



(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)



1-0031348

(51)⁸ G06F 21/32; H04W 88/02

(13) B

(21) 1-2018-04911

(22) 05/04/2016

(86) PCT/CN2016/078465 05/04/2016

(87) WO2017/173575 12/10/2017

(45) 25/03/2022 408

(43) 25/01/2019 370A

(73) HUAWEI TECHNOLOGIES CO., LTD. (CN)

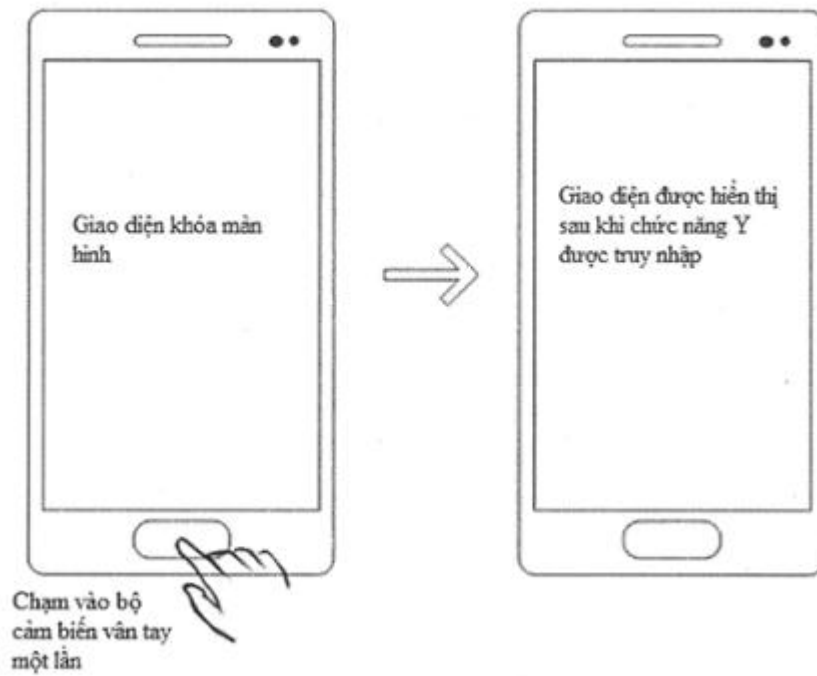
Huawei Administration Building Bantian, Longgang District Shenzhen, Guangdong
518129, China

(72) YIN, Junjie (CN); SONG, Lei (CN).

(74) Công ty Luật TNHH Phạm và Liên danh (PHAM & ASSOCIATES)

(54) PHƯƠNG PHÁP TRUY NHẬP ỨNG DỤNG MỤC TIÊU VÀ THIẾT BỊ TRẠM
ĐẦU CUỐI

(57) Sáng chế đề xuất phương pháp và thiết bị đầu cuối truy nhập ứng dụng đích, trong đó phương pháp được áp dụng cho thiết bị đầu cuối mà trên đó ứng dụng đích được cài đặt, ứng dụng đích được thiết lập bằng mật khẩu ứng dụng được sử dụng để truy nhập ứng dụng đích, thiết bị đầu cuối được thiết lập bằng thông tin vân tay thứ nhất được sử dụng để mở khóa thiết bị đầu cuối, thiết bị đầu cuối còn được thiết lập bằng chuỗi thao tác tương ứng với thông tin vân tay thứ nhất, và chuỗi thao tác gồm mở khóa thiết bị đầu cuối và truy nhập ứng dụng đích. Phương pháp gồm: tiếp nhận mật khẩu ứng dụng đầu vào; gửi, đến máy chủ ứng dụng, thông điệp thứ nhất mà mang mật khẩu ứng dụng; tiếp nhận thông điệp thứ hai mà chỉ báo rằng việc kiểm chứng của mật khẩu ứng dụng thành công và được gửi bởi máy chủ ứng dụng; thiết lập phép tương ứng giữa mật khẩu ứng dụng và thông tin vân tay thứ nhất dựa trên thông điệp thứ hai; tiếp nhận thông tin vân tay thứ hai đầu vào; và khi mức độ so khớp giữa thông tin vân tay thứ hai đầu vào và thông tin vân tay thứ nhất vượt quá ngưỡng định trước, thực hiện chuỗi thao tác dựa trên phép tương ứng giữa mật khẩu ứng dụng và thông tin vân tay thứ nhất.



Lĩnh vực kỹ thuật được đề cập

Sáng chế đề cập đến lĩnh vực công nghệ truyền thông di động, và cụ thể là, đến phương pháp truy nhập ứng dụng đích, và thiết bị đầu cuối.

Tình trạng kỹ thuật của sáng chế

Vì lý do bảo mật, người dùng thường thiết lập mật khẩu khóa màn hình cho điện thoại di động, và người dùng có thể mở khóa màn hình bằng cách nhập vào mật khẩu, cử chỉ, ảnh vân tay, hoặc cách tương tự. Nhiều ứng dụng thường được cài trên điện thoại di động. Đối với một số ứng dụng quan trọng hoặc liên quan đến tính riêng tư, chẳng hạn, album, ứng dụng xã hội, và ứng dụng thanh toán, người dùng cũng thường thiết lập các mật khẩu ứng dụng, và người dùng có thể truy nhập các ứng dụng này chỉ khi nhập mật khẩu đúng. Theo cách này, việc bảo mật thông tin người dùng trong các ứng dụng này có thể được đảm bảo thậm chí nếu điện thoại di động ở trạng thái mở khóa. Tuy nhiên, trong trường hợp này, như được thể hiện trên Fig.1A và Fig.1B, nếu người dùng muốn truy nhập, khi thiết bị đầu cuối ở trạng thái khóa màn hình, ứng dụng X được thiết lập bằng mật khẩu ứng dụng, người dùng có thể truy nhập ứng dụng X chỉ sau khi người dùng trước hết nhập vào mật khẩu mở khóa màn hình, tìm thấy ứng dụng X, khởi động ứng dụng X, và nhập vào mật khẩu ứng dụng. Nếu người dùng cũng muốn truy nhập thêm chức năng Y được thiết lập bằng mật khẩu chức năng trong ứng dụng X, người dùng còn cần tìm chức năng Y, khởi động chức năng Y, và nhập vào mật khẩu chức năng, để truy nhập chức năng Y. Có thể biết rằng các thao tác nêu trên không chỉ tương đối rối rắm, mà còn mất thời gian dài.

Bản chất kỹ thuật của sáng chế

Để giải quyết vấn đề nêu trên, các phương án thực hiện sáng chế đề xuất phương pháp truy nhập ứng dụng đích, sao cho người dùng có thể nhanh chóng

truy nhập ứng dụng đích mà được thiết lập bằng mật khẩu ứng dụng.

Để mô tả ngắn gọn, theo các phương án thực hiện sáng chế, mật khẩu, cử chỉ, hoặc ảnh vân tay được sử dụng để mở khóa màn hình được gọi là mật khẩu mở khóa màn hình hoặc mật khẩu mở khóa, mật khẩu được sử dụng để truy nhập ứng dụng cụ thể được gọi là mật khẩu ứng dụng, và mật khẩu được sử dụng để truy nhập chức năng cụ thể của ứng dụng cụ thể được gọi là mật khẩu chức năng. Mật khẩu khóa màn hình, mật khẩu ứng dụng, và mật khẩu chức năng có thể được thiết lập bằng cách sử dụng ứng dụng, hoặc có thể được thiết lập bằng cách sử dụng ứng dụng bên thứ ba. Ngoài ra, đối với ứng dụng được thiết lập bằng mật khẩu ứng dụng, theo các phương án thực hiện sáng chế, kích hoạt ứng dụng để chạy được gọi là “khởi động ứng dụng”. Giao diện kiểm chứng mật khẩu thường được hiển thị sau khi ứng dụng được khởi động. Theo các phương án thực hiện sáng chế, vượt qua kiểm chứng mật khẩu hoặc bỏ qua kiểm chứng mật khẩu được gọi là “truy nhập ứng dụng”. Chẳng hạn, đối với ứng dụng album được thiết lập bằng mật khẩu ứng dụng, sau khi người dùng gõ biểu tượng ứng dụng, ứng dụng album bắt đầu chạy, tức là, ứng dụng album được khởi động. Tuy nhiên, người dùng không truy nhập ứng dụng ở thời điểm này. Người dùng truy nhập ứng dụng album chỉ sau khi người dùng còn nhập vào mật khẩu, kiểm chứng mật khẩu thành công, và thiết bị đầu cuối hiển thị các album hoặc các ảnh trong ứng dụng.

Theo khía cạnh thứ nhất, phương án thực hiện sáng chế đề xuất phương pháp truy nhập ứng dụng đích, trong đó phương pháp được áp dụng cho thiết bị đầu cuối mà trên đó ứng dụng đích được cài đặt, ứng dụng đích được thiết lập bằng mật khẩu ứng dụng được sử dụng để truy nhập ứng dụng đích, thiết bị đầu cuối được thiết lập bằng thông tin vân tay thứ nhất được sử dụng để mở khóa thiết bị đầu cuối, thiết bị đầu cuối còn được thiết lập bằng chuỗi thao tác tương ứng với thông tin vân tay thứ nhất, và chuỗi thao tác gồm mở khóa thiết bị đầu cuối và truy nhập ứng dụng đích. Phương pháp gồm các bước: tiếp nhận mật khẩu ứng dụng đầu vào; gửi, đến máy chủ ứng dụng, thông điệp thứ nhất mà mang mật khẩu ứng dụng; tiếp nhận thông điệp thứ hai mà chỉ báo rằng việc kiểm chứng của mật khẩu ứng dụng thành công và được gửi bởi máy chủ ứng

dụng; thiết lập phép tương ứng giữa mật khẩu ứng dụng và thông tin vân tay thứ nhất dựa trên thông điệp thứ hai; tiếp nhận thông tin vân tay thứ hai đầu vào; và khi mức độ so khớp giữa thông tin vân tay thứ hai đầu vào và thông tin vân tay thứ nhất vượt quá ngưỡng định trước, thực hiện chuỗi thao tác dựa trên phép tương ứng giữa mật khẩu ứng dụng và thông tin vân tay thứ nhất. Theo phương pháp, người dùng nhập vào thông tin vân tay chỉ một lần và không cần nhập vào mật khẩu ứng dụng, để truy nhập ngay ứng dụng đích được thiết lập bằng mật khẩu ứng dụng khi ứng dụng đích không bắt đầu chạy. Điều này đơn giản hóa hoạt động người dùng và cải thiện trải nghiệm người dùng khi bảo mật được đảm bảo.

Theo phương pháp truy nhập ứng dụng đích theo khía cạnh thứ nhất, phương án thực hiện sáng chế còn đề xuất các triển khai dưới đây, và các triển khai này có thể được sử dụng cùng nhau để đạt được hiệu quả kỹ thuật tốt hơn.

Theo triển khai, việc thực hiện, bởi thiết bị đầu cuối, chuỗi thao tác dựa trên phép tương ứng giữa mật khẩu ứng dụng và thông tin vân tay thứ nhất gồm: mở khóa thiết bị đầu cuối; gửi, đến máy chủ ứng dụng dựa trên phép tương ứng giữa mật khẩu ứng dụng và thông tin vân tay thứ nhất, thông điệp thứ ba chỉ báo rằng thành công kiểm chứng vân tay (tức là, mức độ so khớp giữa thông tin vân tay thứ hai và thông tin vân tay thứ nhất vượt quá ngưỡng định trước); và tiếp nhận thông điệp thứ tư mà chỉ báo rằng thành công xác thực được báo nhận và được gửi bởi máy chủ ứng dụng, và sau đó truy nhập ứng dụng đích. Trong quá trình thực hiện chuỗi thao tác, thiết bị đầu cuối bỏ qua hoặc xác định không thực hiện bước trong đó thiết bị đầu cuối hiển thị giao diện nhập vào mật khẩu ứng dụng, và thiết bị đầu cuối cũng bỏ qua hoặc xác định không thực hiện bước trong đó thiết bị đầu cuối gửi mật khẩu ứng dụng đến máy chủ ứng dụng. Do vậy, thao tác người dùng được đơn giản hóa, và trải nghiệm người dùng được cải thiện.

Theo triển khai khác, thiết bị đầu cuối tiếp nhận nhập vào thông tin vân tay thứ ba trước khi tiếp nhận mật khẩu ứng dụng đầu vào. Khi mức độ so khớp giữa thông tin vân tay thứ ba được nhập vào và thông tin vân tay thứ nhất vượt quá ngưỡng định trước, thiết bị đầu cuối sau đó tiếp nhận mật khẩu ứng dụng

đầu vào, để cải thiện bảo mật.

Theo triển khai khác, thiết bị đầu cuối tiếp nhận thông tin vân tay thứ hai đầu vào khi ứng dụng đích không bắt đầu chạy.

Theo triển khai khác, ứng dụng đích còn gồm chức năng đích (Chẳng hạn, ứng dụng đích là album, và chức năng đích là thư mục đặc biệt trong album; theo cách khác, ứng dụng đích là ứng dụng IM (instant messaging – nhắn tin nhanh, và chức năng đích là chức năng “ví” trong ứng dụng IM). Chức năng đích được thiết lập bằng mật khẩu chức năng được sử dụng để truy nhập chức năng đích, và chuỗi thao tác còn gồm truy nhập chức năng đích, tức là, chuỗi thao tác gồm mở khóa thiết bị đầu cuối, truy nhập ứng dụng đích, và truy nhập chức năng đích. Trong trường hợp này, sau khi thiết lập phép tương ứng giữa mật khẩu ứng dụng và thông tin vân tay thứ nhất, thiết bị đầu cuối còn thực hiện: tiếp nhận mật khẩu chức năng đầu vào; gửi, đến máy chủ ứng dụng, thông điệp thứ năm mà mang mật khẩu chức năng; tiếp nhận thông điệp thứ sáu mà chỉ báo rằng việc kiểm chứng của mật khẩu chức năng thành công và được gửi bởi máy chủ ứng dụng; và thiết lập phép tương ứng giữa mật khẩu chức năng và thông tin vân tay thứ nhất dựa trên thông điệp thứ sáu.

Theo triển khai khác, sau khi phép tương ứng giữa mật khẩu chức năng và thông tin vân tay thứ nhất được thiết lập, việc thực hiện, bởi thiết bị đầu cuối, chuỗi thao tác dựa trên phép tương ứng giữa mật khẩu ứng dụng và thông tin vân tay thứ nhất gồm: mở khóa thiết bị đầu cuối; gửi, đến máy chủ ứng dụng dựa trên phép tương ứng giữa mật khẩu ứng dụng và thông tin vân tay thứ nhất, thông điệp thứ ba chỉ báo rằng thành công kiểm chứng vân tay (tức là, mức độ so khớp giữa thông tin vân tay thứ hai và thông tin vân tay thứ nhất vượt quá ngưỡng định trước); tiếp nhận thông điệp thứ tư mà chỉ báo rằng thành công xác thực được báo nhận và được gửi bởi máy chủ ứng dụng, và sau đó truy nhập ứng dụng đích; gửi, đến máy chủ ứng dụng dựa trên phép tương ứng giữa mật khẩu chức năng và thông tin vân tay thứ nhất, thông điệp thứ bảy chỉ báo rằng thành công kiểm chứng vân tay; và tiếp nhận thông điệp thứ tám mà chỉ báo rằng thành công xác thực được báo nhận và được gửi bởi máy chủ ứng dụng, và sau đó truy nhập chức năng đích. Mặc dù cả thông điệp thứ ba và

thông điệp thứ bảy là các thông điệp chỉ báo rằng thành công kiểm chứng vân tay và được gửi bởi thiết bị đầu cuối đến máy chủ ứng dụng, hai thông điệp là cùng một thông điệp, hoặc có thể là các thông điệp đáp ứng khác nhau được gửi bởi thiết bị đầu cuối cho các thông điệp giao dịch khác nhau được gửi bởi máy chủ ứng dụng. Mặc dù cả thông điệp thứ tư lẫn thông điệp thứ tám là các thông điệp chỉ báo rằng thành công xác thực được báo nhận và được gửi bởi máy chủ ứng dụng, hai thông điệp là cùng một thông điệp, hoặc có thể là các thông điệp khác nhau chỉ báo rằng thành công xác thực được báo nhận và được gửi bởi máy chủ ứng dụng cho các giao dịch khác nhau. Trong quá trình thực hiện chuỗi thao tác, thiết bị đầu cuối bỏ qua hoặc xác định không thực hiện bước trong đó thiết bị đầu cuối hiển thị các giao diện nhập vào mật khẩu ứng dụng và mật khẩu chức năng, và thiết bị đầu cuối cũng bỏ qua hoặc xác định không thực hiện bước trong đó thiết bị đầu cuối gửi mật khẩu ứng dụng và mật khẩu chức năng đến máy chủ ứng dụng. Do vậy, thao tác người dùng được đơn giản hóa, và trải nghiệm người dùng được cải thiện.

Theo triển khai khác, khi thiết bị đầu cuối ở trạng thái mở khóa trước khi bắt đầu thực hiện chuỗi thao tác, thiết bị đầu cuối bỏ qua hoặc xác định không thực hiện bước mở khóa thiết bị đầu cuối trong quá trình thực hiện chuỗi thao tác.

Theo triển khai khác, trước khi thiết lập phép tương ứng giữa mật khẩu ứng dụng và thông tin vân tay thứ nhất, thiết bị đầu cuối trước hết tạo khóa, gắn khóa với thông tin vân tay thứ nhất, và gửi, đến máy chủ ứng dụng, thông điệp thứ tám mà mang khóa, sao cho máy chủ ứng dụng sử dụng khóa để đánh dấu thông tin vân tay thứ nhất.

Theo khía cạnh thứ hai, phương án thực hiện sáng chế đề xuất phương pháp truy nhập ứng dụng đích, trong đó phương pháp được áp dụng cho thiết bị đầu cuối mà trên đó ứng dụng đích được cài đặt, ứng dụng đích được thiết lập bằng mật khẩu ứng dụng được sử dụng để truy nhập ứng dụng đích, thiết bị đầu cuối được thiết lập bằng thông tin vân tay thứ nhất được sử dụng để mở khóa thiết bị đầu cuối, thiết bị đầu cuối còn được thiết lập bằng chuỗi thao tác tương ứng với thông tin vân tay thứ nhất, chuỗi thao tác gồm mở khóa thiết bị đầu

cuối và truy nhập ứng dụng đích, và thiết bị đầu cuối còn được thiết lập bằng phép tương ứng giữa mật khẩu ứng dụng và thông tin vân tay thứ nhất. Phương pháp gồm: tiếp nhận thông tin vân tay thứ hai đầu vào; gửi thông điệp kiểm chứng vân tay thành công đến máy chủ ứng dụng, trong đó thông điệp kiểm chứng vân tay thành công chỉ báo rằng mức độ so khớp giữa thông tin vân tay thứ hai và thông tin vân tay thứ nhất vượt quá ngưỡng định trước; tiếp nhận thông điệp báo nhận được gửi bởi máy chủ ứng dụng; và đáp ứng thông điệp báo nhận, và nhảy từ giao diện màn hình khóa sang giao diện được hiển thị sau khi ứng dụng đích được truy nhập. Theo phương pháp, người dùng nhập vào thông tin vân tay chỉ một lần và không cần nhập vào mật khẩu ứng dụng, để truy nhập ngay ứng dụng đích được thiết lập bằng mật khẩu ứng dụng khi ứng dụng đích không bắt đầu chạy. Điều này đơn giản hóa thao tác người dùng và cải thiện trải nghiệm người dùng trong khi đảm bảo tính bảo mật.

Theo phương pháp truy nhập ứng dụng đích theo khía cạnh thứ hai, phương án thực hiện sáng chế còn đề xuất các triển khai sau, và các triển khai này có thể được sử dụng cùng nhau để đạt được hiệu quả kỹ thuật tốt hơn.

Theo triển khai, thiết bị đầu cuối tiếp nhận thông tin vân tay thứ hai đầu vào khi ứng dụng đích không bắt đầu chạy.

Theo triển khai khác, ứng dụng đích còn gồm chức năng đích, chức năng đích được thiết lập bằng mật khẩu chức năng được sử dụng để truy nhập chức năng đích, và chuỗi thao tác còn gồm truy nhập chức năng đích, tức là, chuỗi thao tác gồm mở khóa thiết bị đầu cuối, truy nhập ứng dụng đích, và truy nhập chức năng đích. Trong phương pháp truy nhập ứng dụng đích theo khía cạnh thứ hai, “giao diện được hiển thị sau khi ứng dụng đích được truy nhập” là giao diện được hiển thị sau khi chức năng đích của ứng dụng đích được truy nhập.

Theo triển khai khác, trước khi tiếp nhận thông tin vân tay thứ hai đầu vào, thiết bị đầu cuối gửi khóa được gắn với thông tin vân tay thứ nhất đến máy chủ ứng dụng.

Theo khía cạnh thứ ba, phương án thực hiện sáng chế đề xuất thiết bị đầu cuối, gồm: bộ cảm biến vân tay; ít nhất một bộ nhớ, được tạo cấu hình để lưu trữ ứng dụng đích, thông tin vân tay thứ nhất được sử dụng để mở khóa thiết bị

đầu cuối, và chuỗi thao tác tương ứng với thông tin vân tay thứ nhất, trong đó ứng dụng đích được thiết lập bằng mật khẩu ứng dụng được sử dụng để truy nhập ứng dụng đích, và chuỗi thao tác gồm mở khóa thiết bị đầu cuối và truy nhập ứng dụng đích; màn hình cảm ứng, được tạo cấu hình để nhận mật khẩu ứng dụng đầu vào; bộ truyền, được tạo cấu hình để gửi, đến máy chủ ứng dụng, thông điệp thứ nhất mà mang mật khẩu ứng dụng; bộ tiếp nhận, được tạo cấu hình để nhận thông điệp thứ hai mà chỉ báo rằng việc kiểm chứng của mật khẩu ứng dụng thành công và được gửi bởi máy chủ ứng dụng; và ít nhất một bộ xử lý, được tạo cấu hình để: thiết lập phép tương ứng giữa mật khẩu ứng dụng và thông tin vân tay thứ nhất dựa trên thông điệp thứ hai, và thực hiện chuỗi thao tác dựa trên phép tương ứng giữa mật khẩu ứng dụng và thông tin vân tay thứ nhất khi mức độ so khớp giữa thông tin vân tay thứ hai được dò bởi bộ cảm biến vân tay khi ứng dụng đích không bắt đầu chạy và thông tin vân tay thứ nhất vượt quá ngưỡng định trước.

Trên thiết bị đầu cuối, người dùng nhập vào thông tin vân tay chỉ một lần và không cần nhập vào mật khẩu ứng dụng, để truy nhập ngay ứng dụng đích được thiết lập bằng mật khẩu ứng dụng khi ứng dụng đích không bắt đầu chạy. Điều này đơn giản hóa thao tác người dùng và cải thiện trải nghiệm người dùng trong khi bảo mật được đảm bảo.

Theo thiết bị đầu cuối theo khía cạnh thứ ba, phương án thực hiện sáng chế còn đề xuất các triển khai sau, và các triển khai này có thể được sử dụng cùng nhau để đạt được hiệu quả kỹ thuật tốt hơn.

Theo triển khai, việc bộ xử lý được tạo cấu hình để thực hiện chuỗi thao tác dựa trên phép tương ứng giữa mật khẩu ứng dụng và thông tin vân tay thứ nhất gồm: bộ xử lý được tạo cấu hình để: mở khóa thiết bị đầu cuối; ra lệnh, dựa trên phép tương ứng giữa mật khẩu ứng dụng và thông tin vân tay thứ nhất, bộ truyền gửi, đến máy chủ ứng dụng, thông điệp thứ ba chỉ báo rằng thành công kiểm chứng vân tay; và truy nhập ứng dụng đích dựa trên thông điệp thứ tư được tiếp nhận bởi bộ tiếp nhận từ máy chủ ứng dụng, trong đó thông điệp thứ tư chỉ báo rằng thành công xác thực được báo nhận. Trong quá trình thực hiện chuỗi thao tác, bộ xử lý bỏ qua hoặc xác định không thực hiện bước trong đó

bộ xử lý ra lệnh màn hình cảm ứng hiển thị giao diện nhập vào mật khẩu ứng dụng, và thiết bị đầu cuối cũng bỏ qua hoặc xác định không thực hiện bước trong đó thiết bị đầu cuối ra lệnh bộ truyền gửi mật khẩu ứng dụng đến máy chủ ứng dụng. Do vậy, thao tác người dùng được đơn giản hóa, và trải nghiệm người dùng được cải thiện.

Theo triển khai khác, bộ cảm biến vân tay tiếp nhận thông tin vân tay thứ ba được nhập vào trước khi màn hình cảm ứng tiếp nhận mật khẩu ứng dụng đầu vào. Khi mức độ so khớp giữa thông tin vân tay thứ ba được nhập vào và thông tin vân tay thứ nhất vượt quá ngưỡng định trước, sau đó màn hình cảm ứng tiếp nhận mật khẩu ứng dụng đầu vào, để cải thiện bảo mật.

Theo triển khai khác, bộ cảm biến vân tay tiếp nhận thông tin vân tay thứ hai đầu vào khi ứng dụng đích không bắt đầu chạy.

Theo triển khai khác, ứng dụng đích gồm chức năng đích, chức năng đích được thiết lập bằng mật khẩu chức năng được sử dụng để truy nhập chức năng đích, và chuỗi thao tác còn gồm truy nhập chức năng đích. Theo triển khai này, bộ xử lý còn được tạo cấu hình để: ra lệnh bộ truyền gửi thông điệp thứ năm đến máy chủ ứng dụng, trong đó thông điệp thứ năm mang nhập vào mật khẩu chức năng được tiếp nhận bởi màn hình cảm ứng; và thiết lập phép tương ứng giữa mật khẩu chức năng và thông tin vân tay thứ nhất dựa trên thông điệp thứ sáu được tiếp nhận bởi bộ tiếp nhận từ máy chủ ứng dụng, trong đó thông điệp thứ sáu được sử dụng để chỉ báo rằng việc kiểm chứng của mật khẩu chức năng thành công.

Theo triển khai khác, sau khi phép tương ứng giữa mật khẩu chức năng và thông tin vân tay thứ nhất được thiết lập, việc bộ xử lý được tạo cấu hình để thực hiện chuỗi thao tác dựa trên phép tương ứng giữa mật khẩu ứng dụng và thông tin vân tay thứ nhất gồm: bộ xử lý được tạo cấu hình để: mở khóa thiết bị đầu cuối; ra lệnh, dựa trên phép tương ứng giữa mật khẩu ứng dụng và thông tin vân tay thứ nhất, bộ truyền gửi, đến máy chủ ứng dụng, thông điệp thứ ba chỉ báo rằng thành công kiểm chứng vân tay; truy nhập ứng dụng đích dựa trên thông điệp thứ tư được tiếp nhận bởi bộ tiếp nhận từ máy chủ ứng dụng, trong đó thông điệp thứ tư chỉ báo rằng thành công xác thực được báo nhận; còn ra

lệnh, dựa trên phép tương ứng giữa mật khẩu chức năng và thông tin vân tay thứ nhất, bộ truyền gửi, đến máy chủ ứng dụng, thông điệp thứ bảy chỉ báo rằng thành công kiểm chứng vân tay; và truy nhập ứng dụng đích dựa trên thông điệp thứ tám được tiếp nhận bởi bộ tiếp nhận từ máy chủ ứng dụng, trong đó thông điệp thứ tám chỉ báo rằng thành công xác thực được báo nhận. Trong quá trình thực hiện chuỗi thao tác, bộ xử lý bỏ qua hoặc xác định không ra lệnh màn hình cảm ứng hiển thị các giao diện nhập vào mật khẩu ứng dụng và mật khẩu chức năng, và thiết bị đầu cuối cũng bỏ qua hoặc xác định không thực hiện bước trong đó thiết bị đầu cuối ra lệnh bộ truyền gửi mật khẩu ứng dụng và mật khẩu chức năng đến máy chủ ứng dụng. Do vậy, thao tác người dùng được đơn giản hóa, và trải nghiệm người dùng được cải thiện.

Theo triển khai khác, khi màn hình cảm ứng ở trạng thái mở khóa trước khi bộ xử lý bắt đầu thực hiện chuỗi thao tác, bộ xử lý bỏ qua hoặc xác định không thực hiện bước mở khóa thiết bị đầu cuối trong quá trình thực hiện chuỗi thao tác.

Theo triển khai khác, bộ xử lý còn được tạo cấu hình để: tạo khóa; gắn khóa với thông tin vân tay thứ nhất; và ra lệnh bộ truyền gửi, đến máy chủ ứng dụng, thông điệp thứ tám mà mang khóa.

Theo khía cạnh thứ tư, phương án thực hiện sáng chế đề xuất thiết bị đầu cuối, gồm: ít nhất một bộ nhớ, được tạo cấu hình để lưu trữ ứng dụng đích, thông tin vân tay thứ nhất được sử dụng để mở khóa thiết bị đầu cuối, chuỗi thao tác tương ứng với thông tin vân tay thứ nhất, và phép tương ứng giữa mật khẩu ứng dụng và thông tin vân tay thứ nhất, trong đó mật khẩu ứng dụng được sử dụng để truy nhập ứng dụng đích, và chuỗi thao tác gồm mở khóa thiết bị đầu cuối và truy nhập ứng dụng đích; bộ cảm biến vân tay, được tạo cấu hình để nhận thông tin vân tay thứ hai đầu vào; bộ truyền, được tạo cấu hình để gửi thông điệp kiểm chứng vân tay thành công đến máy chủ ứng dụng, trong đó thông điệp kiểm chứng vân tay thành công chỉ báo rằng mức độ so khớp giữa thông tin vân tay thứ hai và thông tin vân tay thứ nhất vượt quá ngưỡng định trước; bộ tiếp nhận, được tạo cấu hình để nhận thông điệp báo nhận được gửi bởi máy chủ ứng dụng; và màn hình cảm ứng, được tạo cấu hình để đáp ứng

thông điệp báo nhận, hoặc theo chỉ báo đáp ứng thông điệp báo nhận và được gửi bởi bộ xử lý, nhảy từ giao diện khóa màn hình sang giao diện được hiển thị sau khi ứng dụng đích được truy nhập.

Trên thiết bị đầu cuối, người dùng nhập vào thông tin vân tay chỉ một lần và không cần nhập vào mật khẩu ứng dụng, để truy nhập ngay ứng dụng đích that được thiết lập bằng mật khẩu ứng dụng khi ứng dụng đích không bắt đầu chạy. Điều này đơn giản hóa thao tác người dùng và cải thiện trải nghiệm người dùng trong khi đảm bảo bảo mật.

Theo thiết bị đầu cuối theo khía cạnh thứ tư, phương án thực hiện sáng chế còn đề xuất các triển khai sau, và các triển khai này có thể được sử dụng cùng nhau để đạt được hiệu quả kỹ thuật tốt hơn.

Theo triển khai, bộ cảm biến vân tay tiếp nhận thông tin vân tay thứ hai đầu vào khi ứng dụng đích không bắt đầu chạy.

Theo triển khai khác, ứng dụng đích gồm chức năng đích, chức năng đích được thiết lập bằng mật khẩu chức năng được sử dụng để truy nhập chức năng đích, chuỗi thao tác còn gồm truy nhập chức năng đích, và “giao diện được hiển thị sau khi ứng dụng đích được truy nhập” là giao diện được hiển thị sau khi chức năng đích của ứng dụng đích được truy nhập.

Theo triển khai khác, bộ truyền còn được tạo cấu hình để gửi khóa được gắn với thông tin vân tay thứ nhất đến máy chủ ứng dụng.

Mô tả vắn tắt các hình vẽ

Để mô tả rõ ràng hơn các giải pháp kỹ thuật theo các phương án thực hiện sáng chế, phần sau mô tả vắn tắt các hình vẽ đi kèm cần để mô tả các phương án thực hiện. Rõ ràng là, các hình vẽ đi kèm trong phần mô tả sau chỉ thể hiện một số phương án thực hiện sáng chế, và người có kiến thức trung bình trong lĩnh vực có thể vẫn suy ra các hình vẽ khác từ các hình vẽ đi kèm này mà không cần nỗ lực sáng tạo.

Fig.1A và Fig.1B là sơ đồ của phương pháp truy nhập chức năng đích của ứng dụng đích theo giải pháp kỹ thuật đã biết;

Fig.2 là phần đăng ký vân tay theo phương án thực hiện sáng chế;

Fig.3 là lưu đồ ủy nhiệm vân tay theo phương án thực hiện sáng chế;

Fig.4 là lưu đồ của phương pháp truy nhập ứng dụng đích theo phương án thực hiện sáng chế;

Fig.5 là sơ đồ của phương pháp truy nhập chức năng đích của ứng dụng đích theo phương án thực hiện sáng chế; và

Fig.6 là sơ đồ cấu trúc của thiết bị đầu cuối theo phương án thực hiện sáng chế.

Mô tả chi tiết sáng chế

Để khiến các mục đích, các giải pháp kỹ thuật, và các ưu điểm của sáng chế rõ ràng hơn, phần sau còn mô tả chi tiết các phương án thực hiện sáng chế dựa vào các hình vẽ đi kèm.

Như được thể hiện trên Fig.1A và Fig.1B, đối với điện thoại di động được thiết lập bằng cả mật khẩu khóa màn hình lẫn mật khẩu ứng dụng, khi điện thoại di động ở trạng thái khóa màn hình, nếu người dùng muốn khởi động ứng dụng đích được thiết lập bằng mật khẩu ứng dụng, người dùng cần trước hết nhập vào mật khẩu khóa màn hình, đợi cho đến khi màn hình điện thoại di động được mở khóa, tìm thấy ứng dụng đích, và sau đó nhập vào mật khẩu ứng dụng. Các hoạt động tương đối rối rắm. Nếu chức năng đích mà người dùng muốn sử dụng trong ứng dụng đích cũng được thiết lập bằng mật khẩu chức năng, người dùng còn cần nhập vào mật khẩu chức năng. Có thể biết rằng, từ việc mở khóa màn hình đến việc sử dụng chức năng đích, người dùng cần nhập vào mật khẩu tổng cộng ba lần và việc kiểm chứng được thực hiện ba lần. Các hoạt động không chỉ khá rối rắm, mà còn mất nhiều thời gian.

Bằng độc quyền Trung Quốc số CN104182275A bộc lộ rằng, khi người dùng cần nhanh chóng khởi động ứng dụng cụ thể, thiết bị đầu cuối có thể thu thập thông tin vân tay của người dùng, sau đó tìm kiếm ứng dụng được liên kết với thông tin vân tay thu được, và trực tiếp khởi động ứng dụng sau khi tìm thấy ứng dụng được liên kết với thông tin vân tay thu được.

Tuy nhiên, đối với ứng dụng được thiết lập bằng mật khẩu ứng dụng, khi phương pháp nêu trên được sử dụng, sau khi ứng dụng được liên kết với thông

tin vân tay thu được được tìm thấy, ứng dụng không thể được trực tiếp khởi động, và người dùng có thể chỉ ở nguyên trong giao diện khóa màn hình hoặc giao diện nhập vào mật khẩu ứng dụng. Người dùng trước hết cần nhập bằng tay mật khẩu và sau đó khởi động ứng dụng sau khi kiểm chứng mật khẩu thành công. Điều này không nhanh và đủ tiện dụng.

Phương án thực hiện sáng chế đề xuất phương pháp truy nhập ứng dụng đích, sao cho người dùng có thể nhanh chóng truy nhập ứng dụng đích được thiết lập bằng mật khẩu ứng dụng bằng cách nhập vào thông tin vân tay chỉ một lần. Khi sử dụng phương pháp để truy nhập ứng dụng đích, người dùng trước hết cần đăng ký vân tay trên thiết bị đầu cuối. Fig.2 là phần đăng ký vân tay theo phương án thực hiện sáng chế.

Như được thể hiện trên Fig.2, giả sử rằng ba vân tay được ghi nhận trên thiết bị đầu cuối: vân tay A, vân tay B, và vân tay C, và thiết bị đầu cuối ghi nhận chuỗi thao tác được đăng ký cho (hoặc tương ứng với) mỗi vân tay. Trên Fig.2, chuỗi thao tác được đăng ký cho vân tay A gồm mở khóa màn hình, chuỗi thao tác được đăng ký cho vân tay B gồm mở khóa màn hình và truy nhập ứng dụng X, và chuỗi thao tác được đăng ký cho vân tay C gồm mở khóa màn hình, truy nhập ứng dụng X, và truy nhập chức năng Y của ứng dụng X. Chuỗi thao tác ở đây đề cập đến một hoặc nhiều hoạt động được thực hiện theo thứ tự. Chẳng hạn, khi thiết bị đầu cuối dò thấy rằng thông tin vân tay được nhập vào, trong đó mức độ so khớp giữa thông tin vân tay và vân tay B vượt quá ngưỡng định trước, thiết bị đầu cuối mở khóa màn hình và sau đó truy nhập ứng dụng X. Lưu ý rằng, khi thiết bị đầu cuối dò thấy, trong quá trình thực hiện chuỗi thao tác, rằng hoạt động đã được thực hiện xong, thiết bị đầu cuối bỏ qua hoạt động này và tiếp tục thực hiện hoạt động tiếp theo. Chẳng hạn, khi thiết bị đầu cuối ở trạng thái mở khóa dò thấy rằng thông tin vân tay được nhập vào, trong đó mức độ so khớp giữa thông tin vân tay và vân tay B vượt quá ngưỡng định trước, thiết bị đầu cuối bỏ qua hoạt động mở khóa màn hình, và trực tiếp truy nhập ứng dụng X. Khi thực hiện mỗi hoạt động trong chuỗi thao tác, thiết bị đầu cuối gọi API liên quan (application programming interface – giao diện lập trình ứng dụng). Chẳng hạn, khi thiết bị đầu cuối ở trạng thái

mở khóa dò thấy rằng thông tin vân tay được nhập vào, trong đó mức độ so khớp giữa thông tin vân tay và vân tay C vượt quá ngưỡng định trước, thiết bị đầu cuối trước hết gọi API_1 để mở khóa màn hình, sau đó gọi API_2 để truy nhập ứng dụng X, và cuối cùng gọi API_3 truy nhập chức năng Y của ứng dụng X. Fig.2 được sử dụng chỉ làm ví dụ. Khi chuyên gia trong lĩnh vực triển khai phương án thực hiện sáng chế, thiết bị đầu cuối có thể sử dụng dạng bất kỳ để đăng ký chuỗi thao tác tương ứng với vân tay cụ thể. Thiết bị đầu cuối cũng có thể nhận bản ghi vân tay mới, và sau đó đăng ký ngay chuỗi thao tác cho vân tay mới.

Sau khi hoàn thành đăng ký vân tay, thiết bị đầu cuối còn cần ủy nhiệm vân tay. Fig.3 là lưu đồ ủy nhiệm vân tay sử dụng vân tay C trên Fig.2 làm ví dụ theo phương án thực hiện sáng chế. Sau khi hoàn thành đăng ký chuỗi thao tác tương ứng với vân tay C, do chuỗi thao tác được đăng ký cho vân tay C gồm mở khóa màn hình, truy nhập ứng dụng X, và truy nhập chức năng Y của ứng dụng X, thiết bị đầu cuối ủy nhiệm vân tay C, tức là, thiết bị đầu cuối liên kết mật khẩu ứng dụng của ứng dụng X và mật khẩu chức năng của chức năng Y với vân tay C. Như được thể hiện trên Fig.3, khi vân tay C đang được ủy nhiệm, thiết bị đầu cuối trước hết thực hiện kiểm chứng trên mật khẩu mở khóa màn hình. Thiết bị đầu cuối tiếp nhận mật khẩu mở khóa được nhập vào (như được thể hiện trên 301), và khi thiết bị đầu cuối xác định rằng mật khẩu mở khóa được nhập vào so khớp mật khẩu mở khóa định trước, báo nhận rằng kiểm chứng thành công (như được thể hiện trên 302), và sau đó thiết bị đầu cuối thiết lập phép tương ứng giữa vân tay C và mật khẩu mở khóa trong cơ sở dữ liệu (như được thể hiện trên 303). Nếu kiểm chứng thất bại, thiết bị đầu cuối ở lại trong giao diện đợi nhập vào mật khẩu mở khóa (không được thể hiện trên hình vẽ).

Thiết bị đầu cuối còn tiếp nhận mật khẩu ứng dụng đầu vào (như được thể hiện trên 304). Sau khi tiếp nhận mật khẩu ứng dụng đầu vào, thiết bị đầu cuối gửi ứng dụng nhận được mật khẩu đến máy chủ ứng dụng (như được thể hiện trên 305). Máy chủ ứng dụng thực hiện kiểm chứng trên ứng dụng nhận được mật khẩu, và khi kiểm chứng thành công, máy chủ ứng dụng gửi kết quả kiểm

chúng đến thiết bị đầu cuối (như được thể hiện trên 306), và sau đó thiết bị đầu cuối thiết lập phép tương ứng giữa vân tay C và mật khẩu ứng dụng trong cơ sở dữ liệu (như được thể hiện trên 307). Nếu kiểm chứng không được, thiết bị đầu cuối nằm trong giao diện đợi nhập vào mật khẩu ứng dụng (không được thể hiện trong hình vẽ).

Ngược lại, do thông tin về vân tay C được lưu lại trong môi trường thực thi đáng tin cậy (Trusted Execution Environment – TEE) của thiết bị đầu cuối, vì lý do bảo mật thông tin vân tay, thiết bị đầu cuối không gửi thông tin về vân tay C đến máy chủ ứng dụng, nhưng tạo khóa, gắn khóa với vân tay C, và sau đó gửi khóa đến máy chủ ứng dụng. Máy chủ ứng dụng lưu lại khóa làm thẻ của vân tay C để đánh dấu vân tay C. Các bước này có thể được thực hiện trước khi, sau khi, hoặc khi thiết bị đầu cuối thiết lập phép tương ứng giữa vân tay C và mật khẩu ứng dụng (không được thể hiện trong hình vẽ).

Thiết bị đầu cuối còn tiếp nhận mật khẩu chức năng đầu vào (như được thể hiện trên 308), và thực hiện các bước (như được thể hiện trên 309 và 310) giống như các bước được thực hiện sau khi thiết bị đầu cuối tiếp nhận mật khẩu ứng dụng đầu vào, để thiết lập phép tương ứng giữa vân tay C và mật khẩu chức năng (như được thể hiện trên 311).

Trên Fig.3, nếu vân tay C đã được thiết lập làm mật khẩu mở khóa màn hình trước khi kiểm chứng vân tay, bước kiểm chứng mật khẩu mở khóa màn hình có thể bị bỏ qua, và kiểm chứng có thể được thực hiện trên mật khẩu ứng dụng và mật khẩu chức năng. Nếu trước khi ủy nhiệm vân tay được thực hiện cho vân tay C, ít nhất một trong mật khẩu ứng dụng hoặc mật khẩu chức năng đã được thiết lập làm vân tay C, tức là, thiết bị đầu cuối được thiết lập để truy nhập ứng dụng X và/hoặc chức năng Y của ứng dụng X khi xác định rằng mức độ so khớp giữa thông tin vân tay đầu vào và thông tin về vân tay C vượt quá ngưỡng định trước, có thể xem xét rằng phép tương ứng giữa mật khẩu ứng dụng và/hoặc mật khẩu chức năng và vân tay C đã được thiết lập. Thiết bị đầu cuối có thể bỏ qua pha kiểm chứng của mật khẩu ứng dụng và/hoặc mật khẩu chức năng để cải thiện hiệu suất, hoặc thiết bị đầu cuối có thể không bỏ qua pha kiểm chứng để tăng cường bảo mật. Nếu trước khi ủy nhiệm vân tay được

thực hiện cho vân tay C, ít nhất một trong mật khẩu ứng dụng hoặc mật khẩu chức năng đã được thiết lập làm vân tay khác chẳng hạn vân tay B, khi thực hiện ủy nhiệm vân tay cho vân tay C, thiết bị đầu cuối có thể xóa thông tin về liên kết giữa vân tay B và mật khẩu ứng dụng hoặc mật khẩu chức năng. Nếu ứng dụng X không được thiết lập bằng mật khẩu ứng dụng hoặc chức năng Y không được thiết lập bằng mật khẩu chức năng, thiết bị đầu cuối thiết lập chỉ phép tương ứng giữa mật khẩu ứng dụng hoặc mật khẩu chức năng và vân tay C. Ngoài ra, khi ủy nhiệm vân tay, thiết bị đầu cuối có thể trước hết kiểm chứng vân tay một lần để đảm bảo bảo mật.

Fig.4 là lưu đồ của phương pháp truy nhập ứng dụng đích sử dụng vân tay C trên Fig.2 làm ví dụ. Sau khi hoàn thành ủy nhiệm vân tay, thiết bị đầu cuối có thể nhanh chóng truy nhập ứng dụng đích bằng cách nhập vào thông tin vân tay một lần. Trước khi truy nhập ứng dụng đích, thiết bị đầu cuối có thể ở trạng thái khóa màn hình hoặc ở trạng thái mở khóa. Khi thiết bị đầu cuối ở trạng thái mở khóa, thiết bị đầu cuối có thể hiển thị giao diện bất kỳ. Khi thiết bị đầu cuối dò thấy rằng thông tin vân tay được nhập vào (như được thể hiện trên 401), thiết bị đầu cuối thực hiện kiểm chứng trên thông tin vân tay đầu vào. Khi thiết bị đầu cuối xác định rằng thành công kiểm chứng vân tay (như được thể hiện trên 402), tức là, mức độ so khớp giữa thông tin vân tay đầu vào và vân tay bất kỳ (Chẳng hạn, vân tay A, vân tay B, hoặc vân tay C) được đăng ký trước trong thiết bị đầu cuối vượt quá ngưỡng định trước, thiết bị đầu cuối tìm kiếm chuỗi thao tác tương ứng với vân tay so khớp. Dựa vào Fig.2 để mô tả, nếu vân tay so khớp là vân tay C, chuỗi thao tác tương ứng với vân tay C và được tìm thấy bởi thiết bị đầu cuối gồm mở khóa màn hình, truy nhập ứng dụng X, và truy nhập chức năng Y của ứng dụng X (như được thể hiện trên 403), và sau đó thiết bị đầu cuối xác định liệu phép tương ứng giữa vân tay C và mật khẩu mở khóa được lưu trữ. Nếu phép tương ứng giữa vân tay C và mật khẩu mở khóa được lưu trữ (như được thể hiện trên 404), thiết bị đầu cuối không còn tiếp nhận và kiểm chứng mật khẩu mở khóa, nhưng sử dụng kết quả kiểm chứng của vân tay C để thay thế kiểm chứng mật khẩu mở khóa.

Thiết bị đầu cuối còn xác định liệu phép tương ứng giữa vân tay C và mật

khẩu ứng dụng của ứng dụng X được lưu trữ. Nếu phép tương ứng giữa vân tay C và mật khẩu ứng dụng của ứng dụng X được lưu trữ (như được thể hiện trên 405), thiết bị đầu cuối gửi thông điệp yêu cầu xác thực thứ nhất đến máy chủ ứng dụng (như được thể hiện trên 406). Sau khi tiếp nhận thông điệp yêu cầu xác thực, máy chủ ứng dụng gửi thông điệp giao dịch thứ nhất đến thiết bị đầu cuối (như được thể hiện trên 407). Một cách tùy chọn, thông điệp giao dịch thứ nhất được gửi đến TA (Trusted Application - ứng dụng tin cậy, và TA và ứng dụng X có thể được cung cấp bởi cùng nhà cung cấp) trong TEE của thiết bị đầu cuối. Sau khi TA xác định rằng thành công kiểm chứng vân tay, thiết bị đầu cuối gửi vân tay kết quả kiểm chứng và khóa được gắn với vân tay C đến máy chủ ứng dụng (như được thể hiện trên 408). Máy chủ ứng dụng so sánh khóa nhận được với khóa được lưu trữ trước đó. Nếu khóa nhận được nhất quán với khóa được lưu trữ trước đó, máy chủ ứng dụng gửi, đến thiết bị đầu cuối theo vân tay kết quả kiểm chứng được nhận, thông điệp báo nhận thứ nhất chỉ báo rằng việc kiểm chứng của mật khẩu ứng dụng thành công (như được thể hiện trên 409).

Theo phương án thực hiện sáng chế, thiết bị đầu cuối không hiển thị giao diện nhập mật khẩu ứng dụng, và máy chủ ứng dụng không kiểm chứng mật khẩu ứng dụng, mà sử dụng vân tay kết quả kiểm chứng ở bước 402 để thay thế kết quả kiểm chứng của mật khẩu ứng dụng. Nếu thành công kiểm chứng vân tay ở 402, máy chủ ứng dụng trực tiếp gửi, đến thiết bị đầu cuối, thông điệp báo nhận thứ nhất chỉ báo rằng việc kiểm chứng mật khẩu ứng dụng thành công.

Thiết bị đầu cuối còn xác định liệu phép tương ứng giữa vân tay C và mật khẩu chức năng của chức năng Y được lưu trữ. Nếu phép tương ứng giữa vân tay C và mật khẩu chức năng của chức năng Y được lưu trữ (như được thể hiện trên 410), thiết bị đầu cuối và máy chủ ứng dụng thực hiện riêng rẽ các bước tương tự từ 406 đến 409 (như được thể hiện trên 411 đến 414), và cuối cùng, máy chủ ứng dụng gửi, đến thiết bị đầu cuối theo vân tay kết quả kiểm chứng nhận được, thông điệp báo nhận thứ hai chỉ báo rằng việc kiểm chứng của mật khẩu chức năng thành công (như được thể hiện trên 414).

Sau khi tiếp nhận thông điệp báo nhận chỉ báo rằng việc kiểm chứng mật khẩu chức năng thành công, thiết bị đầu cuối gọi API_1, API_2, và API_4 sau đó để thực hiện các hoạt động mở khóa màn hình, truy nhập ứng dụng X, và truy nhập chức năng Y của ứng dụng X. Nên lưu ý rằng, “mở khóa màn hình”, “truy nhập ứng dụng X”, và “truy nhập chức năng Y của ứng dụng X” được thực hiện liên tục. Đối với phương án thực hiện sáng chế, giao diện được hiển thị sau khi chức năng Y được truy nhập thường là giao diện thứ nhất được hiển thị sau khi thiết bị đầu cuối được mở khóa. Theo cách khác, sau khi thiết bị đầu cuối được mở khóa, thiết bị đầu cuối có thể vẫn hiển thị giao diện hệ thống (cũng có thể được gọi là giao diện chính hoặc màn hình trang chủ) và giao diện tải của ứng dụng X trong thời gian ngắn, và sau đó hiển thị giao diện được hiển thị sau khi chức năng Y được truy nhập. “Giao diện truy nhập ứng dụng X” có thể là giao diện chính hoặc màn hình chủ của ứng dụng X, hoặc có thể là giao diện của chức năng bất kỳ trong ứng dụng X. “Giao diện được hiển thị sau khi chức năng Y được truy nhập” có thể là giao diện chính hoặc màn hình chủ của chức năng Y, hoặc có thể là giao diện của chức năng phụ bất kỳ trong chức năng Y.

Theo phương án thực hiện, sau khi thiết bị đầu cuối tìm thấy chuỗi thao tác tương ứng với vân tay so khớp, nếu tìm thấy rằng ít nhất một hoạt động trong chuỗi thao tác đã được thực hiện, thiết bị đầu cuối bỏ qua hoạt động đã được thực hiện, và sau đó đến lượt, thực hiện hoạt động mà đã không được thực hiện. Vân tay C vẫn được sử dụng làm ví dụ. Sau khi thiết bị đầu cuối tiếp nhận thông điệp báo nhận chỉ báo rằng kiểm chứng mật khẩu chức năng thành công, nếu đã thấy rằng thiết bị đầu cuối được mở khóa và truy nhập ứng dụng X, thiết bị đầu cuối nhảy từ giao diện của ứng dụng X sang giao diện được hiển thị sau khi chức năng Y được truy nhập. Nếu ứng dụng X không được thiết lập bằng mật khẩu ứng dụng hoặc chức năng Y không được thiết lập bằng mật khẩu chức năng, theo phương án thực hiện, thiết bị đầu cuối gửi thông điệp yêu cầu xác thực chỉ một lần cho mật khẩu ứng dụng hoặc mật khẩu chức năng.

Fig.5 là sơ đồ của phương pháp truy nhập chức năng đích của ứng dụng đích theo phương án thực hiện sáng chế. Như được thể hiện trên Fig.5, so với

phương pháp trên Fig.1A và Fig.1B, sử dụng phương pháp truy nhập ứng dụng đích theo phương án thực hiện sáng chế có thể cho phép người dùng truy nhập nhanh chóng chức năng đích bằng cách nhập vào thông tin vân tay ngay khi thiết bị đầu cuối ở trạng thái khóa màn hình. Điều này cải thiện đáng kể trải nghiệm người dùng khi bảo mật được đảm bảo. Rõ ràng là, người dùng cũng có thể nhanh chóng truy nhập ứng dụng đích hoặc chức năng đích bằng cách nhập vào thông tin vân tay ngay khi thiết bị đầu cuối ở trạng thái mở khóa hiển thị giao diện bất kỳ. Điều này không bị giới hạn ở ví dụ trên Fig.5.

Fig.6 thể hiện thiết bị 60 truy nhập ứng dụng đích theo phương án thực hiện sáng chế, gồm:

bộ cảm biến vân tay 61; ít nhất một bộ nhớ 62, được tạo cấu hình để lưu trữ ứng dụng đích, thông tin vân tay thứ nhất được sử dụng để mở khóa thiết bị đầu cuối, và chuỗi thao tác tương ứng với thông tin vân tay thứ nhất, trong đó ứng dụng đích được thiết lập bằng mật khẩu ứng dụng được sử dụng để truy nhập ứng dụng đích, và chuỗi thao tác gồm mở khóa thiết bị đầu cuối và truy nhập ứng dụng đích; màn hình cảm ứng 63, được tạo cấu hình để nhận mật khẩu ứng dụng đầu vào; bộ truyền 64, được tạo cấu hình để gửi, đến máy chủ ứng dụng, thông điệp thứ nhất mà mang mật khẩu ứng dụng; bộ tiếp nhận 65, được tạo cấu hình để nhận thông điệp thứ hai mà chỉ báo rằng việc kiểm chứng của mật khẩu ứng dụng thành công và được gửi bởi máy chủ ứng dụng; và ít nhất một bộ xử lý 66, được tạo cấu hình để: thiết lập phép tương ứng giữa mật khẩu ứng dụng và thông tin vân tay thứ nhất dựa trên thông điệp thứ hai, và thực hiện chuỗi thao tác dựa trên phép tương ứng giữa mật khẩu ứng dụng và thông tin vân tay thứ nhất khi mức độ so khớp giữa thông tin vân tay thứ hai được dò bởi bộ cảm biến vân tay và thông tin vân tay thứ nhất vượt quá ngưỡng định trước.

Nên hiểu rằng, thiết bị đầu cuối theo phương án thực hiện sáng chế có thể được tạo cấu hình để triển khai phương pháp nêu trên theo các phương án thực hiện. Chẳng hạn, màn hình cảm ứng được tạo cấu hình để nhận mật khẩu ứng dụng đầu vào hoặc mật khẩu chức năng, bộ cảm biến vân tay được tạo cấu hình để nhận thông tin vân tay đầu vào, bộ truyền và bộ tiếp nhận được tạo cấu hình để trao đổi thông tin với máy chủ ứng dụng, bộ nhớ được tạo cấu hình để lưu

trữ thông tin vân tay, phép tương ứng giữa thông tin vân tay và mật khẩu ứng dụng và/hoặc mật khẩu chức năng, và chuỗi thao tác tương ứng với thông tin vân tay, và bộ xử lý được tạo cấu hình để: gửi lệnh đến linh kiện khác, và thực hiện các hoạt động xử lý khác nhau. Các phần mô tả của các ví dụ khác nhau và các giải pháp tùy chọn ở phương pháp nêu trên theo các phương án thực hiện có thể áp dụng cho thiết bị đầu cuối theo phương án thực hiện sáng chế.

Nên hiểu rằng theo tất cả các phương án thực hiện nêu trên của sáng chế, bộ xử lý có thể là khối xử lý trung tâm (Central Processing Unit – CPU), hoặc bộ xử lý có thể là bộ xử lý đa năng khác, bộ xử lý tín hiệu số (digital signal processor – DSP), ASIC (mạch tích hợp ứng dụng cụ thể), mảng cổng lập trình được dạng trường (field programmable gate array – FPGA), hoặc thiết bị logic lập trình được khác, cổng rời rạc hoặc thiết bị logic tranzito, linh kiện phần cứng rời rạc, hoặc tương tự. Bộ xử lý đa năng có thể là bộ vi xử lý hoặc bộ xử lý có thể là bộ xử lý thông thường bất kỳ, hoặc tương tự.

Bộ nhớ có thể gồm bộ nhớ chỉ đọc (read-only memory – ROM) và bộ nhớ truy nhập ngẫu nhiên (random access memory – RAM), lưu trữ mã chương trình, và cấp lệnh và dữ liệu cho bộ xử lý.

Đường truyền thông có thể còn bao gồm đường truyền điện, đường truyền điều khiển, đường truyền tín hiệu trạng thái, và tương tự, bên cạnh đường truyền dữ liệu. Tuy nhiên, để mô tả rõ ràng, các loại đường truyền khác nhau trên hình vẽ được đánh dấu làm đường truyền truyền thông.

Theo quá trình triển khai, các bước ở các phương pháp nêu trên có thể được triển khai bằng cách sử dụng mạch logic tích hợp phần cứng trong bộ xử lý, hoặc bằng cách sử dụng các lệnh ở dạng phần mềm. Các bước của phương pháp được bộc lộ dựa vào các phương án thực hiện sáng chế có thể được thực hiện trực tiếp bởi bộ xử lý phần cứng, hoặc có thể được thực hiện bằng cách sử dụng tổ hợp phần cứng trong bộ xử lý và môđun phần mềm. Môđun phần mềm có thể được đặt trong vật lưu trữ theo giải pháp kỹ thuật đã biết, chẳng hạn RAM, bộ nhớ nhanh, ROM, ROM lập trình được, bộ nhớ lập trình được xóa được bằng điện, thanh ghi, hoặc tương tự. Vật lưu trữ được đặt trong bộ nhớ, và bộ xử lý đọc thông tin trong bộ nhớ và hoàn thành các bước trong các

phương pháp nêu trên cùng với phần cứng của bộ xử lý. Để tránh lặp lại, các chi tiết không được mô tả lại ở đây.

Người có hiểu biết trung bình trong lĩnh vực có thể hiểu rằng, để mô tả dễ và ngắn gọn, đối với quá trình làm việc chi tiết của hệ thống, thiết bị, và khối nêu trên, tham khảo quá trình tương ứng ở phương pháp nêu trên theo các phương án thực hiện, và các chi tiết không được mô tả lại ở đây.

YÊU CẦU BẢO HỘ

1. Phương pháp truy nhập ứng dụng mục tiêu bao gồm các bước:

nhận, bằng thiết bị đầu cuối, mật khẩu ứng dụng, trong đó ứng dụng mục tiêu được cài đặt trên thiết bị đầu cuối được thiết lập với mật khẩu ứng dụng để truy nhập ứng dụng mục tiêu, trong đó thiết bị đầu cuối được thiết lập với thông tin vân tay thứ nhất để mở khóa thiết bị đầu cuối và chuỗi hoạt động tương ứng với thông tin vân tay thứ nhất, và trong đó chuỗi hoạt động bao gồm mở khóa thiết bị đầu cuối và truy nhập ứng dụng mục tiêu;

gửi, bằng thiết bị đầu cuối đến máy chủ ứng dụng, thông điệp thứ nhất mang mật khẩu ứng dụng;

nhận, bằng thiết bị đầu cuối, thông điệp thứ hai từ máy chủ ứng dụng chỉ báo rằng kiểm chứng mật khẩu ứng dụng thành công;

thiết lập và lưu trữ, bằng thiết bị đầu cuối, phép tương ứng giữa mật khẩu ứng dụng và thông tin vân tay thứ nhất dựa trên thông điệp thứ hai;

nhận, bằng thiết bị đầu cuối, thông tin vân tay thứ hai;

so sánh, bằng thiết bị đầu cuối, thông tin vân tay thứ nhất và thông tin vân tay thứ hai để xác định mức độ so khớp; và

thực hiện, bằng thiết bị đầu cuối, chuỗi hoạt động dựa trên phép tương ứng giữa mật khẩu ứng dụng và thông tin vân tay thứ nhất khi mức độ so khớp giữa thông tin vân tay thứ hai và thông tin vân tay thứ nhất vượt quá ngưỡng định trước.

2. Phương pháp theo điểm 1, trong đó việc thực hiện chuỗi hoạt động bao gồm các bước:

mở khóa, bằng thiết bị đầu cuối, thiết bị đầu cuối;

gửi, bằng thiết bị đầu cuối đến máy chủ ứng dụng dựa trên phép tương ứng giữa mật khẩu ứng dụng và thông tin vân tay thứ nhất, thông điệp thứ ba chỉ báo rằng mức độ so khớp giữa thông tin vân tay thứ hai và thông tin vân tay thứ nhất vượt quá ngưỡng định trước;

nhận, bằng thiết bị đầu cuối, thông điệp thứ tư từ máy chủ ứng dụng chỉ báo rằng báo nhận xác thực thành công; và

truy nhập, bằng thiết bị đầu cuối, ứng dụng mục tiêu theo thông điệp thứ tư.

3. Phương pháp theo điểm 1, trong đó ứng dụng mục tiêu bao gồm chức năng mục tiêu, trong đó chức năng mục tiêu được thiết lập với mật khẩu chức năng để truy nhập chức năng mục tiêu, trong đó chuỗi hoạt động còn bao gồm truy nhập chức năng mục tiêu, và trong đó sau khi thiết lập phép tương ứng giữa mật khẩu ứng dụng và thông tin vân tay thứ nhất, phương pháp còn bao gồm các bước:

nhận, bằng thiết bị đầu cuối, mật khẩu chức năng;

gửi, bằng thiết bị đầu cuối đến máy chủ ứng dụng, thông điệp thứ năm mang mật khẩu chức năng;

nhận, bằng thiết bị đầu cuối, thông điệp thứ sáu từ máy chủ ứng dụng chỉ báo rằng kiểm chứng mật khẩu chức năng thành công; và

thiết lập, bằng thiết bị đầu cuối, phép tương ứng giữa mật khẩu chức năng và thông tin vân tay thứ nhất dựa trên thông điệp thứ sáu.

4. Phương pháp theo điểm 3, trong đó việc thực hiện chuỗi hoạt động bao gồm các bước:

mở khóa, bằng thiết bị đầu cuối, thiết bị đầu cuối;

gửi, bằng thiết bị đầu cuối đến máy chủ ứng dụng dựa trên phép tương ứng giữa mật khẩu ứng dụng và thông tin vân tay thứ nhất, thông điệp thứ ba chỉ báo rằng mức độ so khớp giữa thông tin vân tay thứ hai và thông tin vân tay thứ nhất vượt quá ngưỡng định trước;

nhận, bằng thiết bị đầu cuối từ máy chủ ứng dụng, thông điệp thứ tư chỉ báo rằng báo nhận xác thực thành công;

truy nhập, bằng thiết bị đầu cuối, ứng dụng mục tiêu theo thông điệp thứ tư;

gửi, bằng thiết bị đầu cuối đến máy chủ ứng dụng dựa trên phép tương ứng giữa mật khẩu chức năng và thông tin vân tay thứ nhất, thông điệp thứ bảy chỉ báo rằng mức độ so khớp giữa thông tin vân tay thứ hai và thông tin vân tay

thứ nhất vượt quá ngưỡng định trước;

nhận, bằng thiết bị đầu cuối, thông điệp thứ tám từ máy chủ ứng dụng chỉ báo rằng báo nhận xác thực thành công; và

truy nhập, bằng thiết bị đầu cuối, chức năng mục tiêu theo thông điệp thứ tám.

5. Phương pháp theo điểm bất kỳ trong số các điểm từ 1 đến 4, trong đó phương pháp còn bao gồm bước bỏ qua, bằng thiết bị đầu cuối bước mở khóa thiết bị đầu cuối trong quá trình thực hiện chuỗi hoạt động khi thiết bị đầu cuối ở trạng thái được mở khóa trước khi bắt đầu thực hiện chuỗi hoạt động.

6. Phương pháp theo điểm bất kỳ trong số các điểm từ 1 đến 5, trước khi thiết lập phép tương ứng giữa mật khẩu ứng dụng và thông tin vân tay thứ nhất, phương pháp còn bao gồm các bước:

tạo, bằng thiết bị đầu cuối, khóa;

kết nối, bằng thiết bị đầu cuối, khóa với thông tin vân tay thứ nhất; và

gửi, bằng thiết bị đầu cuối đến máy chủ ứng dụng, thông điệp thứ chín mang khóa.

7. Phương pháp theo điểm 1, trong đó phương pháp còn bao gồm bước xác định, bằng thiết bị đầu cuối, không thực hiện bước mở khóa thiết bị đầu cuối trong quá trình thực hiện chuỗi hoạt động khi thiết bị đầu cuối ở trạng thái được mở khóa trước khi bắt đầu thực hiện chuỗi hoạt động.

8. Phương pháp truy nhập ứng dụng mục tiêu bao gồm các bước:

nhận, bằng thiết bị đầu cuối, thông tin vân tay thứ hai trong đó ứng dụng mục tiêu được cài đặt trên thiết bị đầu cuối và được thiết lập với mật khẩu ứng dụng để truy nhập ứng dụng mục tiêu, trong đó thiết bị đầu cuối được thiết lập với thông tin vân tay thứ nhất để mở khóa thiết bị đầu cuối và chuỗi hoạt động tương ứng với thông tin vân tay thứ nhất, trong đó chuỗi hoạt động bao gồm mở khóa thiết bị đầu cuối và truy nhập ứng dụng mục tiêu, và trong đó thiết bị

đầu cuối còn được thiết lập với phép tương ứng giữa mật khẩu ứng dụng và thông tin vân tay thứ nhất;

gửi, bằng thiết bị đầu cuối, thông điệp kiểm chứng vân tay thành công đến máy chủ ứng dụng, trong đó thông điệp kiểm chứng vân tay thành công chỉ báo rằng mức độ so khớp giữa thông tin vân tay thứ hai và thông tin vân tay thứ nhất vượt quá ngưỡng định trước;

nhận, bằng thiết bị đầu cuối, thông điệp báo nhận từ máy chủ ứng dụng; và

đáp lại, bằng thiết bị đầu cuối, thông điệp báo nhận, và

chuyển đổi, bằng thiết bị đầu cuối, từ giao diện khóa màn hình sang giao diện được hiển thị sau khi ứng dụng mục tiêu được truy nhập.

9. Phương pháp theo điểm 8, trong đó ứng dụng mục tiêu bao gồm chức năng mục tiêu, trong đó chức năng mục tiêu được thiết lập với mật khẩu chức năng để truy nhập chức năng mục tiêu, trong đó chuỗi hoạt động còn bao gồm truy nhập chức năng mục tiêu, và trong đó giao diện được hiển thị sau khi ứng dụng mục tiêu được truy nhập bao gồm giao diện được hiển thị sau khi chức năng mục tiêu được truy nhập.

10. Phương pháp theo điểm 8 hoặc 9, trong đó trước khi nhận thông tin vân tay thứ hai, phương pháp còn bao gồm bước:

gửi khóa được kết nối với thông tin vân tay thứ nhất đến máy chủ ứng dụng.

11. Thiết bị đầu cuối bao gồm:

bộ cảm biến vân tay;

ít nhất một bộ nhớ, được tạo cấu hình để lưu trữ ứng dụng mục tiêu, trong đó thông tin vân tay thứ nhất mở khóa thiết bị đầu cuối, trong đó chuỗi hoạt động tương ứng với thông tin vân tay thứ nhất, trong đó ứng dụng mục tiêu được thiết lập với mật khẩu ứng dụng để truy nhập ứng dụng mục tiêu, và trong đó chuỗi hoạt động bao gồm mở khóa thiết bị đầu cuối và truy nhập ứng dụng

mục tiêu;

màn hình cảm ứng, được tạo cấu hình để nhận mật khẩu ứng dụng;

bộ truyền, được tạo cấu hình để gửi đến máy chủ ứng dụng, thông điệp thứ nhất mang mật khẩu ứng dụng;

bộ nhận, được tạo cấu hình để nhận thông điệp thứ hai từ máy chủ ứng dụng chỉ báo rằng kiểm chứng mật khẩu ứng dụng thành công; và

ít nhất một bộ xử lý được ghép nối với bộ cảm biến vân tay, ít nhất một bộ nhớ, màn hình cảm ứng, bộ truyền, và bộ nhận và được tạo cấu hình để:

thiết lập và lưu trữ phép tương ứng giữa mật khẩu ứng dụng và thông tin vân tay thứ nhất dựa trên thông điệp thứ hai,

so sánh thông tin vân tay thứ nhất và thông tin vân tay thứ hai để xác định mức độ so khớp; và

thực hiện chuỗi hoạt động dựa trên phép tương ứng giữa mật khẩu ứng dụng và thông tin vân tay thứ nhất khi mức độ so khớp giữa thông tin vân tay thứ hai được dò thấy bởi bộ cảm biến vân tay và thông tin vân tay thứ nhất vượt quá ngưỡng định trước.

12. Thiết bị đầu cuối theo điểm 11, trong đó trong cách thức thực hiện chuỗi hoạt động, ít nhất một bộ xử lý còn được tạo cấu hình để:

mở khóa thiết bị đầu cuối;

ra lệnh, dựa trên phép tương ứng giữa mật khẩu ứng dụng và thông tin vân tay thứ nhất, bộ truyền gửi đến máy chủ ứng dụng, thông điệp thứ ba chỉ báo rằng mức độ so khớp giữa thông tin vân tay thứ hai và thông tin vân tay thứ nhất vượt quá ngưỡng định trước; và

truy nhập ứng dụng mục tiêu dựa trên thông điệp thứ tư được nhận bởi bộ nhận từ máy chủ ứng dụng, thông điệp thứ tư chỉ báo rằng báo nhận xác thực thành công.

13. Thiết bị đầu cuối theo điểm 11, trong đó ứng dụng mục tiêu bao gồm chức năng mục tiêu, trong đó chức năng mục tiêu được thiết lập với mật khẩu chức năng để truy nhập chức năng mục tiêu, trong đó chuỗi hoạt động còn bao gồm

truy nhập chức năng mục tiêu; và trong đó the ít nhất một bộ xử lý còn được tạo cấu hình để:

ra lệnh bộ truyền gửi thông điệp thứ năm đến máy chủ ứng dụng, trong đó thông điệp thứ năm mang mật khẩu chức năng được nhận bởi màn hình cảm ứng; và

thiết lập phép tương ứng giữa mật khẩu chức năng và thông tin vân tay thứ nhất dựa trên thông điệp thứ sáu được nhận bởi bộ nhận từ máy chủ ứng dụng, trong đó thông điệp thứ sáu chỉ báo rằng kiểm chứng mật khẩu chức năng thành công.

14. Thiết bị đầu cuối theo điểm 13, trong cách thức thực hiện chuỗi hoạt động dựa trên phép tương ứng giữa mật khẩu ứng dụng và thông tin vân tay thứ nhất, ít nhất một bộ xử lý còn được tạo cấu hình để:

mở khóa thiết bị đầu cuối;

ra lệnh, dựa trên phép tương ứng giữa mật khẩu ứng dụng và thông tin vân tay thứ nhất, bộ truyền gửi đến máy chủ ứng dụng, thông điệp thứ ba chỉ báo rằng mức độ so khớp giữa thông tin vân tay thứ hai và thông tin vân tay thứ nhất vượt quá ngưỡng định trước;

truy nhập ứng dụng mục tiêu dựa trên thông điệp thứ tư được nhận bởi bộ nhận từ máy chủ ứng dụng, thông điệp thứ tư chỉ báo rằng báo nhận xác thực thành công;

ra lệnh, dựa trên phép tương ứng giữa mật khẩu chức năng và thông tin vân tay thứ nhất, bộ truyền gửi đến máy chủ ứng dụng, thông điệp thứ bảy chỉ báo rằng mức độ so khớp giữa thông tin vân tay thứ hai và thông tin vân tay thứ nhất vượt quá ngưỡng định trước; và

truy nhập ứng dụng mục tiêu dựa trên thông điệp thứ tám được nhận bởi bộ nhận từ máy chủ ứng dụng, trong đó thông điệp thứ tám chỉ báo rằng báo nhận xác thực thành công.

15. Thiết bị đầu cuối theo điểm bất kỳ trong số các điểm từ 11 đến 14, trong đó ít nhất một bộ xử lý còn được tạo cấu hình để skip bước mở khóa thiết bị đầu

cuối trong quá trình thực hiện chuỗi hoạt động khi màn hình cảm ứng ở trạng thái được mở khóa trước khi ít nhất một bộ xử lý bắt đầu thực hiện chuỗi hoạt động.

16. Thiết bị đầu cuối theo điểm bất kỳ trong số các điểm từ 10 đến 15, trong đó ít nhất một bộ xử lý còn được tạo cấu hình để:

tạo khóa;

gắn khóa với thông tin vân tay thứ nhất; và

ra lệnh bộ truyền gửi đến máy chủ ứng dụng, thông điệp thứ chín mang khóa.

17. Thiết bị đầu cuối theo điểm 11, trong đó ít nhất một bộ xử lý còn được tạo cấu hình để xác định không thực hiện bước mở khóa thiết bị đầu cuối trong quá trình thực hiện chuỗi hoạt động when màn hình cảm ứng ở trạng thái được mở khóa trước khi ít nhất một bộ xử lý bắt đầu thực hiện chuỗi hoạt động.

18. Thiết bị đầu cuối bao gồm:

ít nhất một bộ nhớ, được tạo cấu hình để lưu trữ:

ứng dụng mục tiêu, trong đó ứng dụng mục tiêu được thiết lập với mật khẩu ứng dụng để truy nhập ứng dụng mục tiêu;

thông tin vân tay thứ nhất để mở khóa thiết bị đầu cuối;

chuỗi hoạt động tương ứng với thông tin vân tay thứ nhất, trong đó chuỗi hoạt động bao gồm mở khóa thiết bị đầu cuối và truy nhập ứng dụng mục tiêu; và

phép tương ứng giữa mật khẩu ứng dụng và thông tin vân tay thứ nhất;

bộ cảm biến vân tay, được tạo cấu hình để nhận thông tin vân tay thứ hai;

bộ truyền, được tạo cấu hình để gửi thông điệp kiểm chứng vân tay thành công đến máy chủ ứng dụng, trong đó thông điệp kiểm chứng vân tay thành công chỉ báo rằng mức độ so khớp giữa thông tin vân tay thứ hai và thông tin vân tay thứ nhất vượt quá ngưỡng định trước;

bộ nhận, được tạo cấu hình để nhận thông điệp báo nhận từ máy chủ ứng

dụng; và

màn hình cảm ứng được ghép nối với ít nhất một bộ nhớ, bộ cảm biến vân tay, bộ truyền, và bộ nhận và được tạo cấu hình để:

đáp lại thông điệp báo nhận, và

chuyển đổi từ giao diện khóa màn hình sang giao diện được hiển thị sau khi ứng dụng mục tiêu được truy nhập.

19. Thiết bị đầu cuối theo điểm 18, trong đó ứng dụng mục tiêu bao gồm chức năng mục tiêu, trong đó chức năng mục tiêu được thiết lập với mật khẩu chức năng để truy nhập chức năng mục tiêu, trong đó chuỗi hoạt động còn bao gồm truy nhập chức năng mục tiêu, và trong đó giao diện được hiển thị sau khi ứng dụng mục tiêu được truy nhập là giao diện được hiển thị sau khi chức năng mục tiêu được truy nhập.

20. Thiết bị đầu cuối theo điểm 18 hoặc 19, trong đó bộ truyền còn được tạo cấu hình để gửi khóa được gắn với thông tin vân tay thứ nhất đến máy chủ ứng dụng.

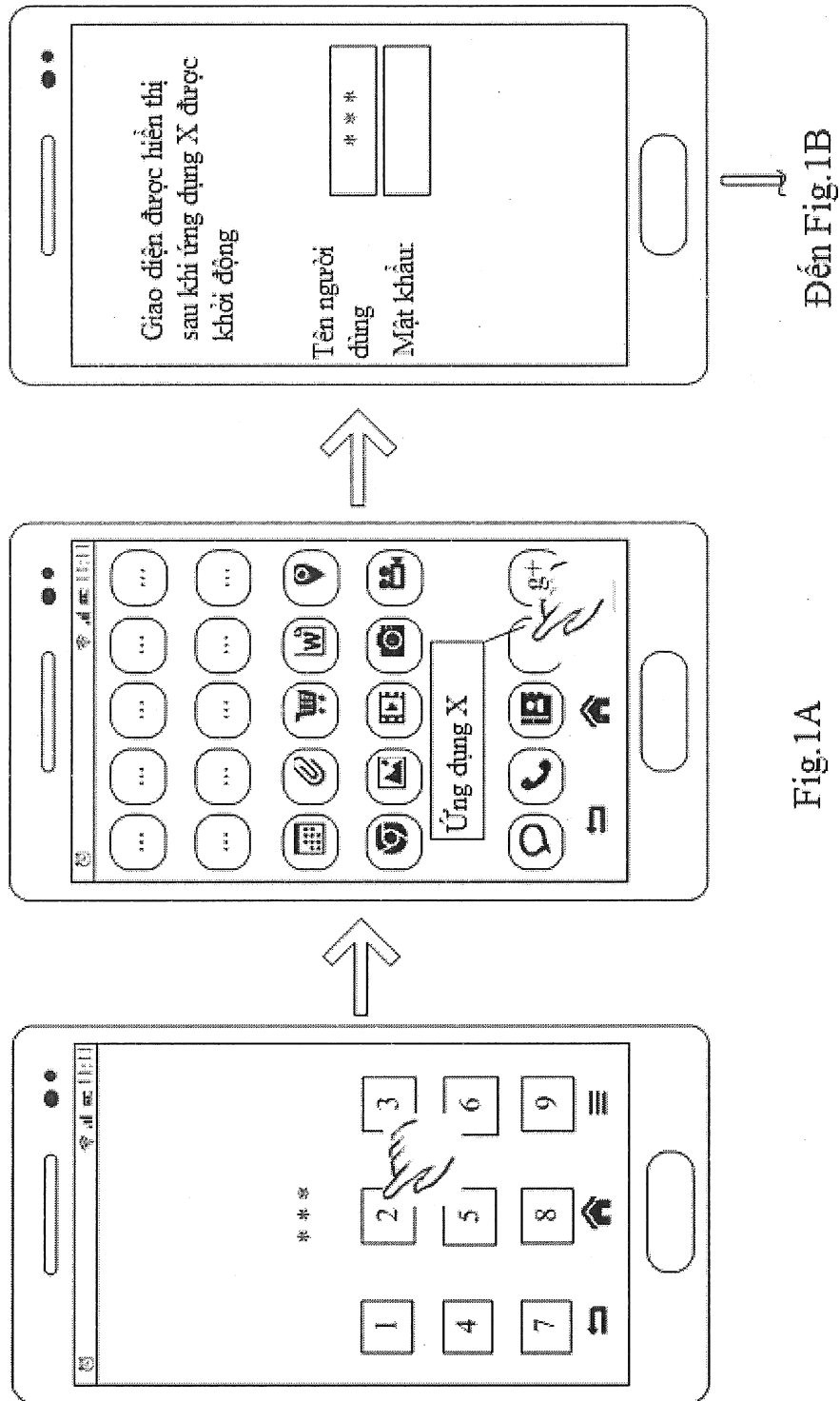


Fig.1A

Tiếp tục từ Fig.1A

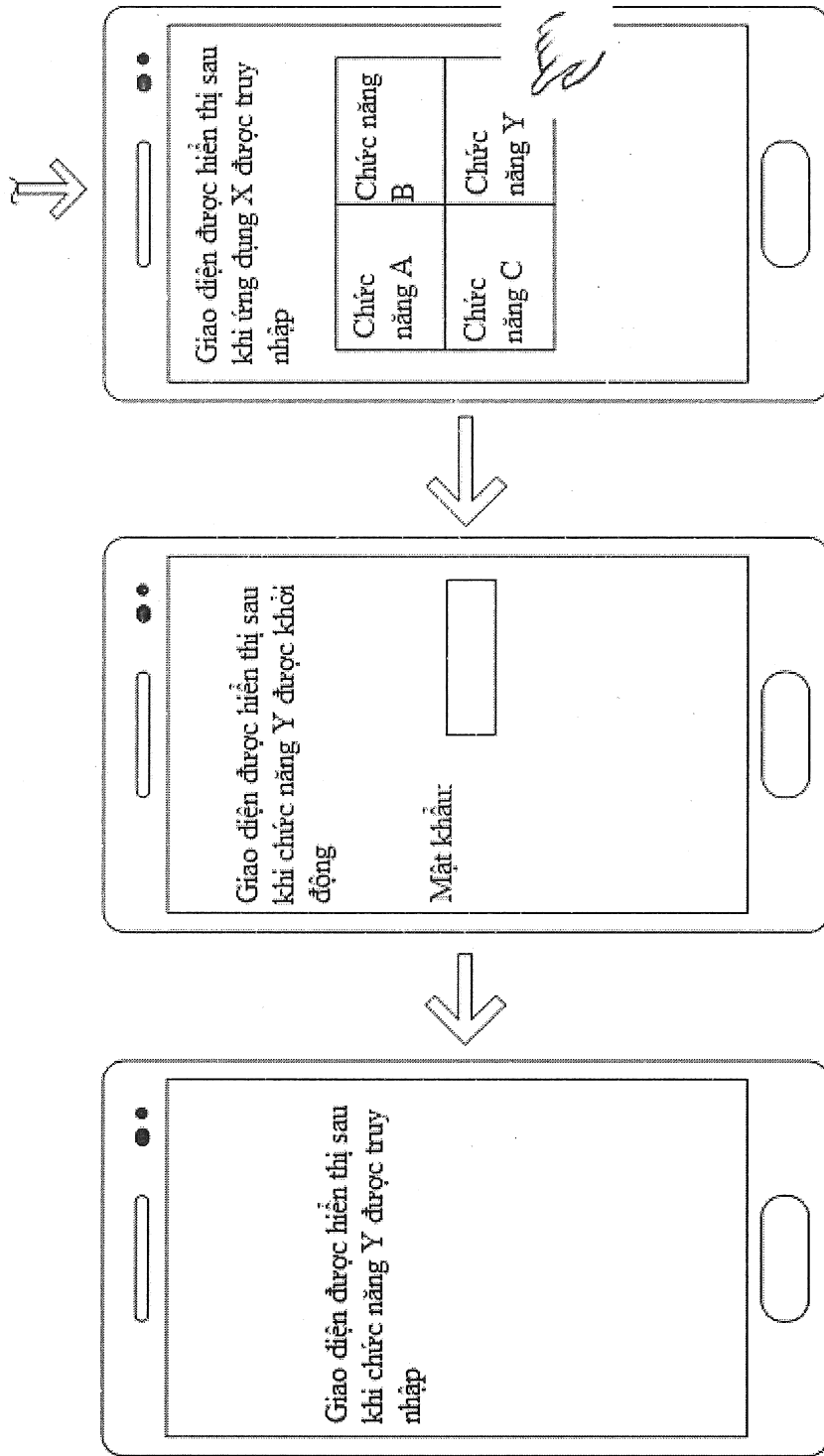


Fig.1B

Chỉ mục vân tay	Chuỗi hoạt động	Gọi API
Vân tay A	Mở khóa màn hình	API_1
Vân tay B	Mở khóa màn hình	API_1
	Truy nhập ứng dụng X	API_2
Vân tay C	Mở khóa màn hình	API_1
	Truy nhập ứng dụng X	API_2
	Truy nhập chức năng Y trong ứng dụng X	API_3

Fig.2

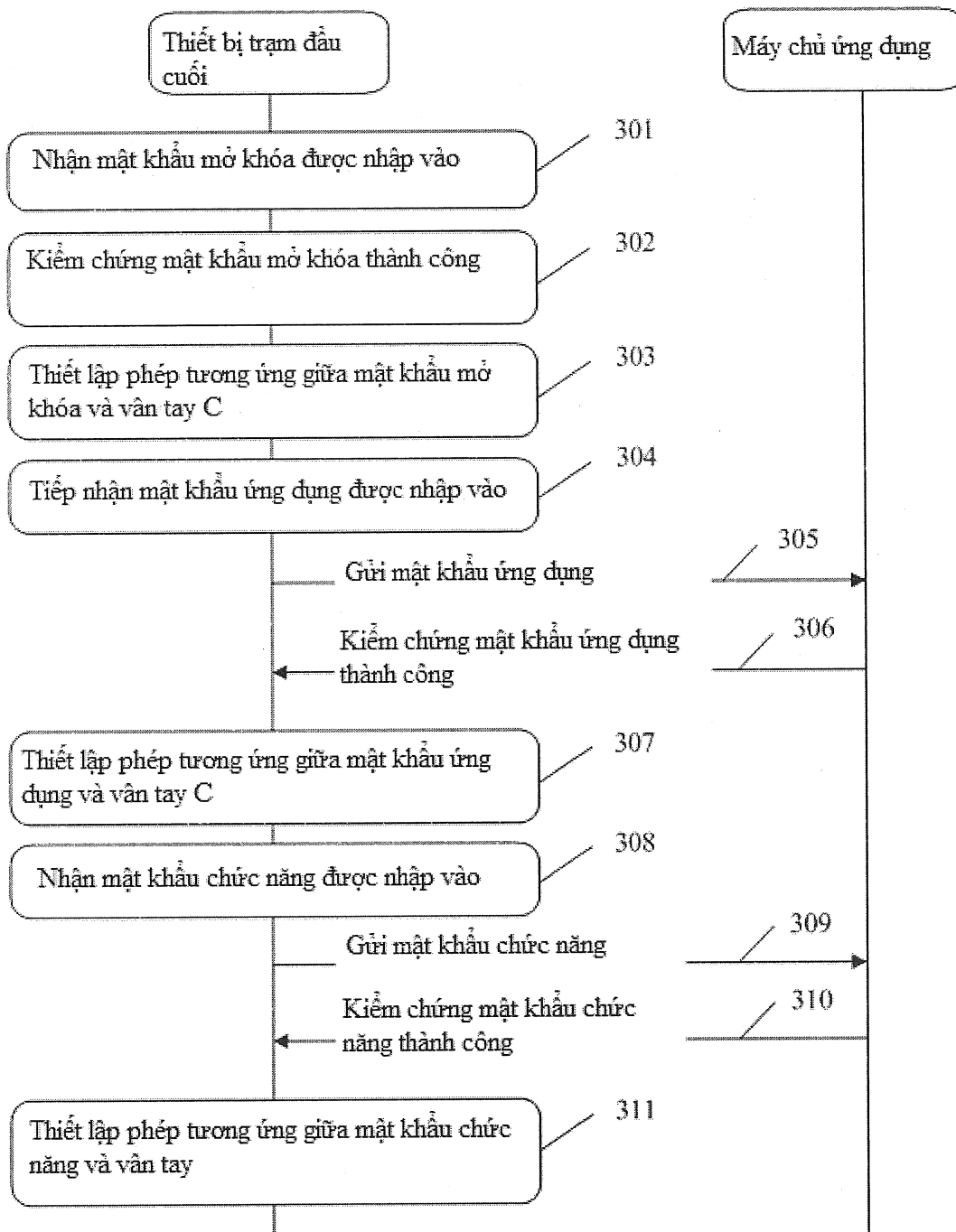


Fig.3

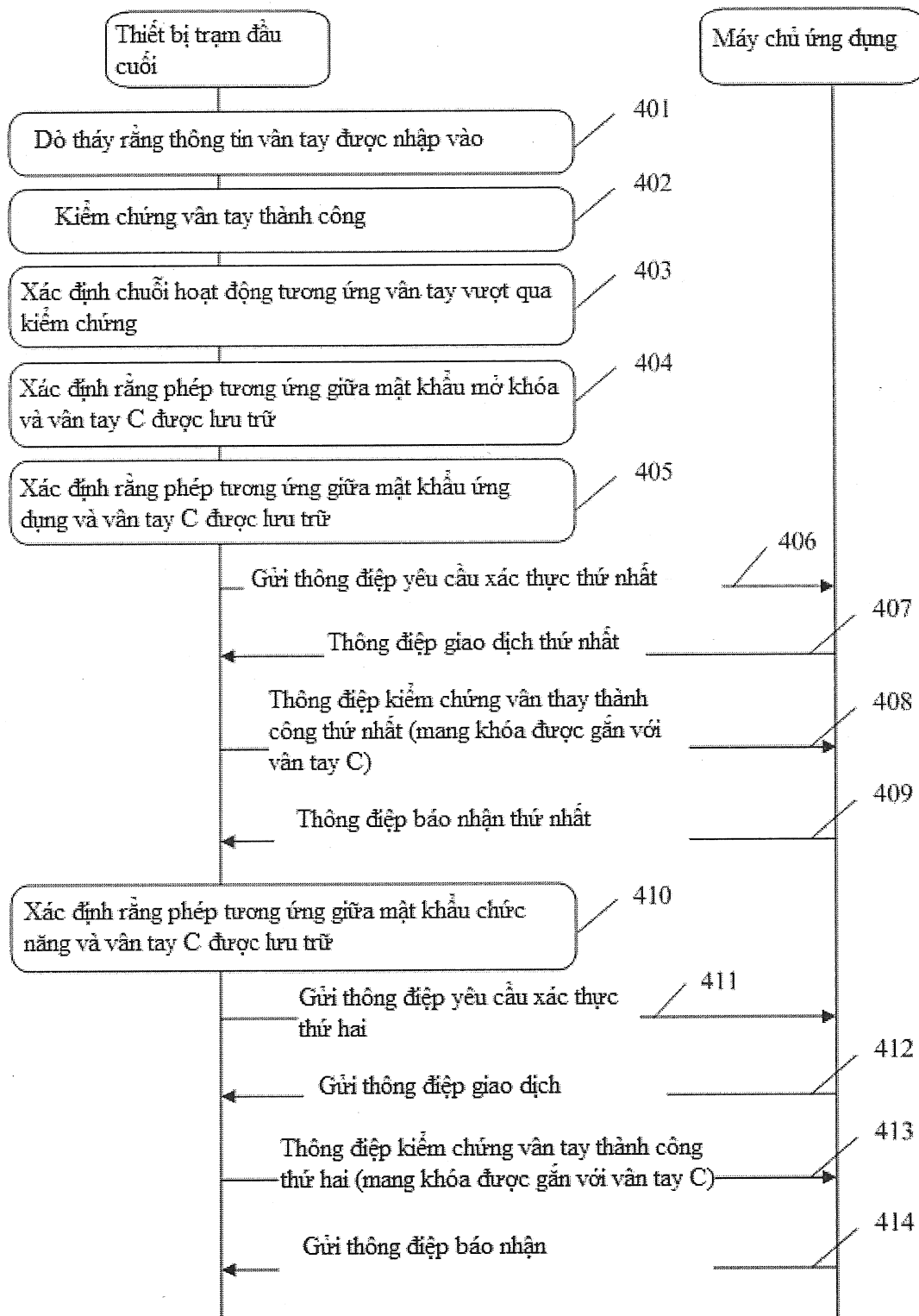


Fig.4

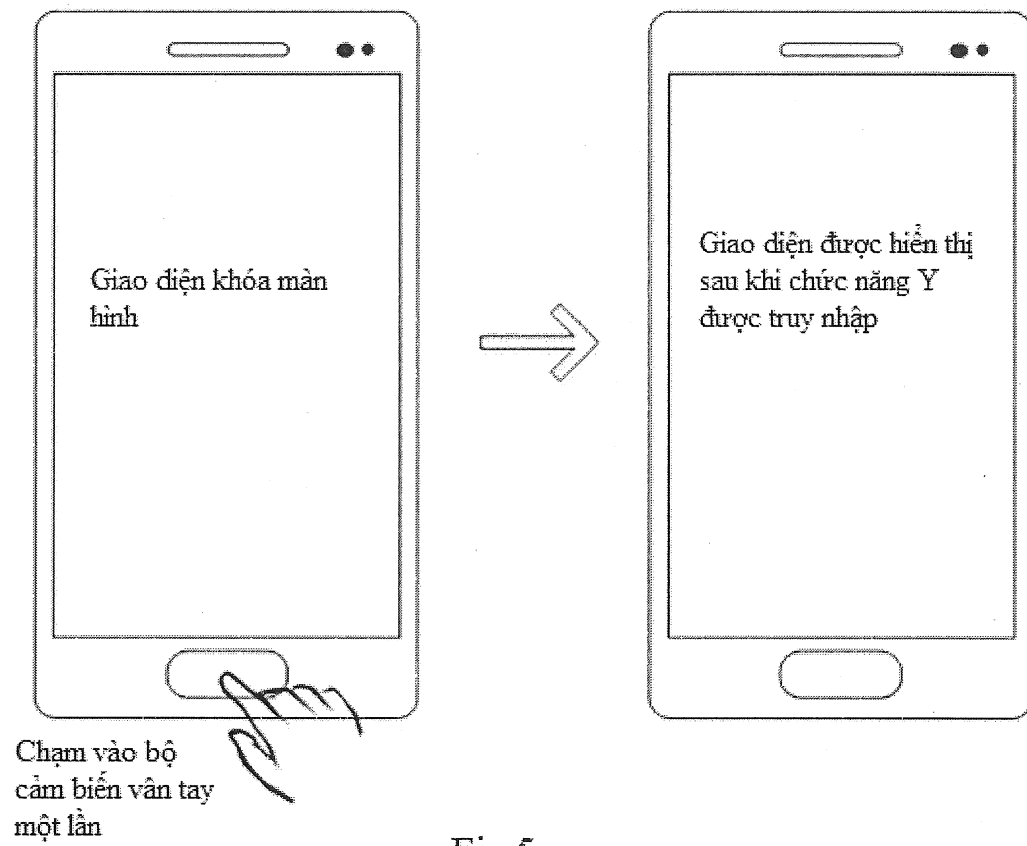


Fig.5

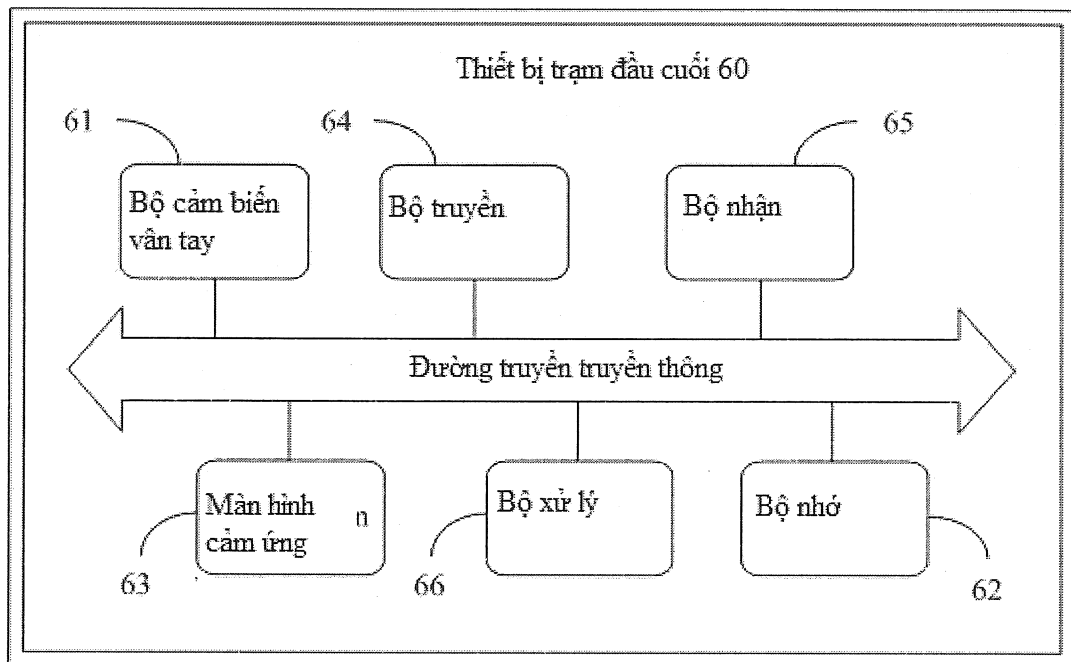


Fig.6