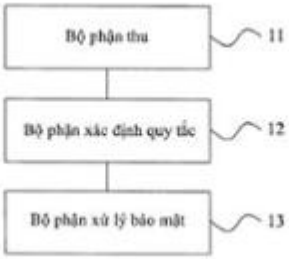
(12) BẢN MÔ TẢ SÁNG CHẾ THUỘC BẰNG ĐỘC QUYỀN SÁNG CHẾ
(19) **Cộng hòa xã hội chủ nghĩa Việt Nam (VN)**
CỤC SỞ HỮU TRÍ TUỆ
(11) **1-0027539**
(51)[7] **H04L 29/06**
(13) **B**

(21) 1-2016-05054
(22) 19/11/2014
(86) PCT/CN2014/091678 19/11/2014
(87) WO 2015/180427 A1 03/12/2015
(30) 201410239109.0 30/05/2014 CN
(45) 25/02/2021 395
(43) 27/02/2017 347A
(73) HUAWEI TECHNOLOGIES CO., LTD. (CN)
Huawei Administration Building, Bantian, Longgang District, Shenzhen, Guangdong 518129, China
(72) HE, Chengkai (CN); KONG, Tao (CN).
(74) Công ty TNHH một thành viên Sở hữu trí tuệ VCCI (VCCI-IP CO.,LTD)

(54) PHƯƠNG PHÁP VÀ THIẾT BỊ XỬ LÝ DỮ LIỆU NGƯỜI DÙNG

(57) Sáng chế đề cập đến thiết bị và phương pháp xử lý dữ liệu người dùng. Thiết bị xử lý dữ liệu người dùng theo sáng chế bao gồm: bộ phận thu, được tạo cấu hình để thu yêu cầu thu nhận thông tin không dây được gửi bởi thiết bị thành phần mạng, trong đó yêu cầu thu nhận thông tin không dây được sử dụng để yêu cầu thu nhận dữ liệu người dùng tương ứng với ứng dụng dịch vụ; bộ phận xác định quy tắc, được tạo cấu hình để xác định, theo ứng dụng dịch vụ và sự tương ứng giữa ứng dụng dịch vụ và quy tắc bảo vệ bảo mật, quy tắc bảo vệ bảo mật tương ứng với ứng dụng dịch vụ; và bộ phận xử lý bảo mật, được tạo cấu hình để: khi quy tắc bảo vệ bảo mật được sử dụng để lệnh thực hiện quy trình bảo mật, thực hiện quy trình bảo mật cho dữ liệu người dùng theo quy tắc bảo vệ bảo mật. Thiết bị được đề xuất trong các phương án của sáng chế có thể nâng cao tính an toàn của dữ liệu người dùng.



Lĩnh vực kỹ thuật được đề cập

Các phương án của sáng chế đề cập đến các kỹ thuật truyền thông, và cụ thể là, sáng chế đề cập đến phương pháp và bị xử lý dữ liệu người dùng.

Tình trạng kỹ thuật của sáng chế

Với sự phát triển nhanh chóng của dịch vụ băng rộng di động (Mobile Broad Band, viết tắt là MBB), thiết bị mạng không dây lưu trữ các tài nguyên dữ liệu phong phú. Nhà cung cấp dịch vụ phân tích dữ liệu có thể sử dụng dữ liệu để khai thác hành vi của người dùng, và người khai thác cũng mong muốn sử dụng hiệu quả các tài nguyên dữ liệu được xử lý, và mở thông tin không dây bằng cách sử dụng hệ thống mở thông tin mạng không dây.

Trong hệ thống mở thông tin không dây, một số dữ liệu, ví dụ, một số dữ liệu liên quan đến sự bảo mật người dùng, cần được bảo vệ, nhưng hệ thống mở thông tin không dây hiện có thiếu kỹ thuật để bảo vệ dữ liệu, mà khiến cho sự bảo mật dữ liệu kém.

Bản chất kỹ thuật của sáng chế

Các phương án của sáng chế đề xuất thiết bị và phương pháp xử lý dữ liệu người dùng, để nâng cao độ bảo mật dữ liệu.

Theo khía cạnh thứ nhất, phương án của sáng chế đề cập đến thiết bị xử lý dữ liệu người dùng, bao gồm:

bộ phận thu, được tạo cấu hình để thu yêu cầu thu nhận thông tin không dây được gửi bởi thiết bị thành phần mạng, trong đó yêu cầu thu nhận thông tin không dây được sử dụng để yêu cầu thu nhận dữ liệu người dùng tương ứng với ứng dụng dịch vụ;

bộ phận xác định quy tắc, được tạo cấu hình để xác định, theo ứng dụng dịch vụ và sự tương ứng giữa ứng dụng dịch vụ và quy tắc bảo vệ bảo mật, quy tắc bảo vệ bảo mật tương ứng với ứng dụng dịch vụ; và

bộ phận xử lý bảo mật, được tạo cấu hình để: khi quy tắc bảo vệ bảo mật được sử dụng để lệnh thực hiện quy trình bảo mật, thực hiện quy trình bảo

mật cho dữ liệu người dùng theo quy tắc bảo vệ bảo mật.

Dựa vào khía cạnh thứ nhất, theo cách thực hiện có thể thứ nhất của khía cạnh thứ nhất, bộ phận xử lý bảo mật bao gồm:

bộ phận thu nhận kết quả dàn xếp, được tạo cấu hình để: khi quy tắc bảo vệ bảo mật được sử dụng để lệnh thực hiện sự dàn xếp bảo mật, thực hiện, theo quy tắc bảo vệ bảo mật, sự dàn xếp bảo mật với thiết bị người dùng tương ứng với dữ liệu người dùng, để thu nhận kết quả dàn xếp bảo mật; và

bộ phận xử lý kết quả dàn xếp, được tạo cấu hình để: khi kết quả dàn xếp bảo mật được sử dụng để lệnh mở dữ liệu người dùng cho ứng dụng dịch vụ, cung cấp dữ liệu người dùng cho ứng dụng dịch vụ; hoặc khi kết quả dàn xếp bảo mật được sử dụng để lệnh không mở dữ liệu người dùng cho ứng dụng dịch vụ, gửi thông tin chỉ báo tới thiết bị thành phần mạng, trong đó thông tin chỉ báo được sử dụng để chỉ báo rằng dữ liệu người dùng không thể được thu nhận.

Dựa vào khía cạnh thứ nhất, trong cách thực hiện có thể thứ hai của khía cạnh thứ nhất, bộ phận thu nhận kết quả dàn xếp còn được tạo cấu hình để: khi quy tắc bảo vệ bảo mật được sử dụng để lệnh sử dụng kết quả dàn xếp bảo mật được lưu trữ trước, thu nhận trực tiếp kết quả dàn xếp bảo mật được lưu trữ trước theo quy tắc bảo vệ bảo mật; và

bộ phận xử lý kết quả dàn xếp được tạo cấu hình để: khi kết quả dàn xếp bảo mật được sử dụng để lệnh mở dữ liệu người dùng cho ứng dụng dịch vụ, cung cấp dữ liệu người dùng cho ứng dụng dịch vụ; hoặc khi kết quả dàn xếp bảo mật được sử dụng để lệnh không mở dữ liệu người dùng cho ứng dụng dịch vụ, gửi thông tin chỉ báo tới thiết bị thành phần mạng, trong đó thông tin chỉ báo được sử dụng để chỉ báo rằng dữ liệu người dùng không thể được thu nhận.

Dựa vào khía cạnh thứ nhất và hoặc cách thực hiện có thể thứ nhất hoặc cách thực hiện có thể thứ hai của khía cạnh thứ nhất, theo cách thực hiện có thể thứ ba của khía cạnh thứ nhất, bộ phận xử lý bảo mật còn được tạo cấu hình để: khi quy tắc bảo vệ bảo mật được sử dụng để lệnh không thực hiện quy trình bảo mật, cung cấp dữ liệu người dùng cho ứng dụng dịch vụ.

Theo khía cạnh thứ hai, phương án của sáng chế đề cập đến phương pháp xử lý dữ liệu người dùng, bao gồm các bước:

thu, bởi thiết bị xử lý dữ liệu người dùng, yêu cầu thu nhận thông tin không dây được gửi bởi thiết bị thành phần mạng, trong đó yêu cầu thu nhận thông tin không dây được sử dụng để yêu cầu thu nhận dữ liệu người dùng tương ứng với ứng dụng dịch vụ;

xác định, bởi thiết bị xử lý dữ liệu người dùng theo ứng dụng dịch vụ và sự tương ứng giữa ứng dụng dịch vụ và quy tắc bảo vệ bảo mật, quy tắc bảo vệ bảo mật tương ứng với ứng dụng dịch vụ; và

khi quy tắc bảo vệ bảo mật được sử dụng để lệnh thực hiện quy trình bảo mật, thực hiện, bởi thiết bị xử lý dữ liệu người dùng, quy trình bảo mật cho dữ liệu người dùng theo quy tắc bảo vệ bảo mật.

Dựa vào khía cạnh thứ hai, theo cách thực hiện có thể thứ nhất của khía cạnh thứ hai, quy tắc bảo vệ bảo mật được sử dụng để lệnh thực hiện quy trình bảo mật cụ thể là: quy tắc bảo vệ bảo mật được sử dụng để lệnh thực hiện sự dàn xếp bảo mật; và

sự thực hiện, bởi thiết bị xử lý dữ liệu người dùng, quy trình bảo mật cho dữ liệu người dùng theo quy tắc bảo vệ bảo mật bao gồm:

thực hiện, bởi thiết bị xử lý dữ liệu người dùng theo quy tắc bảo vệ bảo mật, sự dàn xếp bảo mật với thiết bị người dùng tương ứng với dữ liệu người dùng, để thu nhận kết quả dàn xếp bảo mật; và

khi kết quả dàn xếp bảo mật được sử dụng để lệnh mở dữ liệu người dùng cho ứng dụng dịch vụ, cung cấp, bởi thiết bị xử lý dữ liệu người dùng, dữ liệu người dùng cho ứng dụng dịch vụ; hoặc

khi kết quả dàn xếp bảo mật được sử dụng để lệnh không mở dữ liệu người dùng cho ứng dụng dịch vụ, gửi, bởi thiết bị xử lý dữ liệu người dùng, thông tin chỉ báo tới thiết bị thành phần mạng, trong đó thông tin chỉ báo được sử dụng để chỉ báo rằng dữ liệu người dùng không thể được thu nhận.

Dựa vào khía cạnh thứ hai, trong cách thực hiện có thể thứ hai của khía cạnh thứ hai, quy tắc bảo vệ bảo mật được sử dụng để lệnh thực hiện quy trình bảo mật cụ thể là: quy tắc bảo vệ bảo mật được sử dụng để lệnh sử dụng kết quả dàn xếp bảo mật được lưu trữ trước; và

sự thực hiện, bởi thiết bị xử lý dữ liệu người dùng, quy trình bảo mật

cho dữ liệu người dùng theo quy tắc bảo vệ bảo mật bao gồm:

thu nhận trực tiếp, bởi thiết bị xử lý dữ liệu người dùng, kết quả dàn xếp bảo mật được lưu trữ trước theo quy tắc bảo vệ bảo mật; và

khi kết quả dàn xếp bảo mật được sử dụng để lệnh mở dữ liệu người dùng cho ứng dụng dịch vụ, cung cấp, bởi thiết bị xử lý dữ liệu người dùng, dữ liệu người dùng cho ứng dụng dịch vụ; hoặc

khi kết quả dàn xếp bảo mật được sử dụng để lệnh không mở dữ liệu người dùng cho ứng dụng dịch vụ, gửi, bởi thiết bị xử lý dữ liệu người dùng, thông tin chỉ báo tới thiết bị thành phần mạng, trong đó thông tin chỉ báo được sử dụng để chỉ báo rằng dữ liệu người dùng không thể được thu nhận.

Dựa vào khía cạnh thứ hai và hoặc cách thực hiện có thể thứ nhất hoặc cách thực hiện có thể thứ hai của khía cạnh thứ hai, theo cách thực hiện có thể thứ ba của khía cạnh thứ hai, phương pháp còn bao gồm:

khi quy tắc bảo vệ bảo mật được sử dụng để lệnh không thực hiện quy trình bảo mật, cung cấp, bởi thiết bị xử lý dữ liệu người dùng, dữ liệu người dùng cho ứng dụng dịch vụ.

Theo thiết bị và phương pháp xử lý dữ liệu người dùng trong các phương án của sáng chế, đối với các ứng dụng dịch vụ khác, các quy tắc bảo vệ bảo mật tương ứng với các ứng dụng dịch vụ khác được xác định, và quy trình bảo mật được thực hiện cho dữ liệu người dùng theo các quy tắc bảo vệ bảo mật, mà nâng cao tính bảo mật của dữ liệu người dùng ngoài việc mở đúng dữ liệu người dùng.

Mô tả vắn tắt các hình vẽ

Để mô tả các giải pháp kỹ thuật trong các phương án của sáng chế hoặc theo tình tạng kỹ thuật một cách rõ ràng hơn, phần dưới đây giới thiệu vắn tắt các hình vẽ kèm theo được yêu cầu để mô tả các phương án hoặc tình trạng kỹ thuật. Rõ ràng là, các hình vẽ kèm theo trong phần mô tả dưới đây thể hiện một số phương án của sáng chế, và người có hiểu biết trung bình trong lĩnh vực kỹ thuật vẫn có thể có được các hình vẽ khác từ các kình vẽ kèm theo này mà không cần nỗ lực sáng tạo.

Fig.1 là lưu đồ của phương pháp xử lý dữ liệu người dùng theo phương án của sáng chế;

Fig.2 là sơ đồ cấu trúc giản lược của hệ thống xử lý dữ liệu người dùng theo phương án của sáng chế;

Fig.3 là lưu đồ báo hiệu của phương pháp tạo cấu hình bảo mật theo phương án của sáng chế;

Fig.4 là lưu đồ báo hiệu của phương pháp dàn xếp bảo mật theo phương án của sáng chế;

Fig.5 là lưu đồ báo hiệu của sự dàn xếp bảo mật khác theo phương án của sáng chế;

Fig.6 là lưu đồ báo hiệu của sự dàn xếp bảo mật khác nữa theo phương án của sáng chế;

Fig.7 là lưu đồ của phương pháp xử lý dữ liệu người dùng khác theo phương án của sáng chế;

Fig.8 là lưu đồ của phương pháp xử lý dữ liệu người dùng khác nữa theo phương án của sáng chế;

Fig.9 là lưu đồ của phương pháp xử lý dữ liệu người dùng khác nữa theo phương án của sáng chế;

Fig.10 là sơ đồ cấu trúc giản lược của thiết bị xử lý dữ liệu người dùng theo phương án của sáng chế;

Fig.11 là sơ đồ cấu trúc giản lược của thiết bị xử lý dữ liệu người dùng khác theo phương án của sáng chế;

Fig.12 là sơ đồ cấu trúc giản lược của thiết bị xử lý dữ liệu người dùng theo phương án của sáng chế; và

Fig.13 là sơ đồ cấu trúc giản lược của thiết bị xử lý dữ liệu người dùng khác theo phương án của sáng chế.

Mô tả chi tiết sáng chế

Để hiểu các mục đích, các giải pháp kỹ thuật, và các lợi ích của các phương án của sáng chế rõ ràng hơn, phần dưới đây mô tả chi tiết và rõ ràng các giải pháp kỹ thuật trong các phương án của sáng chế dựa vào các hình vẽ kèm

theo trong các phương án của sáng chế. Rõ ràng là, các phương án được mô tả một số không phải tất cả các phương án của sáng chế. Tất cả các phương án khác được thu nhận người có hiểu biết trung bình trong lĩnh vực kỹ thuật dựa vào các phương án của sáng chế mà không có sự nỗ lực sáng tạo sẽ nằm trong phạm vi bảo hộ của sáng chế.

Fig.1 là lưu đồ của phương pháp xử lý dữ liệu người dùng theo phương án của sáng chế. Như được thể hiện trên Fig.1, phương pháp bao gồm:

Bước 101: thiết bị xử lý dữ liệu người dùng thu yêu cầu thu nhận thông tin không dây được gửi bởi thiết bị thành phần mạng, trong đó yêu cầu thu nhận thông tin không dây được sử dụng để yêu cầu thu nhận dữ liệu người dùng tương ứng với ứng dụng dịch vụ.

Phương pháp này được thực hiện bởi thiết bị xử lý dữ liệu người dùng. Thiết bị có thể được tích hợp với kho dữ liệu, thiết bị mạng lõi, phần tử mạng mà có các chức năng thu thập và phân tích dữ liệu người dùng, hoặc tương tự, hoặc có thể được sử dụng làm thiết bị thành phần mạng độc lập. Thiết bị thành phần mạng trong phương pháp này có thể là máy chủ ứng dụng mà được bố trí bên trong mạng truyền thông không dây, có thể là máy chủ ứng dụng mà được bố trí trên Internet hoặc mạng doanh nghiệp, hoặc có thể là phần tử mạng của mạng lõi ở mạng truyền thông không dây. Trong phương pháp này, ứng dụng dịch vụ có thể là ứng dụng mà cần sử dụng dữ liệu người dùng, chẳng hạn như ứng dụng cảnh báo thiên tai, ứng dụng quy hoạch giao thông, hoặc ứng dụng tiếp thị chính xác. Các ứng dụng dịch vụ khác có các yêu cầu khác nhau đối với dữ liệu người dùng. Ví dụ, ứng dụng cảnh báo thiên tai yêu cầu thu nhận thông tin thuộc tính của danh sách người dùng quanh điểm có nguy cơ, để gửi cảnh báo thiên tai tới các người dùng này; ứng dụng quy hoạch giao thông yêu cầu thu nhận thông tin thuộc tính của thông tin quy hoạch giao thông chẳng hạn như thu thập thống kê và kết quả phân tích của các thuộc tính đám đông, để giúp việc quy hoạch giao thông trở nên dễ dàng hơn; ứng dụng tiếp thị chính xác yêu cầu thu nhận thông tin không dây, chẳng hạn như thông tin vị trí cá nhân và chất lượng thu tín hiệu không dây, để giúp việc phân tích tiếp thị trở nên dễ dàng hơn. Trong phương pháp này, yêu cầu thu nhận thông tin không dây có thể bao gồm

ký hiệu nhận dạng của ứng dụng dịch vụ, và ký hiệu nhận dạng của ứng dụng dịch vụ có thể được sử dụng để nhận dạng ứng dụng dịch vụ mà yêu cầu dữ liệu người dùng.

Bước 102: thiết bị xử lý dữ liệu người dùng xác định, theo ứng dụng dịch vụ và sự tương ứng giữa ứng dụng dịch vụ và quy tắc bảo vệ bảo mật, quy tắc bảo vệ bảo mật tương ứng với ứng dụng dịch vụ.

Trong phương pháp này, sự tương ứng giữa ứng dụng dịch vụ và quy tắc bảo vệ bảo mật có thể được lưu trữ trong thiết bị xử lý dữ liệu người dùng, hoặc có thể được lưu trữ trong phần tử mạng khác. Ví dụ, bảng tương ứng có thể được thiết đặt, trong đó bảng lưu trữ ký hiệu nhận dạng của ứng dụng dịch vụ và ký hiệu nhận dạng của quy tắc bảo vệ bảo mật tương ứng với ứng dụng dịch vụ. Trong phương pháp này, quy tắc bảo vệ bảo mật có thể được phân loại thành hai loại, trong đó một loại là quy tắc trong đó quy trình bảo mật cần được thực hiện, và loại khác là quy tắc trong đó quy trình bảo mật không cần được thực hiện. Ví dụ, quy tắc trong đó quy trình bảo mật cần được thực hiện có thể là quy tắc mà lệnh thực hiện quy trình bảo mật bằng cách dàn xếp bảo mật, hoặc có thể là quy tắc mà lệnh thực hiện quy trình bảo mật bằng cách sử dụng kết quả dàn xếp bảo mật được lưu trữ trước. Kết quả dàn xếp bảo mật được sử dụng để lệnh xem có mở dữ liệu người dùng cho ứng dụng dịch vụ hay không. Sự dàn xếp bảo mật có thể là sự dàn xếp giữa thiết bị xử lý dữ liệu người dùng và thiết bị người dùng, hoặc có thể là sự dàn xếp giữa thiết bị xử lý dữ liệu người dùng, thiết bị người dùng, và phần tử mạng khác, sao cho kết quả dàn xếp bảo mật có thể được thu nhận bằng cách dàn xếp bảo mật.

Trong phương pháp này, các ứng dụng dịch vụ khác có thể tương ứng với các quy tắc bảo vệ bảo mật khác. Ví dụ, đối với ứng dụng cảnh báo thiên tai, do ứng dụng dịch vụ này ứng dụng được khi khẩn cấp, quy tắc bảo vệ bảo mật trong đó quy trình bảo mật không cần được thực hiện có thể được thiết đặt; đối với ứng dụng quy hoạch giao thông, do ứng dụng dịch vụ này thuộc về ứng dụng phân tích nhóm đó là dựa vào lợi ích cộng đồng, có thể được xem xét theo mặc định rằng tất cả các thiết bị người dùng (User Equipment, viết tắt là UE) chấp nhận việc thu thập dữ liệu của ứng dụng dịch vụ, và cũng có thể được xem

xét cho phép UE dành riêng quyền lựa chọn xem có cung cấp dữ liệu người dùng hay không, và do đó, ý kiến người dùng có thể được thăm dò trước, ví dụ, khi người dùng thực hiện sự tán thành, sự dàn xếp bảo mật được thực hiện trước, và kết quả dàn xếp bảo mật được lưu lại, và khi ứng dụng quy hoạch giao thông cần yêu cầu dữ liệu người dùng, việc xem có cung cấp dữ liệu người dùng hay không có thể được xác định trực tiếp theo kết quả dàn xếp bảo mật được lưu trữ trước, và xét về vấn đề này, quy tắc bảo vệ bảo mật mà lệnh sử dụng kết quả dàn xếp bảo mật được lưu trữ trước có thể được thiết đặt cho ứng dụng quy hoạch giao thông; đối với ứng dụng tiếp thị chính xác, do ứng dụng dịch vụ này là ứng dụng thương mại, có thể được xem xét để cấp phát quyền lựa chọn tới người dùng mỗi lần dữ liệu người dùng được yêu cầu, đó là, mỗi lần dữ liệu người dùng được yêu cầu, sự dàn xếp bảo mật với thiết bị người dùng cần được thực hiện để thu nhận kết quả dàn xếp bảo mật, và việc xem có cung cấp dữ liệu người dùng hay không được xác định theo kết quả dàn xếp bảo mật được thu nhận, và xét về vấn đề này, quy tắc bảo vệ bảo mật mà lệnh thực hiện sự dàn xếp bảo mật có thể được thiết đặt cho ứng dụng tiếp thị chính xác.

Bước 103: khi quy tắc bảo vệ bảo mật được sử dụng để lệnh thực hiện quy trình bảo mật, thiết bị xử lý dữ liệu người dùng thực hiện quy trình bảo mật cho dữ liệu người dùng theo quy tắc bảo vệ bảo mật.

Ví dụ, đối với quy tắc bảo vệ bảo mật mà lệnh thực hiện sự dàn xếp bảo mật, thiết bị xử lý dữ liệu người dùng có thể bắt đầu, theo quy tắc bảo vệ bảo mật, sự dàn xếp bảo mật với thiết bị người dùng, thu nhận kết quả dàn xếp bảo mật bằng cách dàn xếp bảo mật, và sau đó thực hiện sự xử lý dữ liệu người dùng theo kết quả dàn xếp bảo mật. Ví dụ khác, đối với quy tắc bảo vệ bảo mật mà lệnh sử dụng kết quả dàn xếp bảo mật được lưu trữ trước, thiết bị xử lý dữ liệu người dùng có thể thu nhận kết quả dàn xếp bảo mật được lưu trữ trước theo quy tắc bảo vệ bảo mật, và thực hiện sự xử lý dữ liệu người dùng theo kết quả dàn xếp bảo mật được lưu trữ trước.

Một cách tùy chọn, trong phương pháp này, khi quy tắc bảo vệ bảo mật được sử dụng để lệnh không thực hiện quy trình bảo mật, thiết bị xử lý dữ liệu người dùng có thể cung cấp trực tiếp dữ liệu người dùng cho ứng dụng dịch vụ.

Theo phương pháp xử lý dữ liệu người dùng được thể hiện trên Fig.1, đối với các ứng dụng dịch vụ khác, các quy tắc bảo vệ bảo mật tương ứng với các ứng dụng dịch vụ khác được xác định, và quy trình bảo mật được thực hiện cho dữ liệu người dùng theo các quy tắc bảo vệ bảo mật, mà có thể nâng cao tính an toàn của dữ liệu người dùng ngoài việc mở đúng dữ liệu người dùng.

Để áp dụng phương pháp xử lý dữ liệu người dùng được thể hiện trên Fig.1, như được thể hiện trên Fig.2, phương án của sáng chế đề cập đến hệ thống xử lý dữ liệu người dùng. Người có hiểu biết trung bình trong lĩnh vực kỹ thuật sẽ biết rằng hệ thống được thể hiện trên Fig.2 là một ví dụ, và không có mục đích giới hạn kịch bản ứng dụng của phương pháp được thể hiện trên Fig.1.

Hệ thống bao gồm: thiết bị phân tích và mở dữ liệu 11, máy chủ dàn xếp bảo mật 12, UE 13, máy chủ ứng dụng 14, thiết bị tạo cấu hình và quản lý 15, và thiết bị mạng không dây 16.

Thiết bị phân tích và mở dữ liệu 11 là thiết bị thành phần mạng mà có các chức năng phân tích dữ liệu người dùng và đưa ra dữ liệu người dùng hoặc kết quả phân tích dữ liệu người dùng. Trên thiết bị, các chức năng của thiết bị xử lý dữ liệu người dùng theo phương pháp được thể hiện trên Fig.1 được tích hợp. Để thực hiện các chức năng của thiết bị xử lý dữ liệu người dùng, thiết bị có thể bao gồm: bộ phận thu, bộ phận xác định quy tắc, và bộ phận xử lý kết quả dàn xếp. Bộ phận thu được tạo cấu hình để thu yêu cầu thu nhận thông tin không dây được gửi bởi thiết bị thành phần mạng, trong đó yêu cầu thu nhận thông tin không dây được sử dụng để yêu cầu thu nhận dữ liệu người dùng tương ứng với ứng dụng dịch vụ; bộ phận xác định quy tắc được tạo cấu hình để xác định, theo ứng dụng dịch vụ và sự tương ứng giữa ứng dụng dịch vụ và quy tắc bảo vệ bảo mật, quy tắc bảo vệ bảo mật tương ứng với ứng dụng dịch vụ; bộ phận xử lý kết quả dàn xếp được tạo cấu hình để: khi quy tắc bảo vệ bảo mật được sử dụng để lệnh thực hiện quy trình bảo mật, thực hiện quy trình bảo mật cho dữ liệu người dùng theo quy tắc bảo vệ bảo mật. Ngoài ra, bộ phận xử lý kết quả dàn xếp còn được tạo cấu hình để: khi quy tắc bảo vệ bảo mật được sử dụng để lệnh không thực hiện quy trình bảo mật, cung cấp dữ liệu người dùng cho ứng dụng dịch vụ.

Máy chủ dàn xếp bảo mật 12 có thể là trang mạng dạng cổng thông tin

điện tử (Web Portal) của người khai thác, có thể là trung tâm dịch vụ thông báo ngắn của người khai thác, hoặc tương tự. Chức năng chính của máy chủ dàn xếp bảo mật 12 là chuyển tiếp yêu cầu dàn xếp bảo mật được gửi bởi thiết bị phân tích và mở dữ liệu 11 tới UE, sau đó thu sự lựa chọn, được thực hiện bởi người dùng cho yêu cầu dàn xếp bảo mật, của việc xem có mở dữ liệu người dùng hay không, và thông báo thiết bị phân tích và mở dữ liệu 11 kết quả lựa chọn của người dùng. Ngoài ra, máy chủ dàn xếp bảo mật 12 có thể còn gửi yêu cầu dàn xếp bảo mật tới một UE theo yêu cầu của thiết bị phân tích và mở dữ liệu 11. Ví dụ, đối với yêu cầu dàn xếp bảo mật, người dùng lựa chọn việc cho phép ứng dụng dịch vụ sử dụng dữ liệu của người dùng, nhưng dữ liệu có khoảng thời gian sử dụng, và do đó, khi khoảng thời gian sử dụng của dữ liệu người dùng gần kết thúc, thiết bị phân tích và mở dữ liệu 11 yêu cầu máy chủ dàn xếp bảo mật 12 gửi lại yêu cầu dàn xếp bảo mật tới UE.

Một cách tùy chọn, chức năng của máy chủ dàn xếp bảo mật 12 có thể cũng được tích hợp vào trong thiết bị phân tích và mở dữ liệu 11, làm bộ phận chức năng của thiết bị phân tích và mở dữ liệu 11.

UE 13 có thể là thiết bị di động, chẳng hạn như điện thoại di động hoặc máy tính bảng. UE 13 có thể bao gồm môđun dàn xếp bảo mật và môđun lựa chọn bảo mật. Môđun dàn xếp bảo mật có vai trò tương tác với máy chủ dàn xếp bảo mật 12, thu yêu cầu dàn xếp bảo mật được gửi bởi máy chủ dàn xếp bảo mật 12, và phản hồi kết quả dàn xếp tới máy chủ dàn xếp bảo mật 12 theo sự lựa chọn của người dùng. Yêu cầu dàn xếp bảo mật có thể bao gồm thông tin chẳng hạn như mục đích, thời gian, và vị trí của dữ liệu ứng dụng, sao cho người dùng có thể được yêu cầu xem có chấp nhận việc thu thập dữ liệu người dùng hay không, phân tích dữ liệu, và mở dữ liệu bằng cách sử dụng thiết bị mạng không dây. Môđun lựa chọn bảo mật có vai trò cung cấp giao diện tương tác người-máy tính lựa chọn được cho người dùng, sao cho người dùng có thể lựa chọn, bằng cách sử dụng phần mềm điện thoại di động hoặc bằng cách đăng nhập vào trang mạng dạng cổng thông tin điện tử của người khai thác, xem có mở dữ liệu của người dùng hay không, đó là, người dùng nhập ký hiệu nhận dạng người dùng của người dùng, chẳng hạn như địa chỉ điều khiển truy cập phương tiện (Media

Access Control, viết tắt là MAC), hoặc số nhận dạng thuê bao di động quốc tế (International Mobile Subscriber Identification Number, viết tắt là IMSI), để thông báo người khai thác rằng dữ liệu người dùng của người dùng không thể/có thể được sử dụng, và thông báo người khai thác phạm vi ứng dụng, khoảng thời gian, và phạm vi khu vực của dữ liệu người dùng.

Máy chủ ứng dụng 14 có vai trò hỗ trợ nhiều loại ứng dụng dịch vụ trong mạng chẳng hạn như mạng truyền thông không dây, Internet, hoặc mạng doanh nghiệp, trong đó các ứng dụng dịch vụ có thể là các ứng dụng mà cần sử dụng dữ liệu người dùng, chẳng hạn như ứng dụng cảnh báo thiên tai, ứng dụng quy hoạch giao thông, và ứng dụng tiếp thị chính xác. Máy chủ ứng dụng 14 gửi yêu cầu thu nhận thông tin không dây tới thiết bị phân tích và mở dữ liệu 11, trong đó yêu cầu thu nhận thông tin không dây được sử dụng để yêu cầu thu nhận dữ liệu người dùng tương ứng với ứng dụng dịch vụ.

Thiết bị tạo cấu hình và quản lý 15 được tạo cấu hình để quản lý thông tin cấu hình bảo mật. Thông tin cấu hình bảo mật bao gồm danh sách trắng hoặc danh sách đen, trong đó danh sách trắng được sử dụng để chỉ báo phạm vi của dữ liệu người dùng được phép mở cho ứng dụng dịch vụ, và danh sách đen được sử dụng để chỉ báo phạm vi của dữ liệu người dùng không được phép mở cho ứng dụng dịch vụ. Các phạm vi được chỉ báo bởi danh sách trắng và danh sách đen có thể là phạm vi người dùng, khoảng thời gian, phạm vi khu vực, và tương tự mà ở đó dữ liệu người dùng thuộc về. Dữ liệu người dùng được cho phép được thu thập và phân tích có thể được xác định theo danh sách trắng hoặc danh sách đen. Thiết bị tạo cấu hình và quản lý 15 gửi thông tin cấu hình bảo mật tới hệ thống phân tích và mở dữ liệu 11 hoặc thiết bị mạng không dây 16, sao cho hệ thống phân tích và mở dữ liệu 11 gửi, tới máy chủ ứng dụng 14, dữ liệu người dùng mà thuộc phạm vi được chỉ báo bởi danh sách trắng hoặc dữ liệu người dùng mà không thuộc phạm vi được chỉ báo bởi danh sách đen, hoặc thiết bị mạng không dây 16 chỉ thu thập dữ liệu người dùng mà thuộc phạm vi được chỉ báo bởi danh sách trắng hoặc dữ liệu người dùng mà không thuộc phạm vi được chỉ báo bởi danh sách đen.

Một cách tùy chọn, thiết bị tạo cấu hình và quản lý 15 có thể còn có các

chức năng chẳng hạn như quản lý nhật ký, duy trì và truy vấn thông tin cấu hình bảo mật, hoặc tương tự. Thiết bị tạo cấu hình và quản lý 15 cần thực hiện sự quản lý cấp phép đặc biệt đối với các chức năng duy trì thao tác này.

Thiết bị mạng không dây 16 được tạo cấu hình để tập hợp dữ liệu người dùng. Ngoài ra, thiết bị quản lý mạng không dây 16 có thể thu thập một cách tùy chọn dữ liệu người dùng theo thông tin cấu hình bảo mật được gửi bởi thiết bị tạo cấu hình và quản lý 15, hoặc có thể thu thập một cách tùy chọn dữ liệu người dùng theo quy tắc bảo vệ bảo mật được thu nhận sau khi thiết bị phân tích và mở dữ liệu 11 thực hiện sự dàn xếp bảo mật với UE 13. Thiết bị mạng không dây 16, ví dụ, có thể là bộ điều khiển trạm gốc (Base Station Controller, viết tắt là BSC), bộ điều khiển mạng radio (Radio Network Controller, viết tắt là RNC), hoặc NodeB cải tiến (Evolved NodeB, viết tắt là eNodeB). Thiết bị mạng không dây 16 có thể tương tác với thiết bị phân tích và mở dữ liệu 11, thu kết quả dàn xếp bảo mật được gửi bởi thiết bị phân tích và mở dữ liệu 11, và tập hợp dữ liệu người dùng theo kết quả dàn xếp bảo mật; thiết bị mạng không dây 16 có thể còn tương tác với thiết bị tạo cấu hình và quản lý 15, và tập hợp dữ liệu người dùng theo thông tin cấu hình bảo mật.

Trong hệ thống được thể hiện trên Fig.2, cấu hình bảo mật có thể được thực hiện giữa thiết bị phân tích và mở dữ liệu 11, thiết bị tạo cấu hình và quản lý 15, và thiết bị mạng không dây. Cấu hình bảo mật là cấu hình toàn cầu và chủ yếu được sử dụng để tạo cấu hình trước danh sách trắng hoặc danh sách đen mặc định, và có thể còn bao gồm thông tin cấu hình bảo mật khác. Fig.3 là lưu đồ báo hiệu của phương pháp tạo cấu hình bảo mật theo phương án của sáng chế, và thể hiện làm ví dụ phương pháp tạo cấu hình bảo mật. Phương pháp này bao gồm các bước:

S301. Thiết bị tạo cấu hình và quản lý 15 chuyển, tới thiết bị phân tích và mở dữ liệu 11, danh sách đen hoặc danh sách trắng để lọc dựa trên người dùng.

S301'. Thiết bị tạo cấu hình và quản lý 15 chuyển, tới thiết bị mạng không dây 16, danh sách đen hoặc danh sách trắng để lọc dựa trên người dùng.

Bước lọc dựa trên người dùng có thể được thiết đặt dựa vào địa chỉ MAC, IMSI, số ISDN thuê bao di động (Mobile Subscriber ISDN Number, viết tắt là

MSISDN), hoặc đối tượng tương tự của UE 13. Sau khi thu danh sách đen hoặc danh sách trắng mà được sử dụng để lọc dựa trên người dùng và mà được gửi bởi thiết bị tạo cấu hình và quản lý 15, thiết bị phân tích và mở dữ liệu 11 không phân tích hoặc mở dữ liệu người dùng của các người dùng này, hoặc phân tích và mở dữ liệu người dùng của các người dùng này (đó là, gửi dữ liệu người dùng tới máy chủ ứng dụng 14). Sau khi thu danh sách đen hoặc danh sách trắng mà được sử dụng để lọc dựa trên người dùng, thiết bị mạng không dây 16 không tập hợp hoặc thu thập dữ liệu người dùng của các người dùng này.

S302. Thiết bị tạo cấu hình và quản lý 15 chuyển, tới thiết bị phân tích và mở dữ liệu 11, danh sách đen hoặc danh sách trắng để lọc dựa trên thời gian.

S302'. Thiết bị tạo cấu hình và quản lý 15 chuyển, tới thiết bị mạng không dây 16, danh sách đen hoặc danh sách trắng để lọc dựa trên thời gian.

Sự hỗ trợ lọc dựa trên thời gian được thiết đặt theo năm, tháng, ngày, phút, hoặc tương tự. Sau khi thu danh sách đen hoặc danh sách trắng mà được sử dụng để lọc dựa trên thời gian và mà được gửi bởi thiết bị tạo cấu hình và quản lý 15, thiết bị phân tích và mở dữ liệu 11 không phân tích hoặc mở dữ liệu người dùng nằm trong các khoảng thời gian này, hoặc phân tích và mở dữ liệu người dùng nằm trong các khoảng thời gian này. Sau khi thu danh sách đen hoặc danh sách trắng để lọc dựa trên thời gian, thiết bị mạng không dây không tập hợp hoặc thu thập dữ liệu người dùng nằm trong các khoảng thời gian này.

S303. Thiết bị tạo cấu hình và quản lý 15 chuyển, tới thiết bị phân tích và mở dữ liệu 11, danh sách đen hoặc danh sách trắng để lọc dựa trên khu vực.

S303'. Thiết bị tạo cấu hình và quản lý 15 chuyển, tới thiết bị mạng không dây 16, danh sách đen hoặc danh sách trắng để lọc dựa trên khu vực.

Ký hiệu nhận dạng khu vực có thể là số nhận dạng ô (identity, viết tắt là ID), có thể là ký hiệu nhận dạng khu vực mà bao gồm nhiều điểm kinh độ và vĩ độ, hoặc tương tự. Sau khi thu danh sách đen hoặc danh sách trắng mà được sử dụng để lọc dựa trên khu vực và mà được gửi bởi thiết bị tạo cấu hình và quản lý 15, thiết bị phân tích và mở dữ liệu 11 không phân tích hoặc mở dữ liệu người dùng nằm trong các phạm vi khu vực này, hoặc phân tích và mở dữ liệu người dùng nằm trong các phạm vi khu vực này. Sau khi thu danh sách đen hoặc danh

sách trắng được thu nhận bằng cách lọc dựa trên người dùng, thiết bị mạng không dây không tập hợp hoặc thu thập dữ liệu người dùng nằm trong các phạm vi khu vực này.

S304. Thiết bị tạo cấu hình và quản lý 15 chuyển, tới thiết bị phân tích và mở dữ liệu 11, danh sách đen hoặc danh sách trắng dùng cho ứng dụng dịch vụ.

S304'. Thiết bị tạo cấu hình và quản lý 15 chuyển, tới thiết bị mạng không dây 16, danh sách đen hoặc danh sách trắng dùng cho ứng dụng dịch vụ.

Đối với một số ứng dụng điện thoại di động gải mạo, phần mềm nạp, hoặc tương tự, ứng dụng dịch vụ có thể được thiết đặt với danh sách đen hoặc danh sách trắng. Đối với ứng dụng mà có uy tín cao hơn và điểm số cao hơn, dữ liệu người dùng có thể được mở cho ứng dụng, và ứng dụng được thiết đặt nằm trong danh sách trắng. Tuy nhiên, đối với một số ứng dụng mà tiêu tốn lưu lượng như trong phần tình trạng kỹ thuật của sáng chế hoặc ứng dụng quảng cáo, dữ liệu người dùng bị ngăn không được mở cho các ứng dụng, và các ứng dụng được thiết đặt nằm trong danh sách đen. Thiết bị phân tích và mở dữ liệu 11 và thiết bị mạng không dây 16 có thể thực hiện xử lý tương ứng theo danh sách trắng hoặc danh sách đen.

Có thể được hiểu rằng các bước từ S301 (S301') đến S304 (S304') nêu trên là các bước tùy chọn, và không cần tạo cấu hình cho tất cả các trường hợp.

Ngoài ra, thiết bị tạo cấu hình và quản lý 15 có thể cũng chỉ tạo cấu hình thiết bị phân tích và mở dữ liệu 11, sao cho thiết bị phân tích và mở dữ liệu 11 có thể thực hiện, dựa vào thông tin cấu hình bảo mật, sự bảo vệ bảo mật của dữ liệu người dùng.

Ngoài ra, sự tương ứng giữa ứng dụng dịch vụ và quy tắc bảo vệ bảo mật theo phương pháp được thể hiện trên Fig.1 có thể cũng được tạo cấu hình trước bởi thiết bị tạo cấu hình và quản lý 15 trên thiết bị phân tích và mở dữ liệu 11.

Bảng 1 thể hiện ví dụ của quy tắc bảo vệ bảo mật, trong đó các loại khác của các ứng dụng dịch vụ tương ứng với các quy tắc bảo vệ bảo mật khác.

Bảng 1

Loại ứng dụng	Quy tắc bảo vệ bảo mật
Sự khẩn cấp, ví dụ, cảnh báo thiên tai	Thiết đặt quy tắc bảo vệ bảo mật trong đó quy trình bảo mật không cần được thực hiện
Sự phân tích nhóm, được sử dụng cho các dịch vụ công cộng, ví dụ, quy hoạch giao thông	Thiết đặt quy tắc bảo vệ bảo mật mà lệnh sử dụng kết quả dàn xếp bảo mật được lưu trữ trước
Thực hiện sự khai thác thương mại theo vị trí cá nhân, ví dụ, ứng dụng tiếp thị chính xác	Thiết đặt quy tắc bảo vệ bảo mật mà lệnh thực hiện sự dàn xếp bảo mật

Sự dàn xếp bảo mật là các thiết bị khác nhau xác định, bằng cách dàn xếp, các vấn đề liên quan đến bảo mật. Trong phương án này của sáng chế, kết quả dàn xếp bảo mật có thể được thu nhận bằng cách dàn xếp bảo mật, và kết quả dàn xếp bảo mật được sử dụng để lệnh xem có mở dữ liệu người dùng cho ứng dụng dịch vụ hay không.

Ví dụ, trong hệ thống được thể hiện trên Fig.2, sự dàn xếp bảo mật có thể được thực hiện giữa thiết bị phân tích và mở dữ liệu 11 và UE 13 bằng cách sử dụng máy chủ dàn xếp bảo mật 12. Fig.4 là lưu đồ báo hiệu của phương pháp dàn xếp bảo mật theo phương án của sáng chế. Các bước từ S402 đến S408 thể hiện quá trình trong đó thiết bị phân tích và mở dữ liệu 11 thực hiện sự dàn xếp bảo mật với UE 13 bằng cách sử dụng máy chủ dàn xếp bảo mật 12, và trong bước S401, thiết bị phân tích và mở dữ liệu 11 có thể được kích hoạt để bắt đầu sự dàn xếp bảo mật. Như được thể hiện trên Fig.4:

S401. Thiết bị phân tích và mở dữ liệu 11 thu yêu cầu thu nhận thông tin không dây được gửi bởi máy chủ ứng dụng 14.

Yêu cầu thu nhận thông tin không dây được sử dụng để yêu cầu thu nhận dữ liệu người dùng tương ứng với ứng dụng dịch vụ. Sau khi thu yêu cầu thu

nhận thông tin không dây, thiết bị phân tích và mở dữ liệu 11 có thể thu nhận quy tắc bảo vệ bảo mật tương ứng theo sự tương ứng được tạo cấu hình trước giữa ứng dụng dịch vụ và quy tắc bảo vệ bảo mật. Ví dụ, theo nội dung của bảng 1, nếu yêu cầu thu nhận thông tin không dây được sử dụng để yêu cầu thu nhận dữ liệu người dùng được yêu cầu bởi dịch vụ tiếp thị chính xác, quy tắc bảo vệ bảo mật được thu nhận bởi thiết bị phân tích và mở dữ liệu 11 là quy tắc bảo vệ bảo mật mà lệnh thực hiện sự dàn xếp bảo mật.

S402. Thiết bị phân tích và mở dữ liệu 11 gửi yêu cầu dàn xếp bảo mật tới máy chủ dàn xếp bảo mật 12 theo quy tắc bảo vệ bảo mật.

Yêu cầu dàn xếp bảo mật được sử dụng để yêu cầu thu nhận sự chỉ báo về việc xem có mở dữ liệu người dùng cho ứng dụng dịch vụ hay không.

Ví dụ, sau khi thiết bị phân tích và mở dữ liệu 11 thu được quy tắc bảo vệ bảo mật mà được sử dụng để lệnh thực hiện sự dàn xếp bảo mật, thiết bị phân tích và mở dữ liệu 11 có thể chuyển linh hoạt yêu cầu dàn xếp bảo mật tới máy chủ dàn xếp bảo mật 12, trong đó yêu cầu dàn xếp bảo mật có thể bao gồm nội dung chẳng hạn như ký hiệu nhận dạng người dùng, thông tin về ứng dụng dịch vụ mà yêu cầu dữ liệu người dùng, yêu cầu thông tin về việc xem có chấp nhận thu thập và phân tích dữ liệu người dùng hay không, yêu cầu thông tin về việc xem có chấp nhận mở dữ liệu người dùng cho ứng dụng dịch vụ hay không, phạm vi khu vực mà ở đó dữ liệu người dùng được yêu cầu thuộc về, khoảng thời gian mà ở đó dữ liệu người dùng được yêu cầu thuộc về, và sự sử dụng dữ liệu người dùng.

S403. Máy chủ dàn xếp bảo mật 12 chuyển tiếp yêu cầu dàn xếp bảo mật tới UE 13.

Sau khi thu yêu cầu dàn xếp bảo mật của thiết bị phân tích và mở dữ liệu 11, máy chủ dàn xếp bảo mật 12 có thể gửi yêu cầu dàn xếp bảo mật tới UE 13 theo cách thông báo dịch vụ thông báo ngắn hoặc sự hoạt động của trang mạng (Web).

S404. UE 13 thực hiện sự lựa chọn bảo mật.

Người dùng có thể lựa chọn xem có mở dữ liệu người dùng cho ứng dụng dịch vụ hay không, phạm vi khu vực trong đó dữ liệu người dùng được cho phép

để được sử dụng, khoảng thời gian trong đó dữ liệu người dùng được cho phép để được sử dụng, hoặc tương tự.

S405. UE 13 gửi kết quả dàn xếp bảo mật tới máy chủ dàn xếp bảo mật 12.

UE 13 có thể gửi kết quả dàn xếp bảo mật tới máy chủ dàn xếp bảo mật 12 theo cách thông báo dịch vụ thông báo ngắn hoặc sự hoạt động của trang mạng (Web). Kết quả dàn xếp bảo mật chủ yếu được sử dụng để lệnh xem có mở dữ liệu người dùng cho ứng dụng dịch vụ hay không, và có thể còn bao gồm thông tin khác được sử dụng cho quy trình bảo mật.

S406. Máy chủ dàn xếp bảo mật 12 gửi kết quả dàn xếp bảo mật tới thiết bị phân tích và mở dữ liệu 11.

Ví dụ, kết quả dàn xếp bảo mật có thể bao gồm nội dung chẳng hạn như ký hiệu nhận dạng người dùng, xem có cho phép thu thập và phân tích dữ liệu người dùng hay không, xem có mở dữ liệu người dùng cho ứng dụng dịch vụ hay không, phạm vi khu vực trong đó dữ liệu người dùng được cho phép để được sử dụng, khoảng thời gian trong đó dữ liệu người dùng được cho phép để được sử dụng, thông tin về việc xem sự dàn xếp bảo mật có cần được thực hiện lại theo chu kỳ với người dùng hay không.

S407. Thiết bị phân tích và mở dữ liệu 11 thu nhận kết quả dàn xếp bảo mật.

Ngoài ra, sau khi thu nhận kết quả dàn xếp bảo mật, thiết bị phân tích và mở dữ liệu 11 có thể lưu kết quả dàn xếp bảo mật, hoặc có thể phản hồi yêu cầu thu nhận thông tin không dây theo kết quả dàn xếp bảo mật.

Do đó, thiết bị phân tích và mở dữ liệu 11 thu nhận thành công kết quả dàn xếp bảo mật được thu nhận bằng cách thực hiện sự dàn xếp bảo mật với UE 13.

Một cách tùy chọn, máy chủ dàn xếp bảo mật 12 có thể gửi thông báo xác nhận tới UE 13 để thông báo UE 13 rằng sự dàn xếp bảo mật đã hoàn thành. Ví dụ:

S408. Máy chủ dàn xếp bảo mật 12 gửi thông báo xác nhận tới UE 13.

Fig.4 thể hiện quá trình của sự dàn xếp bảo mật được kích hoạt bởi yêu

cầu thu nhận thông tin không dây. Khác với Fig.4, trong phương pháp dàn xếp bảo mật được thể hiện trên Fig.5, máy chủ dàn xếp bảo mật 12 bắt đầu linh hoạt sự dàn xếp bảo mật.

Như được thể hiện trên Fig.5:

S501. Máy chủ dàn xếp bảo mật 12 thực hiện sự bắt đầu bảo mật.

Trong phương pháp này, khi người dùng đăng ký cổng vào mạng, hoặc sau khi người dùng đăng ký ứng dụng dịch vụ mới, máy chủ dàn xếp bảo mật có thể gửi linh hoạt báo cáo bảo mật tới UE 13. Đối với chức năng và nội dung của báo cáo bảo mật, sự tham khảo có thể được thực hiện cho nội dung liên quan của yêu cầu dàn xếp bảo mật trên Fig.4, và các chi tiết không được mô tả lại ở đây.

S502. UE 13 thực hiện sự lựa chọn bảo mật.

Đối với nội dung liên quan của bước này, sự tham khảo có thể được thực hiện cho nội dung liên quan của S404 trên Fig.4.

S503. UE 13 gửi kết quả dàn xếp bảo mật tới máy chủ dàn xếp bảo mật 12.

Đối với nội dung liên quan của bước này, sự tham khảo có thể được thực hiện cho nội dung liên quan của S405 trên Fig.4.

S504. Máy chủ dàn xếp bảo mật 12 gửi kết quả dàn xếp bảo mật tới thiết bị phân tích và mở dữ liệu 11.

Đối với nội dung liên quan của bước này, sự tham khảo có thể được thực hiện cho nội dung liên quan của S406 trên Fig.4.

S505. Thiết bị phân tích và mở dữ liệu 11 lưu lại kết quả dàn xếp bảo mật.

Sau khi thiết bị phân tích và mở dữ liệu 11 lưu lại kết quả dàn xếp bảo mật, khi quy tắc bảo vệ bảo mật là sử dụng kết quả dàn xếp bảo mật được lưu trữ trước, thiết bị phân tích và mở dữ liệu 11 có thể thực hiện trực tiếp quy trình bảo mật cho dữ liệu người dùng bằng cách sử dụng kết quả dàn xếp bảo mật đã được lưu.

S506. Máy chủ dàn xếp bảo mật 12 gửi thông báo xác nhận tới UE 13.

Bước này là bước tùy chọn, và sự tham khảo có thể được thực hiện cho nội dung liên quan của S408 trên Fig.4.

Fig.5 thể hiện quá trình trong đó máy chủ dàn xếp bảo mật 12 bắt đầu linh

hoạt sự dàn xếp bảo mật. Khác với Fig.5, quá trình dàn xếp bảo mật được thể hiện trên Fig.6 được bắt đầu linh hoạt bởi thiết bị phân tích và mở dữ liệu 11, trong đó thiết bị phân tích và mở dữ liệu có thể bắt đầu theo chu kỳ sự dàn xếp bảo mật với UE 13, để thu nhận lại kết quả dàn xếp bảo mật được thu nhận sau khi dàn xếp với UE 13.

Như được thể hiện trên Fig.6:

S601. Thiết bị phân tích và mở dữ liệu 11 gửi yêu cầu dàn xếp bảo mật tới máy chủ dàn xếp bảo mật 12.

Thiết bị phân tích và mở dữ liệu 11 có thể bắt đầu theo chu kỳ và linh hoạt sự dàn xếp bảo mật với UE 13 theo thông tin chỉ báo dàn xếp bảo mật theo chu kỳ. Quy tắc bảo vệ bảo mật tương ứng với ứng dụng dịch vụ, cấu hình bảo mật được chuyển bởi thiết bị tạo cấu hình và quản lý 15, hoặc kết quả dàn xếp bảo mật được phản hồi bởi UE 13 có thể bao gồm thông tin chỉ báo dàn xếp bảo mật theo chu kỳ. Ngoài ra, kết quả dàn xếp bảo mật có thể được thiết đặt với khoảng thời gian hiệu lực, và khi khoảng thời gian hiệu lực kết thúc, thiết bị phân tích và mở dữ liệu 11 có thể cũng bắt đầu linh hoạt sự dàn xếp bảo mật.

Đối với nội dung liên quan của yêu cầu dàn xếp bảo mật, sự tham khảo có thể được thực hiện cho nội dung liên quan của S402 trên Fig.4.

S602. Máy chủ dàn xếp bảo mật 12 chuyển tiếp yêu cầu dàn xếp bảo mật tới UE 13.

Đối với nội dung liên quan của bước này, sự tham khảo có thể được thực hiện cho nội dung liên quan của S403 trên Fig.4.

S603. UE 13 thực hiện sự lựa chọn bảo mật.

Đối với nội dung liên quan của bước này, sự tham khảo có thể được thực hiện cho nội dung liên quan của S404 trên Fig.4.

S604. UE 13 gửi kết quả dàn xếp bảo mật tới máy chủ dàn xếp bảo mật 12.

Đối với nội dung liên quan của bước này, sự tham khảo có thể được thực hiện cho nội dung liên quan của S405 trên Fig.4.

S605. Máy chủ dàn xếp bảo mật 12 gửi kết quả dàn xếp bảo mật tới thiết bị phân tích và mở dữ liệu 11.

Đối với nội dung liên quan của bước này, sự tham khảo có thể được thực hiện cho nội dung liên quan của S406 trên Fig.4.

S606. Thiết bị phân tích và mở dữ liệu 11 thu nhận kết quả dàn xếp bảo mật.

Đối với nội dung liên quan của bước này, sự tham khảo có thể được thực hiện cho nội dung liên quan của S407 trên Fig.4.

S607. Máy chủ dàn xếp bảo mật 12 gửi thông báo xác nhận tới UE 13.

Bước này là bước tùy chọn, và đối với nội dung liên quan của nó, sự tham khảo có thể được thực hiện cho nội dung liên quan của S408 trên Fig.4.

Người có hiểu biết trung bình trong lĩnh vực kỹ thuật sẽ biết rằng sự dàn xếp bảo mật có thể cũng được bắt đầu linh hoạt bởi UE 13. Ví dụ, UE 13 bắt đầu yêu cầu kích hoạt dàn xếp bảo mật tới máy chủ dàn xếp bảo mật 12, để kích hoạt máy chủ dàn xếp bảo mật 12 để gửi yêu cầu dàn xếp bảo mật tới UE 13, và các chi tiết không được mô tả lại ở đây.

Để mô tả phương pháp xử lý dữ liệu người dùng được đề xuất trong phương án của sáng chế rõ ràng hơn, phần mô tả riêng rẽ sau đây cho ứng dụng tiếp thị chính xác, ứng dụng quy hoạch giao thông, và ứng dụng cảnh báo thiên tai làm các ví dụ và dựa vào hệ thống được thể hiện trên Fig.2.

Fig.7 thể hiện lưu đồ của phương pháp xử lý dữ liệu người dùng theo phương án của sáng chế bằng cách sử dụng ví dụ trong đó ứng dụng tiếp thị chính xác yêu cầu thu nhận dữ liệu người dùng. Ứng dụng tiếp thị chính xác là ứng dụng dịch vụ mà thực hiện sự khai thác thương mại, và ứng dụng dịch vụ chủ yếu thu nhận dữ liệu người dùng chẳng hạn như vị trí thông tin người dùng, để thực hiện các giới thiệu quảng cáo chính xác. Đối với loại này của ứng dụng dịch vụ, quy tắc bảo vệ bảo mật mà lệnh thực hiện sự dàn xếp bảo mật trong bảng 1 có thể được sử dụng. Sự tương ứng giữa ứng dụng tiếp thị chính xác và quy tắc bảo vệ bảo mật có thể được tạo cấu hình trước bởi thiết bị tạo cấu hình và quản lý 15 trên thiết bị phân tích và mở dữ liệu 11.

Như được thể hiện trên Fig.7:

S701. Máy chủ ứng dụng 14 gửi yêu cầu thu nhận thông tin không dây tới thiết bị phân tích và mở dữ liệu 11.

Yêu cầu thu nhận thông tin không dây có thể bao gồm ứng dụng ký hiệu nhận dạng của ứng dụng tiếp thị chính xác, ký hiệu nhận dạng người dùng của UE 13 mà ở đó dữ liệu người dùng được yêu cầu thuộc về, và loại của dữ liệu người dùng được yêu cầu (ví dụ, thông tin vị trí và chất lượng tín hiệu không dây).

S702. Thiết bị phân tích và mở dữ liệu 11 thu nhận quy tắc bảo vệ bảo mật tương ứng với ứng dụng tiếp thị chính xác.

Quy tắc bảo vệ bảo mật được sử dụng để lệnh thực hiện sự dàn xếp bảo mật.

S703. Thiết bị phân tích và mở dữ liệu 11 thực hiện sự dàn xếp bảo mật với UE 13 thông qua máy chủ dàn xếp bảo mật 12, để thu nhận kết quả dàn xếp bảo mật.

Đối với quy trình dàn xếp bảo mật, sự tham khảo có thể được thực hiện cho nội dung liên quan của sự dàn xếp bảo mật quá trình được thể hiện trên Fig.4.

S704. Thiết bị phân tích và mở dữ liệu 11 xác định rằng kết quả dàn xếp bảo mật được sử dụng để lệnh mở dữ liệu người dùng cho ứng dụng tiếp thị chính xác.

Sau khi xác định để mở dữ liệu người dùng cho ứng dụng tiếp thị chính xác, thiết bị phân tích và mở dữ liệu 11 có thể cung cấp dữ liệu người dùng cho ứng dụng tiếp thị chính xác. Ở đây, thiết bị phân tích và mở dữ liệu 11 có thể gửi trực tiếp dữ liệu người dùng tới máy chủ ứng dụng 14.

S705. Thiết bị phân tích và mở dữ liệu 11 gửi dữ liệu người dùng của UE 13 tới máy chủ ứng dụng 14.

Dữ liệu người dùng có thể mang thông tin chẳng hạn như ký hiệu nhận dạng của UE 13, và thông tin vị trí và chất lượng tín hiệu không dây mà là của UE 13.

Ngoài ra, nếu dữ liệu người dùng được yêu cầu không xuất hiện trong thiết bị phân tích và mở dữ liệu 11 hoặc dữ liệu người dùng được lưu trữ trong thiết bị phân tích và mở dữ liệu 11 là tương đối cũ, thiết bị phân tích và mở dữ liệu có thể còn gửi việc thu thập dữ liệu thông tin chỉ báo tới thiết bị mạng

không dây 16. Sau khi thu việc thu thập dữ liệu thông tin chỉ báo, thiết bị mạng không dây 16 thu thập dữ liệu người dùng được yêu cầu bởi ứng dụng tiếp thị chính xác, và gửi dữ liệu người dùng được thu thập tới thiết bị phân tích và mở dữ liệu 11.

Do đó, ứng dụng tiếp thị chính xác thu được chính xác dữ liệu người dùng của UE 13.

Một cách tùy chọn, khi thiết bị phân tích và mở dữ liệu 11 xác định rằng kết quả dàn xếp bảo mật được sử dụng để lệnh không mở dữ liệu người dùng cho ứng dụng tiếp thị chính xác, thiết bị phân tích và mở dữ liệu 11 không gửi dữ liệu người dùng của UE 13 tới ứng dụng dịch vụ. Trong trường hợp này, S706 có thể được thực hiện.

S706. Thiết bị phân tích và mở dữ liệu 11 gửi thông tin chỉ báo tới máy chủ ứng dụng 14, trong đó thông tin chỉ báo được sử dụng để chỉ báo rằng dữ liệu người dùng không thể được thu nhận.

Theo phương pháp xử lý dữ liệu người dùng được thể hiện trên Fig.7, khi ứng dụng tiếp thị chính xác yêu cầu thu nhận dữ liệu người dùng của UE 13, UE 13 có thể thực hiện sự xác nhận, và chỉ khi UE 13 cho phép mở dữ liệu người dùng cho ứng dụng tiếp thị chính xác, dữ liệu người dùng của UE 13 được đề xuất cho ứng dụng tiếp thị chính xác, mà nâng cao tính bảo mật của dữ liệu người dùng của UE 13.

Fig.8 thể hiện lưu đồ của phương pháp xử lý dữ liệu người dùng theo phương án của sáng chế bằng cách sử dụng ví dụ trong đó ứng dụng quy hoạch giao thông yêu cầu thu nhận dữ liệu người dùng. Ứng dụng quy hoạch giao thông là ứng dụng dịch vụ để quản lý dịch vụ công cộng, và ứng dụng dịch vụ chủ yếu thu nhận dữ liệu người dùng chẳng hạn như thông tin phân tích thống kê của tuyến di chuyển người dùng, để quyết định về việc quy hoạch giao thông. Đối với loại này của ứng dụng dịch vụ, quy tắc bảo vệ bảo mật mà lệnh sử dụng kết quả dàn xếp bảo mật được lưu trữ trước trong bảng 1 có thể được sử dụng. Sự tương ứng giữa ứng dụng quy hoạch giao thông và quy tắc bảo vệ bảo mật có thể được tạo cấu hình trước bởi thiết bị tạo cấu hình và quản lý 15 trên thiết bị phân tích và mở dữ liệu 11.

Như được thể hiện trên Fig.8:

S801. UE 13, máy chủ dàn xếp bảo mật 12, và thiết bị phân tích và mở dữ liệu 11 thực hiện sự dàn xếp bảo mật.

Đối với quy trình dàn xếp bảo mật, sự tham khảo có thể được thực hiện cho sự dàn xếp bảo mật quá trình được thể hiện trên Fig.5. Ví dụ, sự dàn xếp bảo mật quá trình trong S801 có thể được thực hiện khi người dùng đăng ký cổng vào mạng, hoặc có thể được thực hiện sau khi ứng dụng quy hoạch giao thông được triển khai trên máy chủ ứng dụng 14.

Sau khi UE 13 đăng ký cổng vào mạng, khi ứng dụng quy hoạch giao thông cần yêu cầu người dùng, ứng dụng quy hoạch giao thông có thể bắt đầu yêu cầu tới thiết bị phân tích và mở dữ liệu 11 để thu nhận dữ liệu người dùng, mà được thể hiện như sau:

S802. Máy chủ ứng dụng 14 gửi yêu cầu thu nhận thông tin không dây tới thiết bị phân tích và mở dữ liệu 11.

Yêu cầu có thể bao gồm nội dung chẳng hạn như ứng dụng ký hiệu nhận dạng của ứng dụng quy hoạch giao thông, loại của dữ liệu người dùng (ví dụ, thông tin phân tích thống kê của tuyến di chuyển người dùng), và phạm vi người dùng mà ở đó dữ liệu người dùng thuộc về (ví dụ, người dùng nằm trong khu vực hành chính A).

S803. Thiết bị phân tích và mở dữ liệu 11 thu nhận quy tắc bảo vệ bảo mật tương ứng với ứng dụng quy hoạch giao thông.

Quy tắc lệnh để sử dụng kết quả dàn xếp bảo mật được lưu trữ trước.

Khi kết quả dàn xếp bảo mật được sử dụng để lệnh để cung cấp dữ liệu người dùng cho ứng dụng quy hoạch giao thông, các bước sau đây được bao gồm:

S804. Thiết bị phân tích và mở dữ liệu 11 xác định rằng dữ liệu người dùng của UE 13 được bao gồm trong phân tích thống kê của tuyến di chuyển người dùng.

Sau khi được xác định rằng dữ liệu người dùng của UE 13 được bao gồm trong phân tích thống kê của tuyến di chuyển người dùng, dữ liệu người dùng của UE 13 có thể được cung cấp cho ứng dụng quy hoạch giao thông, đó là, dữ

liệu người dùng của UE 13 được cho phép được bao gồm trong phân tích thống kê của tuyến di chuyển người dùng.

S805. Thiết bị phân tích và mở dữ liệu 11 thực hiện phân tích thống kê của tuyến di chuyển người dùng theo dữ liệu người dùng liên quan, để thu nhận kết quả phân tích thống kê.

S806. Thiết bị phân tích và mở dữ liệu 11 trả kết quả phân tích thống kê về máy chủ ứng dụng 14.

Một cách tùy chọn, khi kết quả dàn xếp bảo mật được sử dụng để lệnh không cung cấp dữ liệu người dùng cho ứng dụng quy hoạch giao thông, thiết bị phân tích và mở dữ liệu 11 xác định rằng dữ liệu người dùng của UE 13 không được bao gồm trong phân tích thống kê của tuyến di chuyển người dùng. Do đó, khi phân tích thống kê của tuyến di chuyển người dùng được thực hiện, dữ liệu người dùng của UE 13 không được sử dụng là một ví dụ, và kết quả phân tích thống kê được thu nhận bởi thiết bị phân tích và mở dữ liệu 11 cũng không bao gồm dữ liệu người dùng của UE 13.

Theo phương pháp xử lý dữ liệu người dùng được thể hiện trên Fig.8, trước khi ứng dụng quy hoạch giao thông yêu cầu thu nhận dữ liệu người dùng, UE 13 và thiết bị phân tích và mở dữ liệu 11 thực hiện sự dàn xếp bảo mật trước và lưu kết quả dàn xếp bảo mật, và khi ứng dụng quy hoạch giao thông cần gọi dữ liệu người dùng, kết quả dàn xếp bảo mật được lưu trữ trước có thể được thu nhận trực tiếp, và việc xem có cung cấp dữ liệu người dùng của UE 13 cho ứng dụng quy hoạch giao thông hay không được xác định theo kết quả dàn xếp bảo mật, mà có thể nâng cao tính an toàn của dữ liệu người dùng ngoài việc mở đúng dữ liệu người dùng.

Fig.9 thể hiện lưu đồ của phương pháp xử lý dữ liệu người dùng theo phương án của sáng chế bằng cách sử dụng ví dụ trong đó ứng dụng cảnh báo thiên tai yêu cầu thu nhận dữ liệu người dùng. Ứng dụng cảnh báo thiên tai là ứng dụng mà đối phó tình trạng khẩn cấp, và ứng dụng chủ yếu được sử dụng để thu nhận dữ liệu người dùng của người dùng quanh địa điểm thiên tai, để thực hiện cảnh báo thiên tai. Đối với loại này của ứng dụng dịch vụ, quy tắc bảo vệ bảo mật trong đó quy trình bảo mật không cần được thực hiện trong bảng 1 có

thể được sử dụng. Sự tương ứng giữa ứng dụng cảnh báo thiên tai và quy tắc bảo vệ bảo mật có thể được tạo cấu hình trước bởi thiết bị tạo cấu hình và quản lý 15 trên thiết bị phân tích và mở dữ liệu 11.

Như được thể hiện trên Fig.9:

S901. Ứng dụng cảnh báo thiên tai nhận biết rằng có rủi ro thiên tai ở địa điểm A.

S902. Máy chủ ứng dụng 14 gửi yêu cầu thu nhận thông tin không dây tới thiết bị phân tích và mở dữ liệu 11.

Yêu cầu có thể mang nội dung chẳng hạn như ứng dụng ký hiệu nhận dạng của ứng dụng cảnh báo thiên tai, phạm vi người dùng mà ở đó dữ liệu người dùng thuộc về (ví dụ, người dùng nằm trong 10 kilomét từ địa điểm A), và loại của dữ liệu người dùng (ví dụ, khoảng cách giữa người dùng và địa điểm A).

S903. Thiết bị phân tích và mở dữ liệu 11 thu nhận quy tắc bảo vệ bảo mật tương ứng với ứng dụng cảnh báo thiên tai.

Quy tắc bảo vệ bảo mật chỉ báo rằng quy trình bảo mật không cần được thực hiện.

S904. Thiết bị phân tích và mở dữ liệu 11 gửi dữ liệu người dùng tới máy chủ ứng dụng 14.

Do quy tắc bảo vệ bảo mật chỉ báo rằng quy trình bảo mật không cần được thực hiện, thiết bị phân tích và mở dữ liệu 11 có thể cung cấp trực tiếp dữ liệu người dùng của UE 13 cho ứng dụng cảnh báo thiên tai.

S905. Ứng dụng cảnh báo thiên tai thực hiện quá trình tiếp theo được thu dữ liệu người dùng.

Theo phương pháp xử lý dữ liệu người dùng được thể hiện trên Fig.9, quy tắc bảo vệ bảo mật trong đó quy trình bảo mật không cần được thực hiện được thiết đặt cho ứng dụng cảnh báo thiên tai, mà có thể giúp ứng dụng cảnh báo thiên tai dễ dàng thu được nhanh chóng dữ liệu người dùng được yêu cầu, và thể hiện việc mở đúng dữ liệu người dùng.

Để thực hiện các phương pháp được thể hiện trên Fig.1, và Fig.2 tới Fig.9, phương án của sáng chế còn đề xuất thiết bị xử lý dữ liệu người dùng, và thiết bị

có thể được tích hợp trong thiết bị phân tích và mở dữ liệu 11.

Như được thể hiện trên Fig.10, thiết bị bao gồm: bộ phận thu 11, bộ phận xác định quy tắc 12, và bộ phận xử lý bảo mật 13, trong đó bộ phận thu 11 được tạo cấu hình để thu yêu cầu thu nhận thông tin không dây được gửi bởi thiết bị thành phần mạng, trong đó yêu cầu thu nhận thông tin không dây được sử dụng để yêu cầu thu nhận dữ liệu người dùng tương ứng với ứng dụng dịch vụ; bộ phận xác định quy tắc 12 được tạo cấu hình để xác định, theo ứng dụng dịch vụ và sự tương ứng giữa ứng dụng dịch vụ và quy tắc bảo vệ bảo mật, quy tắc bảo vệ bảo mật tương ứng với ứng dụng dịch vụ; và bộ phận xử lý bảo mật 13 được tạo cấu hình để: khi quy tắc bảo vệ bảo mật được sử dụng để lệnh thực hiện quy trình bảo mật, thực hiện quy trình bảo mật cho dữ liệu người dùng theo quy tắc bảo vệ bảo mật.

Đối với cơ cấu dùng để thực hiện việc xử lý dữ liệu người dùng bởi thiết bị, sự tham khảo có thể được thực hiện cho các phương pháp được thể hiện trên Fig.1, và Fig.2 tới Fig.9, và các nguyên lý thực hiện và các hiệu quả kỹ thuật của thiết bị tương tự với chúng của các phương pháp, và các chi tiết không được mô tả lại ở đây.

Theo thiết bị xử lý dữ liệu người dùng được thể hiện trên Fig.10, đối với các ứng dụng dịch vụ khác, các quy tắc bảo vệ bảo mật tương ứng với các ứng dụng dịch vụ khác có thể được xác định, và quy trình bảo mật được thực hiện cho dữ liệu người dùng theo các quy tắc bảo vệ bảo mật, mà có thể nâng cao tính an toàn của dữ liệu người dùng ngoài việc mở đúng dữ liệu người dùng.

Trong cách thực hiện tùy chọn, dựa vào thiết bị được thể hiện trên Fig.10, phương án của sáng chế còn đề xuất thiết bị xử lý dữ liệu người dùng khác nữa. Thiết bị xử lý dữ liệu người dùng được thể hiện trên Fig.11 cũng bao gồm bộ phận thu 11, bộ phận xác định quy tắc 12, và bộ phận xử lý bảo mật 13. Ngoài ra, bộ phận xử lý bảo mật của thiết bị xử lý dữ liệu người dùng được thể hiện trên Fig.11 bao gồm bộ phận thu nhận kết quả dàn xếp 131 và bộ phận xử lý kết quả dàn xếp 132, trong đó bộ phận thu nhận kết quả dàn xếp 131 được tạo cấu hình để: khi quy tắc bảo vệ bảo mật được sử dụng để lệnh thực hiện sự dàn xếp bảo mật, thực hiện, theo quy tắc bảo vệ bảo mật, sự dàn xếp bảo mật với thiết bị

người dùng tương ứng với dữ liệu người dùng, để thu nhận kết quả dàn xếp bảo mật; và bộ phận xử lý kết quả dàn xếp 132 được tạo cấu hình để: khi kết quả dàn xếp bảo mật được sử dụng để lệnh mở dữ liệu người dùng cho ứng dụng dịch vụ, cung cấp dữ liệu người dùng cho ứng dụng dịch vụ; hoặc khi kết quả dàn xếp bảo mật được sử dụng để lệnh không mở dữ liệu người dùng cho ứng dụng dịch vụ, gửi thông tin chỉ báo tới thiết bị thành phần mạng, trong đó thông tin chỉ báo được sử dụng để chỉ báo rằng dữ liệu người dùng không thể được thu nhận.

Ngoài ra, bộ phận thu nhận kết quả dàn xếp 131 được tạo cấu hình riêng biệt để: gửi yêu cầu dàn xếp bảo mật tới thiết bị người dùng, trong đó yêu cầu dàn xếp bảo mật được sử dụng để yêu cầu thu nhận sự chỉ báo về việc xem có mở dữ liệu người dùng cho ứng dụng dịch vụ hay không; và thu phản hồi yêu cầu dàn xếp bảo mật được gửi bởi thiết bị người dùng, trong đó phản hồi yêu cầu dàn xếp bảo mật bao gồm kết quả dàn xếp bảo mật.

Ngoài ra, bộ phận thu nhận kết quả dàn xếp 131 còn được tạo cấu hình để: khi quy tắc bảo vệ bảo mật được sử dụng để lệnh sử dụng kết quả dàn xếp bảo mật được lưu trữ trước, thu nhận trực tiếp kết quả dàn xếp bảo mật được lưu trữ trước theo quy tắc bảo vệ bảo mật; và bộ phận xử lý kết quả dàn xếp 132 được tạo cấu hình để: khi kết quả dàn xếp bảo mật được sử dụng để lệnh mở dữ liệu người dùng cho ứng dụng dịch vụ, cung cấp dữ liệu người dùng cho ứng dụng dịch vụ; hoặc khi kết quả dàn xếp bảo mật được sử dụng để lệnh không mở dữ liệu người dùng cho ứng dụng dịch vụ, gửi thông tin chỉ báo tới thiết bị thành phần mạng, trong đó thông tin chỉ báo được sử dụng để chỉ báo rằng dữ liệu người dùng không thể được thu nhận.

Ngoài ra, bộ phận thu nhận kết quả dàn xếp 131 còn được tạo cấu hình để: trước khi bộ phận thu 11 thu yêu cầu thu nhận thông tin không dây được gửi bởi thiết bị thành phần mạng, thu kết quả dàn xếp bảo mật được gửi bởi thiết bị người dùng, và lưu kết quả dàn xếp bảo mật.

Ngoài ra, bộ phận xử lý bảo mật 13 còn được tạo cấu hình để: khi quy tắc bảo vệ bảo mật được sử dụng để lệnh không thực hiện quy trình bảo mật, cung cấp dữ liệu người dùng cho ứng dụng dịch vụ.

Ngoài ra, bộ phận thu 11 còn được tạo cấu hình để thu thông tin cấu hình

bảo mật, trong đó thông tin cấu hình bảo mật bao gồm danh sách trắng hoặc danh sách đen, danh sách trắng được sử dụng để chỉ báo phạm vi của dữ liệu người dùng được phép mở cho ứng dụng dịch vụ, và danh sách đen được sử dụng để chỉ báo phạm vi của dữ liệu người dùng không được phép mở cho ứng dụng dịch vụ. Khi bộ phận xử lý kết quả dàn xếp được tạo cấu hình để cung cấp dữ liệu người dùng cho ứng dụng dịch vụ, bộ phận xử lý bảo mật 13 được tạo cấu hình riêng biệt để cung cấp dữ liệu người dùng cho ứng dụng dịch vụ, trong đó dữ liệu người dùng thuộc về phạm vi được chỉ báo bởi danh sách trắng hoặc không thuộc về phạm vi được chỉ báo bởi danh sách đen.

Thiết bị xử lý dữ liệu người dùng được thể hiện trên Fig.11 có thể được tạo cấu hình để thực hiện các phương pháp được thể hiện trên Fig.1, và Fig.2 tới Fig.9, và các nguyên lý thực hiện của thiết bị và các hiệu quả kỹ thuật được tạo ra bởi thiết bị tương tự với chúng của các phương pháp, và các chi tiết không được mô tả lại ở đây.

Theo thiết bị xử lý dữ liệu người dùng được thể hiện trên Fig.11, đối với các ứng dụng dịch vụ khác, các quy tắc bảo vệ bảo mật tương ứng với các ứng dụng dịch vụ khác có thể được xác định, và quy trình bảo mật được thực hiện cho dữ liệu người dùng theo các quy tắc bảo vệ bảo mật, mà có thể nâng cao tính an toàn của dữ liệu người dùng ngoài việc mở đúng dữ liệu người dùng.

Trong cách thực hiện tùy chọn, các thiết bị xử lý dữ liệu người dùng được thể hiện trên Fig.10 và Fig.11 có thể được thực hiện bởi phần cứng, ví dụ, thiết bị xử lý dữ liệu người dùngs được thể hiện trên Fig.12 và Fig.13, và các thiết bị có thể cũng được tích hợp vào trong thiết bị phân tích và mở dữ liệu.

Như được thể hiện trên Fig.12, thiết bị xử lý dữ liệu người dùng có thể bao gồm: bộ thu 11 và bộ xử lý 12, trong đó bộ thu 11 được tạo cấu hình để thu yêu cầu thu nhận thông tin không dây được gửi bởi thiết bị thành phần mạng, trong đó yêu cầu thu nhận thông tin không dây được sử dụng để yêu cầu thu nhận dữ liệu người dùng tương ứng với ứng dụng dịch vụ; và bộ xử lý 12 được tạo cấu hình để: xác định, theo ứng dụng dịch vụ và sự tương ứng giữa ứng dụng dịch vụ và quy tắc bảo vệ bảo mật, quy tắc bảo vệ bảo mật tương ứng với ứng dụng dịch vụ, và khi quy tắc bảo vệ bảo mật được sử dụng để lệnh thực hiện quy

trình bảo mật, thực hiện quy trình bảo mật cho dữ liệu người dùng theo quy tắc bảo vệ bảo mật.

Đối với cơ cấu dùng để thực hiện việc xử lý dữ liệu người dùng bởi thiết bị xử lý dữ liệu người dùng được thể hiện trên Fig.12, sự tham khảo có thể được thực hiện cho các phương pháp được thể hiện trên Fig.1, và Fig.2 tới Fig.9, và các nguyên lý thực hiện và các hiệu quả kỹ thuật của thiết bị tương tự với chúng của các phương pháp, và các chi tiết không được mô tả lại ở đây.

Fig.13 là sơ đồ cấu trúc giản lược của thiết bị xử lý dữ liệu người dùng khác theo phương án của sáng chế. Như được thể hiện trên Fig.13, dựa vào thiết bị xử lý dữ liệu người dùng được thể hiện trên Fig.12, thiết bị còn bao gồm bộ truyền 13.

Khi quy tắc bảo vệ bảo mật được sử dụng để lệnh thực hiện quy trình bảo mật cụ thể là: quy tắc bảo vệ bảo mật được sử dụng để lệnh thực hiện sự dàn xếp bảo mật, bộ truyền 13 được tạo cấu hình để gửi yêu cầu dàn xếp bảo mật tới thiết bị người dùng, trong đó yêu cầu dàn xếp bảo mật được sử dụng để yêu cầu thu nhận sự chỉ báo về việc xem có mở dữ liệu người dùng cho ứng dụng dịch vụ hay không; bộ thu 11 được tạo cấu hình để thu phản hồi yêu cầu dàn xếp bảo mật được gửi bởi thiết bị người dùng, trong đó phản hồi yêu cầu dàn xếp bảo mật bao gồm kết quả dàn xếp bảo mật; và bộ truyền 13 còn được tạo cấu hình để: khi kết quả dàn xếp bảo mật được sử dụng để lệnh mở dữ liệu người dùng cho ứng dụng dịch vụ, cung cấp dữ liệu người dùng cho ứng dụng dịch vụ; hoặc khi kết quả dàn xếp bảo mật được sử dụng để lệnh không mở dữ liệu người dùng cho ứng dụng dịch vụ, gửi thông tin chỉ báo tới thiết bị thành phần mạng, trong đó thông tin chỉ báo được sử dụng để chỉ báo rằng dữ liệu người dùng không thể được thu nhận; hoặc

khi quy tắc bảo vệ bảo mật được sử dụng để lệnh thực hiện quy trình bảo mật cụ thể là: quy tắc bảo vệ bảo mật được sử dụng để lệnh sử dụng kết quả dàn xếp bảo mật được lưu trữ trước, bộ truyền 13 được tạo cấu hình để: khi kết quả dàn xếp bảo mật được lưu trữ trước được sử dụng để lệnh mở dữ liệu người dùng cho ứng dụng dịch vụ, cung cấp dữ liệu người dùng cho ứng dụng dịch vụ; hoặc khi kết quả dàn xếp bảo mật được lưu trữ trước được sử dụng để lệnh

không mở dữ liệu người dùng cho ứng dụng dịch vụ, gửi thông tin chỉ báo tới thiết bị thành phần mạng, trong đó thông tin chỉ báo được sử dụng để chỉ báo rằng dữ liệu người dùng không thể được thu nhận.

Ngoài ra, bộ truyền 13 còn được tạo cấu hình để: khi quy tắc bảo vệ bảo mật được sử dụng để lệnh không thực hiện quy trình bảo mật, cung cấp dữ liệu người dùng cho ứng dụng dịch vụ.

Ngoài ra, bộ thu 11 còn được tạo cấu hình để thu thông tin cấu hình bảo mật, trong đó thông tin cấu hình bảo mật bao gồm danh sách trắng hoặc danh sách đen, danh sách trắng được sử dụng để chỉ báo phạm vi của dữ liệu người dùng được phép mở cho ứng dụng dịch vụ, và danh sách đen được sử dụng để chỉ báo phạm vi của dữ liệu người dùng không được phép mở cho ứng dụng dịch vụ, Khi bộ truyền 13 cung cấp dữ liệu người dùng cho ứng dụng dịch vụ, bộ truyền 13 được tạo cấu hình riêng biệt để cung cấp dữ liệu người dùng cho ứng dụng dịch vụ, trong đó dữ liệu người dùng thuộc về phạm vi được chỉ báo bởi danh sách trắng hoặc không thuộc về phạm vi được chỉ báo bởi danh sách đen.

Thiết bị xử lý dữ liệu người dùng được thể hiện trên Fig.13 có thể được tạo cấu hình để thực hiện các phương pháp được thể hiện trên Fig.1, và Fig.2 tới Fig.9, và các nguyên lý thực hiện của thiết bị và các hiệu quả kỹ thuật được tạo ra bởi thiết bị tương tự với chúng của các phương pháp, và các chi tiết không được mô tả lại ở đây.

Theo thiết bị xử lý dữ liệu người dùng được thể hiện trên Fig.13, đối với các ứng dụng dịch vụ khác, các quy tắc bảo vệ bảo mật tương ứng với các ứng dụng dịch vụ khác có thể được xác định, và quy trình bảo mật được thực hiện cho dữ liệu người dùng theo các quy tắc bảo vệ bảo mật, mà có thể nâng cao tính an toàn của dữ liệu người dùng ngoài việc mở đúng dữ liệu người dùng.

Người có hiểu biết trung bình trong lĩnh vực kỹ thuật có thể hiểu rằng tất cả hoặc một số bước của các phương án của phương pháp có thể được thực hiện bởi chương trình mà lệnh phần cứng liên quan. Chương trình có thể được lưu trữ trong vật ghi đọc được bằng máy tính. Khi chương trình chạy, các bước của các phương án của phương pháp được thực hiện. Vật ghi nêu trên bao gồm: vật ghi

bất kỳ mà có thể lưu trữ mã chương trình, chẳng hạn như ROM, RAM, ổ đĩa từ, hoặc đĩa quang.

Cuối cùng, chú ý rằng các phương án nêu trên chỉ có mục đích mô tả các giải pháp kỹ thuật của sáng chế, mà không có mục đích giới hạn sáng chế. Mặc dù sáng chế được mô tả chi tiết dựa vào các phương án nêu trên, người có hiểu biết trung bình trong lĩnh vực kỹ thuật sẽ hiểu rằng họ vẫn có thể tạo ra các cải biến từ các giải pháp kỹ thuật được mô tả trong các phương án nêu trên hoặc tạo ra các thay thế tương đương cho một số hoặc tất cả các đặc tính kỹ thuật của chúng, mà không chệch khỏi phạm vi của các giải pháp kỹ thuật trong các phương án của sáng chế.

YÊU CẦU BẢO HỘ

1. Thiết bị xử lý dữ liệu người dùng bao gồm:

bộ phận thu, được tạo cấu hình để thu yêu cầu thu nhận thông tin không dây được gửi bởi thiết bị thành phần mạng, trong đó yêu cầu thu nhận thông tin không dây được sử dụng để yêu cầu thu nhận dữ liệu người dùng tương ứng với ứng dụng dịch vụ;

bộ phận xác định quy tắc, được tạo cấu hình để xác định, theo ứng dụng dịch vụ và sự tương ứng giữa ứng dụng dịch vụ và quy tắc bảo vệ bảo mật, quy tắc bảo vệ bảo mật tương ứng với ứng dụng dịch vụ; và

bộ phận xử lý bảo mật, được tạo cấu hình để: khi quy tắc bảo vệ bảo mật được sử dụng để lệnh thực hiện quy trình bảo mật, thực hiện quy trình bảo mật trên dữ liệu người dùng theo quy tắc bảo vệ bảo mật;

trong đó bộ phận xử lý bảo mật bao gồm:

bộ phận thu nhận kết quả dàn xếp, được tạo cấu hình để: khi quy tắc bảo vệ bảo mật được sử dụng để lệnh thực hiện sự dàn xếp bảo mật, thực hiện, theo quy tắc bảo vệ bảo mật, sự dàn xếp bảo mật với thiết bị người dùng tương ứng với dữ liệu người dùng, để thu được kết quả dàn xếp bảo mật; và

bộ phận xử lý kết quả dàn xếp, được tạo cấu hình để: khi kết quả dàn xếp bảo mật được sử dụng để lệnh mở dữ liệu người dùng cho ứng dụng dịch vụ, cung cấp dữ liệu người dùng cho ứng dụng dịch vụ; hoặc khi kết quả dàn xếp bảo mật được sử dụng để lệnh không mở dữ liệu người dùng cho ứng dụng dịch vụ, gửi thông tin chỉ báo đến thiết bị thành phần mạng, trong đó thông tin chỉ báo được sử dụng để chỉ báo rằng dữ liệu người dùng không thể được thu nhận; và

trong đó bộ phận thu nhận kết quả dàn xếp được tạo cấu hình đặc biệt để: gửi yêu cầu dàn xếp bảo mật đến thiết bị người dùng, trong đó yêu cầu dàn xếp bảo mật được sử dụng để yêu cầu thu nhận chỉ báo về việc xem có mở dữ liệu người dùng cho ứng dụng dịch vụ; và thu phản hồi yêu cầu dàn xếp bảo mật được gửi bởi thiết bị người dùng, trong đó phản hồi yêu cầu dàn xếp bảo mật bao gồm kết quả

dàn xếp bảo mật .

2. Thiết bị theo điểm 1, trong đó bộ phận thu nhận kết quả dàn xếp được tạo cấu hình để: khi quy tắc bảo vệ bảo mật được sử dụng để lệnh sử dụng kết quả dàn xếp bảo mật được lưu trữ trước, thu nhận trực tiếp kết quả dàn xếp bảo mật được lưu trữ trước theo quy tắc bảo vệ bảo mật; và

bộ phận xử lý kết quả dàn xếp được tạo cấu hình để: khi kết quả dàn xếp bảo mật được sử dụng để lệnh mở dữ liệu người dùng cho ứng dụng dịch vụ, cung cấp dữ liệu người dùng cho ứng dụng dịch vụ; hoặc khi kết quả dàn xếp bảo mật được sử dụng để lệnh không mở dữ liệu người dùng cho ứng dụng dịch vụ, gửi thông tin chỉ báo cho thiết bị thành phần mạng, trong đó thông tin chỉ báo được sử dụng để chỉ báo rằng dữ liệu người dùng không thể được thu nhận.

3. Thiết bị theo điểm 2, trong đó bộ phận thu nhận kết quả dàn xếp còn được tạo cấu hình để: trước khi bộ phận thu thu yêu cầu thu nhận thông tin không dây được gửi bởi thiết bị thành phần mạng, thu kết quả dàn xếp bảo mật được gửi bởi thiết bị người dùng, và lưu kết quả dàn xếp bảo mật.

4. Thiết bị theo điểm bất kỳ trong số các điểm từ 1 đến 3, trong đó bộ phận xử lý kết quả dàn xếp còn được tạo cấu hình để: khi quy tắc bảo vệ bảo mật được sử dụng để lệnh không thực hiện quy trình bảo mật, cung cấp dữ liệu người dùng cho ứng dụng dịch vụ.

5. Thiết bị theo điểm 4, trong đó bộ phận thu còn được tạo cấu hình để thu thông tin cấu hình bảo mật, trong đó thông tin cấu hình bảo mật bao gồm danh sách trắng hoặc danh sách đen, danh sách trắng được sử dụng để chỉ báo phạm vi của dữ liệu người dùng được phép mở cho ứng dụng dịch vụ, và danh sách đen được sử dụng để chỉ báo phạm vi của dữ liệu người dùng không được phép mở cho ứng dụng dịch vụ; và

khi bộ phận xử lý kết quả dàn xếp được tạo cấu hình để cung cấp dữ liệu người dùng cho ứng dụng dịch vụ, bộ phận xử lý kết quả dàn xếp được tạo cấu hình riêng biệt để cung cấp dữ liệu người dùng cho ứng dụng dịch vụ, trong đó dữ liệu người dùng thuộc về phạm vi được chỉ báo bởi danh sách trắng hoặc không

thuộc về phạm vi được chỉ báo bởi danh sách đen.

6. Phương pháp xử lý dữ liệu người dùng bao gồm các bước:

thu, bởi thiết bị xử lý dữ liệu người dùng, yêu cầu thu nhận thông tin không dây được gửi bởi thiết bị thành phần mạng, trong đó yêu cầu thu nhận thông tin không dây được sử dụng để yêu cầu thu nhận dữ liệu người dùng tương ứng với ứng dụng dịch vụ;

xác định, bởi thiết bị xử lý dữ liệu người dùng theo ứng dụng dịch vụ và sự tương ứng giữa ứng dụng dịch vụ và quy tắc bảo vệ bảo mật, quy tắc bảo vệ bảo mật tương ứng với ứng dụng dịch vụ; và

khi quy tắc bảo vệ bảo mật được sử dụng để lệnh thực hiện quy trình bảo mật, thực hiện, bởi thiết bị xử lý dữ liệu người dùng, quy trình bảo mật trên dữ liệu người dùng theo quy tắc bảo vệ bảo mật;

trong đó quy tắc bảo vệ bảo mật được sử dụng để lệnh thực hiện quy trình bảo mật cụ thể là: quy tắc bảo vệ bảo mật được sử dụng để lệnh thực hiện sự dàn xếp bảo mật; và

thực hiện, bởi thiết bị xử lý dữ liệu người dùng, quy trình bảo mật trên dữ liệu người dùng theo quy tắc bảo vệ bảo mật bao gồm:

thực hiện, bởi thiết bị xử lý dữ liệu người dùng theo quy tắc bảo vệ bảo mật, sự dàn xếp bảo mật với thiết bị người dùng tương ứng với dữ liệu người dùng, để thu được kết quả dàn xếp bảo mật; và

khi kết quả dàn xếp bảo mật được sử dụng để lệnh mở dữ liệu người dùng cho ứng dụng dịch vụ, cung cấp, bởi thiết bị xử lý dữ liệu người dùng, dữ liệu người dùng cho ứng dụng dịch vụ; hoặc

khi kết quả dàn xếp bảo mật được sử dụng để lệnh không mở dữ liệu người dùng cho ứng dụng dịch vụ, gửi, bởi thiết bị xử lý dữ liệu người dùng, thông tin chỉ báo đến thiết bị thành phần mạng, trong đó thông tin chỉ báo được sử dụng để chỉ báo rằng dữ liệu người dùng không thể được thu nhận; và

trong đó thực hiện, bởi thiết bị xử lý dữ liệu người dùng theo quy tắc bảo vệ

bảo mật, sự dàn xếp bảo mật với thiết bị người dùng tương ứng với dữ liệu người dùng, để thu được kết quả dàn xếp bảo mật bao gồm:

gửi, bởi thiết bị xử lý dữ liệu người dùng, yêu cầu dàn xếp bảo mật đến thiết bị người dùng, trong đó yêu cầu dàn xếp bảo mật được sử dụng để yêu cầu thu nhận chỉ báo về việc xem có mở dữ liệu người dùng cho ứng dụng dịch vụ hay không; và

thu, bởi thiết bị xử lý dữ liệu người dùng, phản hồi yêu cầu dàn xếp bảo mật được gửi bởi thiết bị người dùng, trong đó phản hồi yêu cầu dàn xếp bảo mật bao gồm kết quả dàn xếp bảo mật.

7. Phương pháp theo điểm 6, trong đó quy tắc bảo vệ bảo mật được sử dụng để lệnh thực hiện quy trình bảo mật cụ thể là: quy tắc bảo vệ bảo mật được sử dụng để lệnh sử dụng kết quả dàn xếp bảo mật được lưu trữ trước; và

thực hiện, bởi thiết bị xử lý dữ liệu người dùng, xử lý bảo mật trên dữ liệu người dùng theo quy tắc bảo vệ bảo mật bao gồm:

thu nhận trực tiếp, bởi thiết bị xử lý dữ liệu người dùng, kết quả dàn xếp bảo mật được lưu trữ trước theo quy tắc bảo vệ bảo mật; và

khi kết quả dàn xếp bảo mật được sử dụng để lệnh mở dữ liệu người dùng cho ứng dụng dịch vụ, cung cấp, bởi thiết bị xử lý dữ liệu người dùng, dữ liệu người dùng cho ứng dụng dịch vụ; hoặc

khi kết quả dàn xếp bảo mật được sử dụng để lệnh không mở dữ liệu người dùng cho ứng dụng dịch vụ, gửi, bởi thiết bị xử lý dữ liệu người dùng, thông tin chỉ báo cho thiết bị thành phần mạng, trong đó thông tin chỉ báo được sử dụng để chỉ báo rằng dữ liệu người dùng không thể được thu nhận.

8. Phương pháp theo điểm 7, trong đó trước khi thu, bởi thiết bị xử lý dữ liệu người dùng, yêu cầu thu nhận thông tin không dây được gửi bởi thiết bị thành phần mạng, phương pháp còn bao gồm bước:

thu, bởi thiết bị xử lý dữ liệu người dùng, kết quả dàn xếp bảo mật được gửi bởi thiết bị người dùng; và

lưu, bởi thiết bị xử lý dữ liệu người dùng, kết quả dàn xếp bảo mật.

9. Phương pháp theo điểm 6 hoặc 7, còn bao gồm bước:

khi quy tắc bảo vệ bảo mật được sử dụng để lệnh không thực hiện quy trình xử lý bảo mật, cung cấp, bởi thiết bị xử lý dữ liệu người dùng, dữ liệu người dùng cho ứng dụng dịch vụ.

10. Phương pháp theo điểm 9, còn bao gồm bước:

thu, bởi thiết bị xử lý dữ liệu người dùng, thông tin cấu hình bảo mật, trong đó thông tin cấu hình bảo mật bao gồm danh sách trắng hoặc danh sách đen, danh sách trắng được sử dụng để chỉ báo phạm vi của dữ liệu người dùng được phép để mở cho ứng dụng dịch vụ, và danh sách đen được sử dụng để chỉ báo phạm vi của dữ liệu người dùng không được phép mở cho ứng dụng dịch vụ; và

cung cấp, bởi thiết bị xử lý dữ liệu người dùng, dữ liệu người dùng đối với ứng dụng dịch vụ bao gồm:

cung cấp, bởi thiết bị xử lý dữ liệu người dùng, dữ liệu người dùng đối với ứng dụng dịch vụ, trong đó dữ liệu người dùng thuộc phạm vi được chỉ báo bởi danh sách trắng hoặc không thuộc phạm vi được chỉ báo bởi danh sách đen.

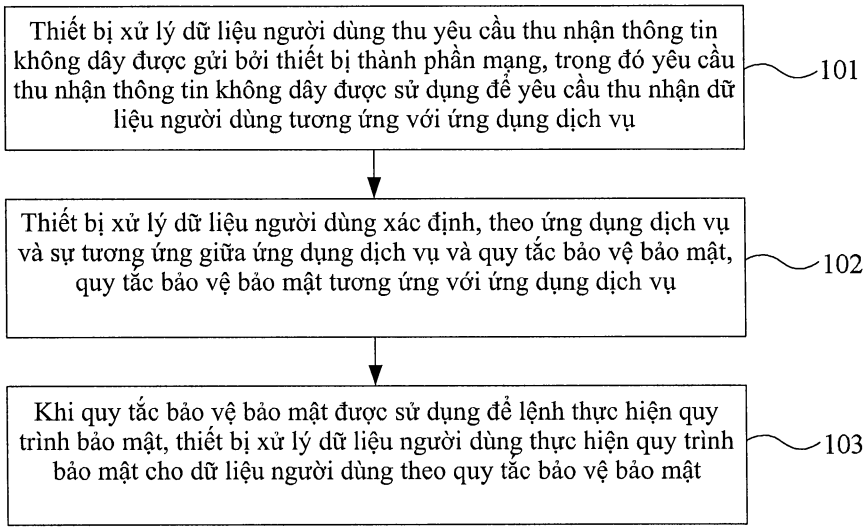

Thiết bị xử lý dữ liệu người dùng thu yêu cầu thu nhận thông tin không dây được gửi bởi thiết bị thành phần mạng, trong đó yêu cầu thu nhận thông tin không dây được sử dụng để yêu cầu thu nhận dữ liệu người dùng tương ứng với ứng dụng dịch vụ
101
Thiết bị xử lý dữ liệu người dùng xác định, theo ứng dụng dịch vụ và sự tương ứng giữa ứng dụng dịch vụ và quy tắc bảo vệ bảo mật, quy tắc bảo vệ bảo mật tương ứng với ứng dụng dịch vụ
102
Khi quy tắc bảo vệ bảo mật được sử dụng để lệnh thực hiện quy trình bảo mật, thiết bị xử lý dữ liệu người dùng thực hiện quy trình bảo mật cho dữ liệu người dùng theo quy tắc bảo vệ bảo mật
103

FIG. 1

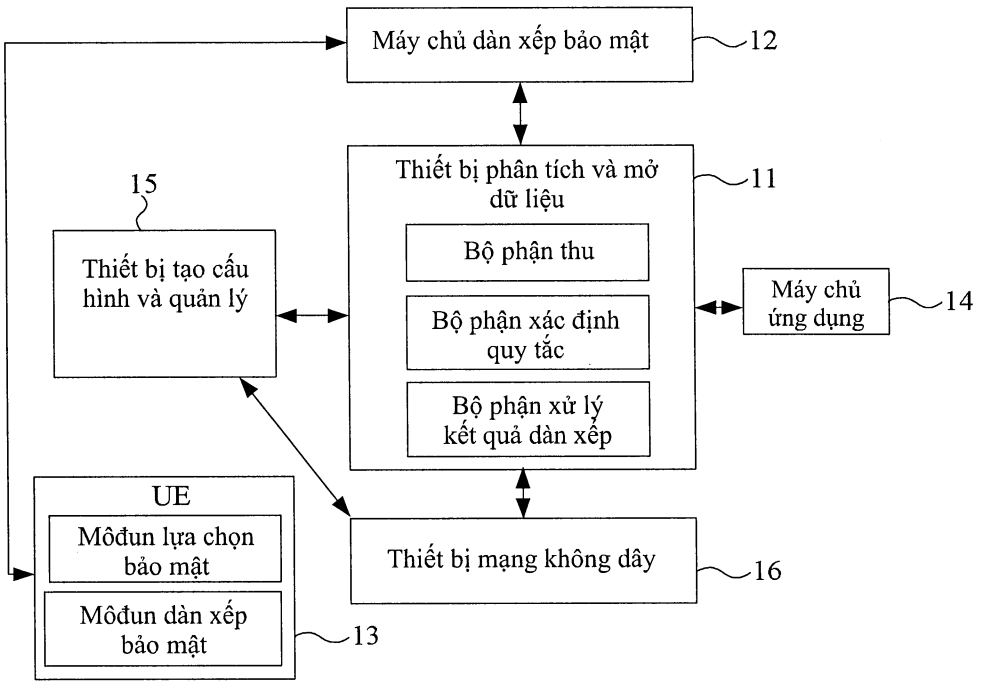

Máy chủ dàn xếp bảo mật
12
Thiết bị phân tích và mở dữ liệu
11
Bộ phận thu
Bộ phận xác định quy tắc
Bộ phận xử lý kết quả dàn xếp
15
Thiết bị tạo cấu hình và quản lý
Máy chủ ứng dụng
14
UE
Môđun lựa chọn bảo mật
Môđun dàn xếp bảo mật
13
Thiết bị mạng không dây
16

FIG. 2

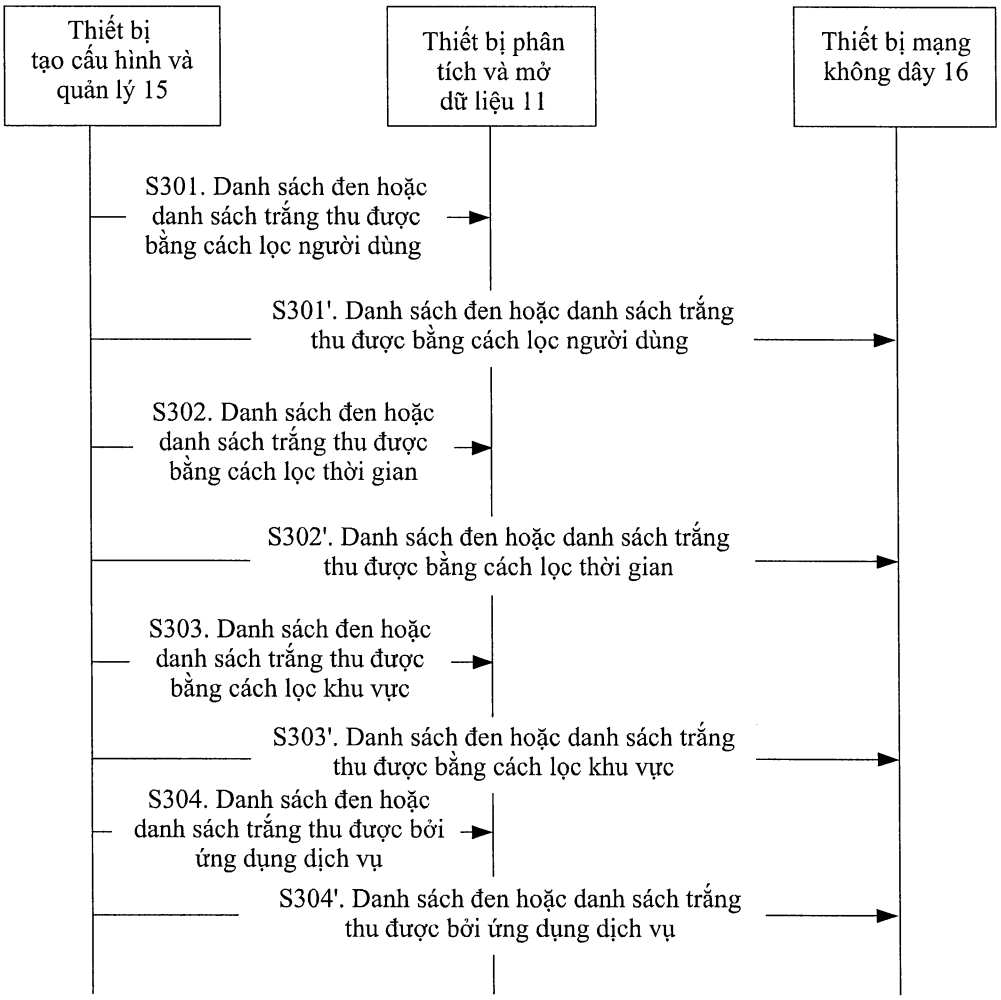

Thiết bị tạo cấu hình và quản lý 15
Thiết bị phân tích và mở dữ liệu 11
Thiết bị mạng không dây 16
S301. Danh sách đen hoặc danh sách trắng thu được bằng cách lọc người dùng
S301'. Danh sách đen hoặc danh sách trắng thu được bằng cách lọc người dùng
S302. Danh sách đen hoặc danh sách trắng thu được bằng cách lọc thời gian
S302'. Danh sách đen hoặc danh sách trắng thu được bằng cách lọc thời gian
S303. Danh sách đen hoặc danh sách trắng thu được bằng cách lọc khu vực
S303'. Danh sách đen hoặc danh sách trắng thu được bằng cách lọc khu vực
S304. Danh sách đen hoặc danh sách trắng thu được bởi ứng dụng dịch vụ
S304'. Danh sách đen hoặc danh sách trắng thu được bởi ứng dụng dịch vụ

FIG. 3

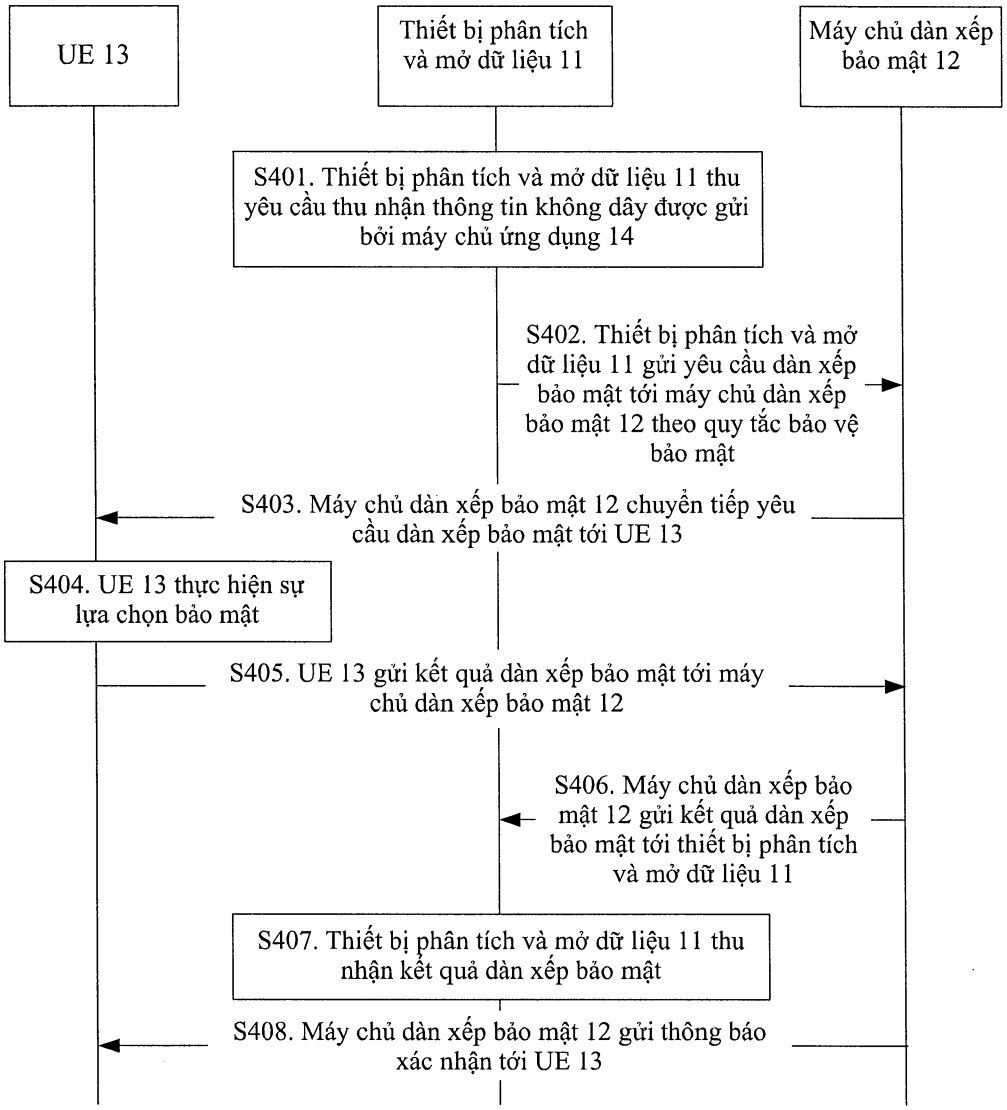

UE 13
Thiết bị phân tích và mở dữ liệu 11
Máy chủ dàn xếp bảo mật 12
S401. Thiết bị phân tích và mở dữ liệu 11 thu yêu cầu thu nhận thông tin không dây được gửi bởi máy chủ ứng dụng 14
S402. Thiết bị phân tích và mở dữ liệu 11 gửi yêu cầu dàn xếp bảo mật tới máy chủ dàn xếp bảo mật 12 theo quy tắc bảo vệ bảo mật
S403. Máy chủ dàn xếp bảo mật 12 chuyển tiếp yêu cầu dàn xếp bảo mật tới UE 13
S404. UE 13 thực hiện sự lựa chọn bảo mật
S405. UE 13 gửi kết quả dàn xếp bảo mật tới máy chủ dàn xếp bảo mật 12
S406. Máy chủ dàn xếp bảo mật 12 gửi kết quả dàn xếp bảo mật tới thiết bị phân tích và mở dữ liệu 11
S407. Thiết bị phân tích và mở dữ liệu 11 thu nhận kết quả dàn xếp bảo mật
S408. Máy chủ dàn xếp bảo mật 12 gửi thông báo xác nhận tới UE 13

FIG. 4

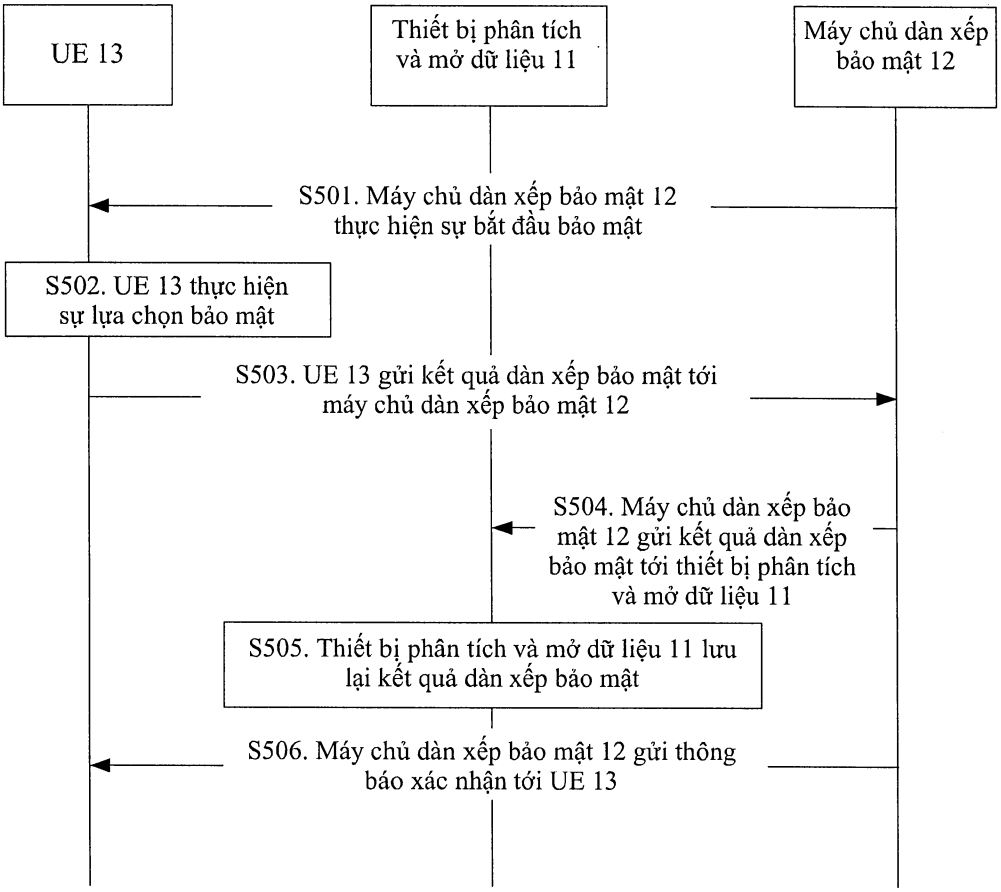

UE 13
Thiết bị phân tích và mở dữ liệu 11
Máy chủ dàn xếp bảo mật 12
S501. Máy chủ dàn xếp bảo mật 12 thực hiện sự bắt đầu bảo mật
S502. UE 13 thực hiện sự lựa chọn bảo mật
S503. UE 13 gửi kết quả dàn xếp bảo mật tới máy chủ dàn xếp bảo mật 12
S504. Máy chủ dàn xếp bảo mật 12 gửi kết quả dàn xếp bảo mật tới thiết bị phân tích và mở dữ liệu 11
S505. Thiết bị phân tích và mở dữ liệu 11 lưu lại kết quả dàn xếp bảo mật
S506. Máy chủ dàn xếp bảo mật 12 gửi thông báo xác nhận tới UE 13

FIG. 5

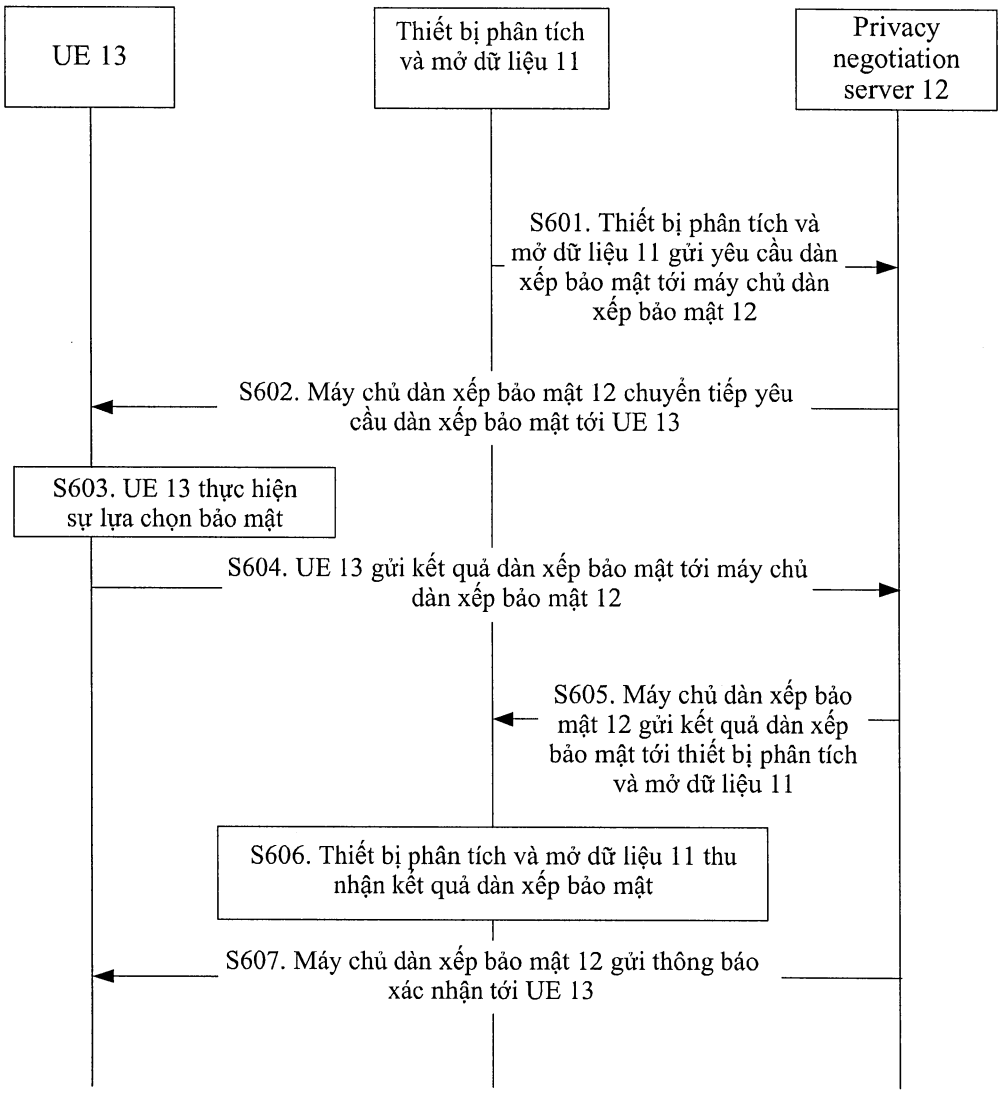

UE 13
Thiết bị phân tích và mở dữ liệu 11
Privacy negotiation server 12
S601. Thiết bị phân tích và mở dữ liệu 11 gửi yêu cầu dàn xếp bảo mật tới máy chủ dàn xếp bảo mật 12
S602. Máy chủ dàn xếp bảo mật 12 chuyển tiếp yêu cầu dàn xếp bảo mật tới UE 13
S603. UE 13 thực hiện sự lựa chọn bảo mật
S604. UE 13 gửi kết quả dàn xếp bảo mật tới máy chủ dàn xếp bảo mật 12
S605. Máy chủ dàn xếp bảo mật 12 gửi kết quả dàn xếp bảo mật tới thiết bị phân tích và mở dữ liệu 11
S606. Thiết bị phân tích và mở dữ liệu 11 thu nhận kết quả dàn xếp bảo mật
S607. Máy chủ dàn xếp bảo mật 12 gửi thông báo xác nhận tới UE 13

FIG. 6

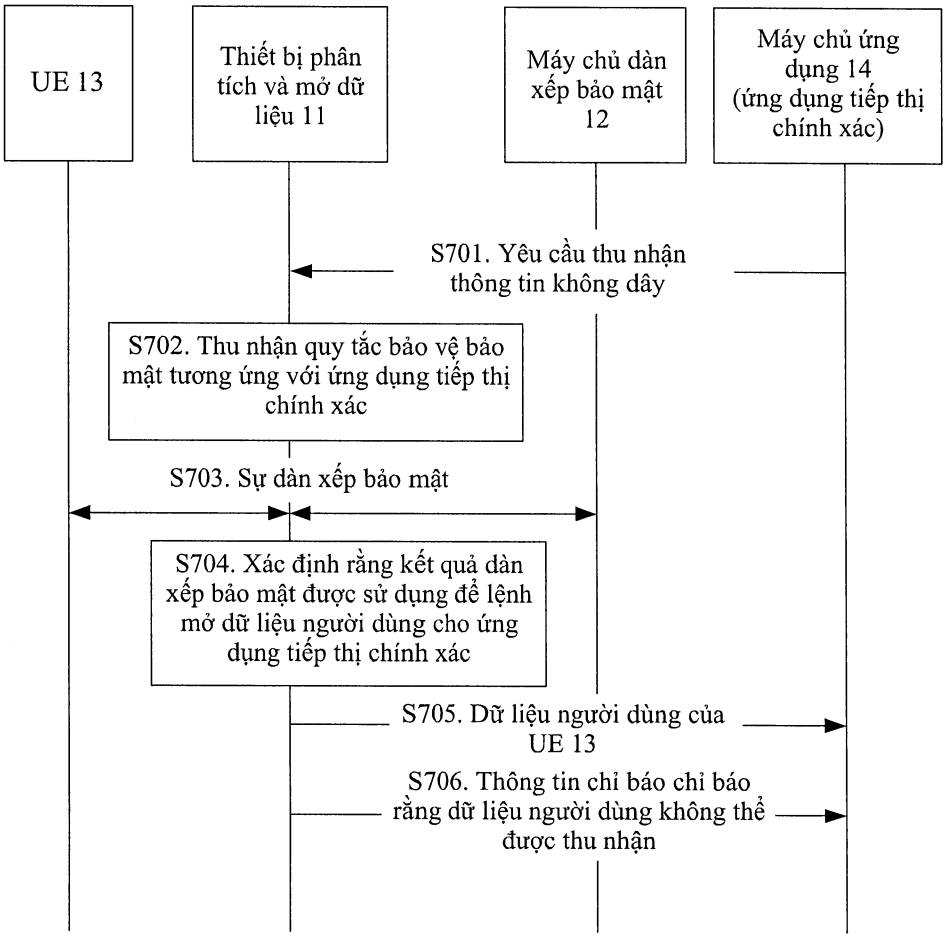

UE 13
Thiết bị phân tích và mở dữ liệu 11
Máy chủ dàn xếp bảo mật 12
Máy chủ ứng dụng 14 (ứng dụng tiếp thị chính xác)
S701. Yêu cầu thu nhận thông tin không dây
S702. Thu nhận quy tắc bảo vệ bảo mật tương ứng với ứng dụng tiếp thị chính xác
S703. Sự dàn xếp bảo mật
S704. Xác định rằng kết quả dàn xếp bảo mật được sử dụng để lệnh mở dữ liệu người dùng cho ứng dụng tiếp thị chính xác
S705. Dữ liệu người dùng của UE 13
S706. Thông tin chỉ báo chỉ báo rằng dữ liệu người dùng không thể được thu nhận

FIG. 7

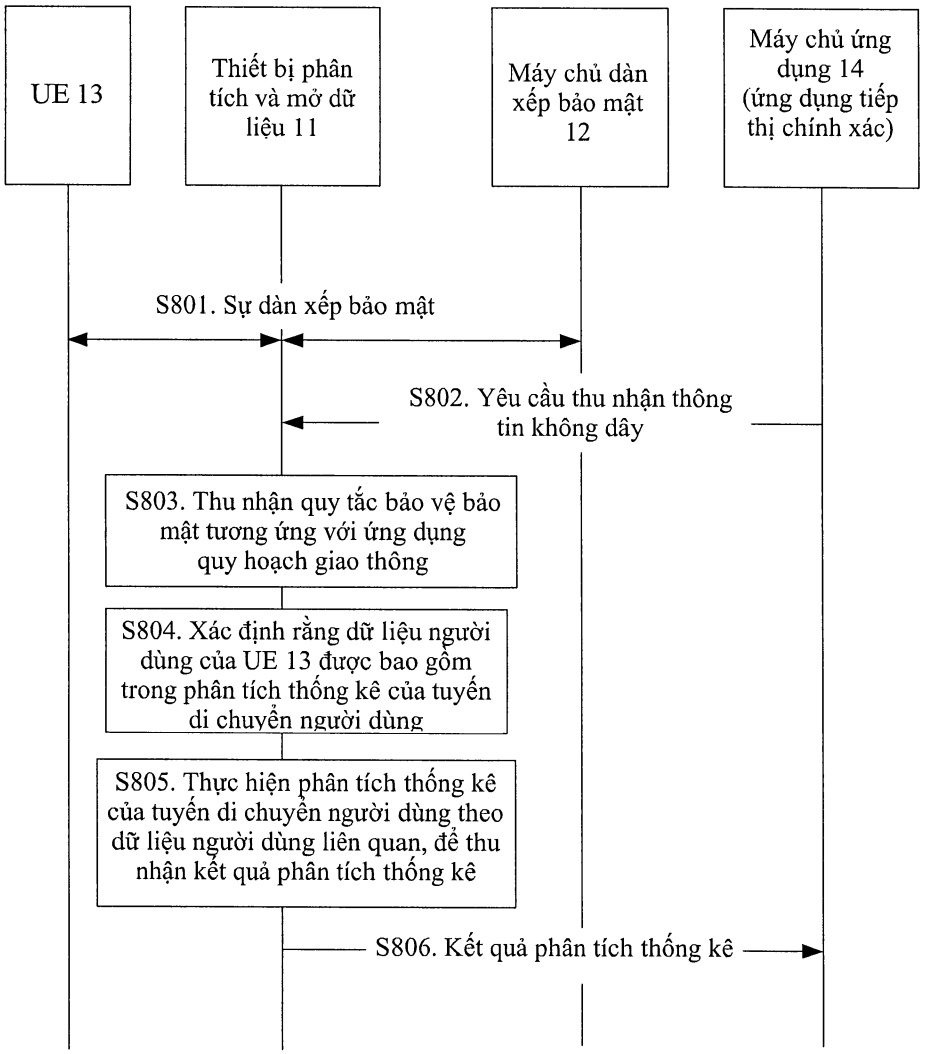

UE 13
Thiết bị phân tích và mở dữ liệu 11
Máy chủ dàn xếp bảo mật 12
Máy chủ ứng dụng 14 (ứng dụng tiếp thị chính xác)
S801. Sự dàn xếp bảo mật
S802. Yêu cầu thu nhận thông tin không dây
S803. Thu nhận quy tắc bảo vệ bảo mật tương ứng với ứng dụng quy hoạch giao thông
S804. Xác định rằng dữ liệu người dùng của UE 13 được bao gồm trong phân tích thống kê của tuyến di chuyển người dùng
S805. Thực hiện phân tích thống kê của tuyến di chuyển người dùng theo dữ liệu người dùng liên quan, để thu nhận kết quả phân tích thống kê
S806. Kết quả phân tích thống kê

FIG. 8

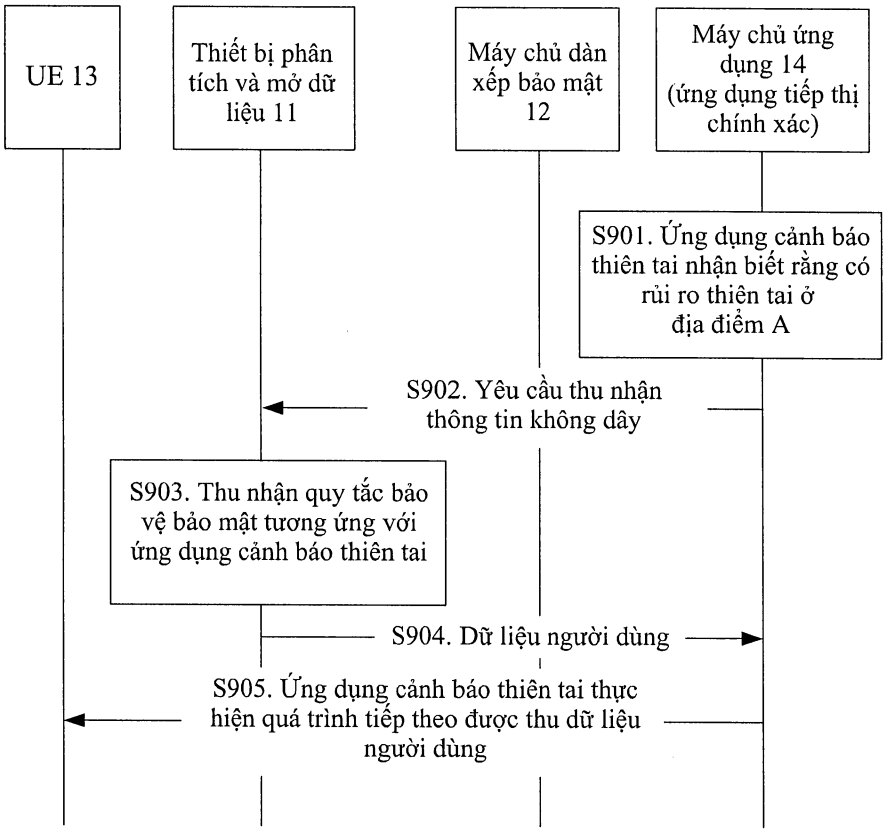

UE 13
Thiết bị phân tích và mở dữ liệu 11
Máy chủ dàn xếp bảo mật 12
Máy chủ ứng dụng 14 (ứng dụng tiếp thị chính xác)
S901. Ứng dụng cảnh báo thiên tai nhận biết rằng có rủi ro thiên tai ở địa điểm A
S902. Yêu cầu thu nhận thông tin không dây
S903. Thu nhận quy tắc bảo vệ bảo mật tương ứng với ứng dụng cảnh báo thiên tai
S904. Dữ liệu người dùng
S905. Ứng dụng cảnh báo thiên tai thực hiện quá trình tiếp theo được thu dữ liệu người dùng

FIG. 9

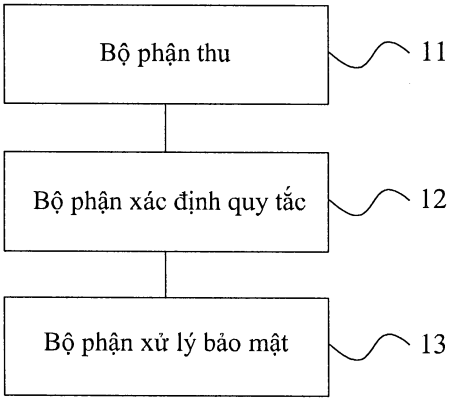

Bộ phận thu
11
Bộ phận xác định quy tắc
12
Bộ phận xử lý bảo mật
13

FIG. 10

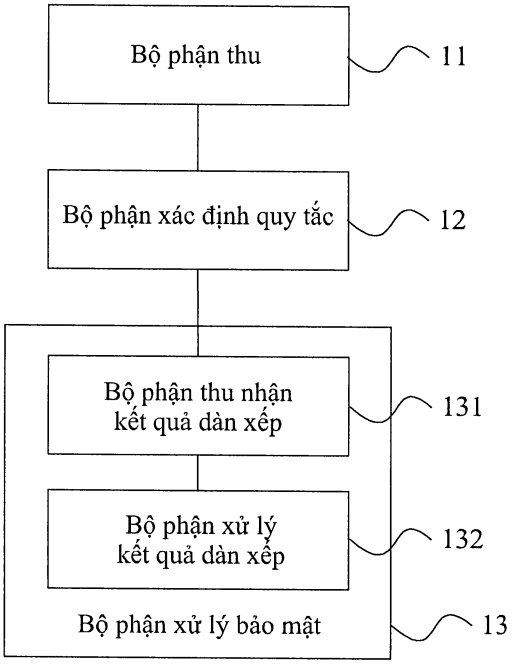

Bộ phận thu
11
Bộ phận xác định quy tắc
12
Bộ phận thu nhận
kết quả dàn xếp
131
Bộ phận xử lý
kết quả dàn xếp
132
Bộ phận xử lý bảo mật
13

FIG. 11

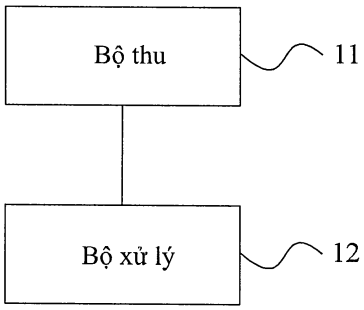

Bộ thu
11
Bộ xử lý
12

FIG. 12

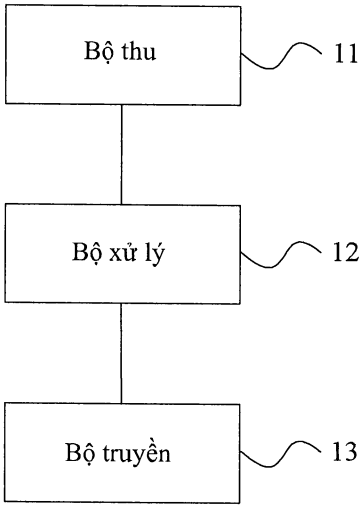


FIG. 13