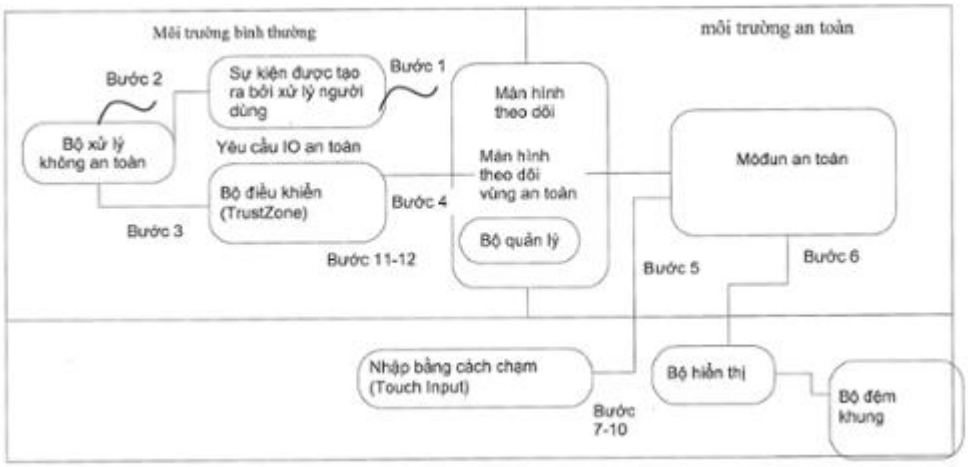
(12) BẢN MÔ TẢ SÁNG CHẾ THUỘC BẰNG ĐỘC QUYỀN SÁNG CHẾ
(19) **Cộng hòa xã hội chủ nghĩa Việt Nam (VN)**
CỤC SỞ HỮU TRÍ TUỆ
(11) **1-0034715**
(51)[8] **G06F 21/55**
(13) **B**

(21) 1-2018-04485
(22) 03/03/2017
(86) PCT/CN2017/075643 03/03/2017
(87) WO 2017/157192 A1 21/09/2017
(30) 201610145990.7 15/03/2016 CN
(45) 25/01/2023 418
(43) 25/01/2019 370A
(73) HUAWEI TECHNOLOGIES CO., LTD. (CN)
Huawei Administration Building, Bantian, Longgang District Shenzhen, Guangdong 518129, China
(72) ZHANG, Peng (CN); WANG, Ji (CN); LI, Hui (CN); XIE, Hongliang (CN); WANG, Xiaopu (CN).
(74) Công ty TNHH một thành viên Sở hữu trí tuệ VCCI (VCCI-IP CO.,LTD)

(54) PHƯƠNG PHÁP NHẬP DỮ LIỆU, THIẾT BỊ TRUYỀN THÔNG VÀ PHƯƠNG TIỆN LƯU TRỮ BẤT BIẾN ĐỌC ĐƯỢC BỞI MÁY TÍNH

(57) Sáng chế đề cập đến phương pháp và thiết bị nhập dữ liệu, và thiết bị người dùng. Phương pháp này bao gồm các bước: khi xác định được là xử lý của người dùng trên thiết bị người dùng (UE, User equipment) không được thực hiện trong vùng hiển thị được thiết lập trước, cấp sự kiện tương ứng với xử lý đến môi trường xử lý thứ nhất để xử lý, trong đó vùng hiển thị được thiết lập trước chạy trong môi trường xử lý thứ hai của thiết bị người dùng (UE), và môi trường xử lý thứ hai có mức độ bảo mật cao hơn so với môi trường xử lý thứ nhất. Việc này có thể cải thiện hơn nữa độ bảo mật của sự kiện được tạo ra khi người dùng xử lý chương trình mà chạy trong môi trường bình thường (Normal World) của thiết bị người dùng, và có thể trực tiếp xử lý sự kiện mà chạy trong môi trường Normal World.



Lĩnh vực kỹ thuật được đề cập

Sáng chế đề cập đến lĩnh vực kỹ thuật truyền thông, và cụ thể, sáng chế đề cập đến phương pháp và thiết bị nhập dữ liệu, và thiết bị người dùng.

Tình trạng kỹ thuật của sáng chế

Với sự phát triển liên tục của các kỹ thuật truyền thông, thiết bị người dùng UE (user equipment) có thể cung cấp chức năng ứng dụng công suất mạnh hơn nữa, và dữ liệu nhiều hơn nữa như tài sản riêng hoặc sự bảo mật được lưu trữ trong thiết bị người dùng.

Thiết bị người dùng liên tục phát triển, và các chức năng hệ thống của thiết bị người dùng cũng tăng liên tục. Với việc tăng các chức năng hệ thống, lỗ hổng bảo mật chắc chắn xuất hiện trong hệ thống của thiết bị người dùng. Tin tặc có thể xâm nhập hệ thống của thiết bị người dùng bằng cách sử dụng lỗ hổng bảo mật, để đoạt dữ liệu được lưu trữ trong thiết bị người dùng, và độ bảo mật của hoạt động nhập của người dùng và việc hiển thị của thiết bị đầu cuối không thể được bảo đảm. Ví dụ, người dùng thực hiện thanh toán bằng cách sử dụng thiết bị người dùng. Khi người dùng đang nhập dữ liệu tại giao diện được cung cấp bởi thiết bị người dùng, tin tặc có thể chặn sự kiện nhập của người dùng và nội dung được hiển thị trên thiết bị người dùng để đoạt dữ liệu được nhập bởi người dùng. Tin tặc có thể sau đó phân tích dữ liệu lịch sử được lưu trữ tương ứng với ứng dụng được sử dụng để thanh toán để chiếm tài khoản của người dùng. Khi tin tặc còn đoạt được mật khẩu được nhập bởi người dùng vào thiết bị người dùng, sẽ có nguy cơ nghiêm trọng đối với tài sản của người dùng. Vì vậy, đã có đề xuất kỹ thuật vùng tin cậy (Trust Zone). Trong kỹ thuật này, có đề xuất là thành phần phần cứng của thiết bị người dùng được chia thành môi trường an toàn (Secure World) và môi trường bình thường (Normal World), và dữ liệu trong giới an toàn có thể được truyền chỉ bằng cách sử dụng màn hình theo dõi (monitor). Hệ điều hành của thiết bị người dùng chạy trong Normal World.

Chương trình chạy trong Secure World có mức độ bảo mật cao hơn so với chương trình chạy trong Normal World. Secure World được cách ly khỏi Normal World bằng cách sử dụng phần cứng. Secure World có quyền truy cập tất cả dữ liệu trong Normal World, nhưng Normal World không có quyền truy cập dữ liệu trong Secure World. Khi thiết bị người dùng được khởi động, Secure World được nhập trước tiên, và sau đó chương trình trong Secure World chịu trách nhiệm chuyển sang Normal World, và khởi động hệ điều hành của thiết bị người dùng. Các khái niệm về Secure World và Normal World được đề xuất trong kỹ thuật TrustZone, để giải quyết vấn đề độ bảo mật nhập dữ liệu trong thiết bị người dùng. Môi trường nhập dữ liệu mà chạy trong Secure World được đề xuất, và người dùng có thể xử lý sự kiện như nhập tài khoản hoặc mật khẩu trong môi trường nhập dữ liệu được đề xuất. Tuy nhiên, nói chung, khi nội dung liên quan được hiển thị hoặc nhập trong môi trường nhập dữ liệu mà chạy trong Secure World, nội dung được hiển thị thường che toàn bộ vùng hiển thị của thiết bị người dùng. Khi người dùng cần xử lý sự kiện khác, ví dụ, khi cửa sổ bật lên của bản tin dịch vụ bản tin ngắn xuất hiện khi người dùng đang nhập tên người dùng và mật khẩu, và người dùng cần xem bản tin dịch vụ bản tin ngắn, hệ thống cần thoát ra môi trường nhập dữ liệu theo lệnh của người dùng để xem bản tin dịch vụ bản tin ngắn, và điều này dẫn đến làm mất sự kiện được xử lý trước đó. Do đó, trong kỹ thuật TrustZone, độ bảo mật của sự kiện được tạo ra khi người dùng xử lý chương trình mà chạy trong Normal World của thiết bị người dùng có thể không được giải quyết hoàn toàn, hoặc sự kiện mà chạy trong Normal World có thể không được xử lý trực tiếp.

Bản chất kỹ thuật của sáng chế

Mục đích của sáng chế là đề xuất phương pháp và thiết bị nhập dữ liệu, và thiết bị người dùng, để độ bảo mật của sự kiện được tạo ra khi người dùng xử lý chương trình mà chạy trong môi trường Normal World của thiết bị người dùng có thể được cải thiện hơn nữa, và sự kiện mà chạy trong môi trường Normal World có thể được xử lý trực tiếp.

Theo khía cạnh thứ nhất, phương pháp nhập dữ liệu được đề xuất và bao

gồm các bước: khi xác định được là xử lý của người dùng trên UE không được thực hiện trong vùng hiển thị được thiết lập trước, cấp sự kiện tương ứng với xử lý đến môi trường xử lý thứ nhất để xử lý, trong đó vùng hiển thị được thiết lập trước chạy trong môi trường xử lý thứ hai của UE, và môi trường xử lý thứ hai có mức độ bảo mật cao hơn so với môi trường xử lý thứ nhất. Điều này có thể cải thiện hơn nữa độ bảo mật của sự kiện được tạo ra khi người dùng xử lý chương trình mà chạy trong Normal World của thiết bị người dùng, và trực tiếp xử lý sự kiện mà chạy trong Normal World.

Tham chiếu khía cạnh thứ nhất, trong dạng thực hiện có thể thứ nhất của khía cạnh thứ nhất, phương pháp này còn bao gồm bước: thu xử lý của người dùng trong vùng nhập được biểu diễn bởi bộ hiển thị cho người dùng, và tạo sự kiện tương ứng với xử lý; xác định việc sự kiện được tạo ra khi người dùng thực hiện xử lý trong vùng nhập có phải là sự kiện nhập an toàn hay không; và nếu xác định được là sự kiện được tạo ra khi người dùng thực hiện xử lý trong vùng nhập là sự kiện nhập an toàn, khởi động vùng hiển thị được thiết lập trước, và biểu diễn vùng hiển thị được thiết lập trước cho người dùng bằng cách sử dụng bộ hiển thị.

Tham chiếu dạng thực hiện có thể thứ nhất của khía cạnh thứ nhất, trong dạng thực hiện có thể thứ hai của khía cạnh thứ nhất, bước khởi động vùng hiển thị được thiết lập trước bao gồm: sao dự phòng sự kiện hiện thời trong môi trường xử lý thứ nhất; kích hoạt bộ ngắt trong môi trường xử lý thứ hai; và khởi động vùng hiển thị được thiết lập trước bằng cách sử dụng bộ ngắt trong môi trường xử lý thứ hai.

Việc xác định được thực hiện trên sự kiện tương ứng được tạo ra khi người dùng thực hiện xử lý trong vùng nhập mà chạy trong môi trường xử lý thứ nhất, và việc sự kiện có phải là sự kiện nhập an toàn hay không được xác định. Khi xác định được là sự kiện là sự kiện nhập an toàn, việc chuyển từ môi trường xử lý thứ nhất sang môi trường xử lý thứ hai được thực hiện, cụ thể là, vùng hiển thị được thiết lập trước được biểu diễn cho người dùng, để thời gian nhập an toàn được tạo ra khi người dùng thực hiện xử lý trên thiết bị người dùng có thể

được chuyển sang môi trường xử lý thứ hai để xử lý. Trong trường hợp này, độ bảo mật của sự kiện được tạo ra khi người dùng thực hiện xử lý trên thiết bị người dùng có thể được đảm bảo tốt hơn.

Tham chiếu bất kỳ trong số khía cạnh thứ nhất, hoặc dạng thực hiện có thể thứ nhất đến dạng thực hiện có thể thứ hai của khía cạnh thứ nhất, trong dạng thực hiện có thể thứ ba của khía cạnh thứ nhất, vùng hiển thị được thiết lập trước và vùng nhập được biểu diễn đồng thời trên màn hình của thiết bị người dùng.

Tham chiếu khía cạnh thứ nhất, trong dạng thực hiện có thể thứ tư của khía cạnh thứ nhất, bước cấp sự kiện tương ứng với xử lý đến môi trường xử lý thứ nhất để xử lý bao gồm: lưu trữ sự kiện tương ứng với xử lý trong vùng lưu trữ được chia sẻ, trong đó vùng lưu trữ được chia sẻ là vùng lưu trữ mà được chia sẻ bởi môi trường xử lý thứ nhất và môi trường xử lý thứ hai; và kích hoạt bộ ngắt trong môi trường xử lý thứ nhất, để cấp sự kiện được lưu trữ trong vùng lưu trữ được chia sẻ đến môi trường xử lý thứ nhất để xử lý.

Tham chiếu dạng thực hiện có thể thứ tư của khía cạnh thứ nhất, trong dạng thực hiện có thể thứ năm của khía cạnh thứ nhất, bước kích hoạt bộ ngắt trong môi trường xử lý thứ nhất, để cấp sự kiện được lưu trữ trong vùng lưu trữ được chia sẻ đến môi trường xử lý thứ nhất để xử lý bao gồm: kích hoạt bộ ngắt trong môi trường xử lý thứ nhất, và gọi ra luồng trình nền (daemon thread) trong môi trường an toàn thứ nhất, để cấp, bằng cách sử dụng luồng trình nền, sự kiện được lưu trữ trong vùng lưu trữ được chia sẻ đến môi trường xử lý thứ nhất để xử lý.

Tham chiếu bất kỳ trong số khía cạnh thứ nhất, hoặc dạng thực hiện có thể thứ nhất đến dạng thực hiện có thể thứ năm của khía cạnh thứ nhất, trong dạng thực hiện có thể thứ sáu của khía cạnh thứ nhất, trước khi xác định được là xử lý của người dùng trên thiết bị người dùng UE không được thực hiện trong vùng hiển thị được thiết lập trước, phương pháp này còn bao gồm bước: khi xác định được là sự kiện tương ứng với xử lý là sự kiện nhập an toàn, hiển thị vùng hiển thị được thiết lập trước, để người dùng thực hiện xử lý trong vùng hiển thị được thiết lập trước, trong đó sự kiện nhập an toàn là sự kiện nhập dữ liệu với thuộc

tính xác nhận quyền.

Tham chiếu bất kỳ trong số khía cạnh thứ nhất, hoặc dạng thực hiện có thể thứ nhất đến dạng thực hiện có thể thứ sáu của khía cạnh thứ nhất, trong dạng thực hiện có thể thứ bảy của khía cạnh thứ nhất, sau khi bước cấp sự kiện tương ứng với xử lý đến môi trường xử lý thứ nhất để xử lý, phương pháp này còn bao gồm bước: ẩn vùng hiển thị được thiết lập trước. Việc này có thể cải thiện độ linh hoạt của xử lý người dùng.

Tham chiếu bất kỳ trong số khía cạnh thứ nhất, hoặc dạng thực hiện có thể thứ nhất đến dạng thực hiện có thể thứ sáu của khía cạnh thứ nhất, trong dạng thực hiện có thể thứ tám của khía cạnh thứ nhất, vùng hiển thị được thiết lập trước bao gồm hộp biên soạn nhập được định dạng.

Tham chiếu dạng thực hiện có thể thứ tám của khía cạnh thứ nhất, trong dạng thực hiện có thể thứ chín của khía cạnh thứ nhất, hộp biên soạn nhập được định dạng bao gồm ít nhất một trong số: loại nhập được xác định có thể là loại nhập như loại số chín phím, loại ký tự Trung Quốc chín phím, loại bảng chữ cái chín phím, loại số và loại lai ký tự Trung Quốc. Việc này có thể cải thiện độ tiện lợi của xử lý người dùng.

Theo khía cạnh thứ hai, thiết bị nhập dữ liệu được đề xuất. Thiết bị nhập dữ liệu có chức năng thực hiện hành động của thiết bị đầu cuối trong thiết kế phương pháp bất kỳ theo khía cạnh thứ nhất và dạng thực hiện có thể thứ nhất đến dạng thực hiện có thể thứ tám của khía cạnh thứ nhất. Chức năng có thể được thực hiện bằng phần cứng, hoặc có thể được thực hiện bằng phần mềm tương ứng thực thi phần cứng. Phần cứng hoặc phần mềm bao gồm một hoặc nhiều môđun tương ứng với chức năng.

Theo khía cạnh thứ ba, thiết bị đầu cuối người dùng được đề xuất. Thiết bị đầu cuối người dùng có chức năng thực hiện hành động của thiết bị đầu cuối trong thiết kế phương pháp bất kỳ theo khía cạnh thứ nhất và dạng thực hiện có thể thứ nhất đến dạng thực hiện có thể thứ tám của khía cạnh thứ nhất. Chức năng có thể được thực hiện bằng phần cứng, hoặc có thể được thực hiện bằng

phần mềm tương ứng chạy phần cứng. Phần cứng hoặc phần mềm bao gồm một hoặc nhiều môđun tương ứng với chức năng.

Tham chiếu khía cạnh thứ ba, trong dạng thực hiện có thể thứ nhất của khía cạnh thứ ba, cấu trúc của thiết bị đầu cuối bao gồm bộ nhớ và bộ xử lý. Bộ nhớ được tạo cấu hình để lưu trữ nhóm các chương trình, và bộ xử lý được tạo cấu hình để gọi ra các chương trình được lưu trữ trong bộ nhớ, để thực hiện phương pháp trong bất kỳ trong số khía cạnh thứ nhất, hoặc dạng thực hiện có thể thứ nhất đến dạng thực hiện có thể thứ tám của khía cạnh thứ nhất.

Theo khía cạnh thứ tư, vật lưu trữ máy tính được đề xuất, và được tạo cấu hình để lưu trữ lệnh phần mềm máy tính được sử dụng bằng thiết bị nhập dữ liệu, và lệnh phần mềm máy tính bao gồm chương trình được thiết kế để thực hiện các khía cạnh trên đây.

Bằng cách sử dụng các giải pháp kỹ thuật trên đây, khi xác định được là xử lý của người dùng trên UE không được thực hiện trong vùng hiển thị được thiết lập trước, sự kiện tương ứng với xử lý được cấp đến môi trường xử lý thứ nhất để xử lý. Trong trường hợp này, khi người dùng xử lý chương trình mà chạy trong Normal World của thiết bị người dùng, ngay cả nếu người dùng cần xử lý sự kiện không an toàn khác, độ bảo mật của sự kiện được tạo ra khi người dùng xử lý chương trình mà chạy trong Normal World của thiết bị người dùng có thể được bảo đảm, và sự kiện mà chạy trong Normal World có thể được xử lý trực tiếp.

Mô tả vắn tắt hình vẽ

Fig.1A và Fig.1B là giản đồ của cấu trúc logic của nút tính toán được áp dụng phương pháp nhập dữ liệu theo một phương án của sáng chế;

Fig.2 là giản đồ của thành phần cấu trúc của thiết bị người dùng theo một phương án của sáng chế;

Fig.3 là giản đồ của thành phần cấu trúc của thiết bị người dùng theo một phương án của sáng chế;

Fig.4 là sơ đồ cấu trúc giản lược của thành phần phần cứng của Secure

World của hệ thống nhập dữ liệu theo một phương án của sáng chế;

Fig.5 là lưu đồ của phương pháp nhập dữ liệu theo một phương án của sáng chế;

Fig.6 là giản đồ của hộp biên soạn nhập theo một phương án của sáng chế;

Fig.7 là giản đồ của vùng hiển thị được thiết lập trước và vùng nhập theo một phương án của sáng chế;

Fig.8 là giản đồ của loại nhập được xác định theo một phương án của sáng chế;

Fig.9 là lưu đồ của phương pháp nhập dữ liệu theo một phương án của sáng chế; và

Fig.10 là giản đồ của thành phần cấu trúc của thiết bị nhập dữ liệu theo một phương án của sáng chế.

Mô tả chi tiết sáng chế

Để giải quyết vấn đề trong kỹ thuật TrustZone, độ bảo mật của sự kiện được tạo ra khi người dùng xử lý chương trình mà chạy trong Normal World của thiết bị người dùng có thể không được giải quyết hoàn toàn, hoặc sự kiện mà chạy trong Normal World có thể được xử lý trực tiếp, trong các giải pháp kỹ thuật được đề xuất trong sáng chế, khi xác định được là xử lý của người dùng trên UE không được thực hiện trong vùng hiển thị được thiết lập trước, sự kiện tương ứng với xử lý được cấp đến môi trường xử lý thứ nhất để xử lý. Vùng hiển thị được thiết lập trước chạy trong môi trường xử lý thứ hai của UE, và môi trường xử lý thứ hai có mức độ bảo mật cao hơn so với môi trường xử lý thứ nhất. Do đó, độ bảo mật của sự kiện được tạo ra khi người dùng xử lý chương trình mà chạy trong Normal World của thiết bị người dùng có thể được cải thiện hơn nữa, và sự kiện mà chạy trong Normal World có thể được xử lý trực tiếp.

Phần dưới đây giải thích các nguyên lý thực hiện chính, các dạng thực hiện cụ thể, và các hiệu quả có lợi khả dụng tương ứng của các giải pháp kỹ thuật trong các phương án của sáng chế có dựa vào các hình vẽ kèm theo.

Trong một giải pháp kỹ thuật được đề xuất trong một phương án của sáng

chế, Fig.1A và Fig.1B được sử dụng làm ví dụ để mô tả cấu trúc logic của nút tính toán được áp dụng phương pháp nhập dữ liệu được đề xuất trong phương án này của sáng chế. Nút tính toán có thể là thiết bị người dùng, và cụ thể là thiết bị người dùng có thể là máy tính để bàn, máy tính xách tay, điện thoại thông minh, máy tính bảng, hoặc tương tự. Như được thể hiện trên Fig.1, lớp phần cứng của thiết bị người dùng bao gồm bộ xử lý trung tâm CPU (Center Processing Unit), bộ xử lý đồ họa GPU (Graphic Processing Unit), và tương tự. Chắc chắn là, lớp phần cứng của thiết bị người dùng có thể còn bao gồm bộ nhớ, thiết bị nhập/xuất (Input Device), giao diện mạng, và tương tự. Thiết bị nhập có thể bao gồm bàn phím, chuột, màn hình chạm, và tương tự. Thiết bị xuất có thể bao gồm thiết bị hiển thị như màn hiển thị tinh thể lỏng LCD (Liquid Crystal Display), ống tia catot CRT (Cathode Ray Tube), thiết bị tạo ảnh toàn ký (Holographic), hoặc máy chiếu (Projector). Hệ điều hành (như Android) và một số chương trình ứng dụng có thể chạy bên trên lớp phần cứng. lớp thư viện nhân là phần lõi của hệ điều hành, và bao gồm dịch vụ nhập/xuất, dịch vụ nhân, giao diện thiết bị đồ họa, cỗ máy đồ họa (Graphics Engine) mà thực hiện xử lý đồ họa của CPU và GPU, và tương tự. Các cỗ máy đồ họa có thể bao gồm cỗ máy 2D, cỗ máy 3D, bộ kết hợp (thành phần), bộ đệm khung (Frame Buffer), và tương tự. Lớp thư viện nhân còn bao gồm dịch vụ phương pháp nhập. Dịch vụ phương pháp nhập bao gồm dịch vụ phương pháp nhập trong thiết bị đầu cuối. Dịch vụ phương pháp nhập còn bao gồm phương pháp nhập dữ liệu được đề xuất trong phương án này của sáng chế. Ngoài ra, thiết bị đầu cuối còn bao gồm lớp bộ điều khiển, lớp khung sườn, và lớp ứng dụng. Lớp bộ điều khiển có thể bao gồm bộ điều khiển CPU, bộ điều khiển GPU, bộ điều khiển thiết bị điều khiển hiển thị, bộ điều khiển TrustZone (Trust Zone Driver), và tương tự. Lớp khung sườn có thể bao gồm dịch vụ đồ họa (Graphic Service), dịch vụ hệ thống (System service), dịch vụ mạng (Web Service), dịch vụ người dùng (Customer Service), và tương tự. Dịch vụ đồ họa có thể bao gồm công cụ (Widget), vải bạt (Canvas), cảnh (Views), kịch bản hoàn trả (render script), và tương tự. Lớp ứng dụng có thể bao gồm màn hình nền (bộ khởi động), trình phát phương tiện (Media Player), trình duyệt (Browser), và

tương tự.

Trong kỹ thuật TrustZone, khi phần cứng và các lệnh chương trình của thiết bị người dùng chạy, có thể có hai môi trường xử lý: môi trường xử lý an toàn và môi trường xử lý không an toàn. Môi trường xử lý không an toàn có thể cũng được gọi là Normal World, và tương ứng với môi trường xử lý thứ nhất được đề xuất trong phương án này của sáng chế. Môi trường xử lý an toàn có thể cũng được gọi là Secure World, và tương ứng với môi trường xử lý thứ hai được đề xuất trong phương án này của sáng chế. Chương trình và phần cứng của thiết bị người dùng mà chạy trong môi trường xử lý an toàn có mức độ bảo mật cao hơn so với chương trình và phần cứng của thiết bị người dùng mà chạy trong môi trường xử lý không an toàn. Secure World có thể cũng là môi trường xử lý ảo được cách ly từ hệ điều hành của thiết bị người dùng.

Thiết bị người dùng được áp dụng phương pháp nhập dữ liệu được đề xuất trong một phương án của sáng chế được thể hiện trên Fig.2. Thiết bị người dùng 200 bao gồm: ít nhất một bộ xử lý 201, ít nhất một giao diện mạng 204 hoặc giao diện người dùng 203 khác, bộ nhớ 205, và ít nhất một buýt truyền thông 202. Buýt truyền thông 202 được tạo cấu hình để thực hiện kết nối và truyền thông giữa các thành phần này. Một cách tùy chọn, thiết bị người dùng 200 bao gồm giao diện người dùng 203 mà bao gồm màn hiển thị (ví dụ, LCD, CRT, Holographic), hoặc Projector được thể hiện trên Fig.1A và Fig.1B), bàn phím hoặc thiết bị nhắp (ví dụ, chuột, bi xoay, bảng điều khiển chạm, hoặc màn hình chạm), và tương tự.

Bộ nhớ 205 có thể bao gồm bộ nhớ chỉ đọc và bộ nhớ truy cập ngẫu nhiên, và cung cấp cho bộ xử lý 201 với lệnh chương trình và dữ liệu được lưu trữ trong bộ nhớ 205. Một phần của bộ nhớ 205 có thể còn bao gồm bộ nhớ truy cập ngẫu nhiên bất khả biến NVRAM (nonvolatile random access memory).

Trong một số dạng thực hiện, bộ nhớ 205 lưu trữ các thành phần sau: môđun hoặc cấu trúc dữ liệu có thể thực thi được, hoặc tập hợp con của chúng, hoặc tập hợp được mở rộng của chúng.

Hệ điều hành 2051 bao gồm các lệnh chương trình hệ thống khác nhau. Các lệnh chương trình có thể chạy trên lớp khung sườn, lớp thư viện nhân, lớp bộ điều khiển, và tương tự được thể hiện trên Fig.1A và Fig.1B, và được sử dụng để thực hiện các dịch vụ cơ bản khác nhau và xử lý các tác vụ dựa vào phần cứng.

Trong giải pháp kỹ thuật được đề xuất trong phương án này của sáng chế, hệ điều hành có thể chạy trong cả môi trường xử lý thứ nhất và môi trường xử lý thứ hai có mức độ bảo mật cao hơn so với môi trường xử lý thứ nhất.

Chương trình ứng dụng 2052 bao gồm các chương trình ứng dụng khác nhau, ví dụ, màn hình nền (bộ khởi động), trình phát đa phương tiện (Media Player), trình duyệt (Browser), và ứng dụng phương pháp nhập được thể hiện trên Fig.1A và Fig.1B, và các chương trình ứng dụng khác nhau được sử dụng để thực hiện các dịch vụ ứng dụng khác nhau.

Các chương trình ứng dụng khác nhau trong chương trình ứng dụng 2052 có thể được áp dụng cho môi trường xử lý thứ nhất, hoặc có thể chạy trong môi trường xử lý thứ hai. Trong giải pháp kỹ thuật được đề xuất trong phương án này của sáng chế, chương trình ứng dụng 2052 lưu trữ lệnh chương trình mà thực hiện phương pháp nhập dữ liệu, và lệnh chương trình chạy trong môi trường xử lý thứ hai.

Trong phương án này của sáng chế, bộ nhớ 205 có thể cũng được gọi là vùng lưu trữ, và được tạo cấu hình để lưu trữ chương trình của phương pháp nhập dữ liệu, và lưu trữ hệ điều hành.

Bộ xử lý 201 gọi ra lệnh chương trình được lưu trữ trong bộ nhớ 205, và theo lệnh chương trình thu được, bộ xử lý 201 được tạo cấu hình để: khi xác định được là xử lý của người dùng trên UE không được thực hiện trong vùng hiển thị được thiết lập trước, cấp sự kiện tương ứng với xử lý đến môi trường xử lý thứ nhất để xử lý.

Một cách tùy chọn, trong một phương án, bộ xử lý 201 còn được tạo cấu hình để: khi xác định được là sự kiện tương ứng với xử lý là sự kiện nhập an toàn, hiển thị vùng hiển thị được thiết lập trước, để người dùng thực hiện xử lý

trong vùng hiển thị được thiết lập trước. Sự kiện nhập an toàn là sự kiện nhập dữ liệu với thuộc tính xác nhận quyền.

Hơn nữa, bộ xử lý 201 được tạo cấu hình đặc biệt để lưu trữ sự kiện tương ứng với xử lý trong vùng lưu trữ được chia sẻ. Vùng lưu trữ được chia sẻ là vùng lưu trữ mà được chia sẻ bởi môi trường xử lý thứ nhất và môi trường xử lý thứ hai.

Thiết bị người dùng còn bao gồm bộ ngắt trong môi trường xử lý thứ nhất (không được thể hiện trên Fig.2). Bộ xử lý 201 kích hoạt bộ ngắt trong môi trường xử lý thứ nhất, và bộ ngắt trong môi trường xử lý thứ nhất cấp sự kiện được lưu trữ trong vùng lưu trữ được chia sẻ đến môi trường xử lý thứ nhất để xử lý. Hơn nữa, bộ xử lý 201 được tạo cấu hình đặc biệt để: kích hoạt bộ ngắt trong môi trường xử lý thứ nhất, và gọi ra luồng trình nền trong môi trường an toàn thứ nhất, để cấp, bằng cách sử dụng luồng trình nền, sự kiện được lưu trữ trong vùng lưu trữ được chia sẻ đến môi trường xử lý thứ nhất để xử lý.

Hơn nữa, bộ xử lý 201 được tạo cấu hình đặc biệt để ẩn vùng hiển thị được thiết lập trước.

Thiết bị người dùng mà được áp dụng phương pháp nhập dữ liệu được đề xuất trong một phương án của sáng chế có thể là điện thoại di động, máy tính bảng, máy hỗ trợ cá nhân kỹ thuật số PDA (Personal Digital Assistant), hoặc tương tự. Tham chiếu Fig.3, Fig.3 là giản đồ của thành phần cấu trúc của thiết bị người dùng 300.

Thiết bị người dùng 300 chủ yếu bao gồm bộ nhớ 320, bộ xử lý 360, và bộ nhập 330. Bộ nhập 330 được tạo cấu hình để thu sự kiện được tạo ra khi người dùng thực hiện xử lý trên thiết bị đầu cuối. Bộ nhớ 320 được tạo cấu hình để lưu trữ các lệnh chương trình của hệ điều hành và các chương trình ứng dụng khác nhau.

Trong giải pháp kỹ thuật được đề xuất trong phương án này của sáng chế, môi trường xử lý thứ nhất và môi trường xử lý thứ hai được đề xuất. Một cách tương ứng, bộ nhớ 320 có thể được chia thành bộ nhớ an toàn (cũng có thể được

gọi là vùng lưu trữ an toàn), bộ nhớ không an toàn (cũng có thể được gọi là vùng lưu trữ không an toàn), và bộ nhớ được chia sẻ (cũng có thể được gọi là vùng lưu trữ được chia sẻ). Bộ nhớ không an toàn được bố trí trong môi trường xử lý thứ nhất, và bộ nhớ an toàn được bố trí trong môi trường xử lý thứ hai. Môi trường xử lý thứ hai có mức độ bảo mật cao hơn so với môi trường xử lý thứ nhất. Bộ xử lý hoặc bộ ngắt được bố trí trong môi trường xử lý thứ nhất không thể trực tiếp truy cập bộ nhớ an toàn trong môi trường xử lý thứ hai. Bộ xử lý hoặc bộ ngắt trong môi trường xử lý thứ hai có thể truy cập bộ xử lý không an toàn được bố trí trong môi trường xử lý thứ nhất, và truy cập vùng lưu trữ không an toàn. Đối với bộ nhớ được chia sẻ, dữ liệu được lưu trữ trong bộ nhớ được chia sẻ là dữ liệu mà có thể được truy cập bằng các bộ xử lý hoặc bộ ngắt trong cả môi trường xử lý thứ nhất và môi trường xử lý thứ hai. Cụ thể là, các bộ xử lý hoặc các bộ ngắt trong môi trường xử lý thứ nhất và môi trường xử lý thứ hai có thể truy cập bộ nhớ được chia sẻ để thu dữ liệu trong bộ nhớ được chia sẻ.

Có thể hiểu được là đối với chức năng thực hiện cụ thể của bộ xử lý 360, có thể tham chiếu các phần mô tả chi tiết của bộ xử lý 201, và các chi tiết không được mô tả lại.

Bộ nhớ 320 có thể là bộ nhớ của thiết bị người dùng 300. Bộ nhớ có thể được chia thành ba khoảng trống lưu trữ. Ba khoảng trống lưu trữ tương ứng riêng rẽ với bộ nhớ an toàn được bố trí trong môi trường xử lý thứ nhất, bộ nhớ không an toàn được bố trí trong môi trường thứ hai, và bộ nhớ được chia sẻ mà có thể được truy cập bằng các chương trình ứng dụng hoặc phần cứng trong cả môi trường xử lý thứ nhất và môi trường xử lý thứ hai. Bộ nhớ an toàn, bộ nhớ không an toàn, và bộ nhớ được chia sẻ có thể có các khoảng trống cùng kích thước, hoặc có thể có các khoảng trống có các kích thước khác nhau theo các sự kiện nhập dữ liệu được lưu trữ khác nhau.

Bộ nhập 330 của thiết bị người dùng có thể được tạo cấu hình để thu thông tin số hoặc ký tự được nhập bởi người dùng, để tạo đầu vào tín hiệu liên quan đến các thiết lập người dùng hoặc điều khiển chức năng của thiết bị người dùng 300. Cụ thể là, trong phương án này của sáng chế, bộ nhập 330 có thể bao gồm

bảng điều khiển chạm 331. Bảng điều khiển chạm 331 có thể lấy xử lý (như xử lý được thực hiện bởi người dùng trên bảng điều khiển chạm 331 bằng cách sử dụng đối tượng hoặc phụ kiện thích hợp bất kỳ, như ngón tay hoặc bút) được thực hiện bởi người dùng trên bảng điều khiển chạm 331, và điều khiển, theo lệnh chương trình được thiết lập trước, thiết bị tương ứng được nối với bảng điều khiển chạm 331. Một cách tùy chọn, bảng điều khiển chạm 331 có thể bao gồm hai phần: thiết bị dò sự chạm và bộ điều khiển sự chạm. Thiết bị dò sự chạm dò vị trí chạm của người dùng, dò tín hiệu do xử lý chạm, và truyền tín hiệu đến bộ điều khiển sự chạm. Bộ điều khiển sự chạm thu thông tin chạm thu được từ thiết bị dò sự chạm, biến đổi thông tin chạm thành các tọa độ chạm, và truyền các tọa độ chạm đến bộ xử lý 360. Bộ điều khiển sự chạm có thể còn thu và thực hiện lệnh được truyền bằng bộ xử lý 360. Ngoài ra, bảng điều khiển chạm 331 có thể được tạo thành bằng cách sử dụng nhiều loại như loại điện trở, loại điện dung, tia hồng ngoại, và sóng âm bề mặt. Ngoài bảng điều khiển chạm 331, bộ nhập 330 có thể còn bao gồm thiết bị nhập 332 khác. Thiết bị nhập 332 khác có thể bao gồm nhưng không bị giới hạn ở một hoặc nhiều trong số bàn phím vật lý, phím chức năng (như phím điều khiển dung lượng hoặc phím bật/tắt), bi xoay, chuột, cần điều khiển, hoặc tương tự.

Thiết bị người dùng 300 có thể còn bao gồm bộ hiển thị 340. Bộ hiển thị 340 có thể được tạo cấu hình để hiển thị thông tin được nhập bởi người dùng hoặc thông tin được cung cấp cho người dùng và các giao diện thực đơn khác nhau của thiết bị người dùng 300. Bộ hiển thị 340 có thể bao gồm bảng hiển thị 341. Một cách tùy chọn, bảng hiển thị 341 có thể được tạo cấu hình ở dạng như LCD (Liquid Crystal Display) hoặc OLED (Organic Light-Emitting Diode).

Tham chiếu Fig.3, trong phương án này của sáng chế, bảng điều khiển chạm 331 che bảng hiển thị 341, để tạo màn hình hiển thị chạm. Màn hình hiển thị chạm cung cấp vùng hiển thị được thiết lập trước cho người dùng. Sau khi dò xử lý chạm trên hoặc gần màn hình hiển thị chạm, màn hình hiển thị chạm 7 truyền xử lý chạm đến bộ xử lý 360 để xác định loại sự kiện chạm. Sau đó bộ xử lý 360 cung cấp đầu ra hình ảnh tương ứng trên màn hình hiển thị chạm theo

loại sự kiện chạm.

Trong phương án này của sáng chế, màn hình hiển thị chạm bao gồm các vùng hiển thị khác nhau. Từng vùng hiển thị có thể bao gồm ít nhất một thành phần giao diện như biểu tượng của chương trình ứng dụng và/hoặc công cụ màn hình trang nhà.

Bộ xử lý 360 là trung tâm điều khiển của thiết bị người dùng 300, được nối với từng phần của toàn bộ điện thoại di động bằng cách sử dụng các giao diện và đường dây khác nhau, và thực hiện các chức năng khác nhau của thiết bị người dùng 300 và xử lý dữ liệu bằng cách chạy hoặc thực hiện chương trình phần mềm và/hoặc môđun mà được lưu trữ trong bộ nhớ 320, để thực hiện toàn bộ hoạt động theo dõi trên thiết bị người dùng 300.

Có thể hiểu được rằng trong khi khởi động, bộ xử lý 360 trước tiên đi vào môi trường xử lý thứ hai, và thực hiện thiết lập khởi động hệ điều hành trong môi trường xử lý thứ hai, để đảm bảo độ bảo mật của hệ điều hành.

Thiết lập khởi động bao gồm khởi động chế độ theo dõi. Trong xử lý khởi động hệ thống, tất cả các bộ nhớ (bộ nhớ an toàn, bộ nhớ không an toàn, và bộ nhớ được chia sẻ) trong hệ điều hành của thiết bị người dùng trong môi trường xử lý thứ hai. Sau đó, ảnh hệ điều hành mà cần chạy trong môi trường xử lý thứ nhất được tải vào bộ nhớ không an toàn, và sau đó ảnh hệ thống trong môi trường xử lý thứ nhất chạy.

Một cách tùy chọn, thiết bị người dùng 300 có thể còn bao gồm mạch RF 310, môđun WiFi 380 được tạo cấu hình để cung cấp kết nối không dây, nguồn cấp điện 390, và mạch tần số auđio 370 được tạo cấu hình để cung cấp đầu vào và đầu ra âm thanh.

Dựa trên thiết bị người dùng 300 với màn hình hiển thị chạm được thể hiện trên Fig.3, trong giải pháp được đề xuất trong phương án này của sáng chế, các môi trường hoạt động của phương pháp nhập dữ liệu được chia thành Normal World (môi trường xử lý thứ nhất) và Secure World (môi trường xử lý thứ hai). Đối với thành phần phần cứng, một thiết bị người dùng có chỉ một tập hợp của

các cấu trúc phần cứng. Tuy nhiên, trong phần cứng, các thuộc tính độ bảo mật của một số phần cứng có thể được thiết lập linh hoạt, nhưng các thuộc tính độ bảo mật của phần cứng khác được cố định. Độ bảo mật của toàn bộ hệ thống thu được bằng cách chia tài nguyên phần cứng và tài nguyên phần mềm của hệ thống trên chip SoC (System on Chip) thành hai giới. Secure World và Normal World là Secure World tương ứng với hệ thống con an toàn và Normal World tương ứng với hệ thống con khác.

Như được thể hiện trên Fig.4, hệ thống SoC bao gồm bộ xử lý (Core) 401. Trong cấu trúc bộ xử lý, từng lõi bộ xử lý cung cấp hai lõi ảo: lõi không an toàn NS (Non-secure) và lõi an toàn (Secure). Cơ chế chuyển giữa lõi không an toàn và lõi an toàn được gọi là chế độ theo dõi (monitor). Lõi không an toàn có thể truy cập chỉ tài nguyên hệ thống của NS, nhưng lõi an toàn có thể truy cập tất cả các tài nguyên trong thiết bị người dùng. SoC còn bao gồm DMA (Direct Memory Access) 402, Secure RAM (Secure Random Access Memory) 403, Secure Boot ROM (Secure Boot Read Only Memory) 404, GIC (Generic Interrupt Controller) 405 được tích hợp với TrustZone hỗ trợ và có thể làm việc trong môi trường xử lý thứ nhất và môi trường xử lý thứ hai, TZIC (Trust Zone Interrupt Controller) 406 có thể được tạo thành độc lập, và tương tự. SoC còn bao gồm TZASC (Trust Zone Address Space Controller) 407 được tạo cấu hình để hỗ trợ ngắt an toàn, TZPC (Trust Zone Protection Controller) 408, DMC (Dynamic Memory Controller) 409, RAM động (Dynamic RAM) 410, và tương tự. TZPC được tạo cấu hình để thiết lập thuộc tính độ bảo mật của thiết bị ngoại vi. Ví dụ, TZPC có thể thiết lập thuộc tính của bộ hiển thị an toàn. Trong trường hợp này, xử lý trong môi trường xử lý thứ nhất không thể truy cập thiết bị mà được thiết lập an toàn. TZASC được tạo cấu hình để điều khiển sự phân loại của thuộc tính độ bảo mật của DRAM. TZASC có thể thiết lập một phần của DRAM an toàn, và thiết lập phần khác của DRAM không an toàn. Nếu bộ xử lý trong môi trường xử lý thứ nhất khởi động yêu cầu truy cập đến bộ nhớ an toàn, yêu cầu truy cập bị từ chối. Truy cập của DMA trong môi trường xử lý thứ nhất đến bộ nhớ an toàn bị từ chối, và việc này đảm bảo là bộ nhớ an toàn không được

truy cập bằng hệ điều hành hoặc phần cứng bất kỳ trong môi trường xử lý thứ nhất. GIC chịu trách nhiệm điều khiển tất cả thông tin ngắt, và GIC có thể thiết lập một số ngắt an toàn, và thiết lập một số ngắt bình thường.

Các thành phần SoC được nối với nhau bằng cách sử dụng AXI (Advanced eXtensible Interactive) 411. SoC truyền thông với thiết bị ngoại vi bằng cách sử dụng cầu AXI2APB (Advanced eXtensible Interactive to Advanced Peripheral Bus Bridge) 412. AXI2APB có thể cảm biến thuộc tính độ bảo mật của sự kiện hiện thời truy cập thiết bị ngoại vi. Khi sự kiện trong môi trường xử lý thứ nhất truy cập thiết bị ngoại vi có thuộc tính được thiết lập an toàn, AXI2APB từ chối truy cập này. RAM an toàn và ROM an toàn được cách ly bằng cách sử dụng cơ cấu phần mềm và phần cứng, và RAM an toàn và ROM an toàn được tạo cấu hình để lưu trữ hệ điều hành mà chạy trong môi trường xử lý thứ hai.

Trong phương pháp nhập dữ liệu được đề xuất trong phương án này của sáng chế, hệ thống SoC được khởi động sau khi được cấp điện. Trong khi khởi động, hệ thống trước tiên đi vào môi trường xử lý thứ hai, và sau đó thực hiện thiết lập khởi động trong môi trường xử lý thứ hai. Thiết lập khởi động bao gồm khởi động hệ điều hành trong môi trường xử lý thứ hai. Trong xử lý khởi động hệ thống, tất cả các bộ nhớ trong hệ điều hành của thiết bị người dùng trong môi trường xử lý thứ hai. Sau đó ảnh hệ điều hành mà cần chạy trong môi trường xử lý thứ nhất được tải vào bộ nhớ, và một số bộ nhớ được cấp phát cho môi trường xử lý thứ nhất. Các thuộc tính độ bảo mật của một số bộ nhớ được cấp phát cho môi trường xử lý thứ nhất được thiết lập không an toàn. Sau đó ảnh hệ thống trong môi trường xử lý thứ nhất chạy.

Phần dưới đây mô tả chi tiết thủ tục xử lý của phương pháp nhập dữ liệu được đề xuất trong một phương án của sáng chế. Như được thể hiện trên Fig.5, xử lý thực hiện cụ thể để cấp sự kiện từ môi trường xử lý thứ nhất đến môi trường xử lý thứ hai để xử lý được mô tả trước tiên.

Bước 1: Bộ hiển thị biểu diễn vùng nhập cho người dùng, và người dùng thực hiện xử lý trong vùng nhập để tạo sự kiện tương ứng với xử lý.

Phần mô tả chi tiết được cung cấp bằng cách sử dụng ví dụ trong đó người dùng nhập mật khẩu thanh toán loại số trong vùng nhập được biểu diễn bởi bộ hiển thị. Bộ hiển thị có thể bao gồm bảng điều khiển chạm tự nhiên. Người dùng chạm bảng điều khiển chạm, nhập tài khoản thanh toán trong vùng nhập, và liên tục nhập mật khẩu thanh toán sau khi nhập tài khoản thanh toán. Bộ xử lý thu sự kiện được tạo ra khi người dùng xử lý bảng điều khiển chạm. Cụ thể là, lõi không an toàn trong môi trường xử lý thứ nhất có thể thu sự kiện được tạo ra khi người dùng xử lý bảng điều khiển chạm.

Bước 2: Bộ xử lý xác định việc sự kiện được tạo ra khi người dùng xử lý thực hiện xử lý trong vùng nhập là sự kiện nhập an toàn. Nếu xác định được là sự kiện không phải là sự kiện nhập an toàn, người dùng liên tục thực hiện xử lý trong vùng nhập để tạo sự kiện tương ứng với xử lý, và bộ xử lý liên tục xử lý sự kiện.

Sự kiện nhập an toàn là sự kiện được tạo ra chỉ khi người dùng nhập mật khẩu với thuộc tính xác nhận quyền. Ví dụ, trong ứng dụng thanh toán, sau khi người dùng nhập tên người dùng, người dùng cần liên tục nhập mật khẩu thanh toán tương ứng với tên người dùng, và sau khi mật khẩu thanh toán và tên người dùng so khớp, thanh toán được hoàn tất. Sự kiện tương ứng với xử lý mà người dùng liên tục nhập mật khẩu thanh toán tương ứng với tên người dùng là sự kiện nhập an toàn.

Thuộc tính độ bảo mật của vùng nhập được biểu diễn bởi bộ hiển thị có thể được biên soạn từ trước. Vùng nhập được thiết lập là vùng hiển thị không an toàn mà chạy trong môi trường xử lý thứ nhất và vùng hiển thị an toàn mà chạy trong môi trường xử lý thứ hai. Ví dụ, trong xử lý thực hiện cụ thể, như được thể hiện trên Fig.6, vùng nhập trong môi trường xử lý thứ nhất có thể là hộp biên soạn nhập với hình dạng và kích thước cố định. Hộp biên soạn nhập có thể có hình dạng bất kỳ. Như được thể hiện trên Fig.6, hình dạng vuông chỉ được sử dụng làm ví dụ. Trong khi thiết lập, thuộc tính độ bảo mật có thể được bổ sung vào hộp biên soạn nhập, và thuộc tính độ bảo mật được thiết lập. Ví dụ, thuộc tính an toàn được thiết lập ở thuộc tính số. Cụ thể là, khi sự kiện thu được được

xử lý bởi người dùng trong hộp biên soạn nhập đang kích hoạt nhập số, xác định được là sự kiện là sự kiện nhập an toàn.

Phần mô tả chi tiết được cung cấp dưới đây bằng cách vẫn sử dụng ví dụ trong đó người dùng nhập mật khẩu thanh toán loại số. Khi người dùng chuẩn bị nhập mật khẩu thanh toán của loại số, ví dụ, mật khẩu thanh toán của người dùng là 12345678, khi người dùng kích hoạt số, xác định được là sự kiện nhập dữ liệu được xử lý bởi người dùng là sự kiện nhập an toàn.

Bước 3: Bộ xử lý kích hoạt bộ điều khiển TZ khi xác định được là sự kiện nhập dữ liệu được xử lý bởi người dùng là sự kiện nhập an toàn. Bộ điều khiển TZ kích hoạt chế độ màn theo dõi (monitor) được sử dụng để chuyển giữa môi trường xử lý thứ nhất và môi trường xử lý thứ hai, và bộ xử lý nhập môi trường xử lý thứ hai bằng cách sử dụng màn theo dõi.

Bước 4: Bộ xử lý sao dự phòng sự kiện hiện thời trong môi trường xử lý thứ nhất trong chế độ theo dõi. Bộ xử lý kích hoạt bộ ngắt trong môi trường xử lý thứ nhất, và lưu trữ sự kiện nhập an toàn được xác định hiện thời trong vùng lưu trữ được chia sẻ. Sau khi việc lưu sự kiện nhập an toàn được hoàn tất, bộ ngắt trong môi trường xử lý thứ hai được kích hoạt trong chế độ theo dõi, và bộ xử lý trong môi trường xử lý thứ hai, cụ thể là, lõi an toàn, được kích hoạt bằng cách sử dụng bộ ngắt trong môi trường xử lý thứ hai.

Bước 5: Lõi an toàn (cụ thể là, bộ xử lý trong môi trường xử lý thứ hai) kích hoạt bộ ngắt, bắt đầu vùng hiển thị được thiết lập trước, và biểu diễn vùng hiển thị được thiết lập trước cho người dùng bằng cách sử dụng bộ hiển thị. Xử lý sau của người dùng được thực hiện trong vùng hiển thị được thiết lập trước.

Vùng hiển thị được thiết lập trước chạy trong môi trường xử lý thứ hai. Vùng hiển thị được thiết lập trước có thể là một phần của màn hình của thiết bị người dùng, và người dùng có thể thực hiện xử lý nhập trong vùng hiển thị được thiết lập trước. Một cách tương ứng, vùng hiển thị được thiết lập trước có thể là hộp biên soạn nhập mà có hình dạng và kích thước cố định và có thuộc tính độ bảo mật. Như được thể hiện trên Fig.7, vùng hiển thị được thiết lập trước được

bắt đầu. Vùng hiển thị được thiết lập trước và vùng nhập có thể đồng thời được biểu diễn trên màn hình của thiết bị người dùng. Vùng hiển thị được thiết lập trước có thể che một phần của vùng nhập và chồng lấn một phần của vùng nhập. Vùng hiển thị được thiết lập trước có thể bao gồm loại nhập được xác định. Như được thể hiện trên Fig.8, loại nhập được xác định có thể là loại nhập như loại số chín phím, loại ký tự Trung Quốc chín phím (không được thể hiện trên Fig.8), loại bảng chữ cái chín phím, loại lai số và ký tự Trung Quốc (không được thể hiện trên Fig.8).

Ví dụ, vùng hiển thị được thiết lập trước được bắt đầu, và giả định là loại nhập được xác định là vùng hiển thị của loại số chín phím. Trong bộ hiển thị, vùng hiển thị của loại số chín phím được biểu diễn cho người dùng, và người dùng nhập mật khẩu thanh toán trong vùng hiển thị được thiết lập trước của loại số chín phím.

Bước 6: Bộ xử lý cung cấp sự kiện đến môi trường xử lý thứ hai để xử lý.

Bằng cách sử dụng giải pháp kỹ thuật nêu trên đây, việc xác định được thực hiện trên sự kiện tương ứng được tạo ra khi người dùng thực hiện xử lý trong vùng nhập mà chạy trong môi trường xử lý thứ nhất, việc sự kiện có phải là sự kiện nhập an toàn hay không được xác định, và khi xác định được là sự kiện là sự kiện nhập an toàn, việc chuyển từ môi trường xử lý thứ nhất sang môi trường xử lý thứ hai được thực hiện, cụ thể là, vùng hiển thị được thiết lập trước được biểu diễn cho người dùng, để thời gian nhập an toàn được tạo ra khi người dùng thực hiện xử lý trên thiết bị người dùng có thể được chuyển sang môi trường xử lý thứ hai để xử lý. Trong trường hợp này, độ bảo mật của sự kiện được tạo ra khi người dùng thực hiện xử lý trên thiết bị người dùng có thể được đảm bảo tốt hơn.

Như được thể hiện trên Fig.5, xử lý thực hiện cụ thể để cấp sự kiện từ môi trường xử lý thứ hai đến môi trường xử lý thứ nhất để xử lý được mô tả sau đó.

Bước 7: Người dùng thực hiện xử lý trong vùng hiển thị được thiết lập trước của thiết bị người dùng.

Bước 8: Bộ xử lý trong môi trường xử lý thứ hai thu sự kiện tương ứng với xử lý.

Để mô tả chi tiết vùng hiển thị được thiết lập trước, tham chiếu phần mô tả chi tiết trong bước 5. Các chi tiết không được mô tả lặp lại.

Một cách tương tự, phần mô tả được thực hiện bằng cách sử dụng ví dụ trong đó người dùng nhập mật khẩu thanh toán loại số. Trong bước 8, người dùng nhập mật khẩu thanh toán trong vùng hiển thị được thiết lập trước.

Bước 9: Bộ xử lý xác định việc xử lý của người dùng trên UE có được thực hiện trong vùng hiển thị được thiết lập trước hay không, và nếu xác định được là xử lý của người dùng trên UE được thực hiện trong vùng hiển thị được thiết lập trước, thực hiện bước 10, hoặc nếu xác định được là xử lý của người dùng trên UE không được thực hiện trong vùng hiển thị được thiết lập trước, thực hiện bước 12.

Cụ thể là, người dùng có thể thực hiện xử lý trong vùng hiển thị được thiết lập trước của bộ hiển thị, hoặc có thể thực hiện xử lý bên ngoài vùng hiển thị được thiết lập trước. Sự kiện tương ứng được tạo ra bằng xử lý của người dùng được truyền đến lõi an toàn. Lõi an toàn xác định việc sự kiện có tương ứng với xử lý mà nằm trong vùng hiển thị được thiết lập trước hay không. Ví dụ, người dùng nhập mật khẩu thanh toán trong vùng hiển thị được thiết lập trước, và lõi an toàn xác định việc điểm chạm của người dùng có trong vùng hiển thị được thiết lập trước hay không. Khi người dùng kích hoạt, ví dụ, nhập loại tài khoản (cụ thể là, thực hiện xử lý trong vùng nhập) trong xử lý trên đây, xác định được là xử lý của người dùng không được thực hiện trong vùng hiển thị được thiết lập trước; hoặc khi người dùng không kích hoạt nhập loại tài khoản, xác định được là xử lý của người dùng được thực hiện trong vùng hiển thị được thiết lập trước. Ví dụ, người dùng chuẩn bị nhập mật khẩu thanh toán 12345678 bằng cách sử dụng vùng hiển thị được thiết lập trước. Khi người dùng nhập 123, thiết bị người dùng thu phần biểu diễn bản tin dịch vụ bản tin ngắn hoặc phần biểu diễn nhận dạng đường dây gọi. Nếu người dùng gõ nhẹ phần biểu diễn bản tin dịch vụ bản tin ngắn, xử lý của người dùng trên thiết bị người dùng lúc này nằm trong hộp

phần biểu diễn bản tin dịch vụ bản tin ngắn. Trong trường hợp này, xác định được là xử lý của người dùng trên UE không được thực hiện trong vùng hiển thị được thiết lập trước.

Bước 10: Tiếp tục thu sự kiện được tạo ra khi người dùng thực hiện xử lý trên thiết bị người dùng trong vùng hiển thị được thiết lập trước.

Bước 11: Khi xác định được là người dùng kết thúc xử lý, bộ xử lý thực hiện xử lý xác nhận trên sự kiện thu được, cấp sự kiện đến môi trường xử lý thứ nhất, và phản hồi kết quả xử lý xác nhận đến người dùng.

Ví dụ, khi người dùng kết thúc nhập mật khẩu thanh toán, mật khẩu thanh toán thu được được xác nhận trong môi trường xử lý thứ hai, và kết quả xác nhận được phản hồi đến người dùng.

Bước 12: Khi xác định được là xử lý của người dùng trên thiết bị người dùng không được thực hiện trong vùng hiển thị được thiết lập trước, bộ xử lý cấp sự kiện tương ứng với xử lý đến môi trường xử lý thứ nhất để xử lý.

Có thể có hai dạng thực hiện cấp sự kiện tương ứng với xử lý đến môi trường xử lý thứ nhất để xử lý.

Cách 1: Bộ ngắt có thể được kích hoạt để cấp sự kiện tương ứng với xử lý đến môi trường xử lý thứ nhất để xử lý.

Theo cách 1, bộ xử lý có thể kích hoạt bộ ngắt trong môi trường xử lý thứ hai, và lưu trữ, bằng cách sử dụng bộ ngắt trong môi trường xử lý thứ hai, sự kiện tương ứng với xử lý của người dùng trong vùng lưu trữ được chia sẻ. Trong trường hợp này, trong chế độ theo dõi, bộ xử lý kích hoạt bộ ngắt trong môi trường xử lý thứ nhất, để cấp sự kiện được lưu trữ trong vùng lưu trữ được chia sẻ đến môi trường xử lý thứ nhất để xử lý.

Ví dụ, bộ xử lý kích hoạt FIQ (Fast Interrupt Request), và lưu trữ sự kiện tương ứng với xử lý của người dùng trong vùng lưu trữ được chia sẻ. Sau đó trong chế độ theo dõi, bộ xử lý kích hoạt bộ ngắt trong môi trường xử lý thứ nhất để thu được sự kiện được lưu trữ trong vùng lưu trữ được chia sẻ. Bộ ngắt trong môi trường xử lý thứ nhất cấp sự kiện thu được đến môi trường xử lý thứ

nhất để xử lý.

Cách 2: Sự kiện tương ứng với xử lý được cấp, bằng cách sử dụng luồng trình nền, đến môi trường xử lý thứ nhất để xử lý.

Theo cách 2, xử lý chương trình máy tính chạy ngầm trên hệ thống (daemon) là xử lý với tuổi thọ tương đối dài, và thường độc lập với thiết bị người dùng và định kỳ thực hiện nhiệm vụ hoặc chờ xử lý sự kiện mà sẽ xuất hiện. Xử lý trình nền (daemon) thường được bắt đầu khi hệ thống được khởi động, và kết thúc khi hệ thống được vô hiệu. Theo cách 2, bộ xử lý có thể kích hoạt bộ ngắt trong môi trường xử lý thứ hai, và lưu trữ sự kiện tương ứng với xử lý của người dùng trong vùng lưu trữ được chia sẻ. Sau đó trong chế độ theo dõi, bộ xử lý kích hoạt bộ ngắt trong môi trường xử lý thứ nhất, và kích hoạt luồng trình nền trong môi trường xử lý thứ nhất bằng cách sử dụng bộ ngắt trong môi trường xử lý thứ nhất. Luồng trình nền thu được sự kiện được lưu trữ trong vùng lưu trữ được chia sẻ, và luồng trình nền truyền sự kiện thu được đến môi trường xử lý thứ nhất để xử lý.

Trong hai dạng thực hiện cụ thể trên đây để cấp sự kiện tương ứng với xử lý đến môi trường xử lý thứ nhất để xử lý, trước khi sự kiện được cấp, sự kiện hiện thời cần được lưu trữ trong vùng lưu trữ được chia sẻ. Trong trường hợp này, bộ ngắt trong môi trường xử lý thứ hai có thể được kích hoạt, và sự kiện có thể được lưu trữ trong vùng lưu trữ được chia sẻ bằng cách sử dụng bộ ngắt mà chạy trong môi trường thứ hai. Theo cách khác, bộ điều khiển của bộ hiển thị có thể truyền sự kiện đến ứng dụng lớp trên, và sự kiện có thể được lưu trữ trong vùng lưu trữ được chia sẻ bằng cách sử dụng ứng dụng lớp trên.

Một cách tùy chọn, sau khi cấp sự kiện tương ứng với xử lý đến môi trường xử lý thứ nhất để xử lý, phương pháp này còn bao gồm bước: ẩn vùng hiển thị được thiết lập trước.

Ví dụ, sau khi nhập 12345678, người dùng không cần thực hiện xử lý khác bất kỳ, và trong trường hợp này, bộ xử lý ẩn vùng hiển thị được thiết lập trước.

Một cách tương ứng, một phương án của sáng chế còn đề xuất phương

pháp nhập dữ liệu. Như được thể hiện trên Fig.9, thủ tục xử lý cụ thể như sau:

Bước 91: Người dùng thực hiện xử lý trong vùng hiển thị được thiết lập trước của thiết bị người dùng.

Bước 92: Bộ xử lý trong môi trường xử lý thứ hai thu được sự kiện tương ứng với xử lý.

Để mô tả chi tiết vùng hiển thị được thiết lập trước, tham chiếu phần mô tả chi tiết trong bước 5. Các chi tiết không được mô tả lặp lại.

Một cách tương tự, phần mô tả được cung cấp bằng cách sử dụng ví dụ trong đó người dùng nhập mật khẩu thanh toán loại số. Người dùng nhập mật khẩu thanh toán trong vùng hiển thị được thiết lập trước.

Bước 93: Bộ xử lý xác định việc xử lý của người dùng trên UE được thực hiện trong vùng hiển thị được thiết lập trước, và nếu xác định được là xử lý của người dùng trên UE được thực hiện trong vùng hiển thị được thiết lập trước, thực hiện bước 94, hoặc nếu xác định được là xử lý của người dùng trên UE không được thực hiện trong vùng hiển thị được thiết lập trước, thực hiện bước 96.

Bước 94: Tiếp tục thu sự kiện được tạo ra khi người dùng thực hiện xử lý trên thiết bị người dùng trong vùng hiển thị được thiết lập trước.

Bước 95: Khi xác định được là người dùng kết thúc xử lý, bộ xử lý thực hiện xử lý xác nhận trên sự kiện thu được, cấp sự kiện thu được đến môi trường xử lý thứ nhất, và phản hồi kết quả xử lý xác nhận đến người dùng.

Ví dụ, khi người dùng kết thúc nhập mật khẩu thanh toán, mật khẩu thanh toán thu được được xác nhận trong môi trường xử lý thứ hai, và kết quả xác nhận được phản hồi đến người dùng.

Bước 96: Khi xác định được là xử lý của người dùng trên thiết bị người dùng không được thực hiện trong vùng hiển thị được thiết lập trước, bộ xử lý cấp sự kiện tương ứng với xử lý đến môi trường xử lý thứ nhất để xử lý.

Có thể có hai dạng thực hiện để cấp sự kiện tương ứng với xử lý đến môi trường xử lý thứ nhất để xử lý.

Cách 1: Bộ ngắt có thể được kích hoạt để cấp sự kiện tương ứng với xử lý đến môi trường xử lý thứ nhất để xử lý.

Theo cách 1, bộ xử lý có thể kích hoạt bộ ngắt trong môi trường xử lý thứ hai, và lưu trữ, bằng cách sử dụng bộ ngắt trong môi trường xử lý thứ hai, sự kiện tương ứng với xử lý của người dùng trong vùng lưu trữ được chia sẻ. Trong trường hợp này, trong chế độ theo dõi, bộ xử lý kích hoạt bộ ngắt trong môi trường xử lý thứ nhất, để cấp sự kiện được lưu trữ trong vùng lưu trữ được chia sẻ đến môi trường xử lý thứ nhất để xử lý.

Ví dụ, bộ xử lý kích hoạt FIQ (Fast Interrupt Reques), và lưu trữ sự kiện tương ứng với xử lý của người dùng trong vùng lưu trữ được chia sẻ. Sau đó trong chế độ theo dõi, bộ xử lý kích hoạt bộ ngắt trong môi trường xử lý thứ nhất để thu được sự kiện được lưu trữ trong vùng lưu trữ được chia sẻ. Bộ ngắt trong môi trường xử lý thứ nhất cấp sự kiện thu được đến môi trường xử lý thứ nhất để xử lý.

Cách 2: Sự kiện tương ứng với xử lý được cấp, bằng cách sử dụng luồng trình nền, đến môi trường xử lý thứ nhất để xử lý.

Theo cách 2, xử lý trình nền (daemon) là xử lý với tuổi thọ tương đối dài, và thường độc lập với thiết bị người dùng và định kỳ thực hiện nhiệm vụ hoặc chờ xử lý sự kiện sẽ xảy ra. Xử lý trình nền (daemon) thường được bắt đầu khi hệ thống được khởi động, và kết thúc khi hệ thống được vô hiệu. Theo cách 2, bộ xử lý có thể kích hoạt bộ ngắt trong môi trường xử lý thứ hai, và lưu trữ sự kiện tương ứng với xử lý của người dùng trong vùng lưu trữ được chia sẻ. Sau đó trong chế độ theo dõi, bộ xử lý kích hoạt bộ ngắt trong môi trường xử lý thứ nhất, và kích hoạt luồng trình nền trong môi trường xử lý thứ nhất bằng cách sử dụng bộ ngắt trong môi trường xử lý thứ nhất. Luồng trình nền thu được sự kiện được lưu trữ trong vùng lưu trữ được chia sẻ, và luồng trình nền truyền sự kiện thu được đến môi trường xử lý thứ nhất để xử lý.

Trong hai dạng thực hiện cụ thể trên đây để cấp sự kiện tương ứng với xử lý đến môi trường xử lý thứ nhất để xử lý, trước khi sự kiện được cấp, sự kiện

hiện thời cần được lưu trữ trong vùng lưu trữ được chia sẻ. Trong trường hợp này, bộ ngắt trong môi trường xử lý thứ hai có thể được kích hoạt, và sự kiện có thể được lưu trữ trong vùng lưu trữ được chia sẻ bằng cách sử dụng bộ ngắt mà chạy trong môi trường thứ hai. Theo cách khác, bộ điều khiển của bộ hiển thị có thể truyền sự kiện đến ứng dụng lớp trên, và sự kiện có thể được lưu trữ trong vùng lưu trữ được chia sẻ bằng cách sử dụng ứng dụng lớp trên.

Một cách tùy chọn, sau khi cấp sự kiện tương ứng với xử lý đến môi trường xử lý thứ nhất để xử lý, phương pháp này còn bao gồm bước: ẩn vùng hiển thị được thiết lập trước.

Ví dụ, sau khi nhập 12345678, người dùng không cần thực hiện xử lý khác bất kỳ, và trong trường hợp này, bộ xử lý ẩn vùng hiển thị được thiết lập trước.

Một cách tương ứng, một phương án của sáng chế còn đề xuất thiết bị nhập dữ liệu. Như được thể hiện trên Fig.10, thành phần cấu trúc của thiết bị bao gồm:

bộ thu 1001, được tạo cấu hình để thu sự kiện được tạo ra khi người dùng thực hiện xử lý trên UE trong vùng hiển thị được thiết lập trước;

bộ xác định 1002, được tạo cấu hình để xác định việc xử lý của người dùng trên UE có được thực hiện trong vùng hiển thị được thiết lập trước hay không; và

bộ thực thi 1003, được tạo cấu hình để: khi xác định được là xử lý của người dùng trên UE không được thực hiện trong vùng hiển thị được thiết lập trước, cấp sự kiện tương ứng với xử lý đến môi trường xử lý thứ nhất để xử lý.

Vùng hiển thị được thiết lập trước chạy trong môi trường xử lý thứ hai của UE, và môi trường xử lý thứ hai có mức độ bảo mật cao hơn so với môi trường xử lý thứ nhất.

Một cách tùy chọn, trong thiết bị trên đây, bộ thực thi 1003 được tạo cấu hình đặc biệt để: lưu trữ sự kiện tương ứng với xử lý trong vùng lưu trữ được chia sẻ, trong đó vùng lưu trữ được chia sẻ là vùng lưu trữ mà được chia sẻ bởi môi trường xử lý thứ nhất và môi trường xử lý thứ hai; và kích hoạt bộ ngắt

trong môi trường xử lý thứ nhất, để cấp sự kiện được lưu trữ trong vùng lưu trữ được chia sẻ đến môi trường xử lý thứ nhất để xử lý.

Cụ thể là, bộ thực thi 1003 được tạo cấu hình đặc biệt để: kích hoạt bộ ngắt trong môi trường xử lý thứ nhất, và gọi ra luồng trình nền trong môi trường an toàn thứ nhất, để cấp, bằng cách sử dụng luồng trình nền, sự kiện được lưu trữ trong vùng lưu trữ được chia sẻ đến môi trường xử lý thứ nhất để xử lý.

Cụ thể là, bộ thực thi 1003 còn được tạo cấu hình để: khi xác định được là sự kiện tương ứng với xử lý là sự kiện nhập an toàn, hiển thị vùng hiển thị được thiết lập trước, để người dùng thực hiện xử lý trong vùng hiển thị được thiết lập trước. Sự kiện nhập an toàn là sự kiện nhập dữ liệu với thuộc tính xác nhận quyền.

Cụ thể là, bộ thực thi 1003 còn được tạo cấu hình để ẩn vùng hiển thị được thiết lập trước sau khi cấp sự kiện tương ứng với xử lý đến môi trường xử lý thứ nhất để xử lý.

Cụ thể là, vùng hiển thị được thiết lập trước bao gồm hộp biên soạn nhập với thuộc tính độ bảo mật.

Sáng chế còn đề xuất vật lưu trữ máy tính, được tạo cấu hình để lưu trữ lệnh phần mềm máy tính được sử dụng bởi thiết bị nhập dữ liệu theo khía cạnh trên đây. Lệnh phần mềm máy tính bao gồm chương trình được thiết kế để thực hiện khía cạnh trên đây.

Người có hiểu biết trung bình về lĩnh vực kỹ thuật này cần hiểu là các phương án của sáng chế có thể được cung cấp là phương pháp, thiết bị (cơ cấu), hoặc sản phẩm chương trình máy tính. Do đó, sáng chế có thể sử dụng dạng các phương án chỉ phần cứng, các phương án chỉ phần mềm, hoặc các phương án với kết hợp của phần mềm và phần cứng. Hơn nữa, sáng chế có thể sử dụng dạng sản phẩm chương trình máy tính được thực hiện trên một hoặc nhiều phương tiện lưu trữ sử dụng được bằng máy tính (bao gồm nhưng không bị giới hạn ở bộ nhớ đĩa, CD-ROM, bộ nhớ quang, và tương tự) mà bao gồm mã chương trình sử dụng được bằng máy tính.

Sáng chế được mô tả có tham chiếu các lưu đồ và/hoặc các sơ đồ khối của phương pháp, thiết bị (cơ cấu), và sản phẩm chương trình máy tính theo các phương án của sáng chế. Cần hiểu rằng các lệnh chương trình máy tính có thể được sử dụng để thực hiện từng xử lý và/hoặc từng khối trong các lưu đồ và/hoặc các sơ đồ khối và kết hợp của xử lý và/hoặc khối trong các lưu đồ và/hoặc các sơ đồ khối. Các lệnh chương trình máy tính này có thể được cung cấp cho máy tính đa năng, máy tính chuyên dụng, bộ xử lý lắp sẵn bên trong, hoặc bộ xử lý của thiết bị xử lý dữ liệu khả lập trình khác bất kỳ để tạo máy, để các lệnh được thực hiện bằng máy tính hoặc bộ xử lý của thiết bị xử lý dữ liệu khả lập trình khác bất kỳ tạo thành thiết bị để thực hiện chức năng cụ thể trong một hoặc nhiều xử lý trong các lưu đồ và/hoặc trong một hoặc nhiều khối trong các sơ đồ khối.

Các lệnh chương trình máy tính này có thể cũng được lưu trữ trong bộ nhớ đọc được bằng máy tính mà có thể lệnh cho máy tính hoặc thiết bị xử lý dữ liệu khả lập trình khác bất kỳ để làm việc theo cách cụ thể, để các lệnh được lưu trữ trong bộ nhớ đọc được bằng máy tính tạo sự giả tạo (artifact) bao gồm thiết bị lệnh. Thiết bị lệnh thực hiện chức năng cụ thể trong một hoặc nhiều xử lý trong các lưu đồ và/hoặc trong một hoặc nhiều khối trong các sơ đồ khối.

Các lệnh chương trình máy tính này có thể cũng được tải trên máy tính hoặc thiết bị xử lý dữ liệu khả lập trình khác, để chuỗi các xử lý và bước được thực hiện trên máy tính hoặc thiết bị khả lập trình khác, để tạo xử lý được thực hiện bằng máy tính. Do đó, các lệnh được thực hiện trên máy tính hoặc thiết bị khả lập trình khác cung cấp các bước để thực hiện chức năng cụ thể trong một hoặc nhiều xử lý trong các lưu đồ và/hoặc trong một hoặc nhiều khối trong các sơ đồ khối.

Mặc dù một số phương án ưu tiên của sáng chế đã được mô tả, người có hiểu biết trung bình về lĩnh vực kỹ thuật này có thể thực hiện các thay đổi và cải biến đối với các phương án này khi biết được khái niệm sáng tạo cơ bản. Do đó, các điểm yêu cầu bảo hộ dưới đây được coi là bao hàm các phương án ưu tiên và tất cả các thay đổi và cải biến nằm trong phạm vi của sáng chế.

Hiển nhiên là người có hiểu biết trung bình về lĩnh vực kỹ thuật này có thể thực hiện các cải biến và biến đổi khác nhau đối với sáng chế mà không nằm ngoài bản chất và phạm vi của sáng chế. Sáng chế nhằm bao hàm các cải biến và biến đổi này với điều kiện các cải biến và biến đổi này được xác định bằng các điểm yêu cầu bảo hộ kèm theo và các kỹ thuật tương đương của chúng.

YÊU CẦU BẢO HỘ

1. Phương pháp nhập dữ liệu, bao gồm:

hiển thị giao diện người dùng đồ họa mà có vùng nhập bởi bộ hiển thị được kết hợp với thiết bị người dùng (UE-user equipment);

xử lý hoạt động thứ nhất của người dùng thu được bởi vùng nhập để xác định rằng sự kiện thứ nhất mà tương ứng với hoạt động thứ nhất có được kết hợp với sự kiện nhập an toàn dựa trên nội dung của hoạt động thứ nhất hay không;

hiển thị vùng hiển thị được thiết lập trước để cho phép người dùng thực hiện sự kiện nhập an toàn trong vùng hiển thị được thiết lập trước dựa trên việc xác định rằng hoạt động thứ nhất được kết hợp với sự kiện nhập an toàn;

dò tìm hoạt động thứ hai thu được bởi vùng nhập phía ngoài vùng hiển thị được thiết lập trước; và

cấp sự kiện thứ hai mà tương ứng với hoạt động thứ hai tới môi trường hoạt động thứ nhất để xử lý,

trong đó vùng hiển thị được thiết lập trước chạy trong môi trường hoạt động thứ hai của UE, và môi trường hoạt động thứ hai có mức bảo mật cao hơn so với môi trường hoạt động thứ nhất, và

bước cấp sự kiện thứ hai mà tương ứng với hoạt động thứ hai tới môi trường hoạt động thứ nhất để xử lý bao gồm:

lưu trữ sự kiện thứ hai trong vùng lưu trữ được chia sẻ, trong đó vùng lưu trữ được chia sẻ là vùng lưu trữ mà được chia sẻ bởi môi trường hoạt động thứ nhất và môi trường hoạt động thứ hai; và

kích hoạt bộ ngắt trong môi trường hoạt động thứ nhất và gọi ra luồng trình nền (daemon thread) trong môi trường hoạt động thứ nhất, để cấp, bằng cách sử dụng luồng trình nền, sự kiện thứ hai được lưu trữ trong vùng lưu trữ được chia sẻ tới môi trường hoạt động thứ nhất để xử lý.

2. Phương pháp theo điểm 1, trong đó nội dung của hoạt động thứ nhất bao gồm thuộc tính xác nhận quyền.

3. Phương pháp theo điểm 1, trong đó sau bước cấp sự kiện thứ hai tới môi trường hoạt động thứ nhất để xử lý, phương pháp này còn bao gồm:

ẩn vùng hiển thị được thiết lập trước.

4. Phương pháp theo điểm bất kỳ trong số các điểm 1 đến 3, trong đó vùng hiển thị được thiết lập trước bao gồm hộp biên soạn nhập được định dạng.

5. Phương pháp theo điểm 1, trong đó môi trường hoạt động thứ nhất được chạy trong lõi ảo thứ nhất của bộ xử lý và môi trường hoạt động thứ hai được chạy trong lõi ảo thứ hai của bộ xử lý.

6. Phương pháp theo điểm 5, trong đó lõi ảo thứ nhất là lõi không an toàn, và lõi ảo thứ hai là lõi an toàn.

7. Phương pháp theo điểm 2, trong đó nội dung của thuộc tính xác nhận quyền là mật khẩu.

8. Phương pháp theo điểm 1, trong đó vùng hiển thị được thiết lập trước được ẩn trừ khi sự kiện nhập an toàn được xác định.

9. Phương pháp theo điểm 1, trong đó vùng hiển thị được thiết lập trước được hiển thị đồng thời với vùng nhập bởi bộ hiển thị.

10. Thiết bị truyền thông, bao gồm:

bộ xử lý; và

bộ nhớ mà có các lệnh đọc được bởi máy tính được lưu trữ trên đó, mà khi được thực thi bởi bộ xử lý, làm cho thiết bị:

hiển thị giao diện người dùng đồ họa mà có vùng nhập bởi bộ hiển thị được kết hợp với thiết bị người dùng (UE-user equipment);

xử lý hoạt động thứ nhất của người dùng thu được bởi vùng nhập để xác định rằng sự kiện thứ nhất mà tương ứng với hoạt động thứ nhất có được kết hợp với sự kiện nhập an toàn dựa trên nội dung của hoạt động thứ nhất hay không;

hiển thị vùng hiển thị được thiết lập trước để cho phép người dùng thực hiện sự kiện nhập an toàn trong vùng hiển thị được thiết lập trước dựa trên việc xác định rằng hoạt động thứ nhất được kết hợp với sự kiện nhập an toàn;

dò tìm hoạt động thứ hai thu được bởi vùng nhập phía ngoài vùng hiển thị được thiết lập trước; và

cấp sự kiện thứ hai mà tương ứng với hoạt động thứ hai tới môi trường hoạt động thứ nhất để xử lý,

trong đó vùng hiển thị được thiết lập trước chạy trong môi trường hoạt động thứ hai của UE, và môi trường hoạt động thứ hai có mức bảo mật cao hơn so với môi trường hoạt động thứ nhất, và

làm cho thiết bị truyền thông cấp sự kiện thứ hai mà tương ứng với hoạt động thứ hai tới môi trường hoạt động thứ nhất để xử lý bằng cách:

lưu trữ sự kiện thứ hai trong vùng lưu trữ được chia sẻ, trong đó vùng lưu trữ được chia sẻ là vùng lưu trữ mà được chia sẻ bởi môi trường hoạt động thứ nhất và môi trường hoạt động thứ hai; và

kích hoạt bộ ngắt trong môi trường hoạt động thứ nhất và gọi ra luồng trình nền (daemon thread) trong môi trường hoạt động thứ nhất, để cấp, bằng cách sử dụng luồng trình nền, sự kiện thứ hai được lưu trữ trong vùng lưu trữ được chia sẻ tới môi trường hoạt động thứ nhất để xử lý.

11. Thiết bị truyền thông theo điểm 10, trong đó nội dung của hoạt động thứ nhất bao gồm thuộc tính xác nhận quyền.

12. Thiết bị truyền thông theo điểm 10, trong đó thiết bị truyền thông còn được tác động để:

ẩn vùng hiển thị được thiết lập trước sau khi cấp sự kiện thứ hai tới môi trường hoạt động thứ nhất để xử lý.

13. Phương tiện lưu trữ bất biến đọc được bởi máy tính, bao gồm các lệnh đọc được bởi máy tính được lưu trữ trên đó, mà khi được thực thi bởi ít nhất một bộ xử lý, làm cho thiết bị:

hiển thị giao diện người dùng đồ họa mà có vùng nhập bởi bộ hiển thị được kết hợp với thiết bị người dùng (UE-user equipment);

xử lý hoạt động thứ nhất của người dùng thu được bởi vùng nhập để xác định rằng sự kiện thứ nhất mà tương ứng với hoạt động thứ nhất có được kết hợp

với sự kiện nhập an toàn dựa trên nội dung của hoạt động thứ nhất hay không;

hiển thị vùng hiển thị được thiết lập trước để cho phép người dùng thực hiện sự kiện nhập an toàn trong vùng hiển thị được thiết lập trước dựa trên việc xác định rằng hoạt động thứ nhất được kết hợp với sự kiện nhập an toàn;

dò tìm hoạt động thứ hai thu được bởi vùng nhập phía ngoài vùng hiển thị được thiết lập trước; và

cấp sự kiện thứ hai mà tương ứng với hoạt động thứ hai tới môi trường hoạt động thứ nhất để xử lý,

trong đó vùng hiển thị được thiết lập trước chạy trong môi trường hoạt động thứ hai của UE, và môi trường hoạt động thứ hai có mức bảo mật cao hơn so với môi trường hoạt động thứ nhất, và

làm cho thiết bị cấp sự kiện thứ hai mà tương ứng với hoạt động thứ hai tới môi trường hoạt động thứ nhất để xử lý bằng cách:

lưu trữ sự kiện thứ hai trong vùng lưu trữ được chia sẻ, trong đó vùng lưu trữ được chia sẻ là vùng lưu trữ mà được chia sẻ bởi môi trường hoạt động thứ nhất và môi trường hoạt động thứ hai; và

kích hoạt bộ ngắt trong môi trường hoạt động thứ nhất và gọi ra luồng trình nền (daemon thread) trong môi trường hoạt động thứ nhất, để cấp, bằng cách sử dụng luồng trình nền, sự kiện thứ hai được lưu trữ trong vùng lưu trữ được chia sẻ tới môi trường hoạt động thứ nhất để xử lý.

14. Phương tiện lưu trữ bất biến theo điểm 13, trong đó nội dung của hoạt động thứ nhất bao gồm thuộc tính xác nhận quyền.

15. Phương tiện lưu trữ bất biến theo điểm 13, trong đó thiết bọ còn được tác động để:

ẩn vùng hiển thị được thiết lập trước sau khi cấp sự kiện thứ hai tới môi trường hoạt động thứ nhất để xử lý.

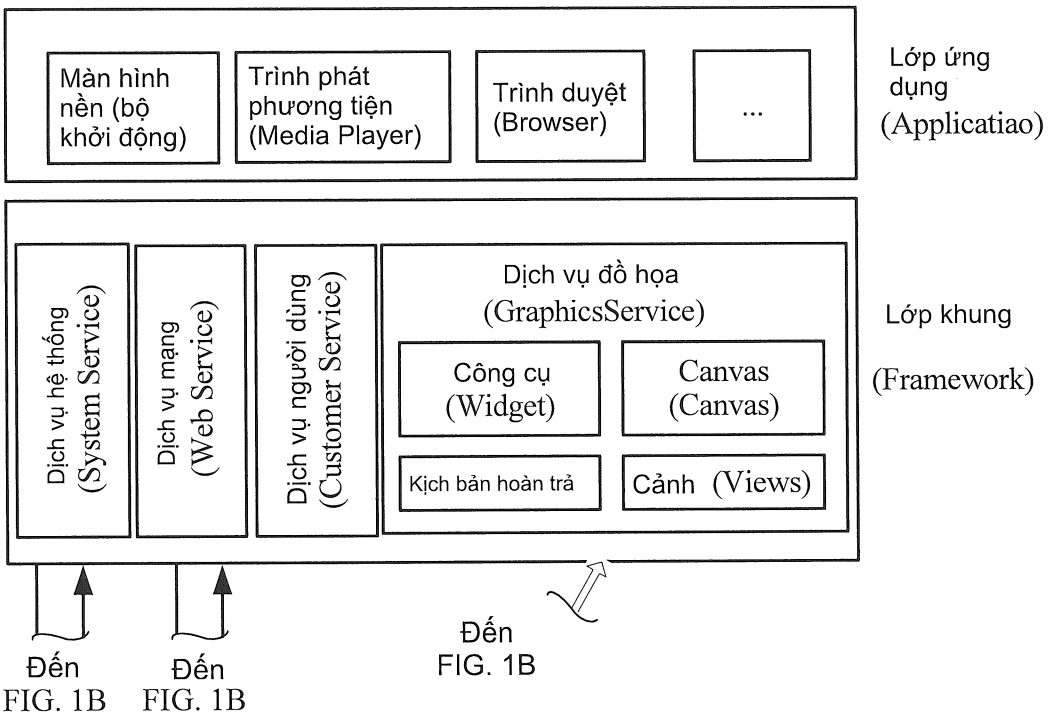

Màn hình nền (bộ khởi động)
Trình phát phương tiện (Media Player)
Trình duyệt (Browser)
...
Lớp ứng dụng (Applicatiao)
Dịch vụ hệ thống (System Service)
Dịch vụ mạng (Web Service)
Dịch vụ người dùng (Customer Service)
Dịch vụ đồ họa (GraphicsService)
Công cụ (Widget)
Canvas (Canvas)
Kịch bản hoàn trả
Cảnh (Views)
Lớp khung (Framework)
Đến FIG. 1B
Đến FIG. 1B
Đến FIG. 1B

FIG. 1A

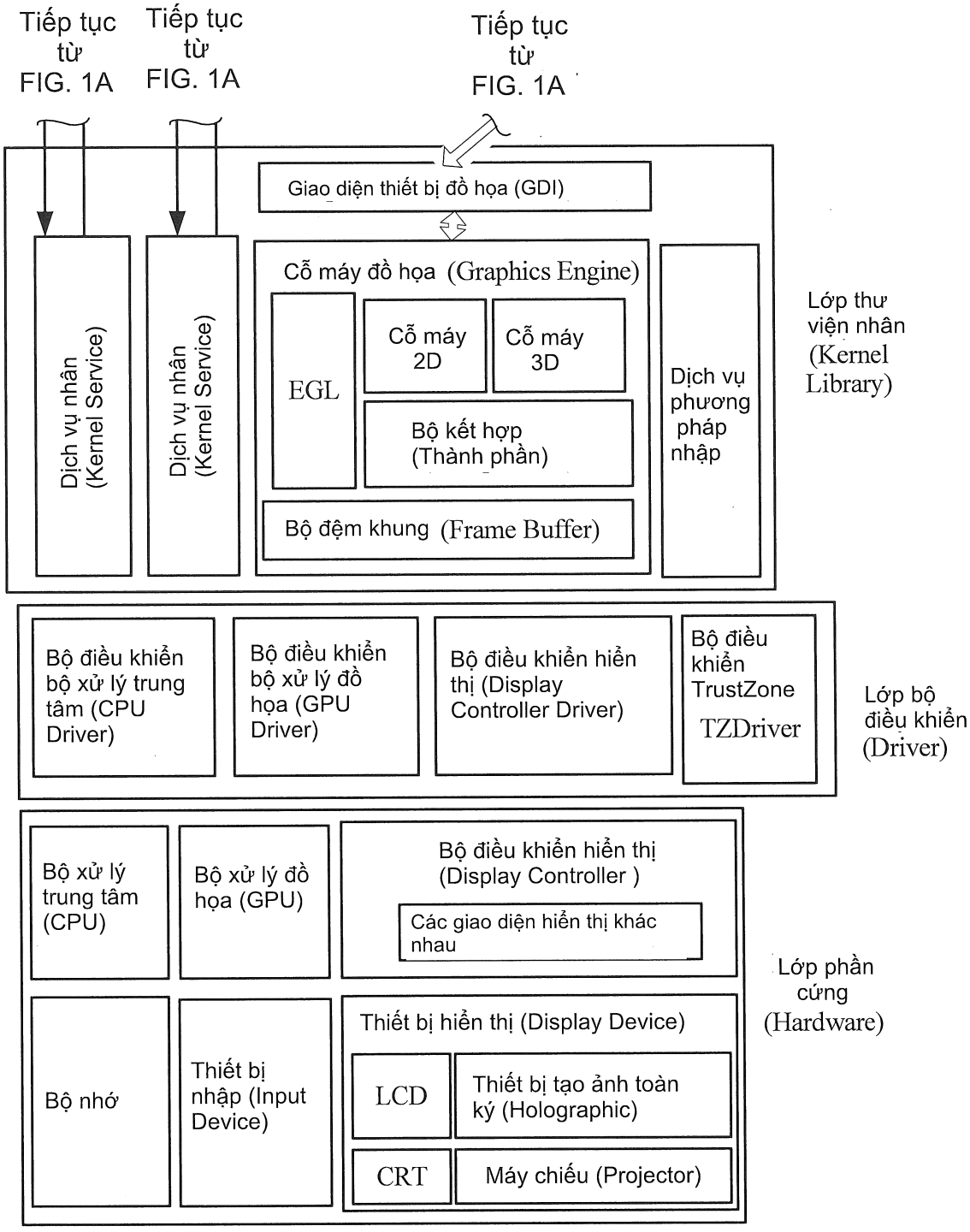

Tiếp tục từ FIG. 1A
Tiếp tục từ FIG. 1A
Tiếp tục từ FIG. 1A
Giao diện thiết bị đồ họa (GDI)
Dịch vụ nhân (Kernel Service)
Dịch vụ nhân (Kernel Service)
Cỗ máy đồ họa (Graphics Engine)
EGL
Cỗ máy 2D
Cỗ máy 3D
Bộ kết hợp (Thành phần)
Bộ đệm khung (Frame Buffer)
Dịch vụ phương pháp nhập
Lớp thư viện nhân (Kernel Library)
Bộ điều khiển bộ xử lý trung tâm (CPU Driver)
Bộ điều khiển bộ xử lý đồ họa (GPU Driver)
Bộ điều khiển hiển thị (Display Controller Driver)
Bộ điều khiển TrustZone TZDriver
Lớp bộ điều khiển (Driver)
Bộ xử lý trung tâm (CPU)
Bộ xử lý đồ họa (GPU)
Bộ điều khiển hiển thị (Display Controller)
Các giao diện hiển thị khác nhau
Bộ nhớ
Thiết bị nhập (Input Device)
Thiết bị hiển thị (Display Device)
LCD
Thiết bị tạo ảnh toàn ký (Holographic)
CRT
Máy chiếu (Projector)
Lớp phần cứng (Hardware)

FIG. 1B

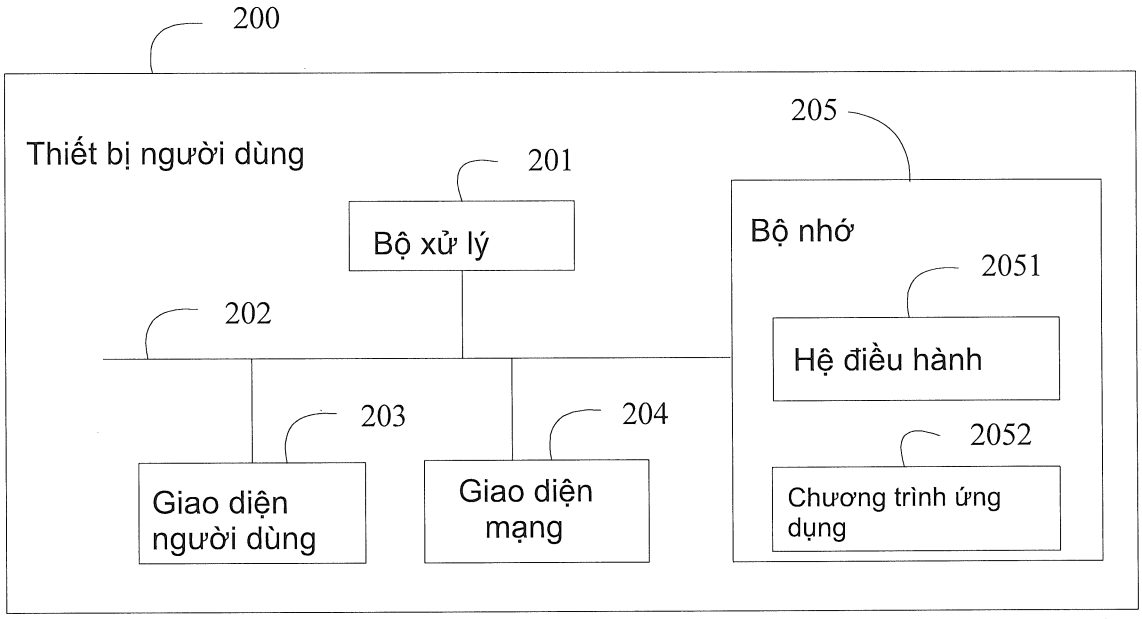

200
Thiết bị người dùng
201
Bộ xử lý
205
Bộ nhớ
2051
Hệ điều hành
202
203
204
2052
Giao diện người dùng
Giao diện mạng
Chương trình ứng dụng

FIG. 2

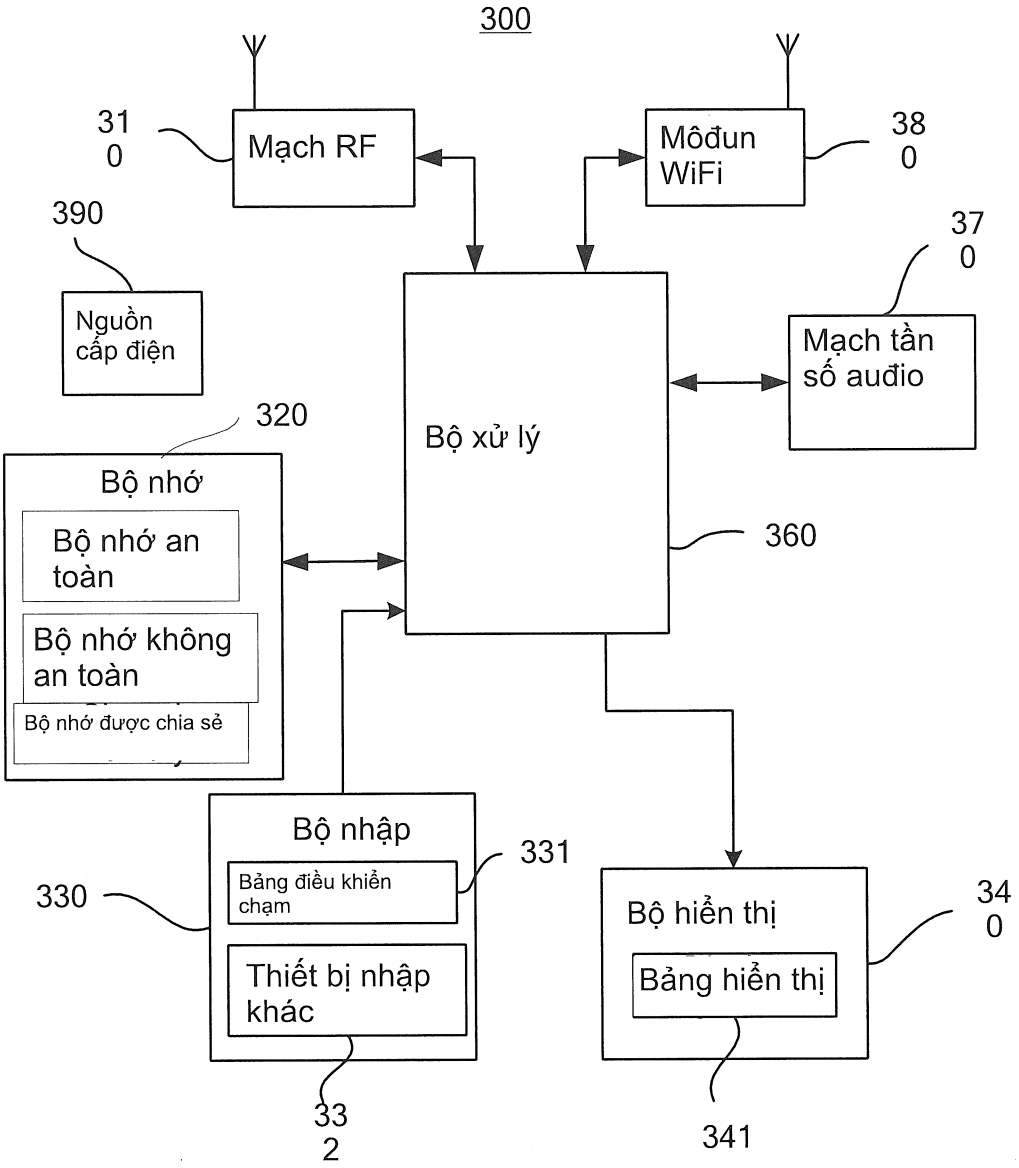

300
310
Mạch RF
Môđun WiFi
380
390
Nguồn cấp điện
370
Mạch tần số audio
Bộ xử lý
320
Bộ nhớ
Bộ nhớ an toàn
Bộ nhớ không an toàn
Bộ nhớ được chia sẻ
360
Bộ nhập
331
330
Bảng điều khiển chạm
Thiết bị nhập khác
332
Bộ hiển thị
340
Bảng hiển thị
341

FIG. 3

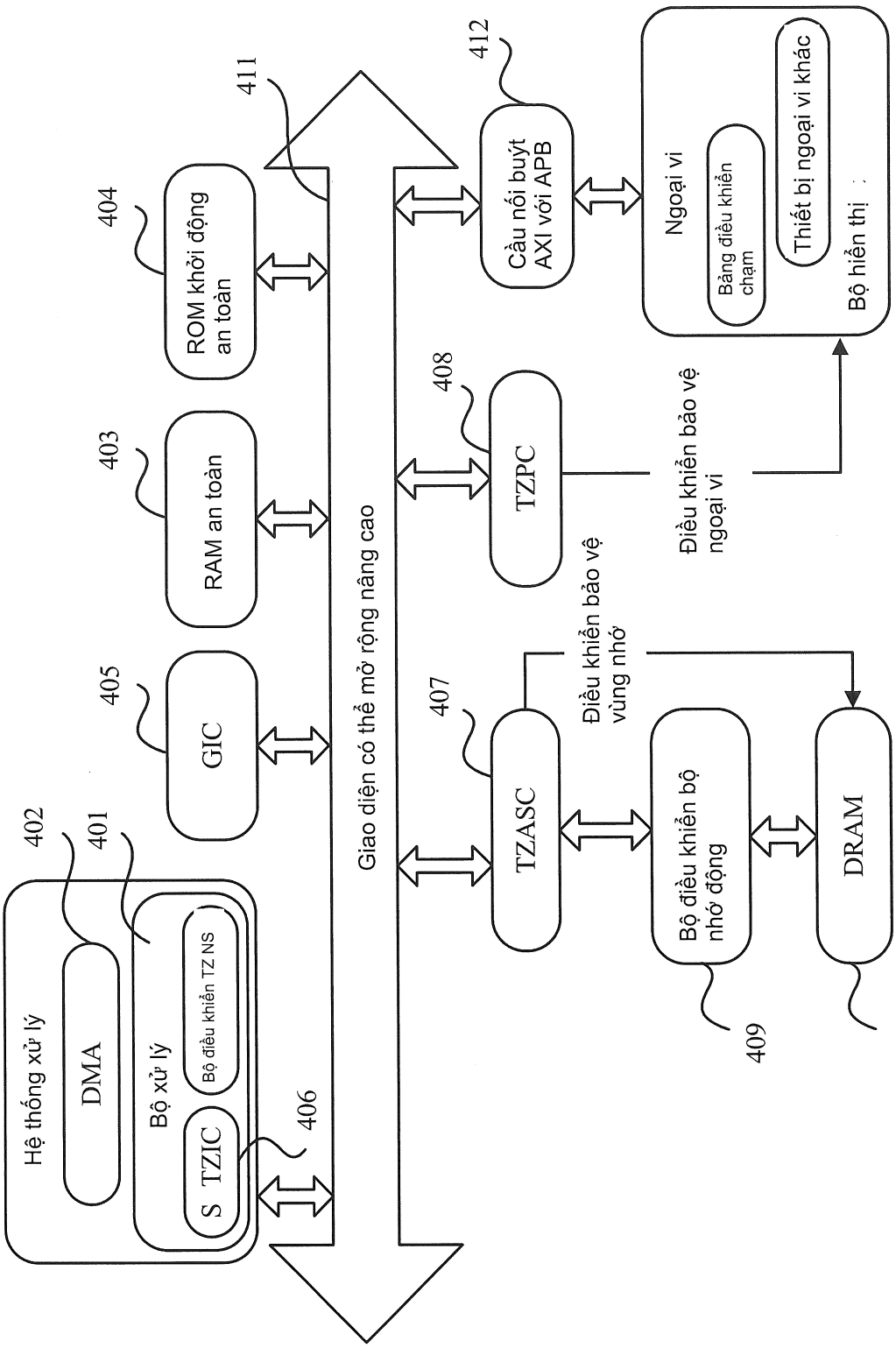

Hệ thống xử lý
DMA
Bộ xử lý
Bộ điều khiển TZ NS
S TZIC
402
401
406
GIC
405
RAM an toàn
403
ROM khởi động an toàn
404
411
Giao diện có thể mở rộng nâng cao
TZPC
408
TZASC
407
Điều khiển bảo vệ vùng nhớ
Bộ điều khiển bộ nhớ động
409
DRAM
410
Điều khiển bảo vệ ngoại vi
Cầu nối buýt AXI với APB
412
Ngoại vi
Bảng điều khiển chạm
Thiết bị ngoại vi khác
Bộ hiển thị

FIG. 4

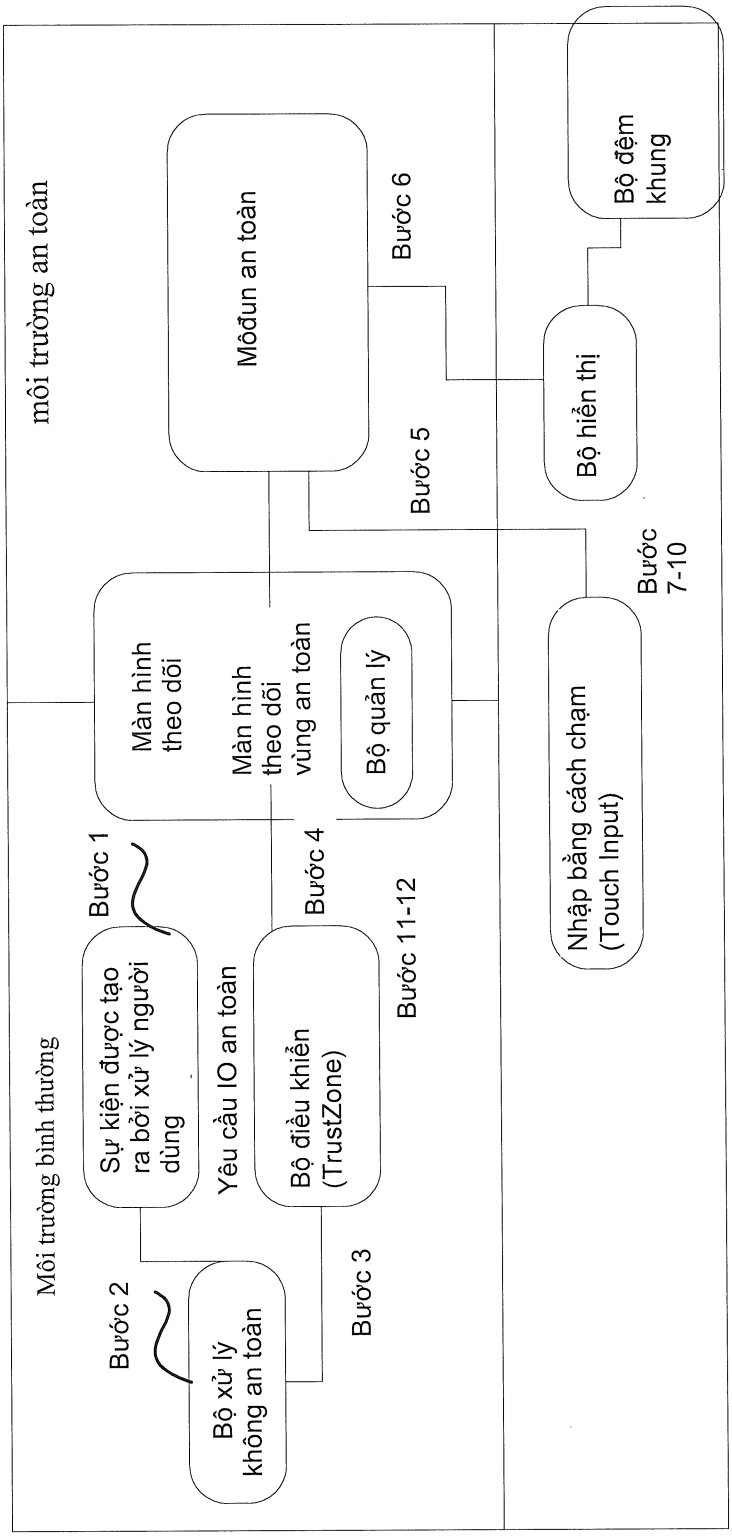

môi trường an toàn
Môđun an toàn
Bước 6
Bộ đệm khung
Bộ hiển thị
Bước 5
Bước 7-10
Màn hình theo dõi
Màn hình theo dõi vùng an toàn
Bộ quản lý
Nhập bằng cách chạm (Touch Input)
Bước 1
Bước 4
Bước 11-12
Môi trường bình thường
Sự kiện được tạo ra bởi xử lý người dùng
Yêu cầu IO an toàn
Bộ điều khiển (TrustZone)
Bước 2
Bước 3
Bộ xử lý không an toàn

FIG. 5

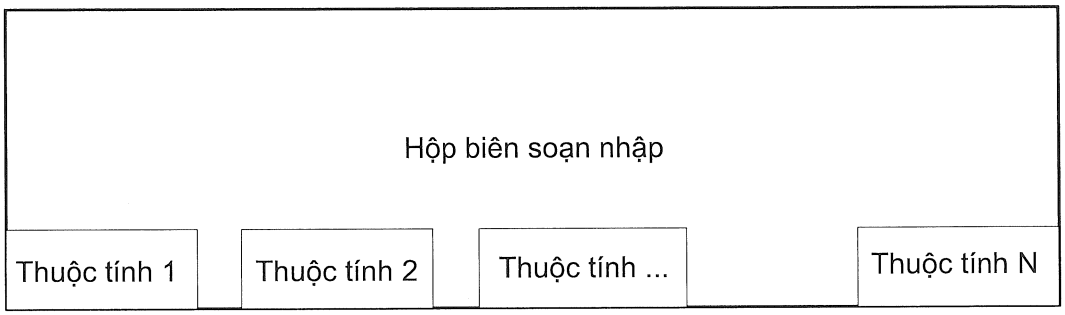


FIG. 6

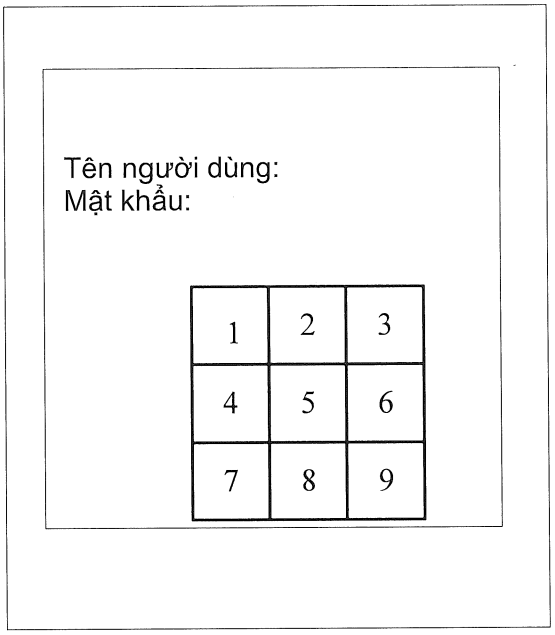


FIG. 7

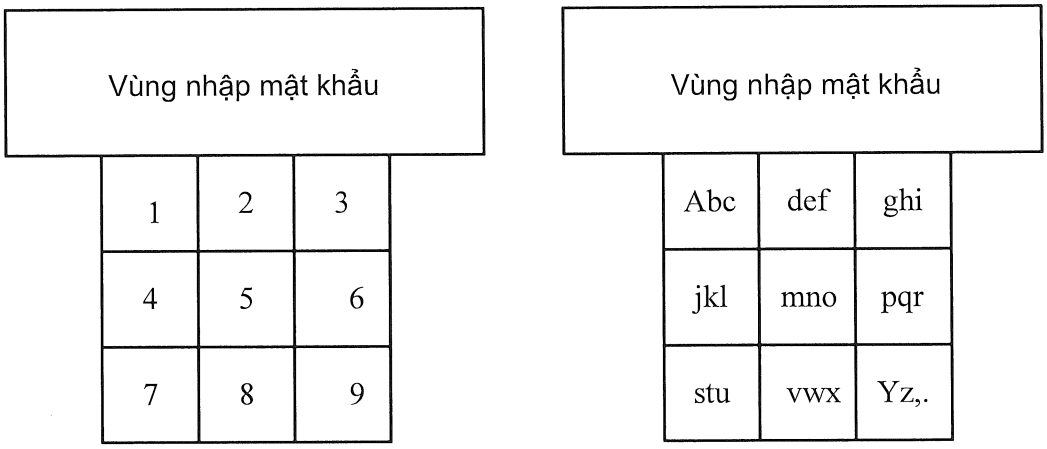


FIG. 8

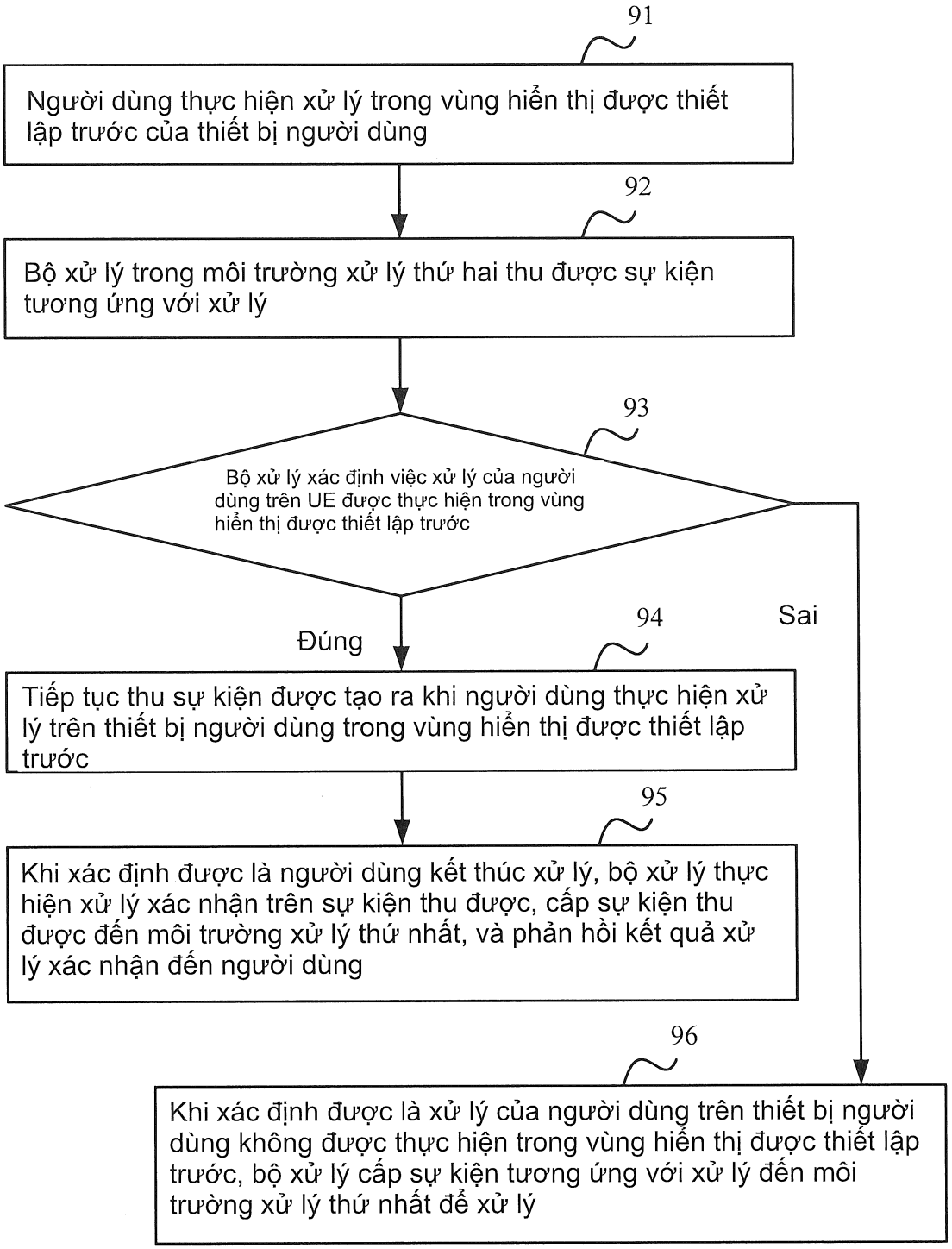

91
Người dùng thực hiện xử lý trong vùng hiển thị được thiết lập trước của thiết bị người dùng
92
Bộ xử lý trong môi trường xử lý thứ hai thu được sự kiện tương ứng với xử lý
93
Bộ xử lý xác định việc xử lý của người dùng trên UE được thực hiện trong vùng hiển thị được thiết lập trước
Đúng
Sai
94
Tiếp tục thu sự kiện được tạo ra khi người dùng thực hiện xử lý trên thiết bị người dùng trong vùng hiển thị được thiết lập trước
95
Khi xác định được là người dùng kết thúc xử lý, bộ xử lý thực hiện xử lý xác nhận trên sự kiện thu được, cấp sự kiện thu được đến môi trường xử lý thứ nhất, và phản hồi kết quả xử lý xác nhận đến người dùng
96
Khi xác định được là xử lý của người dùng trên thiết bị người dùng không được thực hiện trong vùng hiển thị được thiết lập trước, bộ xử lý cấp sự kiện tương ứng với xử lý đến môi trường xử lý thứ nhất để xử lý

FIG. 9

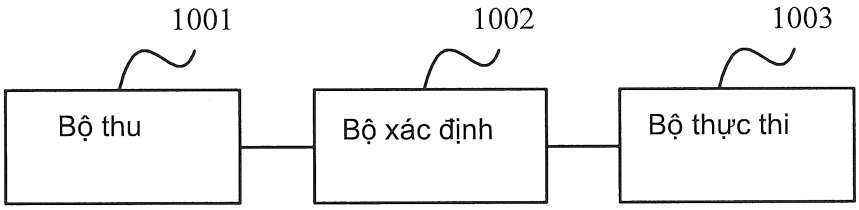


FIG. 10