển thị, và trình điều khiển GPIO và trình điều khiển màn chạm được sử dụng để điều khiển việc chuyển đổi của các chế độ hoạt động của màn chạm. Rõ ràng, nếu thiết bị đầu cuối còn bao gồm thiết bị phần cứng liên quan đến hiển thị khác, trình điều khiển tương ứng có thể được thêm vào REE và TEE.

Ngoài ra, trong phương án này, bước hiển thị giao diện ứng dụng tin cậy (TA) mà của ứng dụng máy khách (CA) và nằm trong TEE trong bước S13 một cách cụ thể có thể bao gồm các bước sau đây.

Bước S131: Chạy, trong TEE, TA tương ứng với CA.

Cụ thể, sau khi thiết bị phần cứng liên quan đến hiển thị đi vào cấu hình chế độ bảo mật, môđun điều khiển TEE trong thiết bị đầu cuối có thể viện dẫn tới TA hoặc chỉ dẫn môđun chức năng liên quan đến hiển hiển thị khác để viện dẫn tới TA, để chạy, trong TEE, ứng dụng.

Bước S132: Hiển thị, trong TEE, giao diện ứng dụng tin cậy (TA) bằng cách viện dẫn tới thiết bị phần cứng trong chế độ bảo mật.

Cụ thể, khi viện dẫn tới TA, thiết bị đầu cuối có thể viện dẫn tới thiết bị phần cứng trong chế độ bảo mật tại cùng thời điểm, để cho phép thiết bị phần cứng hiển thị, trong TEE, giao diện ứng dụng tin cậy (TA), sao cho người dùng thực hiện hoạt động nhập thông tin nhạy cảm trên giao diện ứng dụng tin cậy (TA).

FIG.5 là lưu đồ giản lược của phương pháp chuyển đổi giao diện người dùng theo Phương án 3 của sáng chế. Phương án này là xử lý cụ thể của việc xử lý sự kiện không bảo mật trong việc xử lý thực hiện, bởi thiết bị đầu cuối, hiển

thị TUI trong TEE trong các phương án nêu trên. Dựa trên tất cả các phương án nêu trên, như được thể hiện trên FIG.5, trong phương án này, sau bước hiển thị giao diện ứng dụng tin cậy (TA) mà của ứng dụng máy khách (CA) và nằm trong TEE trong bước S13, phương pháp trong phương án này còn bao gồm các bước sau đây.

Bước S21: Chuyển đổi từ giao diện ứng dụng tin cậy (TA) hiện tại thành giao diện phản hồi của sự kiện thứ nhất trong REE theo bản tin phản hồi sự kiện không bảo mật.

Trong xử lý thực hiện, bởi thiết bị đầu cuối, việc hiển thị TUI, sự kiện thứ nhất như cuộc gọi đến và đồng hồ báo thức có thể diễn ra. Các sự kiện này là các sự kiện không bảo mật. Trong trường hợp này, thiết bị đầu cuối có thể tạm dừng hiển thị TUI để xử lý sự kiện không bảo mật này. Cụ thể, sau khi thiết bị đầu cuối giám sát sự kiện thứ nhất, bản tin phản hồi sự kiện không bảo mật mà được kích hoạt bởi sự kiện thứ nhất được tạo ra. Trong trường hợp này, thiết bị đầu cuối cần chuyển đổi từ giao diện ứng dụng tin cậy (TA) hiện tại thành giao diện phản hồi của sự kiện thứ nhất trong REE, sao cho người dùng xử lý, trong REE, sự kiện không bảo mật bằng cách sử dụng ứng dụng (ví dụ, ứng dụng điện thoại, hoặc ứng dụng đồng hồ báo thức) tương ứng với sự kiện không bảo mật. Một cách tùy chọn, thiết bị đầu cuối có thể lắng nghe sự kiện không bảo mật bằng cách sử dụng thiết bị lắng nghe sự kiện không bảo mật bên trong, và sau đó tạo ra bản tin phản hồi sự kiện không bảo mật.

Bước S22: Hiển thị giao diện ứng dụng tin cậy (TA) lần nữa theo bản tin hồi đáp phản hồi.

Cụ thể, sau khi người dùng hoàn thành việc xử lý sự kiện không bảo mật, thiết bị lắng nghe sự kiện không bảo mật có thể gửi bản tin hồi đáp phản hồi tới môđun điều khiển REE trong thiết bị đầu cuối. Trong đó bản tin hồi đáp phản hồi chỉ báo rằng người dùng của thiết bị đầu cuối hoàn thành việc xử lý của sự kiện không bảo mật bằng cách sử dụng giao diện phản hồi. Sau khi thu bản tin, thiết bị đầu cuối chuyển đổi môi trường hiển thị của CA từ REE thành TEE, để viện dẫn tới TA trong TEE để hiển thị giao diện ứng dụng tin cậy (TA)

(tức là, thực hiện việc hiển thị TUI) lần nữa. Khi hiển thị giao diện ứng dụng tin cậy (TA), thiết bị đầu cuối có thể viện dẫn tới TA lần nữa bằng cách sử dụng ký hiệu nhận dạng được lưu trữ trước của TA mà đang thực hiện việc hiển thị TUI.

Bằng phương pháp chuyển đổi giao diện người dùng được đề xuất trong phương án này, thiết bị đầu cuối chuyển đổi từ giao diện ứng dụng tin cậy (TA) hiện tại thành giao diện phản hồi của sự kiện thứ nhất trong REE theo bản tin phản hồi sự kiện không bảo mật; và sau đó, sau khi hoàn thành việc xử lý của sự kiện không bảo mật trong REE, hiển thị giao diện ứng dụng tin cậy (TA) lần nữa theo bản tin hồi đáp phản hồi. Do đó, sự kiện không bảo mật có thể được xử lý đúng thời điểm trong xử lý hiển thị TUI, và tính linh hoạt là cao.

FIG.6 là lưu đồ giản lược của phương pháp chuyển đổi giao diện người dùng theo Phương án 4 của sáng chế. Phương án này là cách thức thực hiện cụ thể của bước S21 trong phương án được thể hiện trên FIG.5. Dựa trên phương án được thể hiện trên FIG.5, như được thể hiện trên FIG.6, trong phương án này, bước chuyển đổi từ giao diện ứng dụng tin cậy (TA) hiện tại thành giao diện phản hồi của sự kiện thứ nhất trong REE theo bản tin phản hồi sự kiện không bảo mật trong bước S21 một cách cụ thể bao gồm các bước sau đây.

Bước S211: Kích hoạt yêu cầu tạm dừng hiển thị TUI theo bản tin phản hồi sự kiện không bảo mật.

Cụ thể, sau khi lắng nghe và thu nhận sự kiện không bảo mật, thiết bị lắng nghe sự kiện không bảo mật bên trong của thiết bị đầu cuối có thể gửi bản tin phản hồi sự kiện không bảo mật tới môđun điều khiển REE. Môđun điều khiển REE kích hoạt yêu cầu tạm dừng hiển thị TUI theo bản tin phản hồi sự kiện không bảo mật thu được, và sau đó gửi yêu cầu tạm dừng hiển thị TUI tới môđun điều khiển TEE, để chỉ dẫn môđun điều khiển TEE tạm dừng việc hiển thị hiện tại của giao diện TUI.

Bước S212: Điều khiển, theo yêu cầu tạm dừng hiển thị TUI bằng cách sử dụng trình điều khiển mà của thiết bị phần cứng và nằm trong TEE, thiết bị phần cứng để thoát khỏi chế độ bảo mật hiện tại.

Cụ thể, sau khi thu yêu cầu tạm dừng hiển thị TUI, môđun điều khiển

TEE trong thiết bị đầu cuối viện dẫn trình điều khiển trong TEE để làm cho thiết bị phần cứng liên quan đến hiển thị thoát khỏi cấu hình chế độ bảo mật. Tương tự các phương án nêu trên, môđun điều khiển TEE có thể chỉ dẫn, bằng cách gửi bản tin báo hiệu tới trình điều khiển trong TEE, trình điều khiển để làm cho thiết bị phần cứng thoát khỏi cấu hình chế độ bảo mật.

Bước S213: Điều khiển, theo thông tin chuyển đổi thứ hai bằng cách sử dụng trình điều khiển mà của thiết bị phần cứng và nằm trong REE, thiết bị phần cứng để đi vào chế độ không bảo mật.

Cụ thể, sau khi thiết bị phần cứng thoát khỏi cấu hình chế độ không bảo mật, môđun điều khiển TEE trong thiết bị đầu cuối có thể gửi thông tin chuyển đổi thứ hai tới môđun điều khiển REE, để chỉ báo rằng thiết bị phần cứng đã thoát khỏi chế độ bảo mật. Sau khi thu thông tin chuyển đổi thứ hai, môđun điều khiển REE có thể làm cho, bằng cách sử dụng trình điều khiển trong REE, thiết bị phần cứng liên quan đến hiển thị đi vào cấu hình chế độ không bảo mật, để cấp cơ sở phần cứng cho việc xử lý của sự kiện không bảo mật bởi thiết bị đầu cuối. Tương tự các phương án nêu trên, môđun điều khiển REE có thể chỉ dẫn, bằng cách gửi bản tin báo hiệu tới trình điều khiển trong REE, trình điều khiển để làm cho thiết bị phần cứng đi vào cấu hình chế độ không bảo mật. Trong trường hợp này, môi trường hiển thị của CA được chuyển đổi từ REE thành TEE.

Bước S214: Hiển thị giao diện phản hồi của sự kiện thứ nhất trong REE bằng cách viện dẫn tới thiết bị phần cứng mà đã chuyển đổi thành chế độ không bảo mật.

Cụ thể, sau khi thiết bị phần cứng đi vào cấu hình chế độ không bảo mật, môi trường hiển thị của CA được chuyển đổi từ TEE thành REE. Trong trường hợp này, thiết bị đầu cuối có thể viện dẫn tới thiết bị phần cứng trong chế độ không bảo mật bằng cách sử dụng môđun điều khiển REE, để hiển thị giao diện phản hồi của sự kiện thứ nhất trong REE, sao cho người dùng thực hiện hoạt động xử lý sự kiện không bảo mật.

Sau khi người dùng hoàn thành xử lý của sự kiện không bảo mật, thiết

bị đầu cuối cần chuyển đổi môi trường hiển thị quay lại TEE, để tiếp tục thực hiện việc hiển thị TUI. Dựa trên các phương án nêu trên, thiết bị đầu cuối có thể nhận biết, bằng cách sử dụng thiết bị lắng nghe sự kiện không bảo mật, bản tin chỉ báo rằng việc xử lý của sự kiện không bảo mật được hoàn thành, và sau đó gửi bản tin hồi đáp phản hồi tới môđun điều khiển REE trong thiết bị đầu cuối. Sau khi thu bản tin, thiết bị đầu cuối chuyển đổi môi trường hiển thị của CA từ REE thành TEE, và viện dẫn tới TA trong TEE để tiếp tục hiển thị giao diện ứng dụng tin cậy (TA). Xử lý cụ thể là tương tự như xử lý mà trong đó thiết bị đầu cuối chuyển đổi môi trường hiển thị của ứng dụng máy khách (CA) từ REE thành TEE trong phương án được thể hiện trên FIG.4. Các chi tiết không được mô tả lại ở đây lần nữa.

FIG.7 là lưu đồ giản lược của phương pháp chuyển đổi giao diện người dùng theo Phương án 5 của sáng chế. Phương án này là xử lý cụ thể của thiết bị đầu cuối sau khi việc hiển thị TUI được hoàn thành. Dựa trên các phương án nêu trên, như được thể hiện trên FIG.7, trong phương án này, sau bước hiển thị giao diện ứng dụng tin cậy (TA) mà của ứng dụng máy khách (CA) và nằm trong TEE trong bước S13, phương pháp trong phương án này còn bao gồm bước sau đây.

Bước S14: Chuyển đổi từ giao diện ứng dụng tin cậy (TA) hiện tại thành giao diện ứng dụng máy khách (CA) theo yêu cầu thoát khỏi hiển thị TUI.

Sau khi thiết bị đầu cuối hoàn thành xử lý của sự kiện không bảo mật trên giao diện hiển thị TUI, việc hiển thị TUI kết thúc. Trong trường hợp này, thiết bị đầu cuối có thể chuyển đổi môi trường hiển thị quay lại REE, để thực hiện hoạt động CA tiếp theo. Cụ thể, sau khi người dùng hoàn thành việc nhập của thông tin nhạy cảm trên giao diện ứng dụng tin cậy (TA), người dùng thực hiện hoạt động thứ hai (ví dụ, người dùng ấn vào nút nhập liệu) để kích hoạt hoạt động tiếp theo. TA có thể tạo ra yêu cầu thoát khỏi hiển thị TUI theo hoạt động thứ hai, trong đó yêu cầu này được sử dụng để chỉ dẫn thiết bị đầu cuối thoát khỏi việc hiển thị TUI.

Thiết bị đầu cuối có thể thoát khỏi giao diện ứng dụng tin cậy (TA)

hiện tại theo yêu cầu thoát khỏi hiển thị TUI, chuyển đổi môi trường hiển thị của ứng dụng máy khách (CA) từ REE thành TEE, và sau đó viện dẫn tới CA để hiển thị giao diện ứng dụng máy khách (CA) trong REE. Cụ thể, thiết bị đầu cuối có thể viện dẫn tới CA theo các cách thức sau đây. Trong cách thức thứ nhất, tại cùng thời điểm khi thu nhận yêu cầu hiển thị TUI, môđun điều khiển REE trong thiết bị đầu cuối có thể thu nhận ký hiệu nhận dạng của ứng dụng máy khách (CA) mà trên đó người dùng thực hiện hoạt động thứ nhất, ví dụ, ID của ứng dụng máy khách (CA), và lưu trữ ký hiệu nhận dạng của CA; và sau khi thoát khỏi việc hiển thị TUI, thiết bị đầu cuối có thể viện dẫn tới CA theo ký hiệu nhận dạng của CA. Trong cách thức thứ hai, tại cùng thời điểm khi thu nhận yêu cầu thoát khỏi hiển thị TUI được gửi bởi TA, môđun điều khiển TEE trong thiết bị đầu cuối có thể thu nhận ký hiệu nhận dạng của ứng dụng máy khách (CA) tương ứng với TA mà trên đó người dùng thực hiện hoạt động thứ hai, và thiết bị đầu cuối có thể viện dẫn tới CA theo ký hiệu nhận dạng của CA.

Sơ đồ giản lược của việc chuyển đổi giao diện người dùng được thể hiện trên FIG.3 được sử dụng như là ví dụ. Sau khi nhập mật khẩu trên giao diện ứng dụng tin cậy (TA), người dùng ấn "OK" (tức là, hoạt động thứ hai), và sau đó việc hiển thị của giao diện TUI kết thúc. Thiết bị đầu cuối chuyển đổi môi trường chạy từ TEE thành REE theo hoạt động thứ hai, và hiển thị, trong REE, giao diện ứng dụng máy khách (CA) (không được thể hiện) mà bao gồm hoạt động tiếp theo, sao cho người dùng có thể tiếp tục thực hiện hoạt động tiếp theo trên giao diện ứng dụng máy khách (CA).

Lưu ý rằng bước S14 có thể cũng được thực hiện sau bước S22.

Bằng phương pháp chuyển đổi giao diện người dùng được đề xuất trong phương án này, thiết bị đầu cuối chuyển đổi từ giao diện ứng dụng tin cậy (TA) hiện tại thành giao diện ứng dụng máy khách (CA) theo yêu cầu thoát khỏi hiển thị TUI, nhờ đó thực hiện việc chuyển đổi từ hiển thị bảo mật thành hiển thị không bảo mật, và hỗ trợ người dùng thực hiện hoạt động tiếp theo trên giao diện không bảo mật.

FIG.8 là lưu đồ giản lược của phương pháp chuyển đổi giao diện người

dùng theo Phương án 6 của sáng chế. Phương án này là cách thức thực hiện cụ thể của bước S14 trong phương án được thể hiện trên FIG.7. Dựa trên phương án được thể hiện trên FIG.7, như được thể hiện trên FIG.8, trong phương án này, bước chuyển đổi từ giao diện ứng dụng tin cậy (TA) hiện tại thành giao diện ứng dụng máy khách (CA) theo yêu cầu thoát khỏi hiển thị TUI trong bước S14 một cách cụ thể bao gồm các bước sau đây.

Bước S141: Điều khiển, theo yêu cầu thoát khỏi hiển thị TUI bằng cách sử dụng trình điều khiển mà của thiết bị phần cứng và nằm trong TEE, thiết bị phần cứng để thoát khỏi chế độ bảo mật hiện tại.

Cụ thể, sau khi thu yêu cầu thoát khỏi hiển thị TUI, môđun điều khiển TEE trong thiết bị đầu cuối có thể viện dẫn trình điều khiển trong TEE để làm cho thiết bị phần cứng liên quan đến hiển thị thoát khỏi cấu hình chế độ bảo mật. Tương tự các phương án nêu trên, môđun điều khiển TEE có thể chỉ dẫn, bằng cách gửi bản tin báo hiệu tới trình điều khiển trong TEE, trình điều khiển để làm cho thiết bị phần cứng thoát khỏi cấu hình chế độ bảo mật.

Bước S142: Điều khiển, theo thông tin chuyển đổi thứ ba bằng cách sử dụng trình điều khiển mà của thiết bị phần cứng và nằm trong REE, thiết bị phần cứng để đi vào chế độ không bảo mật.

Cụ thể, theo cách thức thực hiện của sáng chế, sau khi thiết bị phần cứng thoát khỏi cấu hình chế độ không bảo mật, môđun điều khiển TEE trong thiết bị đầu cuối có thể gửi thông tin chuyển đổi thứ ba tới môđun điều khiển REE, để chỉ báo rằng thiết bị phần cứng đã thoát khỏi chế độ bảo mật. Sau khi thu thông tin chuyển đổi thứ ba, môđun điều khiển REE có thể làm cho, bằng cách sử dụng trình điều khiển trong REE, thiết bị phần cứng liên quan đến hiển thị đi vào cấu hình chế độ không bảo mật. Điều này cấp cơ sở phần cứng cho việc chuyển đổi từ TEE thành REE bởi thiết bị đầu cuối. Tương tự các phương án nêu trên, môđun điều khiển REE có thể chỉ dẫn, bằng cách gửi bản tin báo hiệu tới trình điều khiển trong REE, trình điều khiển để làm cho thiết bị phần cứng đi vào cấu hình chế độ không bảo mật.

Bước S143: Hiển thị, trong REE, giao diện ứng dụng máy khách (CA)

bằng cách viện dẫn tới thiết bị phần cứng mà đã chuyển đổi thành chế độ không bảo mật.

Cụ thể, sau khi thiết bị phần cứng đi vào cấu hình chế độ không bảo mật, môi trường hiển thị của ứng dụng máy khách (CA) được chuyển đổi từ TEE thành REE. Trong trường hợp này, thiết bị đầu cuối có thể viện dẫn tới thiết bị phần cứng trong chế độ không bảo mật bằng cách sử dụng môđun điều khiển REE, để hiển thị giao diện ứng dụng máy khách (CA) trong REE, sao cho người dùng thực hiện hoạt động tiếp theo trên giao diện ứng dụng máy khách (CA).

FIG.9 là sơ đồ cấu trúc giản lược của thiết bị đầu cuối theo phương án 1 của sáng chế. Trên thiết bị đầu cuối, ứng dụng máy khách (CA) chạy, và môi trường thực thi đầy đủ và môi trường thực thi tin cậy được thiết lập. Như được thể hiện trên FIG.9, thiết bị đầu cuối 100 trong phương án này bao gồm: môđun kích hoạt 110, môđun chuyển đổi 120, và môđun hiển thị 130.

Môđun kích hoạt 110 có cấu trúc để kích hoạt yêu cầu hiển thị giao diện người dùng tin cậy (TUI) của ứng dụng máy khách (CA) theo hoạt động thứ nhất trên giao diện ứng dụng máy khách (CA) của ứng dụng máy khách (CA) bởi người dùng, trong đó giao diện ứng dụng máy khách (CA) là giao diện người dùng mà của ứng dụng máy khách (CA) và nằm trong REE.

Môđun chuyển đổi 120 có cấu trúc để chuyển đổi môi trường hiển thị của ứng dụng máy khách (CA) từ môi trường thực thi đầy đủ thành môi trường thực thi tin cậy theo yêu cầu hiển thị TUI.

Môđun hiển thị 130 có cấu trúc để hiển thị giao diện ứng dụng tin cậy (TA) mà của ứng dụng máy khách (CA) và nằm trong môi trường thực thi tin cậy, trong đó giao diện ứng dụng tin cậy (TA) được sử dụng bởi người dùng của thiết bị đầu cuối để nhập vào thông tin cá nhân.

Chức năng của môđun kích hoạt 110 trong phương án này có thể được thực hiện cụ thể bởi thiết bị xuất/nhập và bộ xử lý mà nằm trong thiết bị đầu cuối. Chức năng của môđun chuyển đổi 120 có thể được thực hiện cụ thể bởi bộ xử lý trong thiết bị đầu cuối. Chức năng của môđun hiển thị 130 có thể được thực hiện cụ thể bởi bộ xử lý và thiết bị hiển thị mà nằm trong thiết bị đầu cuối.

Thiết bị đầu cuối được đề xuất trong phương án này có thể thực hiện phương pháp theo các phương án nêu trên. Thiết bị đầu cuối và phương pháp theo các phương án của sáng chế có cùng nguyên tắc thực hiện và các hiệu quả kỹ thuật. Các chi tiết không được mô tả lại ở đây lần nữa.

Trong phương án của sáng chế, chức năng của môđun chuyển đổi 120 trong phương án được thể hiện trên FIG.9 được tiếp tục mô tả. Trong phương án này, thiết bị đầu cuối bao gồm thiết bị phần cứng liên quan đến hiển thị, và thiết bị phần cứng liên quan đến hiển thị có cấu trúc để hiển thị giao diện ứng dụng máy khách (CA) và giao diện ứng dụng tin cậy (TA).

Theo cách thức thực hiện của sáng chế, môđun chuyển đổi 120 một cách cụ thể bao gồm: bộ điều khiển không bảo mật và bộ điều khiển bảo mật.

Bộ điều khiển không bảo mật có cấu trúc để điều khiển, theo yêu cầu hiển thị TUI của ứng dụng máy khách (CA) bằng cách sử dụng trình điều khiển mà của thiết bị phần cứng và nằm trong REE, thiết bị phần cứng để thoát khỏi chế độ không bảo mật hiện tại, trong đó chế độ không bảo mật là chế độ đang chạy mà tương ứng với thiết bị phần cứng và nằm trong REE.

Bộ điều khiển bảo mật có cấu trúc để điều khiển, theo thông tin chuyển đổi thứ nhất được gửi bởi bộ điều khiển không bảo mật, bằng cách sử dụng trình điều khiển mà của thiết bị phần cứng và nằm trong TEE, thiết bị phần cứng để đi vào chế độ bảo mật, trong đó thông tin chuyển đổi thứ nhất được sử dụng để chỉ báo rằng thiết bị phần cứng đã thoát khỏi chế độ không bảo mật, và chế độ bảo mật là chế độ đang chạy mà tương ứng với thiết bị phần cứng và nằm trong TEE.

Theo cách thức thực hiện khác của sáng chế, môđun chuyển đổi 120 một cách cụ thể bao gồm: môđun điều khiển REE và môđun điều khiển TEE.

Môđun điều khiển REE có cấu trúc để điều khiển, theo yêu cầu hiển thị TUI của ứng dụng máy khách (CA) bằng cách sử dụng trình điều khiển mà của thiết bị phần cứng và nằm trong REE, thiết bị phần cứng để thoát khỏi chế độ không bảo mật hiện tại, trong đó chế độ không bảo mật là chế độ đang chạy mà tương ứng với thiết bị phần cứng và nằm trong REE.

Môđun điều khiển TEE có cấu trúc để điều khiển, theo thông tin chuyển đổi thứ nhất được gửi bởi môđun điều khiển REE, bằng cách sử dụng trình điều khiển mà của thiết bị phần cứng và nằm trong TEE, thiết bị phần cứng để đi vào chế độ bảo mật, trong đó thông tin chuyển đổi thứ nhất được sử dụng để chỉ báo rằng thiết bị phần cứng đã thoát khỏi chế độ không bảo mật, và chế độ bảo mật là chế độ đang chạy mà tương ứng với thiết bị phần cứng và nằm trong TEE.

Trong phương án này, các chức năng của bộ điều khiển không bảo mật và môđun điều khiển REE có thể tương tự một cách cụ thể với môđun điều khiển REE trên FIG.1, và các chức năng của bộ điều khiển bảo mật và môđun điều khiển TEE có thể tương tự một cách cụ thể với môđun điều khiển TEE trên FIG.1. Ngoài ra, trong phương án này, chức năng của trình điều khiển có thể được tích hợp, như là một phần của môđun chuyển đổi 120, thành môđun chuyển đổi 120. Cụ thể, việc thiết lập có thể được thực hiện như được yêu cầu, và không có sự giới hạn đặc biệt trong phương án này. Ngoài ra, trong phương án này, chức năng của bộ điều khiển không bảo mật là tương tự như của môđun điều khiển REE, và chức năng của bộ điều khiển bảo mật là tương tự như của môđun điều khiển TEE. Để thuận tiện cho phần mô tả, phần sau đây mô tả các giải pháp kỹ thuật của sáng chế bằng cách sử dụng trực tiếp bộ điều khiển không bảo mật và bộ điều khiển bảo mật.

Theo cách thức thực hiện tùy chọn của sáng chế, môđun hiển thị 130 có cấu trúc cụ thể để: chạy, trong TEE, TA tương ứng với CA; và viện dẫn tới thiết bị phần cứng trong chế độ bảo mật để hiển thị, trong TEE, giao diện ứng dụng tin cậy (TA).

Dựa trên phương án nêu trên, trong phương án của sáng chế, môđun chuyển đổi 120 còn có cấu trúc để: cho phép thiết bị đầu cuối chuyển đổi từ giao diện ứng dụng tin cậy (TA) hiện tại thành giao diện phản hồi của sự kiện thứ nhất trong REE theo bản tin phản hồi sự kiện không bảo mật bằng cách sử dụng môđun hiển thị 130, và sau đó chỉ dẫn, theo bản tin hồi đáp phản hồi, môđun hiển thị 130 để hiển thị giao diện ứng dụng tin cậy (TA) lần nữa, trong đó bản

tin phản hồi sự kiện không bảo mật được kích hoạt bởi sự kiện thứ nhất trong REE, và bản tin hồi đáp phản hồi chỉ báo rằng người dùng của thiết bị đầu cuối hoàn thành việc xử lý của sự kiện thứ nhất bằng cách sử dụng giao diện phản hồi.

Theo cách thức thực hiện cụ thể của phương án này, bộ điều khiển không bảo mật có cấu trúc để gửi yêu cầu tạm dừng hiển thị TUI tới bộ điều khiển bảo mật theo bản tin phản hồi sự kiện không bảo mật;

bộ điều khiển bảo mật có cấu trúc để điều khiển, theo yêu cầu tạm dừng hiển thị TUI bằng cách sử dụng trình điều khiển mà của thiết bị phần cứng và nằm trong TEE, thiết bị phần cứng để thoát khỏi chế độ bảo mật hiện tại, trong đó chế độ bảo mật là chế độ đang chạy mà tương ứng với thiết bị phần cứng và nằm trong TEE; và

bộ điều khiển không bảo mật còn có cấu trúc để điều khiển, theo thông tin chuyển đổi thứ hai được gửi bởi bộ điều khiển bảo mật, bằng cách sử dụng trình điều khiển mà của thiết bị phần cứng và nằm trong REE, thiết bị phần cứng để đi vào chế độ không bảo mật, và sau đó chỉ dẫn môđun hiển thị 130 để viện dẫn tới thiết bị phần cứng mà đã chuyển đổi thành chế độ không bảo mật, để hiển thị giao diện phản hồi của sự kiện thứ nhất trong REE, trong đó thông tin chuyển đổi thứ hai được sử dụng để chỉ báo rằng thiết bị phần cứng đã thoát khỏi chế độ bảo mật, và chế độ không bảo mật là chế độ đang chạy mà tương ứng với thiết bị phần cứng và nằm trong REE.

Dựa trên các phương án nêu trên, trong phương án khác của sáng chế, môđun chuyển đổi 120 còn có cấu trúc để chỉ dẫn, theo yêu cầu thoát khỏi hiển thị TUI, môđun hiển thị 130 để chuyển đổi từ giao diện ứng dụng tin cậy (TA) hiện tại thành giao diện ứng dụng máy khách (CA), trong đó yêu cầu thoát khỏi hiển thị TUI được kích hoạt bởi môđun kích hoạt 110 theo hoạt động thứ hai trên giao diện ứng dụng tin cậy (TA) bởi người dùng.

Theo cách thức thực hiện cụ thể của phương án này, bộ điều khiển bảo mật có cấu trúc để điều khiển, theo yêu cầu thoát khỏi hiển thị TUI bằng cách sử dụng trình điều khiển mà của thiết bị phần cứng và nằm trong TEE, thiết bị phần

cứng để thoát khỏi chế độ bảo mật hiện tại, trong đó chế độ bảo mật là chế độ đang chạy mà tương ứng với thiết bị phần cứng và nằm trong TEE; và

bộ điều khiển không bảo mật có cấu trúc để điều khiển, theo thông tin chuyển đổi thứ ba được gửi bởi bộ điều khiển bảo mật, bằng cách sử dụng trình điều khiển mà của thiết bị phần cứng và nằm trong REE, thiết bị phần cứng để đi vào chế độ không bảo mật, và sau đó chỉ dẫn môđun hiển thị 130 để viện dẫn tới thiết bị phần cứng mà đã chuyển đổi thành chế độ không bảo mật, để hiển thị, trong REE, giao diện ứng dụng máy khách (CA), trong đó thông tin chuyển đổi thứ ba được sử dụng để chỉ báo rằng thiết bị phần cứng đã thoát khỏi chế độ bảo mật, và chế độ không bảo mật là chế độ đang chạy mà tương ứng với thiết bị phần cứng và nằm trong REE.

Thiết bị đầu cuối được đề xuất trong phương án này của sáng chế có thể thực hiện phương pháp theo các phương án nêu trên. Thiết bị đầu cuối và phương pháp theo các phương án của sáng chế có cùng nguyên tắc thực hiện và các hiệu quả kỹ thuật. Các chi tiết không được mô tả lại ở đây lần nữa.

Sẽ được hiểu rằng, theo cách thức thực hiện, môđun kích hoạt 110, môđun chuyển đổi 120, và môđun hiển thị 130 có thể được thực hiện bởi bộ xử lý thực thi chương trình hoặc chỉ dẫn trong bộ nhớ (tức là, được thực hiện bởi bộ xử lý kết hợp với chỉ dẫn đặc biệt trong bộ nhớ được ghép với bộ xử lý). Ngoài ra, theo cách thức thực hiện khác, môđun kích hoạt 110, môđun chuyển đổi 120, và môđun hiển thị 130 có thể được thực hiện bằng cách sử dụng mạch dành riêng. Đối với cách thức thực hiện cụ thể, có thể viện dẫn tới kỹ thuật đã biết, và các chi tiết không được mô tả lại ở đây. Ngoài ra, theo cách thức thực hiện khác, môđun kích hoạt 110, môđun chuyển đổi 120, và môđun hiển thị 130 có thể được thực hiện bằng cách sử dụng Mảng cổng khả trình dạng trường (FPGA, Field-Programmable Gate Array). Đối với cách thức thực hiện cụ thể, có thể viện dẫn tới kỹ thuật đã biết, và các chi tiết không được mô tả lại ở đây. Sáng chế bao gồm, nhưng không bị giới hạn ở, các cách thức thực hiện nêu trên. Sẽ được hiểu rằng, tất cả các giải pháp được thực hiện theo khái niệm của sáng chế nằm trong phạm vi bảo hộ của các phương án của sáng chế.

Trong một vài phương án được đề xuất theo sáng chế, có thể được hiểu rằng thiết bị và phương pháp được bộc lộ có thể được thực hiện theo các cách khác nhau. Ví dụ, thiết bị theo phương án được mô tả chỉ được sử dụng như là ví dụ. Ví dụ, việc phân chia bộ phận hoặc mô-đun chỉ là việc phân chia chức năng logic và có thể là việc phân chia khác theo phương án thực tế. Ví dụ, các bộ phận hoặc các thành phần có thể được kết hợp hoặc được tích hợp vào hệ thống khác, hoặc một vài đặc điểm có thể được bỏ qua hoặc không được thực hiện. Ngoài ra, các ghép nối liên quan được mô tả hoặc hiển thị hoặc các ghép nối trực tiếp hoặc các kết nối truyền thông có thể được thực hiện bằng cách sử dụng một vài giao diện. Các ghép nối không trực tiếp hoặc các kết nối truyền thông giữa các thiết bị hoặc các bộ phận có thể được thực hiện dưới dạng điện tử, cơ học, hoặc các dạng khác.

Các bộ phận được mô tả như là các thành phần riêng biệt có thể hoặc không phải là được tách biệt vật lý, và các phần được hiển thị như là các bộ phận có thể hoặc không phải là các bộ phận vật lý, có thể nằm trong một vị trí, hoặc có thể được phân phối trên các bộ phận mạng. Một vài hoặc tất cả bộ phận có thể được lựa chọn theo nhu cầu thực tế để đạt được mục đích của các giải pháp của các phương án.

Ngoài ra, các bộ phận chức năng trong các phương án của sáng chế có thể được tích hợp vào một bộ xử lý, hoặc mỗi bộ phận có thể tồn tại riêng lẻ về mặt vật lý, hoặc hai bộ phận hoặc nhiều hơn được tích hợp vào một bộ phận. Bộ phận được tích hợp có thể được thực hiện dưới dạng phần cứng, hoặc có thể được thực hiện dưới dạng đơn vị chức năng phần mềm.

FIG.10 là sơ đồ cấu trúc giản lược của thiết bị đầu cuối theo phương án 2 của sáng chế. Trên thiết bị đầu cuối, ứng dụng máy khách (CA) chạy, và môi trường thực thi đầy đủ và môi trường thực thi tin cậy được thiết lập. Như được thể hiện trên FIG.10, thiết bị đầu cuối 200 trong phương án này bao gồm: ít nhất một bộ xử lý 210, bộ nhớ 220, ít nhất một giao diện mạng 230 hoặc giao diện người dùng khác 240, ít nhất một kênh truyền thông 250, và thiết bị phần cứng 260 mà có cấu trúc để hiển thị giao diện của thiết bị đầu cuối.

Kênh truyền thông 250 có cấu trúc để thực hiện kết nối và truyền thông giữa các thành phần này. Thiết bị đầu cuối 200 một cách tùy chọn bao gồm giao diện người dùng 240, và bao gồm màn hình (ví dụ, màn chạm, LCD, CRT, thiết bị tạo ảnh toàn ký, hoặc máy chiếu), bàn phím, hoặc thiết bị ấn (ví dụ, chuột, bi điều khiển, panen chạm, hoặc màn chạm).

Bộ nhớ 220 có thể bao gồm bộ nhớ chỉ đọc và bộ nhớ truy nhập ngẫu nhiên, và cấp chỉ dẫn và dữ liệu tới bộ xử lý 210.

Theo một vài cách thức thực hiện, bộ nhớ 220 lưu trữ các phần tử sau đây, môđun có thể thực thi được hoặc cấu trúc dữ liệu, hoặc tập hợp con của chúng, hoặc tập hợp mở rộng của chúng:

hệ điều hành 221, bao gồm các chương trình hệ thống khác nhau như môđun điều khiển REE, môđun điều khiển TEE, và các môđun trình điều khiển trên cả hai phía mà được thể hiện trên FIG.1, và có cấu trúc để thực hiện các dịch vụ nền tảng khác nhau và xử lý các tác vụ dựa trên phần cứng; và

môđun chương trình ứng dụng 222, bao gồm các chương trình ứng dụng khác nhau, như CA và TA được thể hiện trên FIG.1, và có cấu trúc để thực hiện các dịch vụ ứng dụng khác nhau.

Thiết bị phần cứng 260 mà có cấu trúc để hiển thị giao diện của thiết bị đầu cuối có thể bao gồm bộ nhớ hiển thị, thiết bị hiển thị, màn chạm, và loại tương tự.

Theo phương án này của sáng chế, bằng cách gọi ra chương trình hoặc chỉ dẫn được lưu trữ trong bộ nhớ 220, bộ xử lý 210 có cấu trúc để:

kích hoạt yêu cầu hiển thị giao diện người dùng tin cậy (TUI) của ứng dụng máy khách (CA) theo hoạt động thứ nhất trên giao diện ứng dụng máy khách (CA) của ứng dụng máy khách (CA) bởi người dùng, trong đó giao diện ứng dụng máy khách (CA) là giao diện người dùng mà của ứng dụng máy khách (CA) và nằm trong môi trường thực thi đầy đủ;

chuyển đổi môi trường hiển thị của ứng dụng máy khách (CA) từ môi trường thực thi đầy đủ thành môi trường thực thi tin cậy theo yêu cầu hiển thị TUI; và

điều khiển thiết bị phần cứng 260 để hiển thị giao diện ứng dụng tin cậy (TA) mà của ứng dụng máy khách (CA) và nằm trong môi trường thực thi tin cậy, trong đó giao diện ứng dụng tin cậy (TA) được sử dụng bởi người dùng của thiết bị đầu cuối để nhập vào thông tin cá nhân.

Ngoài ra, trong cách thức thực hiện cụ thể của sáng chế, trong bước chuyển đổi môi trường hiển thị của ứng dụng máy khách (CA) từ môi trường thực thi đầy đủ thành môi trường thực thi tin cậy theo yêu cầu hiển thị TUI, bộ xử lý 210 có cấu trúc cụ thể để:

điều khiển, theo yêu cầu hiển thị TUI của ứng dụng máy khách (CA) bằng cách sử dụng trình điều khiển mà của thiết bị phần cứng và nằm trong môi trường thực thi đầy đủ, thiết bị phần cứng để thoát khỏi chế độ không bảo mật hiện tại, trong đó chế độ không bảo mật này là chế độ đang chạy mà tương ứng với thiết bị phần cứng và nằm trong môi trường thực thi đầy đủ; và

điều khiển, theo thông tin chuyển đổi thứ nhất bằng cách sử dụng trình điều khiển mà của thiết bị phần cứng và nằm trong môi trường thực thi tin cậy, thiết bị phần cứng để đi vào chế độ bảo mật, trong đó thông tin chuyển đổi thứ nhất được sử dụng để chỉ báo rằng thiết bị phần cứng đã thoát khỏi chế độ không bảo mật, và chế độ bảo mật là chế độ đang chạy mà tương ứng với thiết bị phần cứng và nằm trong môi trường thực thi tin cậy.

Trong bước hiển thị giao diện ứng dụng tin cậy (TA) mà của ứng dụng máy khách (CA) và nằm trong môi trường thực thi tin cậy, bộ xử lý 210 có cấu trúc cụ thể để:

chạy, trong môi trường thực thi tin cậy, TA tương ứng với CA; và

hiển thị, trong môi trường thực thi tin cậy, giao diện ứng dụng tin cậy (TA) bằng cách viện dẫn tới thiết bị phần cứng trong chế độ bảo mật.

Trong phương án của sáng chế, bộ xử lý 210 còn có cấu trúc để: cho phép thiết bị đầu cuối chuyển đổi từ giao diện ứng dụng tin cậy (TA) hiện tại thành giao diện phản hồi của sự kiện thứ nhất trong môi trường thực thi đầy đủ theo bản tin phản hồi sự kiện không bảo mật bằng cách sử dụng thiết bị phần cứng 260, và sau đó điều khiển, theo bản tin hồi đáp phản hồi, thiết bị phần cứng

260 để hiển thị giao diện ứng dụng tin cậy (TA) lần nữa, trong đó bản tin phản hồi sự kiện không bảo mật được kích hoạt bởi sự kiện thứ nhất trong môi trường thực thi đầy đủ, và bản tin hồi đáp phản hồi chỉ báo rằng người dùng của thiết bị đầu cuối hoàn thành việc xử lý của sự kiện thứ nhất bằng cách sử dụng giao diện phản hồi.

Ngoài ra, trong cách thức thực hiện cụ thể của sáng chế, bộ xử lý 210 có cấu trúc cụ thể để:

kích hoạt yêu cầu tạm dừng hiển thị TUI theo bản tin phản hồi sự kiện không bảo mật;

điều khiển, theo yêu cầu tạm dừng hiển thị TUI bằng cách sử dụng trình điều khiển mà của thiết bị phần cứng và nằm trong môi trường thực thi tin cậy, thiết bị phần cứng để thoát khỏi chế độ bảo mật hiện tại, trong đó chế độ bảo mật này là chế độ đang chạy mà tương ứng với thiết bị phần cứng và nằm trong môi trường thực thi tin cậy; và

điều khiển, theo thông tin chuyển đổi thứ hai bằng cách sử dụng trình điều khiển mà của thiết bị phần cứng và nằm trong môi trường thực thi đầy đủ, thiết bị phần cứng để đi vào chế độ không bảo mật, và sau đó hiển thị giao diện phản hồi của sự kiện thứ nhất trong môi trường thực thi đầy đủ bằng cách viện dẫn tới thiết bị phần cứng mà đã chuyển đổi thành chế độ không bảo mật, trong đó thông tin chuyển đổi thứ hai được sử dụng để chỉ báo rằng thiết bị phần cứng đã thoát khỏi chế độ bảo mật, và chế độ không bảo mật là chế độ đang chạy mà tương ứng với thiết bị phần cứng và nằm trong môi trường thực thi đầy đủ.

Theo phương án khác của sáng chế, bộ xử lý 210 còn có cấu trúc để:

cho phép thiết bị đầu cuối chuyển đổi từ giao diện ứng dụng tin cậy (TA) hiện tại thành giao diện ứng dụng máy khách (CA) theo yêu cầu thoát khỏi hiển thị TUI bằng cách sử dụng thiết bị phần cứng 260, trong đó yêu cầu thoát khỏi hiển thị TUI được kích hoạt theo hoạt động thứ hai trên giao diện ứng dụng tin cậy (TA) bởi người dùng.

Ngoài ra, trong cách thức thực hiện cụ thể của sáng chế, trong bước chuyển đổi từ giao diện ứng dụng tin cậy (TA) hiện tại thành giao diện ứng dụng

máy khách (CA) theo yêu cầu thoát khỏi hiển thị TUI, bộ xử lý 210 có cấu trúc cụ thể để:

điều khiển, theo yêu cầu thoát khỏi hiển thị TUI bằng cách sử dụng trình điều khiển mà của thiết bị phần cứng và nằm trong môi trường thực thi tin cậy, thiết bị phần cứng để thoát khỏi chế độ bảo mật hiện tại, trong đó chế độ bảo mật này là chế độ đang chạy mà tương ứng với thiết bị phần cứng và nằm trong môi trường thực thi tin cậy; và

điều khiển, theo thông tin chuyển đổi thứ ba bằng cách sử dụng trình điều khiển mà của thiết bị phần cứng và nằm trong môi trường thực thi đầy đủ, thiết bị phần cứng để đi vào chế độ không bảo mật, và sau đó hiển thị, trong môi trường thực thi đầy đủ, giao diện ứng dụng máy khách (CA) bằng cách viện dẫn tới thiết bị phần cứng mà đã chuyển đổi thành chế độ không bảo mật, trong đó thông tin chuyển đổi thứ ba được sử dụng để chỉ báo rằng thiết bị phần cứng đã thoát khỏi chế độ bảo mật, và chế độ không bảo mật là chế độ đang chạy mà tương ứng với thiết bị phần cứng và nằm trong môi trường thực thi đầy đủ.

Thiết bị đầu cuối được đề xuất trong phương án này của sáng chế có thể thực hiện phương pháp theo các phương án nêu trên. Thiết bị đầu cuối và phương pháp theo các phương án của sáng chế có cùng nguyên tắc thực hiện và các hiệu quả kỹ thuật. Các chi tiết không được mô tả lại ở đây lần nữa.

FIG.11 là sơ đồ cấu trúc giản lược của thiết bị đầu cuối theo phương án 3 của sáng chế. Trên thiết bị đầu cuối, ứng dụng máy khách (CA) chạy, và môi trường thực thi đầy đủ và môi trường thực thi tin cậy được thiết lập. Như được thể hiện trên FIG.11, thiết bị đầu cuối 300 trong phương án này bao gồm các thành phần như mạch tần số vô tuyến (Radio Frequency, RF) 310, bộ nhớ 320, bộ nhập 330, bộ hiển thị 340, bộ cảm biến 350, mạch auđiô 360, môđun WiFi (wireless fidelity, WiFi) 370, bộ xử lý 380, và nguồn điện 390. Người có hiểu biết trung bình trong lĩnh vực kỹ thuật có thể hiểu rằng cấu trúc thiết bị đầu cuối được thể hiện trên FIG.11 không làm giới hạn thiết bị đầu cuối, và thiết bị đầu cuối có thể bao gồm nhiều hơn hoặc ít hơn các thành phần so với các thành phần được thể hiện trên hình vẽ, hoặc một vài thành phần có thể được kết hợp, hoặc

việc áp dụng các thành phần khác có thể được sử dụng.

Phần sau đây mô tả cụ thể một vài thành phần của thiết bị đầu cuối 300 có viện dẫn tới FIG.11.

Trong phương án này, bộ xử lý 380 có thể thực hiện các chức năng của các môđun chức năng được chứa trong thiết bị đầu cuối được thể hiện trên FIG.9. Cụ thể, bộ xử lý 380 có cấu trúc để:

kích hoạt yêu cầu hiển thị giao diện người dùng tin cậy (TUI) của ứng dụng máy khách (CA) theo hoạt động thứ nhất trên giao diện ứng dụng máy khách (CA) của ứng dụng máy khách (CA) bởi người dùng, trong đó giao diện ứng dụng máy khách (CA) là giao diện người dùng mà của ứng dụng máy khách (CA) và nằm trong môi trường thực thi đầy đủ;

chuyển đổi môi trường hiển thị của ứng dụng máy khách (CA) từ môi trường thực thi đầy đủ thành môi trường thực thi tin cậy theo yêu cầu hiển thị TUI; và

điều khiển thiết bị phần cứng liên quan đến hiển thị để hiển thị giao diện ứng dụng tin cậy (TA) mà của ứng dụng máy khách (CA) và nằm trong môi trường thực thi tin cậy, trong đó giao diện ứng dụng tin cậy (TA) được sử dụng bởi người dùng của thiết bị đầu cuối để nhập vào thông tin cá nhân.

Theo cách thức thực hiện cụ thể, trong bước chuyển đổi môi trường hiển thị của ứng dụng máy khách (CA) từ môi trường thực thi đầy đủ thành môi trường thực thi tin cậy theo yêu cầu hiển thị TUI, bộ xử lý 380 có cấu trúc cụ thể để:

điều khiển, theo yêu cầu hiển thị TUI của ứng dụng máy khách (CA) bằng cách sử dụng trình điều khiển mà của thiết bị phần cứng liên quan đến hiển thị và nằm trong môi trường thực thi đầy đủ, thiết bị phần cứng để thoát khỏi chế độ không bảo mật hiện tại, trong đó chế độ không bảo mật này là chế độ đang chạy mà tương ứng với thiết bị phần cứng và nằm trong môi trường thực thi đầy đủ; và

điều khiển, theo thông tin chuyển đổi thứ nhất bằng cách sử dụng trình điều khiển mà của thiết bị phần cứng và nằm trong môi trường thực thi tin

cậy, thiết bị phần cứng để đi vào chế độ bảo mật, trong đó thông tin chuyển đổi thứ nhất được sử dụng để chỉ báo rằng thiết bị phần cứng đã thoát khỏi chế độ không bảo mật, và chế độ bảo mật là chế độ đang chạy mà tương ứng với thiết bị phần cứng và nằm trong môi trường thực thi tin cậy.

Trong bước hiển thị giao diện ứng dụng tin cậy (TA) mà của ứng dụng máy khách (CA) và nằm trong môi trường thực thi tin cậy, bộ xử lý 380 có cấu trúc cụ thể để:

chạy, trong môi trường thực thi tin cậy, TA tương ứng với CA; và

hiển thị, trong môi trường thực thi tin cậy, giao diện ứng dụng tin cậy (TA) bằng cách viện dẫn tới thiết bị phần cứng trong chế độ bảo mật.

Thiết bị phần cứng liên quan đến hiển thị bao gồm bộ nhập 330, bộ hiển thị 340, và thiết bị liên quan đến hiển thị khác như bộ nhớ trong liên quan đến hiển thị trong bộ nhớ 320.

Trong phương án của sáng chế, bộ xử lý 380 còn có cấu trúc để: cho phép thiết bị đầu cuối chuyển đổi từ giao diện ứng dụng tin cậy (TA) hiện tại thành giao diện phản hồi của sự kiện thứ nhất trong môi trường thực thi đầy đủ theo bản tin phản hồi sự kiện không bảo mật bằng cách sử dụng thiết bị phần cứng, và sau đó điều khiển, theo bản tin hồi đáp phản hồi, thiết bị phần cứng để hiển thị giao diện ứng dụng tin cậy (TA) lần nữa, trong đó bản tin phản hồi sự kiện không bảo mật được kích hoạt bởi sự kiện thứ nhất trong môi trường thực thi đầy đủ, và bản tin hồi đáp phản hồi chỉ báo rằng người dùng của thiết bị đầu cuối hoàn thành việc xử lý của sự kiện thứ nhất bằng cách sử dụng giao diện phản hồi.

Ngoài ra, trong cách thức thực hiện cụ thể của sáng chế, bộ xử lý 380 có cấu trúc cụ thể để:

kích hoạt yêu cầu tạm dừng hiển thị TUI theo bản tin phản hồi sự kiện không bảo mật;

điều khiển, theo yêu cầu tạm dừng hiển thị TUI bằng cách sử dụng trình điều khiển mà của thiết bị phần cứng và nằm trong môi trường thực thi tin cậy, thiết bị phần cứng để thoát khỏi chế độ bảo mật hiện tại, trong đó chế độ

bảo mật này là chế độ đang chạy mà tương ứng với thiết bị phần cứng và nằm trong môi trường thực thi tin cậy; và

điều khiển, theo thông tin chuyển đổi thứ hai bằng cách sử dụng trình điều khiển mà của thiết bị phần cứng và nằm trong môi trường thực thi đầy đủ, thiết bị phần cứng để đi vào chế độ không bảo mật, và sau đó hiển thị giao diện phản hồi của sự kiện thứ nhất trong môi trường thực thi đầy đủ bằng cách viện dẫn tới thiết bị phần cứng mà đã chuyển đổi thành chế độ không bảo mật, trong đó thông tin chuyển đổi thứ hai được sử dụng để chỉ báo rằng thiết bị phần cứng đã thoát khỏi chế độ bảo mật, và chế độ không bảo mật là chế độ đang chạy mà tương ứng với thiết bị phần cứng và nằm trong môi trường thực thi đầy đủ.

Theo phương án khác của sáng chế, bộ xử lý 380 còn có cấu trúc để:

cho phép thiết bị đầu cuối chuyển đổi từ giao diện ứng dụng tin cậy (TA) hiện tại thành giao diện ứng dụng máy khách (CA) theo yêu cầu thoát khỏi hiển thị TUI bằng cách sử dụng thiết bị phần cứng, trong đó yêu cầu thoát khỏi hiển thị TUI được kích hoạt theo hoạt động thứ hai trên giao diện ứng dụng tin cậy (TA) bởi người dùng.

Ngoài ra, trong cách thức thực hiện cụ thể của sáng chế, trong bước chuyển đổi từ giao diện ứng dụng tin cậy (TA) hiện tại thành giao diện ứng dụng máy khách (CA) theo yêu cầu thoát khỏi hiển thị TUI, bộ xử lý 380 có cấu trúc cụ thể để:

điều khiển, theo yêu cầu thoát khỏi hiển thị TUI bằng cách sử dụng trình điều khiển mà của thiết bị phần cứng và nằm trong môi trường thực thi tin cậy, thiết bị phần cứng để thoát khỏi chế độ bảo mật hiện tại, trong đó chế độ bảo mật này là chế độ đang chạy mà tương ứng với thiết bị phần cứng và nằm trong môi trường thực thi tin cậy; và

điều khiển, theo thông tin chuyển đổi thứ ba bằng cách sử dụng trình điều khiển mà của thiết bị phần cứng và nằm trong môi trường thực thi đầy đủ, thiết bị phần cứng để đi vào chế độ không bảo mật, và sau đó hiển thị, trong môi trường thực thi đầy đủ, giao diện ứng dụng máy khách (CA) bằng cách viện dẫn tới thiết bị phần cứng mà đã chuyển đổi thành chế độ không bảo mật, trong đó

thông tin chuyển đổi thứ ba được sử dụng để chỉ báo rằng thiết bị phần cứng đã thoát khỏi chế độ bảo mật, và chế độ không bảo mật là chế độ đang chạy mà tương ứng với thiết bị phần cứng và nằm trong môi trường thực thi đầy đủ.

Có thể được hiểu rằng, bộ nhớ 320 có thể là bộ nhớ trong của thiết bị đầu cuối 300, hoặc bộ nhớ trong và bộ nhớ ngoài của thiết bị đầu cuối 300. Bộ nhớ 320 bao gồm bộ nhớ bất biến NVRAM, bộ nhớ truy nhập ngẫu nhiên động DRAM, bộ nhớ truy nhập ngẫu nhiên tĩnh SRAM, ổ đĩa chớp, và đĩa cứng, đĩa quang, đĩa USB, đĩa mềm, hoặc ổ băng.

Bộ nhập 330 có thể còn có cấu trúc để thu chữ số hoặc thông tin ký tự được nhập, như chuỗi ký tự Trung Quốc hoặc chuỗi chữ cái mà được nhập vào bởi người dùng, và tạo ra đầu vào tín hiệu liên quan đến thiết lập người dùng và điều khiển chức năng của thiết bị đầu cuối 300. Cụ thể, trong phương án này của sáng chế, bộ nhập 330 có thể bao gồm panen chạm 331. Panen chạm 331, mà cũng được gọi là màn chạm, có thể thu thập thao tác chạm của người dùng trên hoặc gần panen chạm (ví dụ, thao tác của người dùng trên hoặc gần panen chạm 331 bằng cách sử dụng bất kỳ đối tượng thích hợp hoặc phụ kiện như ngón tay hoặc bút trỏ), và điều hướng thiết bị kết nối tương ứng theo chương trình được thiết lập trước. Một cách tùy chọn, panen chạm 331 có thể bao gồm hai phần: thiết bị dò tìm chạm và bộ điều khiển chạm. Thiết bị dò tìm chạm dò tìm góc phương vị chạm của người dùng, dò tìm tín hiệu được tạo ra từ thao tác chạm, và truyền tín hiệu này tới bộ điều khiển chạm. Bộ điều khiển chạm thu thông tin chạm từ thiết bị dò tìm chạm, chuyển đổi thông tin chạm thành các tọa độ điểm chạm, và sau đó gửi các tọa độ điểm chạm tới bộ xử lý 380. Ngoài ra, bộ điều khiển chạm có thể thu và thực thi lệnh được gửi từ bộ xử lý 380. Ngoài ra, panen chạm 331 có thể là panen chạm kiểu điện trở, điện dung, hồng ngoại, hoặc sóng âm thanh bề mặt. Ngoài panen chạm 331, bộ nhập 330 có thể còn bao gồm thiết bị nhập khác 332. Thiết bị nhập khác 332 có thể bao gồm, nhưng không bị giới hạn ở, một hoặc nhiều trong số bàn phím vật lý, phím chức năng (ví dụ, phím điều khiển âm lượng và phím chuyển đổi), bi điều khiển, chuột, cần chỉnh hướng, hoặc loại tương tự.

Thiết bị đầu cuối 300 có thể còn bao gồm bộ hiển thị 340. Bộ hiển thị 340 có thể có cấu trúc để hiển thị thông tin được nhập vào bởi người dùng và thông tin được cấp tới người dùng hoặc các giao diện thực đơn khác của thiết bị đầu cuối 300. Cụ thể, bộ hiển thị 340 có thể bao gồm panen hiển thị 341, và một cách tùy chọn, panen hiển thị 341 có thể có cấu trúc dưới dạng như màn hình tinh thể lỏng (Liquid Crystal Display, LCD), điốt phát quang hữu cơ (Organic Light-Emitting Diode, OLED), hoặc loại tương tự.

Trong phương án này của sáng chế, panen chạm 331 che phủ panen hiển thị 341, để tạo thành màn hiển thị chạm. Sau khi màn hiển thị chạm phát hiện thao tác chạm trên hoặc gần màn hiển thị chạm, màn hiển thị chạm truyền thao tác chạm tới bộ xử lý 380 để xác định loại của sự kiện chạm, và sau đó bộ xử lý 380 cấp ảnh trực quan tương ứng được xuất ra trên màn hiển thị chạm theo loại của sự kiện chạm.

Trong phương án này của sáng chế, màn hiển thị chạm bao gồm vùng hiển thị giao diện chương trình ứng dụng và vùng hiển thị điều khiển chung. Cách thức bố trí của vùng hiển thị giao diện chương trình ứng dụng và vùng hiển thị điều khiển chung không bị giới hạn, và có thể là cách thức bố trí mà trong đó hai vùng hiển thị có thể được phân biệt, ví dụ, bố trí trên-và-dưới và bố trí trái-và-phải. Vùng hiển thị giao diện chương trình ứng dụng có thể được sử dụng để hiển thị giao diện của chương trình ứng dụng. Mỗi giao diện có thể bao gồm phần tử giao diện như biểu tượng và/hoặc điều khiển màn hình nền của ít nhất một chương trình ứng dụng. Ngoài ra, vùng hiển thị giao diện chương trình ứng dụng có thể là giao diện trống mà không bao gồm bất kỳ nội dung nào. Vùng hiển thị điều khiển chung được sử dụng để hiển thị nút điều khiển mà được sử dụng tương đối thường xuyên, ví dụ, nút thiết lập, số giao diện, thanh cuộn, và biểu tượng chương trình ứng dụng như biểu tương danh bạ điện thoại.

Bộ xử lý 380 là trung tâm điều khiển của thiết bị đầu cuối 300, kết nối các phần của toàn bộ thiết bị đầu cuối bằng cách sử dụng các giao diện và đường dây khác nhau, và thực hiện các chức năng khác nhau của thiết bị đầu cuối 300 và xử lý dữ liệu bằng cách chạy hoặc thực thi chương trình phần mềm và/hoặc

môđun và dữ liệu mà được lưu trữ trong bộ nhớ 320, nhờ đó thực hiện toàn bộ việc giám sát trên thiết bị đầu cuối 300. Một cách tùy chọn, bộ xử lý 380 có thể bao gồm một hoặc nhiều bộ phận xử lý.

Thiết bị đầu cuối được đề xuất trong phương án này có thể thực hiện phương pháp theo các phương án nêu trên. Thiết bị đầu cuối và phương pháp theo các phương án của sáng chế có cùng nguyên tắc thực hiện và hiệu quả kỹ thuật. Các chi tiết không được mô tả lại ở đây.

Mặc dù sáng chế được mô tả chi tiết có viện dẫn tới các phương án nêu trên, người có hiểu biết trung bình trong lĩnh vực kỹ thuật sẽ hiểu rằng vẫn có thể tạo ra các cải biến đối với các giải pháp kỹ thuật được mô tả trong các phương án nêu trên hoặc tạo ra các thay thế tương đương đối với một vài hoặc tất cả các đặc điểm kỹ thuật của nó, mà không đi chệch khỏi phạm vi của các giải pháp kỹ thuật của các phương án theo sáng chế.

YÊU CẦU BẢO HỘ

1. Phương pháp chuyển đổi giao diện người dùng, trong đó phương pháp này được sử dụng cho thiết bị đầu cuối, và ứng dụng máy khách (CA) chạy trên thiết bị đầu cuối, môi trường thực thi đầy đủ và môi trường thực thi tin cậy được thiết lập trên thiết bị đầu cuối, và phương pháp này bao gồm:

kích hoạt yêu cầu hiển thị giao diện người dùng tin cậy (TUI) của ứng dụng máy khách (CA) theo hoạt động thứ nhất trên giao diện ứng dụng máy khách (CA) của ứng dụng máy khách (CA) bởi người dùng, trong đó giao diện ứng dụng máy khách (CA) là giao diện người dùng mà của ứng dụng máy khách (CA) và nằm trong môi trường thực thi đầy đủ;

chuyển đổi môi trường hiển thị của ứng dụng máy khách (CA) từ môi trường thực thi đầy đủ thành môi trường thực thi tin cậy theo yêu cầu hiển thị TUI; và

hiển thị giao diện ứng dụng tin cậy (TA) mà của ứng dụng máy khách (CA) và nằm trong môi trường thực thi tin cậy, trong đó giao diện ứng dụng tin cậy (TA) được sử dụng bởi người dùng của thiết bị đầu cuối để nhập vào thông tin cá nhân

trong đó thiết bị đầu cuối bao gồm thiết bị phần cứng liên quan đến hiển thị, trong đó thiết bị phần cứng liên quan đến hiển thị này có cấu trúc để hiển thị giao diện ứng dụng máy khách (CA) và giao diện ứng dụng tin cậy (TA), và bước chuyển đổi môi trường hiển thị của ứng dụng máy khách (CA) từ môi trường thực thi đầy đủ thành môi trường thực thi tin cậy theo yêu cầu hiển thị TUI bao gồm:

điều khiển, theo yêu cầu hiển thị TUI của ứng dụng máy khách (CA) bằng cách sử dụng trình điều khiển mà của thiết bị phần cứng và nằm trong môi trường thực thi đầy đủ, thiết bị phần cứng để thoát khỏi chế độ không bảo mật hiện tại, trong đó chế độ không bảo mật này là chế độ đang chạy mà tương ứng với thiết bị phần cứng và nằm trong môi trường thực thi đầy đủ; và

điều khiển, theo thông tin chuyển đổi thứ nhất bằng cách sử dụng trình điều khiển mà của thiết bị phần cứng và nằm trong môi trường thực thi tin cậy, thiết bị phần cứng để đi vào chế độ bảo mật, trong đó thông tin chuyển đổi thứ nhất được sử dụng để chỉ báo rằng thiết bị phần cứng đã thoát khỏi chế độ không bảo mật, và chế độ bảo mật là chế độ đang chạy mà tương ứng với thiết bị phần cứng và nằm trong môi trường thực thi tin cậy.

2. Phương pháp theo điểm 1, trong đó bước hiển thị giao diện ứng dụng tin cậy (TA) mà của ứng dụng máy khách (CA) và nằm trong môi trường thực thi tin cậy bao gồm:

chạy, trong môi trường thực thi tin cậy, TA tương ứng với CA; và

hiển thị, trong môi trường thực thi tin cậy, giao diện ứng dụng tin cậy (TA) bằng cách viện dẫn tới thiết bị phần cứng trong chế độ bảo mật.

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

chuyển đổi từ giao diện ứng dụng tin cậy (TA) thành giao diện phản hồi của sự kiện thứ nhất trong môi trường thực thi đầy đủ theo bản tin phản hồi sự kiện không bảo mật, trong đó bản tin phản hồi sự kiện không bảo mật được kích hoạt bởi sự kiện thứ nhất trong môi trường thực thi đầy đủ; và

hiển thị giao diện ứng dụng tin cậy (TA) lần nữa theo bản tin hồi đáp phản hồi, trong đó bản tin hồi đáp phản hồi chỉ báo rằng người dùng của thiết bị đầu cuối hoàn thành xử lý của sự kiện thứ nhất bằng cách sử dụng giao diện phản hồi.

4. Phương pháp theo điểm 3, trong đó bước chuyển đổi từ giao diện ứng dụng tin cậy (TA) thành giao diện phản hồi của sự kiện thứ nhất trong môi trường thực thi đầy đủ theo bản tin phản hồi sự kiện không bảo mật một cách cụ thể bao gồm:

kích hoạt yêu cầu tạm dừng hiển thị TUI theo bản tin phản hồi sự kiện không bảo mật;

điều khiển, theo yêu cầu tạm dừng hiển thị TUI bằng cách sử dụng trình điều khiển mà của thiết bị phần cứng và nằm trong môi trường thực thi tin cậy, thiết bị phần cứng để thoát khỏi chế độ bảo mật hiện tại, trong đó chế độ bảo

mật này là chế độ đang chạy mà tương ứng với thiết bị phần cứng và nằm trong môi trường thực thi tin cậy;

điều khiển, theo thông tin chuyển đổi thứ hai bằng cách sử dụng trình điều khiển mà của thiết bị phần cứng và nằm trong môi trường thực thi đầy đủ, thiết bị phần cứng để đi vào chế độ không bảo mật, trong đó thông tin chuyển đổi thứ hai được sử dụng để chỉ báo rằng thiết bị phần cứng đã thoát khỏi chế độ bảo mật, và chế độ không bảo mật là chế độ đang chạy mà tương ứng với thiết bị phần cứng và nằm trong môi trường thực thi đầy đủ; và

hiển thị giao diện phản hồi của sự kiện thứ nhất trong môi trường thực thi đầy đủ bằng cách viện dẫn tới thiết bị phần cứng mà đã chuyển đổi thành chế độ không bảo mật.

5. Phương pháp theo điểm bất kỳ trong số các điểm 1 đến 4, trong đó phương pháp này còn bao gồm:

chuyển đổi từ giao diện ứng dụng tin cậy (TA) hiện tại thành giao diện ứng dụng máy khách (CA) theo yêu cầu thoát khỏi hiển thị TUI, trong đó yêu cầu thoát khỏi hiển thị TUI được kích hoạt bởi hoạt động thứ hai trên giao diện ứng dụng tin cậy (TA) bởi người dùng.

6. Phương pháp theo điểm 5 bước chuyển đổi từ giao diện ứng dụng tin cậy (TA) hiện tại thành giao diện ứng dụng máy khách (CA) theo yêu cầu thoát khỏi hiển thị TUI một cách cụ thể bao gồm:

điều khiển, theo yêu cầu thoát khỏi hiển thị TUI bằng cách sử dụng trình điều khiển mà của thiết bị phần cứng và nằm trong môi trường thực thi tin cậy, thiết bị phần cứng để thoát khỏi chế độ bảo mật hiện tại, trong đó chế độ bảo mật này là chế độ đang chạy mà tương ứng với thiết bị phần cứng và nằm trong môi trường thực thi tin cậy;

điều khiển, theo thông tin chuyển đổi thứ ba bằng cách sử dụng trình điều khiển mà của thiết bị phần cứng và nằm trong môi trường thực thi đầy đủ, thiết bị phần cứng để đi vào chế độ không bảo mật, trong đó thông tin chuyển đổi thứ ba được sử dụng để chỉ báo rằng thiết bị phần cứng đã thoát khỏi chế độ bảo mật, và chế độ không bảo mật là chế độ đang chạy mà tương ứng với thiết bị phần

cứng và nằm trong môi trường thực thi đầy đủ; và

hiển thị, trong môi trường thực thi đầy đủ, giao diện ứng dụng máy khách (CA) bằng cách viện dẫn tới thiết bị phần cứng mà đã chuyển đổi thành chế độ không bảo mật.

7. Thiết bị đầu cuối, trong đó ứng dụng máy khách (CA) chạy trên thiết bị đầu cuối, môi trường thực thi đầy đủ và môi trường thực thi tin cậy được thiết lập trên thiết bị đầu cuối, và thiết bị đầu cuối này bao gồm:

môđun kích hoạt, có cấu trúc để kích hoạt yêu cầu hiển thị giao diện người dùng tin cậy (TUI) của ứng dụng máy khách (CA) theo hoạt động thứ nhất trên giao diện ứng dụng máy khách (CA) của ứng dụng máy khách (CA) bởi người dùng, trong đó giao diện ứng dụng máy khách (CA) là giao diện người dùng mà của ứng dụng máy khách (CA) và nằm trong môi trường thực thi đầy đủ;

môđun chuyển đổi, có cấu trúc để chuyển đổi môi trường hiển thị của ứng dụng máy khách (CA) từ môi trường thực thi đầy đủ thành môi trường thực thi tin cậy theo yêu cầu hiển thị TUI; và

môđun hiển thị, có cấu trúc để hiển thị giao diện ứng dụng tin cậy (TA) mà của ứng dụng máy khách (CA) và nằm trong môi trường thực thi tin cậy, trong đó giao diện ứng dụng tin cậy (TA) được sử dụng bởi người dùng của thiết bị đầu cuối để nhập vào thông tin cá nhân;

trong đó thiết bị đầu cuối còn bao gồm thiết bị phần cứng liên quan đến hiển thị, và trong bước chuyển đổi môi trường hiển thị của ứng dụng máy khách (CA) từ môi trường thực thi đầy đủ thành môi trường thực thi tin cậy theo yêu cầu hiển thị TUI, môđun chuyển đổi có cấu trúc cụ thể để:

điều khiển, theo yêu cầu hiển thị TUI của ứng dụng máy khách (CA) bằng cách sử dụng trình điều khiển mà của thiết bị phần cứng và nằm trong môi trường thực thi đầy đủ, thiết bị phần cứng để thoát khỏi chế độ không bảo mật hiện tại, trong đó chế độ không bảo mật này là chế độ đang chạy mà tương ứng với thiết bị phần cứng và nằm trong môi trường thực thi đầy đủ; và

điều khiển, theo thông tin chuyển đổi thứ nhất bằng cách sử dụng trình điều khiển mà của thiết bị phần cứng và nằm trong môi trường thực thi tin cậy, thiết

bị phần cứng để đi vào chế độ bảo mật, trong đó thông tin chuyển đổi thứ nhất được sử dụng để chỉ báo rằng thiết bị phần cứng đã thoát khỏi chế độ không bảo mật, và chế độ bảo mật là chế độ đang chạy mà tương ứng với thiết bị phần cứng và nằm trong môi trường thực thi tin cậy.

8. Thiết bị đầu cuối theo điểm 7, trong đó trong bước hiển thị giao diện ứng dụng tin cậy (TA) mà của ứng dụng máy khách (CA) và nằm trong môi trường thực thi tin cậy, môđun hiển thị có cấu trúc cụ thể để:

chạy, trong môi trường thực thi tin cậy, TA tương ứng với CA; và

hiển thị, trong môi trường thực thi tin cậy, giao diện ứng dụng tin cậy (TA) bằng cách viện dẫn tới thiết bị phần cứng trong chế độ bảo mật.

9. Thiết bị đầu cuối theo điểm 7, trong đó môđun chuyển đổi còn có cấu trúc để: cho phép thiết bị đầu cuối chuyển đổi từ giao diện ứng dụng tin cậy (TA) hiện tại thành giao diện phản hồi của sự kiện thứ nhất trong môi trường thực thi đầy đủ theo bản tin phản hồi sự kiện không bảo mật bằng cách sử dụng môđun hiển thị, và sau đó chỉ dẫn, theo bản tin hồi đáp phản hồi, môđun hiển thị để hiển thị giao diện ứng dụng tin cậy (TA) lần nữa, trong đó bản tin phản hồi sự kiện không bảo mật được kích hoạt bởi sự kiện thứ nhất trong môi trường thực thi đầy đủ; và bản tin hồi đáp phản hồi chỉ báo rằng người dùng của thiết bị đầu cuối hoàn thành việc xử lý của sự kiện thứ nhất bằng cách sử dụng giao diện phản hồi.

10. Thiết bị đầu cuối theo điểm 9, trong đó thiết bị phần cứng liên quan đến hiển thị có cấu trúc để hiển thị giao diện ứng dụng máy khách (CA) và giao diện ứng dụng tin cậy (TA), và môđun chuyển đổi có cấu trúc cụ thể để:

kích hoạt yêu cầu tạm dừng hiển thị TUI theo bản tin phản hồi sự kiện không bảo mật;

điều khiển, theo yêu cầu tạm dừng hiển thị TUI bằng cách sử dụng trình điều khiển mà của thiết bị phần cứng và nằm trong môi trường thực thi tin cậy, thiết bị phần cứng để thoát khỏi chế độ bảo mật hiện tại, trong đó chế độ bảo mật này là chế độ đang chạy mà tương ứng với thiết bị phần cứng và nằm trong môi trường thực thi tin cậy; và

điều khiển, theo thông tin chuyển đổi thứ hai bằng cách sử dụng trình điều khiển mà của thiết bị phần cứng và nằm trong môi trường thực thi đầy đủ, thiết bị phần cứng để đi vào chế độ không bảo mật, và sau đó chỉ dẫn môđun hiển thị để hiển thị giao diện phản hồi của sự kiện thứ nhất trong môi trường thực thi đầy đủ bằng cách viện dẫn tới thiết bị phần cứng mà đã chuyển đổi thành chế độ không bảo mật, trong đó thông tin chuyển đổi thứ hai được sử dụng để chỉ báo rằng thiết bị phần cứng đã thoát khỏi chế độ bảo mật, và chế độ không bảo mật là chế độ đang chạy mà tương ứng với thiết bị phần cứng và nằm trong môi trường thực thi đầy đủ.

11. Thiết bị đầu cuối theo điểm bất kỳ trong số các điểm 7 đến 10, trong đó môđun chuyển đổi còn có cấu trúc để:

cho phép thiết bị đầu cuối chuyển đổi từ giao diện ứng dụng tin cậy (TA) hiện tại thành giao diện ứng dụng máy khách (CA) theo yêu cầu thoát khỏi hiển thị TUI bằng cách sử dụng môđun hiển thị, trong đó yêu cầu thoát khỏi hiển thị TUI được kích hoạt bởi môđun kích hoạt theo hoạt động thứ hai trên giao diện ứng dụng tin cậy (TA) bởi người dùng.

12. Thiết bị đầu cuối theo điểm 11, trong đó trong bước chuyển đổi từ giao diện ứng dụng tin cậy (TA) hiện tại thành giao diện ứng dụng máy khách (CA) theo yêu cầu thoát khỏi hiển thị TUI, môđun chuyển đổi có cấu trúc cụ thể để:

điều khiển, theo yêu cầu thoát khỏi hiển thị TUI bằng cách sử dụng trình điều khiển mà của thiết bị phần cứng và nằm trong môi trường thực thi tin cậy, thiết bị phần cứng để thoát khỏi chế độ bảo mật hiện tại, trong đó chế độ bảo mật này là chế độ đang chạy mà tương ứng với thiết bị phần cứng và nằm trong môi trường thực thi tin cậy; và

điều khiển, theo thông tin chuyển đổi thứ ba bằng cách sử dụng trình điều khiển mà của thiết bị phần cứng và nằm trong môi trường thực thi đầy đủ, thiết bị phần cứng để đi vào chế độ không bảo mật, và sau đó chỉ dẫn môđun hiển thị để hiển thị, trong môi trường thực thi đầy đủ, giao diện ứng dụng máy khách (CA) bằng cách viện dẫn tới thiết bị phần cứng mà đã chuyển đổi thành chế độ không bảo mật, trong đó thông tin chuyển đổi thứ ba được sử dụng để chỉ báo

rằng thiết bị phần cứng đã thoát khỏi chế độ bảo mật, và chế độ không bảo mật là chế độ đang chạy mà tương ứng với thiết bị phần cứng và nằm trong môi trường thực thi đầy đủ.

13. Thiết bị đầu cuối, trong đó ứng dụng máy khách (CA) chạy trên thiết bị đầu cuối, môi trường thực thi đầy đủ và môi trường thực thi tin cậy được thiết lập trên thiết bị đầu cuối, và thiết bị đầu cuối bao gồm: bộ xử lý, bộ nhớ, và thiết bị phần cứng có cấu trúc để hiển thị giao diện của thiết bị đầu cuối, trong đó bộ nhớ lưu trữ chương trình hoặc chỉ dẫn, và bộ xử lý viện dẫn chương trình hoặc chỉ dẫn mà được lưu trữ trong bộ nhớ, để:

kích hoạt yêu cầu hiển thị giao diện người dùng tin cậy (TUI) của ứng dụng máy khách (CA) theo hoạt động thứ nhất trên giao diện ứng dụng máy khách (CA) của ứng dụng máy khách (CA) bởi người dùng, trong đó giao diện ứng dụng máy khách (CA) là giao diện người dùng mà của ứng dụng máy khách (CA) và nằm trong môi trường thực thi đầy đủ;

chuyển đổi môi trường hiển thị của ứng dụng máy khách (CA) từ môi trường thực thi đầy đủ thành môi trường thực thi tin cậy theo yêu cầu hiển thị TUI; và

điều khiển thiết bị phần cứng để hiển thị giao diện ứng dụng tin cậy (TA) mà của ứng dụng máy khách (CA) và nằm trong môi trường thực thi tin cậy, trong đó giao diện ứng dụng tin cậy (TA) được sử dụng bởi người dùng của thiết bị đầu cuối để nhập vào thông tin cá nhân;

trong đó trong bước chuyển đổi môi trường hiển thị của ứng dụng máy khách (CA) từ môi trường thực thi đầy đủ thành môi trường thực thi tin cậy theo yêu cầu hiển thị TUI, bộ xử lý có cấu trúc cụ thể để:

điều khiển, theo yêu cầu hiển thị TUI của ứng dụng máy khách (CA) bằng cách sử dụng trình điều khiển mà của thiết bị phần cứng và nằm trong môi trường thực thi đầy đủ, thiết bị phần cứng để thoát khỏi chế độ không bảo mật hiện tại, trong đó chế độ không bảo mật này là chế độ đang chạy mà tương ứng với thiết bị phần cứng và nằm trong môi trường thực thi đầy đủ; và

điều khiển, theo thông tin chuyển đổi thứ nhất bằng cách sử dụng trình điều

khiển mà của thiết bị phần cứng và nằm trong môi trường thực thi tin cậy, thiết bị phần cứng để đi vào chế độ bảo mật, trong đó thông tin chuyển đổi thứ nhất được sử dụng để chỉ báo rằng thiết bị phần cứng đã thoát khỏi chế độ không bảo mật, và chế độ bảo mật là chế độ đang chạy mà tương ứng với thiết bị phần cứng và nằm trong môi trường thực thi tin cậy.

14. Thiết bị đầu cuối theo điểm 13, trong đó trong bước hiển thị giao diện ứng dụng tin cậy (TA) mà của ứng dụng máy khách (CA) và nằm trong môi trường thực thi tin cậy, bộ xử lý có cấu trúc cụ thể để:

chạy, trong môi trường thực thi tin cậy, TA tương ứng với CA; và

hiển thị, trong môi trường thực thi tin cậy, giao diện ứng dụng tin cậy (TA) bằng cách viện dẫn tới thiết bị phần cứng trong chế độ bảo mật.

15. Thiết bị đầu cuối theo điểm 13, trong đó bộ xử lý còn có cấu trúc để: cho phép thiết bị đầu cuối chuyển đổi từ giao diện ứng dụng tin cậy (TA) hiện tại thành giao diện phản hồi của sự kiện thứ nhất trong môi trường thực thi đầy đủ theo bản tin phản hồi sự kiện không bảo mật bằng cách sử dụng thiết bị phần cứng, và sau đó điều khiển, theo bản tin hồi đáp phản hồi, thiết bị phần cứng để hiển thị giao diện ứng dụng tin cậy (TA) lần nữa, trong đó bản tin phản hồi sự kiện không bảo mật được kích hoạt bởi sự kiện thứ nhất trong môi trường thực thi đầy đủ; và bản tin hồi đáp phản hồi chỉ báo rằng người dùng của thiết bị đầu cuối hoàn thành việc xử lý của sự kiện thứ nhất bằng cách sử dụng giao diện phản hồi.

16. Thiết bị đầu cuối theo điểm 15, trong đó bộ xử lý có cấu trúc cụ thể để:

kích hoạt yêu cầu tạm dừng hiển thị TUI theo bản tin phản hồi sự kiện không bảo mật;

điều khiển, theo yêu cầu tạm dừng hiển thị TUI bằng cách sử dụng trình điều khiển mà của thiết bị phần cứng và nằm trong môi trường thực thi tin cậy, thiết bị phần cứng để thoát khỏi chế độ bảo mật hiện tại, trong đó chế độ bảo mật này là chế độ đang chạy mà tương ứng với thiết bị phần cứng và nằm trong môi trường thực thi tin cậy; và

điều khiển, theo thông tin chuyển đổi thứ hai bằng cách sử dụng trình điều

khiển mà của thiết bị phần cứng và nằm trong môi trường thực thi đầy đủ, thiết bị phần cứng để đi vào chế độ không bảo mật, và sau đó hiển thị giao diện phản hồi của sự kiện thứ nhất trong môi trường thực thi đầy đủ bằng cách viện dẫn tới thiết bị phần cứng mà đã chuyển đổi thành chế độ không bảo mật, trong đó thông tin chuyển đổi thứ hai được sử dụng để chỉ báo rằng thiết bị phần cứng đã thoát khỏi chế độ bảo mật, và chế độ không bảo mật là chế độ đang chạy mà tương ứng với thiết bị phần cứng và nằm trong môi trường thực thi đầy đủ.

17. Thiết bị đầu cuối theo điểm bất kỳ trong số các điểm 13 đến 16, trong đó bộ xử lý còn có cấu trúc để:

cho phép thiết bị đầu cuối chuyển đổi từ giao diện ứng dụng tin cậy (TA) hiện tại thành giao diện ứng dụng máy khách (CA) theo yêu cầu thoát khỏi hiển thị TUI bằng cách sử dụng thiết bị phần cứng, trong đó yêu cầu thoát khỏi hiển thị TUI được kích hoạt bởi môđun kích hoạt theo hoạt động thứ hai trên giao diện ứng dụng tin cậy (TA) bởi người dùng.

18. Thiết bị đầu cuối theo điểm 17, trong đó trong bước chuyển đổi từ giao diện ứng dụng tin cậy (TA) hiện tại thành giao diện ứng dụng máy khách (CA) theo yêu cầu thoát khỏi hiển thị TUI, bộ xử lý có cấu trúc cụ thể để:

điều khiển, theo yêu cầu thoát khỏi hiển thị TUI bằng cách sử dụng trình điều khiển mà của thiết bị phần cứng và nằm trong môi trường thực thi tin cậy, thiết bị phần cứng để thoát khỏi chế độ bảo mật hiện tại, trong đó chế độ bảo mật này là chế độ đang chạy mà tương ứng với thiết bị phần cứng và nằm trong môi trường thực thi tin cậy; và

điều khiển, theo thông tin chuyển đổi thứ ba bằng cách sử dụng trình điều khiển mà của thiết bị phần cứng và nằm trong môi trường thực thi đầy đủ, thiết bị phần cứng để đi vào chế độ không bảo mật, và sau đó hiển thị, trong môi trường thực thi đầy đủ, giao diện ứng dụng máy khách (CA) bằng cách viện dẫn tới thiết bị phần cứng mà đã chuyển đổi thành chế độ không bảo mật, trong đó thông tin chuyển đổi thứ ba được sử dụng để chỉ báo rằng thiết bị phần cứng đã thoát khỏi chế độ bảo mật, và chế độ không bảo mật là chế độ đang chạy mà tương ứng với thiết bị phần cứng và nằm trong môi trường thực thi đầy đủ.

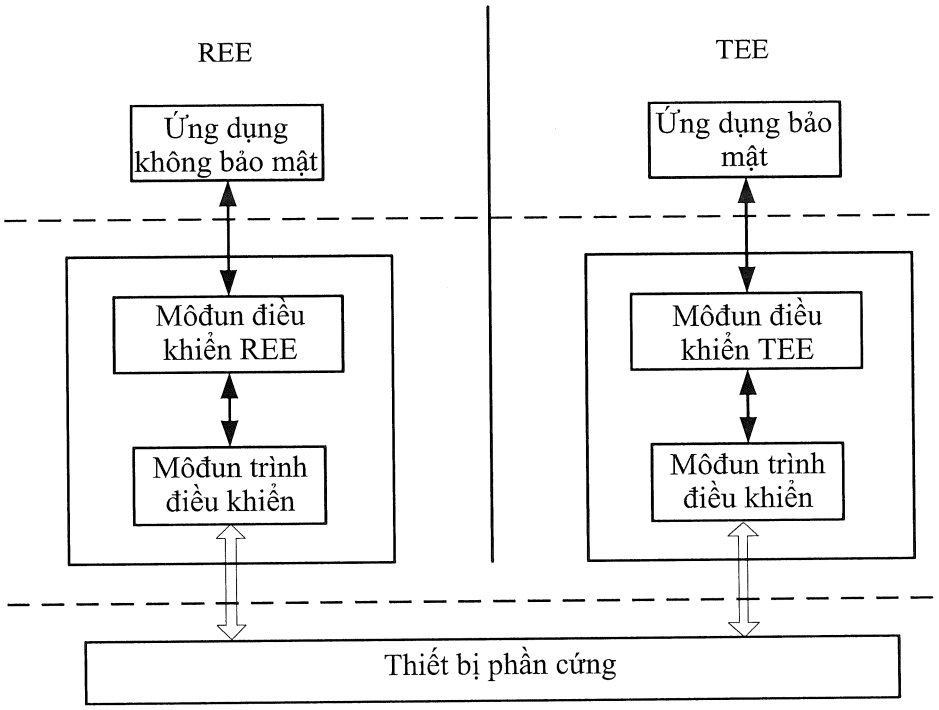
REE
TEE
Ứng dụng không bảo mật
Ứng dụng bảo mật
Môđun điều khiển REE
Môđun trình điều khiển
Môđun điều khiển TEE
Môđun trình điều khiển
Thiết bị phần cứng

FIG. 1

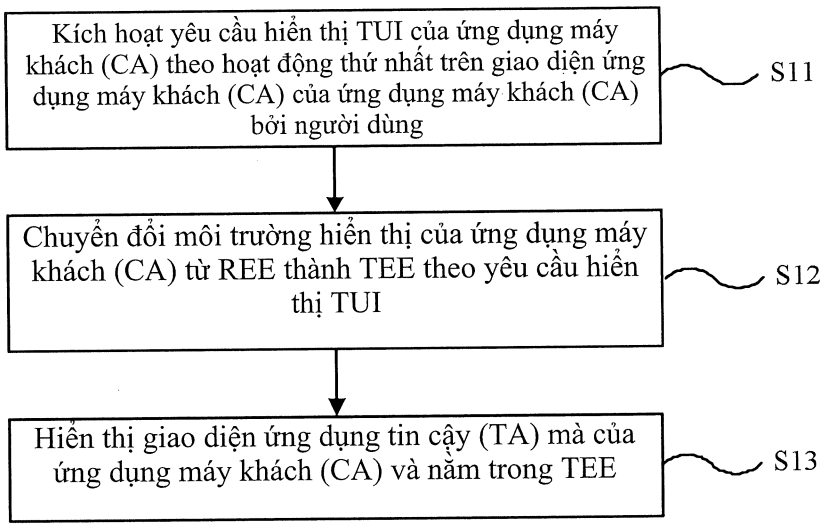
Kích hoạt yêu cầu hiển thị TUI của ứng dụng máy khách (CA) theo hoạt động thứ nhất trên giao diện ứng dụng máy khách (CA) của ứng dụng máy khách (CA) bởi người dùng
S11
Chuyển đổi môi trường hiển thị của ứng dụng máy khách (CA) từ REE thành TEE theo yêu cầu hiển thị TUI
S12
Hiển thị giao diện ứng dụng tin cậy (TA) mà của ứng dụng máy khách (CA) và nằm trong TEE
S13

FIG. 2

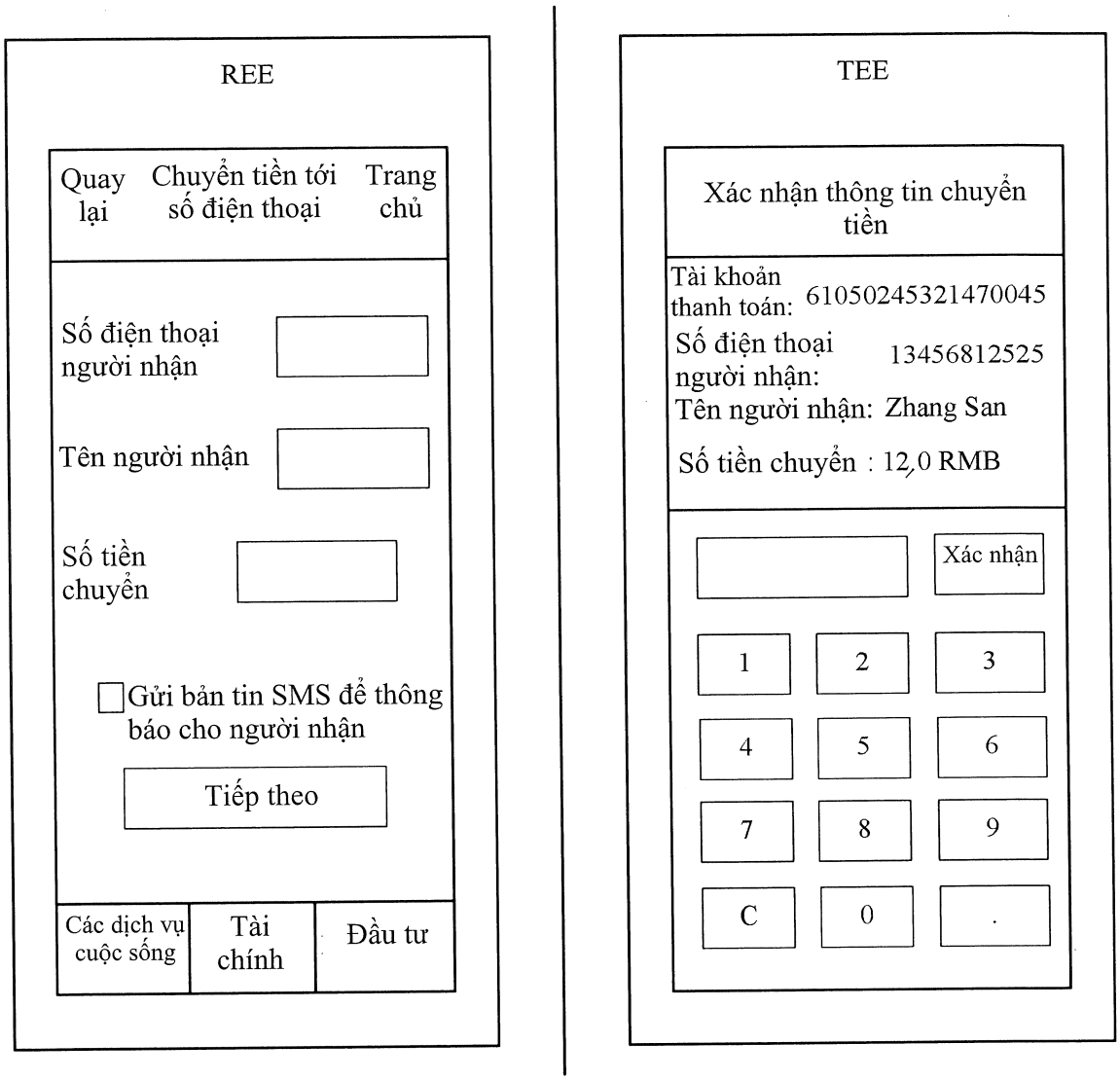
REE
Quay lại
Chuyển tiền tới số điện thoại
Trang chủ
Số điện thoại người nhận
Tên người nhận
Số tiền chuyển
Gửi bản tin SMS để thông báo cho người nhận
Tiếp theo
Các dịch vụ cuộc sống
Tài chính
Đầu tư
TEE
Xác nhận thông tin chuyển tiền
Tài khoản thanh toán: 61050245321470045
Số điện thoại người nhận: 13456812525
Tên người nhận: Zhang San
Số tiền chuyển : 12,0 RMB
Xác nhận
1
2
3
4
5
6
7
8
9
C
0
.

FIG. 3

3/8

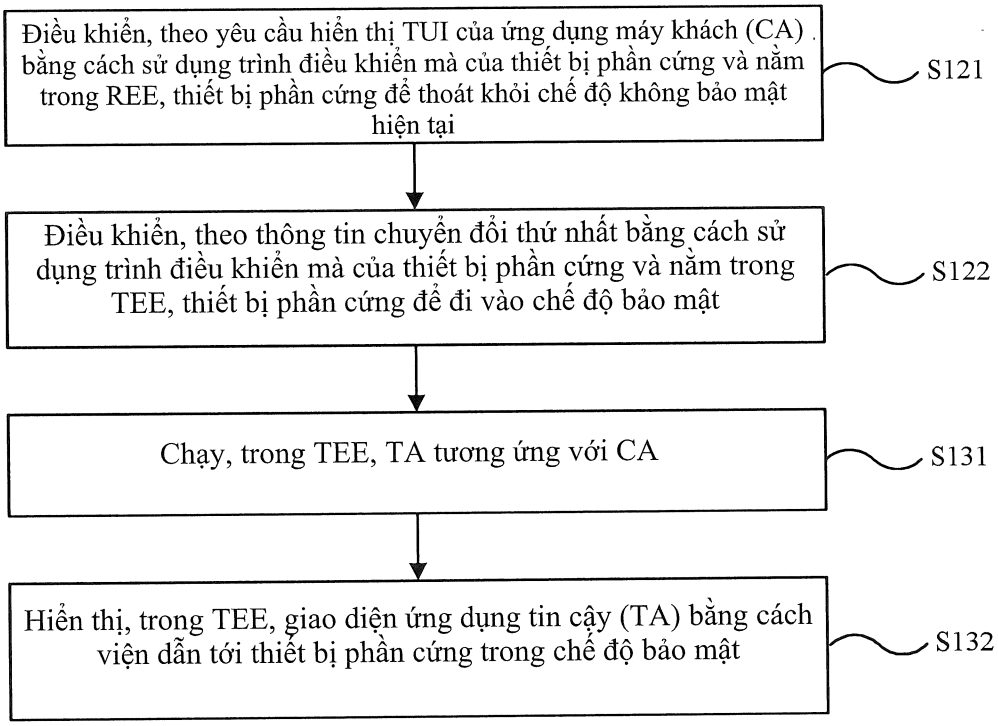
Điều khiển, theo yêu cầu hiển thị TUI của ứng dụng máy khách (CA) bằng cách sử dụng trình điều khiển mà của thiết bị phần cứng và nằm trong REE, thiết bị phần cứng để thoát khỏi chế độ không bảo mật hiện tại
S121
Điều khiển, theo thông tin chuyển đổi thứ nhất bằng cách sử dụng trình điều khiển mà của thiết bị phần cứng và nằm trong TEE, thiết bị phần cứng để đi vào chế độ bảo mật
S122
Chạy, trong TEE, TA tương ứng với CA
S131
Hiển thị, trong TEE, giao diện ứng dụng tin cậy (TA) bằng cách viện dẫn tới thiết bị phần cứng trong chế độ bảo mật
S132

FIG. 4

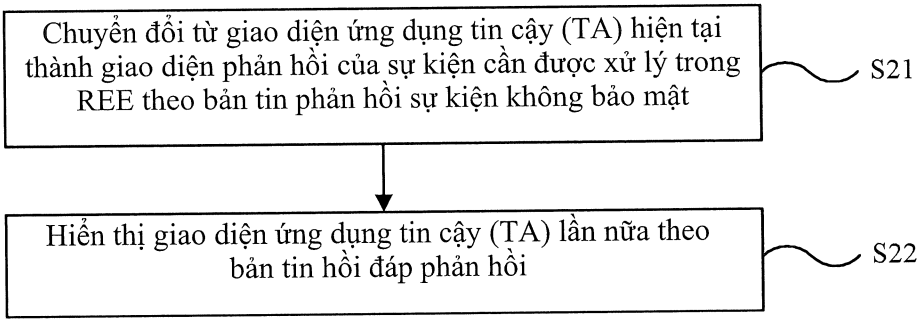
Chuyển đổi từ giao diện ứng dụng tin cậy (TA) hiện tại thành giao diện phản hồi của sự kiện cần được xử lý trong REE theo bản tin phản hồi sự kiện không bảo mật
S21
Hiển thị giao diện ứng dụng tin cậy (TA) lần nữa theo bản tin hồi đáp phản hồi
S22

FIG. 5

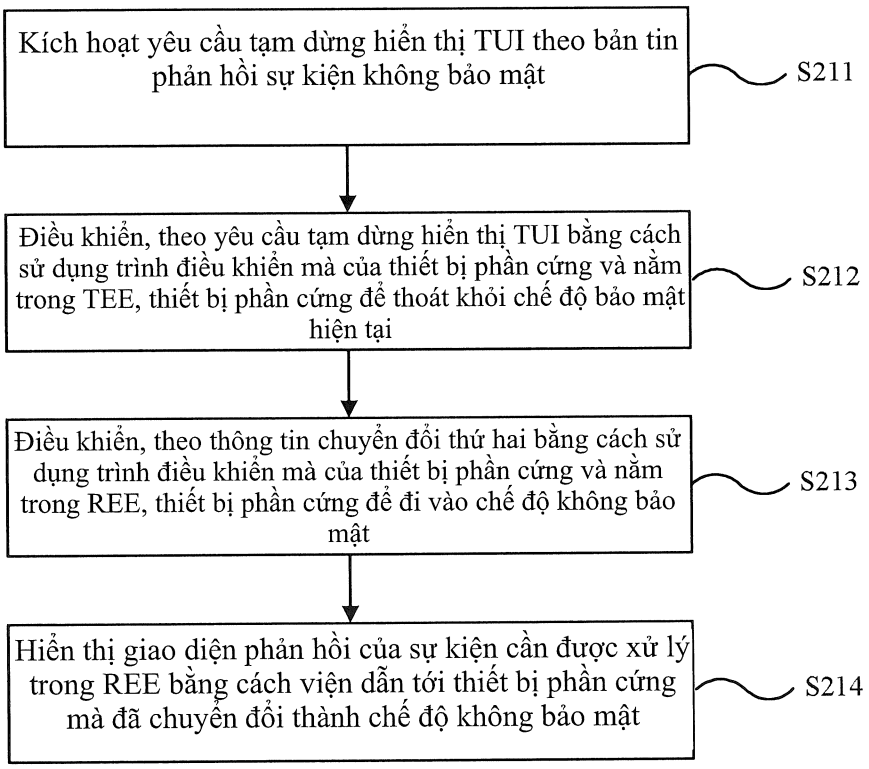
Kích hoạt yêu cầu tạm dừng hiển thị TUI theo bản tin phản hồi sự kiện không bảo mật
S211
Điều khiển, theo yêu cầu tạm dừng hiển thị TUI bằng cách sử dụng trình điều khiển mà của thiết bị phần cứng và nằm trong TEE, thiết bị phần cứng để thoát khỏi chế độ bảo mật hiện tại
S212
Điều khiển, theo thông tin chuyển đổi thứ hai bằng cách sử dụng trình điều khiển mà của thiết bị phần cứng và nằm trong REE, thiết bị phần cứng để đi vào chế độ không bảo mật
S213
Hiển thị giao diện phản hồi của sự kiện cần được xử lý trong REE bằng cách viện dẫn tới thiết bị phần cứng mà đã chuyển đổi thành chế độ không bảo mật
S214

FIG. 6

5/8

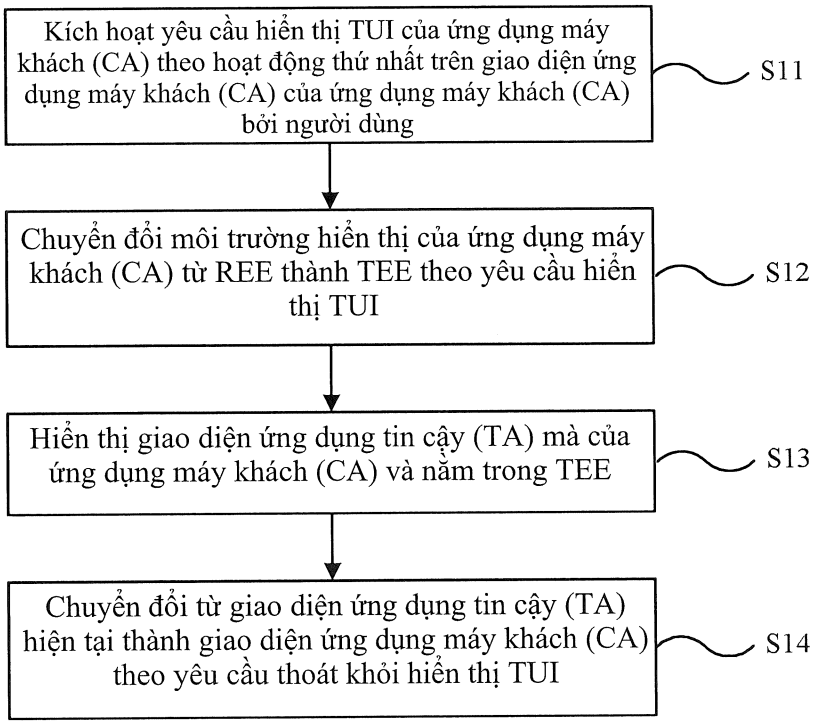
Kích hoạt yêu cầu hiển thị TUI của ứng dụng máy khách (CA) theo hoạt động thứ nhất trên giao diện ứng dụng máy khách (CA) của ứng dụng máy khách (CA) bởi người dùng
S11
Chuyển đổi môi trường hiển thị của ứng dụng máy khách (CA) từ REE thành TEE theo yêu cầu hiển thị TUI
S12
Hiển thị giao diện ứng dụng tin cậy (TA) mà của ứng dụng máy khách (CA) và nằm trong TEE
S13
Chuyển đổi từ giao diện ứng dụng tin cậy (TA) hiện tại thành giao diện ứng dụng máy khách (CA) theo yêu cầu thoát khỏi hiển thị TUI
S14

FIG. 7

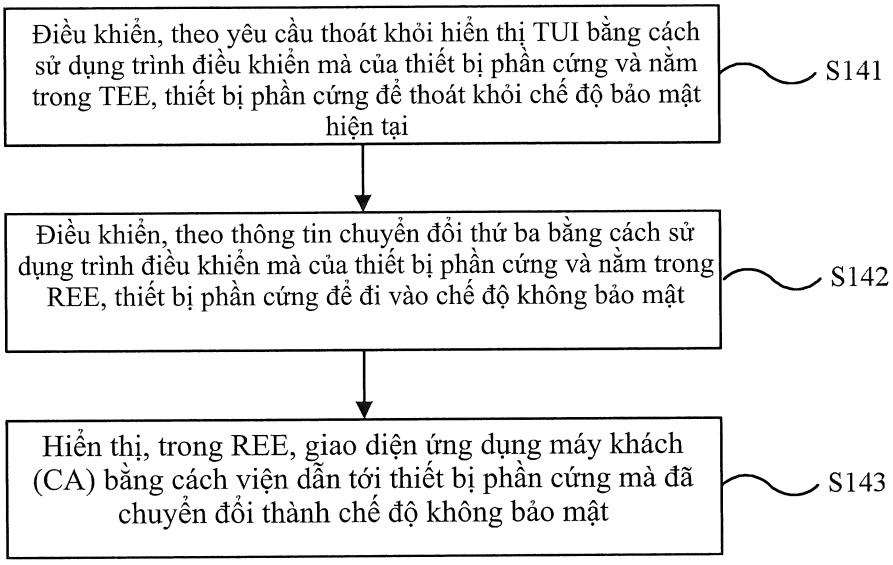
Điều khiển, theo yêu cầu thoát khỏi hiển thị TUI bằng cách sử dụng trình điều khiển mà của thiết bị phần cứng và nằm trong TEE, thiết bị phần cứng để thoát khỏi chế độ bảo mật hiện tại
S141
Điều khiển, theo thông tin chuyển đổi thứ ba bằng cách sử dụng trình điều khiển mà của thiết bị phần cứng và nằm trong REE, thiết bị phần cứng để đi vào chế độ không bảo mật
S142
Hiển thị, trong REE, giao diện ứng dụng máy khách (CA) bằng cách viện dẫn tới thiết bị phần cứng mà đã chuyển đổi thành chế độ không bảo mật
S143

FIG. 8

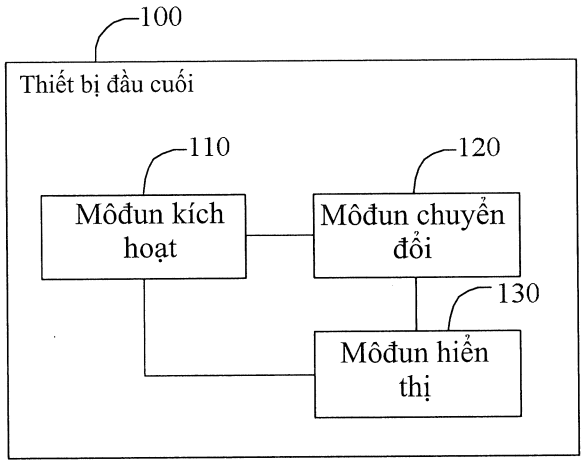
100
Thiết bị đầu cuối
110
Môđun kích hoạt
120
Môđun chuyển đổi
130
Môđun hiển thị

FIG. 9

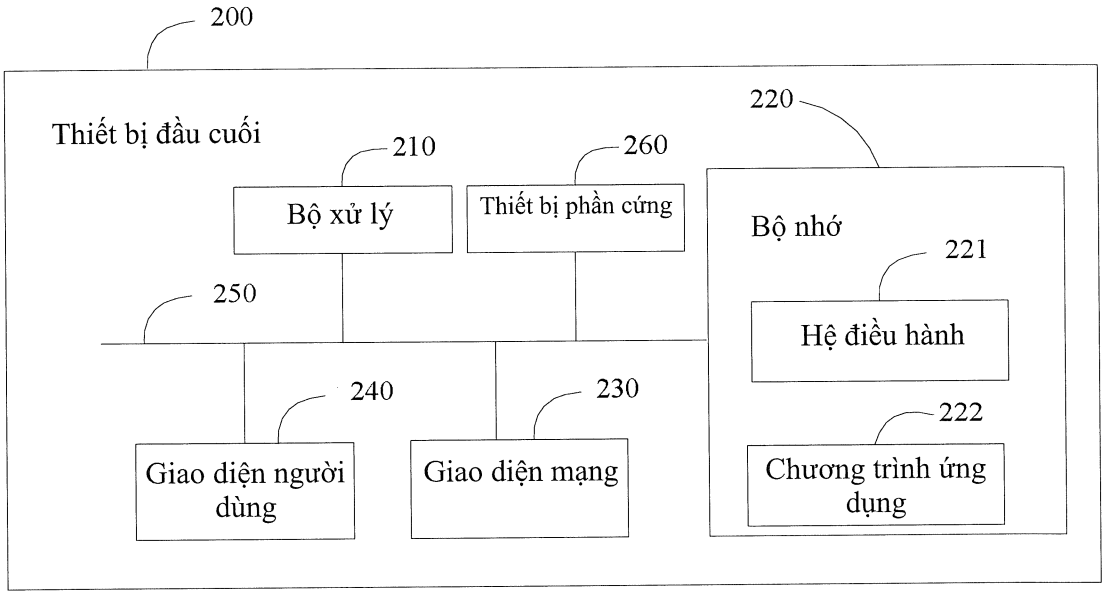
200
Thiết bị đầu cuối
210
Bộ xử lý
260
Thiết bị phần cứng
220
Bộ nhớ
221
Hệ điều hành
250
240
Giao diện người dùng
230
Giao diện mạng
222
Chương trình ứng dụng

FIG. 10

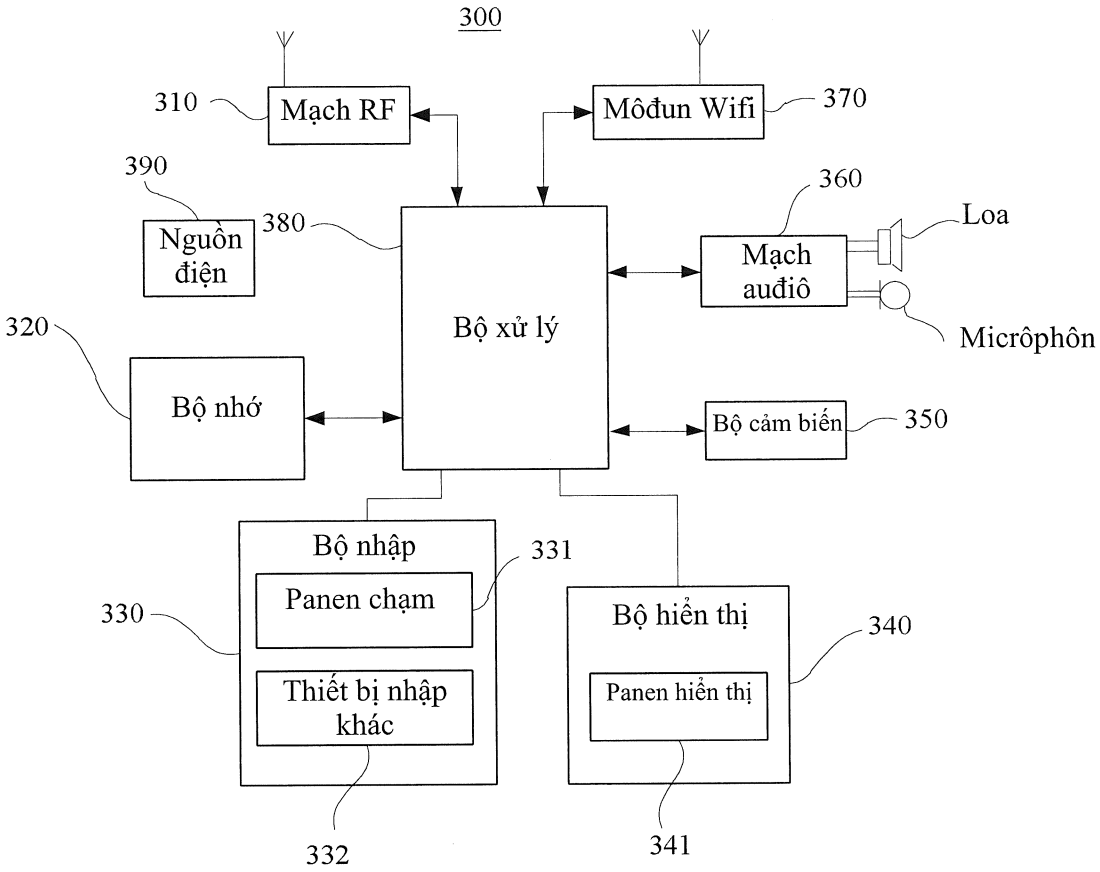
300
310
Mạch RF
Môđun Wifi
370
390
Nguồn điện
380
Bộ xử lý
360
Mạch auđiô
Loa
Micrôphôn
320
Bộ nhớ
Bộ cảm biến
350
Bộ nhập
331
Panen chạm
330
Thiết bị nhập khác
Bộ hiển thị
340
Panen hiển thị
332
341

FIG. 11