(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) **1-0034431**

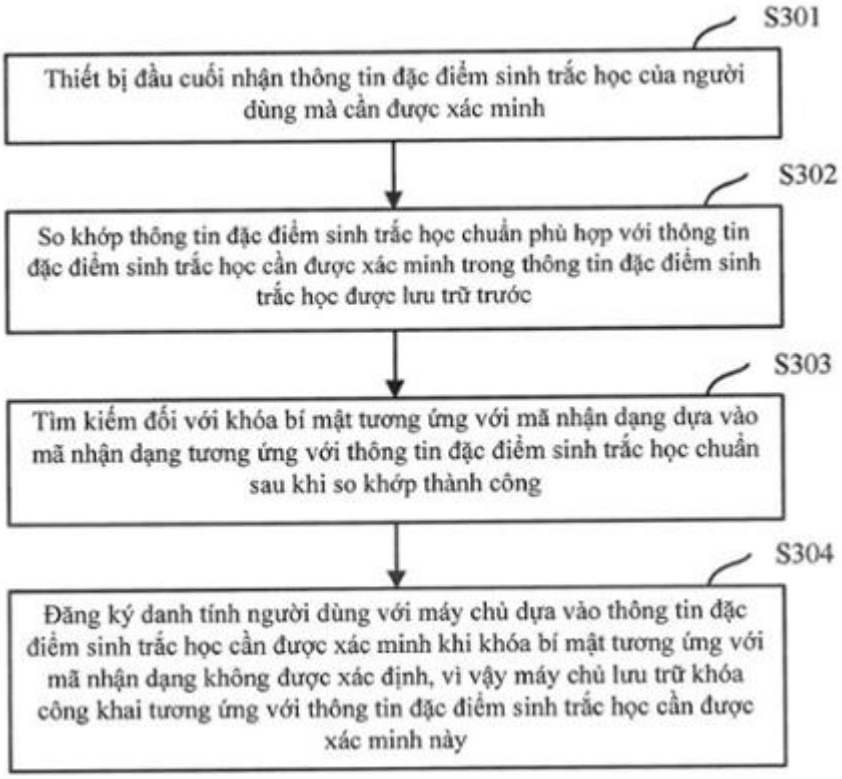
(51)[8] **H04L 9/32**

(13) **B**

(21) 1-2018-04628
(22) 20/03/2017
(86) PCT/CN2017/077247 20/03/2017
(87) WO2017/162112 28/09/2017
(30) 201610180030.4 25/03/2016 CN
(45) 26/12/2022 417
(43) 25/12/2018 369A
(73) Advanced New Technologies Co., Ltd. (KY)
Cayman Corporate Centre, 27 Hospital Road, George Town, Grand Cayman KY1-9008, Cayman Islands
(72) MENG, Fei (CN).
(74) Công ty TNHH Tầm nhìn và Liên danh (VISION & ASSOCIATES CO.LTD.)

(54) PHƯƠNG PHÁP ĐĂNG KÝ DANH TÍNH NGƯỜI DÙNG VÀ THIẾT BỊ ĐĂNG KÝ DANH TÍNH

(57) Sáng chế đề cập đến phương pháp đăng ký danh tính người dùng và thiết bị đăng ký danh tính. Trong phương pháp này, thiết bị đầu cuối nhận thông tin đặc điểm sinh trắc học của người dùng mà cần được xác minh, so khớp thông tin đặc điểm sinh trắc học chuẩn phù hợp với thông tin đặc điểm sinh trắc học cần được xác minh, và khi khóa bí mật tương ứng với mã nhận dạng không được xác định dựa vào mã nhận dạng tương ứng với thông tin đặc điểm sinh trắc học chuẩn, thì đăng ký danh tính người dùng với máy chủ dựa vào thông tin đặc điểm sinh trắc học cần được xác minh. Như vậy, máy chủ lưu trữ khóa công khai tương ứng với thông tin đặc điểm sinh trắc học cần được xác minh. Bằng cách sử dụng phương pháp nêu trên, bất kể thông tin đặc điểm sinh trắc học được sử dụng bởi người dùng để đăng ký, miễn là thông tin đặc điểm sinh trắc học cần được xác minh đã được lưu trữ trong thiết bị đầu cuối, danh tính người dùng có thể được đăng ký trực tiếp dựa vào thông tin đặc điểm sinh trắc học cần được xác minh, để hoàn thành việc xử lý dịch vụ, tạo ra sự thuận tiện tuyệt vời cho người dùng sử dụng dịch vụ, và cũng nâng cao một cách hiệu quả tỷ lệ thành công của việc sử dụng dịch vụ.


S301
Thiết bị đầu cuối nhận thông tin đặc điểm sinh trắc học của người dùng mà cần được xác minh
S302
So khớp thông tin đặc điểm sinh trắc học chuẩn phù hợp với thông tin đặc điểm sinh trắc học cần được xác minh trong thông tin đặc điểm sinh trắc học được lưu trữ trước
S303
Tìm kiếm đối với khóa bí mật tương ứng với mã nhận dạng dựa vào mã nhận dạng tương ứng với thông tin đặc điểm sinh trắc học chuẩn sau khi so khớp thành công
S304
Đăng ký danh tính người dùng với máy chủ dựa vào thông tin đặc điểm sinh trắc học cần được xác minh khi khóa bí mật tương ứng với mã nhận dạng không được xác định, vì vậy máy chủ lưu trữ khóa công khai tương ứng với thông tin đặc điểm sinh trắc học cần được xác minh này

Lĩnh vực kỹ thuật được đề cập

Sáng chế đề cập đến lĩnh vực các công nghệ máy tính, và cụ thể là, phương pháp và thiết bị đăng ký danh tính.

Tình trạng kỹ thuật của sáng chế

Với sự phát triển liên tục của các công nghệ mạng, việc sử dụng các dịch vụ qua mạng đã trở thành một phần không thể thiếu trong cuộc sống của con người, ví dụ, người sử dụng dịch vụ dự báo thời tiết qua mạng.

Hiện nay, để nâng cao độ bảo mật thông tin khi người dùng sử dụng dịch vụ, người dùng cần đăng ký trước danh tính người dùng đối với dịch vụ trước khi sử dụng dịch vụ này. Sau đó, khi sử dụng dịch vụ qua mạng, danh tính người dùng cần được xác minh. Người dùng chỉ có thể sử dụng dịch vụ sau khi việc xác minh thành công. Ví dụ, nếu thông tin dấu vân tay được sử dụng để thể hiện danh tính người dùng, thì thông tin dấu vân tay của người dùng cần được đăng ký trước.

Vì việc nhận diện thông tin dấu vân tay trong các ứng dụng thực tế ngày càng phổ biến trong các thiết bị đầu cuối, ví dụ, thông tin dấu vân tay của người dùng được sử dụng để mở khóa giao diện màn hình được khóa. Đối với dịch vụ bất kỳ, quy trình trong đó máy chủ của dịch vụ đăng ký danh tính người dùng bằng cách sử dụng thông tin dấu vân tay của người dùng, và sau đó xác minh danh tính người dùng bằng cách sử dụng thông tin dấu vân tay của người dùng có thể được hoàn thành bằng cách sử dụng thiết bị đầu cuối.

Hơn nữa, với sự cải tiến liên tục của các công nghệ máy tính, các thông tin dấu vân tay của người dùng có thể được lưu trữ trong thiết bị đầu cuối ở cùng thời điểm. Đối với dịch vụ bất kỳ, khi danh tính người dùng được đăng ký bằng cách sử dụng thông tin dấu vân tay được tải lên bởi người dùng, thì thiết bị đầu cuối trước tiên cần xác minh xem thông tin dấu vân tay có phải là một trong số các thông tin dấu vân tay được lưu trữ trong thiết bị đầu cuối hay không. Nếu có, thiết bị đầu cuối có thể đăng ký danh tính người dùng với máy chủ dựa vào thông tin dấu vân tay, và nếu không, thiết bị đầu cuối thông báo trực tiếp cho người dùng là việc đăng ký danh tính thất bại.

Trong công nghệ hiện có, quy trình đăng ký thông tin dấu vân tay của người dùng được thể hiện trên Fig.1.

S101. Thiết bị đầu cuối nhận hoạt động đăng ký của người dùng.

S102. Thu thập thông tin dấu vân tay của người dùng.

S103. Xác định xem thông tin dấu vân tay đã được lưu trữ trước trong thiết bị đầu cuối hay chưa, và nếu có, thì thực hiện bước S104, hoặc nếu không, thì thực hiện bước S105.

S104. Truy vấn mã nhận dạng tương ứng với thông tin dấu vân tay được lưu trữ trước trong thiết bị đầu cuối, tạo ra khóa bí mật và khóa công khai tương ứng với mã nhận dạng này, lưu trữ mối quan hệ ánh xạ giữa khóa bí mật và mã nhận dạng tương ứng với thông tin dấu vân tay trong thiết bị đầu cuối, và gửi mối quan hệ ánh xạ giữa khóa công khai và mã nhận dạng tương ứng với thông tin dấu vân tay đến máy chủ để lưu trữ.

S105. Thông báo cho người dùng rằng việc đăng ký thất bại.

Sau đó, quy trình của người dùng sử dụng dịch vụ được thể hiện trên Fig.2.

S201. Thiết bị đầu cuối nhận thông tin dấu vân tay của người dùng.

S202. So khớp thông tin đặc điểm sinh trắc học chuẩn phù hợp với thông tin dấu vân tay.

S203. Tìm kiếm đối với khóa bí mật tương ứng với mã nhận dạng dựa vào mã nhận dạng tương ứng với thông tin đặc điểm sinh trắc học chuẩn.

S204. Khi khóa bí mật tương ứng với mã nhận dạng được xác định, thì ký thông tin dịch vụ bằng cách sử dụng khóa bí mật, và thêm thông tin dịch vụ đã ký và mã nhận dạng tương ứng với thông tin dấu vân tay vào yêu cầu xử lý dịch vụ và gửi yêu cầu này đến máy chủ, vì vậy máy chủ xác định khóa công khai tương ứng với mã nhận dạng có trong yêu cầu xử lý dịch vụ đã nhận và thực hiện việc xử lý dịch vụ dựa vào khóa công khai và thông tin dịch vụ. Theo cách khác, khi khóa bí mật tương ứng với mã nhận dạng không được xác định, thì thông báo cho người dùng rằng việc xử lý dịch vụ thất bại.

Tuy nhiên, trong các ứng dụng thực tế, nếu người dùng quên dấu vân tay nào

được nhập vào, thì người dùng cần thực hiện việc xác minh dấu vân tay nhiều lần. Điều này gây ra sự bất tiện lớn đối với người dùng sử dụng dịch vụ, và làm giảm tỷ lệ thành công của việc sử dụng dịch vụ. Ngoài ra, nếu ngón tay của người dùng được sử dụng để đăng ký bị thương trong cuộc sống hàng ngày, thì người dùng không thể được xác thực để sử dụng dịch vụ.

Bản chất kỹ thuật của sáng chế

Các phương án thực hiện theo sáng chế đề xuất phương pháp và thiết bị đăng ký danh tính, để giải quyết các vấn đề công nghệ hiện có: người dùng quên dấu vân tay nào được nhập vào và do đó điều này gây ra sự bất tiện đối với người dùng sử dụng dịch vụ; và nếu ngón tay của người dùng được sử dụng để đăng ký bị thương trong cuộc sống hàng ngày, thì người dùng không thể được xác thực để sử dụng dịch vụ.

Một phương án thực hiện theo sáng chế đề xuất phương pháp đăng ký danh tính, và phương pháp này bao gồm các bước sau: nhận, bởi thiết bị đầu cuối, thông tin đặc điểm sinh trắc học của người dùng mà cần được xác minh; so khớp thông tin đặc điểm sinh trắc học chuẩn phù hợp với thông tin đặc điểm sinh trắc học cần được xác minh trong thông tin đặc điểm sinh trắc học được lưu trữ trước; tìm kiếm đối với khóa bí mật tương ứng với mã nhận dạng dựa vào mã nhận dạng tương ứng với thông tin đặc điểm sinh trắc học chuẩn sau khi so khớp thành công; và đăng ký danh tính người dùng với máy chủ dựa vào thông tin đặc điểm sinh trắc học cần được xác minh khi khóa bí mật tương ứng với mã nhận dạng không được xác định, vì vậy máy chủ lưu trữ khóa công khai tương ứng với thông tin đặc điểm sinh trắc học cần được xác minh.

Một phương án thực hiện theo sáng chế đề xuất thiết bị đăng ký danh tính, và thiết bị này bao gồm các bộ phận sau: môđun nhận, được tạo cấu hình để nhận thông tin đặc điểm sinh trắc học của người dùng mà cần được xác minh; môđun so khớp, được tạo cấu hình để so khớp thông tin đặc điểm sinh trắc học chuẩn phù hợp với thông tin đặc điểm sinh trắc học cần được xác minh trong thông tin đặc điểm sinh trắc học được lưu trữ trước; môđun tìm kiếm, được tạo cấu hình để tìm kiếm khóa bí mật tương ứng với mã nhận dạng dựa vào mã nhận dạng tương ứng với thông tin đặc điểm sinh trắc học chuẩn sau khi so khớp thành công; và môđun đăng ký, được tạo cấu hình để đăng ký danh tính người dùng với máy chủ dựa vào thông tin đặc điểm sinh trắc học cần được xác minh khi khóa bí mật tương ứng với mã nhận dạng không được xác

định, vì vậy máy chủ lưu trữ khóa công khai tương ứng với thông tin đặc điểm sinh trắc học cần được xác minh.

Các phương án thực hiện theo sáng chế bộc lộ phương pháp và thiết bị đăng ký danh tính. Theo phương pháp, thiết bị đầu cuối nhận thông tin đặc điểm sinh trắc học của người dùng mà cần được xác minh, và so khớp thông tin đặc điểm sinh trắc học chuẩn phù hợp với thông tin đặc điểm sinh trắc học cần được xác minh. Sau khi so khớp thành công, thiết bị đầu cuối tìm kiếm đối với khóa bí mật tương ứng với mã nhận dạng dựa vào mã nhận dạng tương ứng với thông tin đặc điểm sinh trắc học chuẩn, và đăng ký danh tính người dùng với máy chủ dựa vào thông tin đặc điểm sinh trắc học cần được xác minh khi khóa bí mật tương ứng với mã nhận dạng không được xác định. Như vậy, máy chủ lưu trữ khóa công khai tương ứng với thông tin đặc điểm sinh trắc học cần được xác minh. Theo phương pháp nêu trên, bất kể thông tin đặc điểm sinh trắc học được sử dụng bởi người dùng để đăng ký, miễn là thiết bị đầu cuối có thể xác định thông tin đặc điểm sinh trắc học chuẩn phù hợp với thông tin đặc điểm sinh trắc học cần được xác minh, ngay cả khi khóa bí mật tương ứng với mã nhận dạng không được xác định trong thiết bị đầu cuối dựa vào mã nhận dạng tương ứng với thông tin đặc điểm sinh trắc học chuẩn, thì thiết bị đầu cuối có thể đăng ký trực tiếp danh tính người dùng dựa vào thông tin đặc điểm sinh trắc học cần được xác minh, để hoàn thành việc xử lý dịch vụ, tạo ra sự thuận tiện tuyệt vời cho người dùng sử dụng dịch vụ và cũng nâng cao một cách hiệu quả tỷ lệ thành công của việc sử dụng dịch vụ.

Mô tả vắn tắt các hình vẽ

Các hình vẽ kèm theo được mô tả trong bản mô tả này nhằm cung cấp sự hiểu biết sâu hơn về sáng chế, và tạo thành một phần sáng chế. Các phương án thực hiện minh họa theo sáng chế và các phần mô tả về các phương án thực hiện nhằm mô tả sáng chế, và không tạo thành các giới hạn đối với sáng chế. Trên các hình vẽ kèm theo:

Fig.1 là sơ đồ sơ lược minh họa quy trình đăng ký thông tin dấu vân tay của người dùng trong công nghệ hiện có, theo một phương án thực hiện của sáng chế;

Fig.2 là sơ đồ sơ lược minh họa quy trình sử dụng dịch vụ bởi người dùng trong công nghệ hiện có, theo một phương án thực hiện của sáng chế;

Fig.3 là sơ đồ sơ lược minh họa quy trình đăng ký danh tính, theo một phương án thực hiện của sáng chế; và

Fig.4 là sơ đồ cấu trúc sơ lược minh họa thiết bị đăng ký danh tính, theo một phương án thực hiện của sáng chế.

Mô tả chi tiết sáng chế

Để làm cho các mục đích, giải pháp kỹ thuật và ưu điểm của sáng chế trở nên rõ ràng hơn, phần sau mô tả các giải pháp kỹ thuật của sáng chế dựa vào các phương án thực hiện cụ thể của sáng chế và các hình vẽ kèm theo tương ứng. Rõ ràng là, các phương án thực hiện được mô tả chỉ là một số chứ không phải tất cả các phương án thực hiện của sáng chế. Các phương án thực hiện khác thu được bởi người có hiểu biết trung bình trong lĩnh vực kỹ thuật dựa vào các phương án thực hiện của sáng chế mà không có các nỗ lực sáng tạo sẽ nằm trong phạm vi bảo hộ của sáng chế.

Fig.3 thể hiện quy trình đăng ký danh tính, theo một phương án thực hiện của sáng chế. Quy trình này bao gồm các bước sau.

S301. Thiết bị đầu cuối nhận thông tin đặc điểm sinh trắc học của người dùng mà cần được xác minh.

Trong các ứng dụng thực tế, để nâng cao độ bảo mật thông tin khi người dùng sử dụng dịch vụ, trong quy trình sử dụng dịch vụ, danh tính của người dùng hiện tại trước tiên cần được xác minh để xác nhận rằng danh tính của người dùng hiện tại là hợp lệ.

Do đó, theo sáng chế, thông tin đặc điểm sinh trắc học của người dùng mà cần được xác minh nhận được trước tiên. Vì việc nhận biết thông tin đặc điểm sinh trắc học ngày càng phổ biến trong các thiết bị đầu cuối (ví dụ, các điện thoại di động) trong các ứng dụng thực tế, nên thông tin đặc điểm sinh trắc học của người dùng mà cần được xác minh có thể nhận được bởi thiết bị đầu cuối. Sau khi nhận thông tin đặc điểm sinh trắc học, thiết bị đầu cuối đưa ra phản hồi tương ứng. Thông tin đặc điểm sinh trắc học biểu thị đặc điểm vật lý của người dùng, và đặc điểm này có thể là mống mắt của mắt hoặc dấu vân tay của ngón tay, và được sử dụng chủ yếu để biểu diễn duy nhất danh tính người dùng.

Ngoài ra, trong các ứng dụng thực tế, để xác minh danh tính của người dùng hiện tại, việc xác minh thông tin dấu vân tay ngày càng phổ biến và công nghệ là tương đối hoàn thiện. Do đó, thông tin đặc điểm sinh trắc học mà là thông tin dấu vân

tay được sử dụng làm một ví dụ đối với phần mô tả chi tiết dưới đây.

Ví dụ, giả sử rằng diễn đàn nhất định cung cấp dịch vụ truy vấn thông tin chỉ dành cho người dùng, người mà đã đăng ký tài khoản, và người dùng có thể đăng nhập bằng cách sử dụng thông tin dấu vân tay. Do đó, khi người dùng cần truy vấn thông tin trong diễn dàn, thì người dùng mở ứng dụng tương ứng với diễn dàn trên điện thoại di động (nghĩa là, thiết bị đầu cuối) và nhấn bằng dấu vân tay. Sau đó, điện thoại di động (nghĩa là, thiết bị đầu cuối) nhận thông tin dấu vân tay của người dùng mà cần được xác minh, và thực hiện bước S302.

S302. So khớp thông tin đặc điểm sinh trắc học chuẩn phù hợp với thông tin đặc điểm sinh trắc học cần được xác minh trong thông tin đặc điểm sinh trắc học được lưu trữ trước.

Vì việc nhận diện thông tin dấu vân tay (nghĩa là, thông tin đặc điểm sinh trắc học) trong các ứng dụng thực tế ngày càng phổ biến trong các thiết bị đầu cuối, ví dụ, thông tin dấu vân tay của người dùng được sử dụng để mở khóa giao diện màn hình được khóa. Đối với dịch vụ bất kỳ, quy trình trong đó máy chủ của dịch vụ đăng ký danh tính người dùng bằng cách sử dụng thông tin dấu vân tay của người dùng, và sau đó xác minh danh tính người dùng bằng cách sử dụng thông tin dấu vân tay của người dùng có thể được hoàn thành bằng cách sử dụng thông tin dấu vân tay mà đã được lưu trữ trong thiết bị đầu cuối. Nói cách khác, miễn là thông tin dấu vân tay được lưu trữ trong thiết bị đầu cuối, thông tin dấu vân tay này có thể được sử dụng để hoàn thành toàn bộ quá trình xử lý dịch vụ theo sáng chế.

Đáng lưu ý trong bản mô tả này rằng thông tin dấu vân tay được lưu trữ trong thiết bị đầu cuối có thể được nhập vào bởi người dùng khi người dùng sử dụng chức năng khác của thiết bị đầu cuối, và không phải là thông tin dấu vân tay được sử dụng bởi người dùng để đăng ký danh tính để sử dụng dịch vụ. Ví dụ, khi người dùng sử dụng chức năng của thiết bị đầu cuối để mở khóa giao diện màn hình được khóa bằng cách sử dụng thông tin dấu vân tay, thì thiết bị đầu cuối có thể lưu trữ một cách cục bộ thông tin dấu vân tay này.

Ngoài ra, theo sáng chế, để phân biệt giữa thông tin dấu vân tay được lưu trữ và thông tin dấu vân tay nhận được bởi thiết bị đầu cuối khi người dùng sử dụng dịch vụ, thông tin dấu vân tay được lưu trữ có thể được sử dụng làm thông tin dấu vân tay

chuẩn (nghĩa là, thông tin đặc điểm sinh trắc học chuẩn), và được sử dụng chủ yếu để kiểm tra xem người dùng có thể được xác thực trong quy trình sử dụng dịch vụ và cung cấp quá trình xử lý dịch vụ này cho người dùng hay không.

Do đó, theo sáng chế, sau khi nhận thông tin dấu vân tay (nghĩa là, thông tin đặc điểm sinh trắc học) của người dùng mà cần được xác minh, thiết bị đầu cuối so khớp trực tiếp thông tin dấu vân tay chuẩn được lưu trữ theo cách cục bộ (nghĩa là, thông tin đặc điểm sinh trắc học chuẩn) phù hợp với thông tin dấu vân tay cần được xác minh.

Tiếp tục với ví dụ được mô tả trước đó, sau khi nhận thông tin dấu vân tay của người dùng mà cần được xác minh, điện thoại di động so khớp thông tin dấu vân tay chuẩn được lưu trữ theo cách cục bộ phù hợp với thông tin dấu vân tay cần được xác minh. Giả sử rằng thông tin dấu vân tay chuẩn phù hợp với thông tin dấu vân tay cần được xác minh được xác định.

S303. Tìm kiếm đối với khóa bí mật tương ứng với mã nhận dạng dựa vào mã nhận dạng tương ứng với thông tin đặc điểm sinh trắc học chuẩn sau khi so khớp thành công.

Theo sáng chế, để phân biệt mỗi đoạn thông tin dấu vân tay (nghĩa là, thông tin đặc điểm sinh trắc học) mà đã được lưu trữ trong thiết bị đầu cuối, thiết bị đầu cuối có thể cấp phát mã nhận dạng thông tin dấu vân tay (nghĩa là, mã nhận dạng thông tin đặc điểm sinh trắc học) cho mỗi đoạn thông tin dấu vân tay khi lưu trữ thông tin dấu vân tay này.

Ngoài ra, để xác minh danh tính người dùng bởi máy chủ tương ứng với dịch vụ trong tương lai, cụ thể là, máy chủ tương ứng với dịch vụ cần biết người dùng nào sử dụng dịch vụ. Theo sáng chế, khóa bí mật và khóa công khai tương ứng với mã nhận dạng cần được tạo ra dựa vào mã nhận dạng này. Mã nhận dạng tương ứng với thông tin dấu vân tay được sử dụng để đăng ký. Khóa bí mật và khóa công khai biểu diễn danh tính người dùng. Khóa bí mật đã tạo ra được lưu trữ trong thiết bị đầu cuối. Khi gửi yêu cầu xử lý dịch vụ đến máy chủ, thiết bị đầu cuối cần sử dụng khóa bí mật để ký vào yêu cầu xử lý dịch vụ, và gửi yêu cầu xử lý dịch vụ đã ký đến máy chủ.

Do đó, theo sáng chế, sau khi xác định thông tin dấu vân tay chuẩn phù hợp với thông tin dấu vân tay cần được xác minh, thiết bị đầu cuối cần tìm kiếm đối với khóa

bí mật tương ứng với mã nhận dạng dựa vào mã nhận dạng tương ứng với thông tin dấu vân tay chuẩn.

Tiếp tục với ví dụ được mô tả trước đó, sau khi xác định thông tin dấu vân tay chuẩn phù hợp với thông tin dấu vân tay cần được xác minh, điện thoại di động tìm kiếm đối với khóa bí mật tương ứng với mã nhận dạng dựa vào mã nhận dạng tương ứng với thông tin dấu vân tay chuẩn.

S304. Đăng ký danh tính người dùng với máy chủ dựa vào thông tin đặc điểm sinh trắc học cần được xác minh khi khóa bí mật tương ứng với mã nhận dạng không được xác định, vì vậy máy chủ lưu trữ khóa công khai tương ứng với thông tin đặc điểm sinh trắc học cần được xác minh.

Theo sáng chế, nếu thiết bị đầu cuối xác định thông tin dấu vân tay chuẩn phù hợp với thông tin dấu vân tay cần được xác minh ở bước S302, nhưng thiết bị đầu cuối không xác định khóa bí mật tương ứng với mã nhận dạng dựa vào mã nhận dạng tương ứng với thông tin dấu vân tay chuẩn, thì biểu thị rằng thông tin dấu vân tay cần được xác minh thuộc về người dùng, nhưng không phải là thông tin dấu vân tay được sử dụng trong quá trình đăng ký. Để tiếp tục cung cấp dịch vụ được yêu cầu cho người dùng, danh tính người dùng có thể được đăng ký trực tiếp với máy chủ dựa vào thông tin dấu vân tay (nghĩa là, thông tin đặc điểm sinh trắc học) mà cần được xác minh.

Ngoài ra, sáng chế đề xuất quy trình cụ thể để đăng ký danh tính người dùng dưới đây:

Khóa bí mật và khóa công khai tương ứng với mã nhận dạng được tạo ra dựa vào mã nhận dạng tương ứng với thông tin đặc điểm sinh trắc học chuẩn mà khớp với thông tin đặc điểm sinh trắc học cần được xác minh; mối quan hệ ánh xạ giữa mã nhận dạng và khóa bí mật đã tạo ra được lưu trữ trong thiết bị đầu cuối; và mối quan hệ ánh xạ giữa mã nhận dạng và khóa công khai đã tạo ra được gửi đến máy chủ để lưu trữ.

Đáng lưu ý trong bản mô tả này rằng thông tin đặc điểm sinh trắc học chuẩn tương ứng duy nhất với mã nhận dạng thông tin đặc điểm sinh trắc học chuẩn, và mã nhận dạng thông tin đặc điểm sinh trắc học chuẩn tương ứng với khóa bí mật và khóa công khai duy nhất. Nói cách khác, thông tin đặc điểm sinh trắc học chuẩn và mã nhận dạng thông tin đặc điểm sinh trắc học chuẩn là mối quan hệ ánh xạ một-một với khóa bí mật và khóa công khai. Theo sáng chế, nếu thông tin đặc điểm sinh trắc học cần

được xác minh tồn tại trong thiết bị đầu cuối, ở bước S302, chỉ một đoạn thông tin đặc điểm sinh trắc học chuẩn có thể được xác định. Nói cách khác, bước gửi mối quan hệ ánh xạ giữa mã nhận dạng và khóa công khai đã tạo ra đến máy chủ để lưu trữ cũng có thể đang lưu trữ, bởi máy chủ, khóa công khai tương ứng với thông tin đặc điểm sinh trắc học cần được xác minh.

Mặc dù khóa bí mật tương ứng với thông tin dấu vân tay (nghĩa là, thông tin đặc điểm sinh trắc học) không được tìm thấy theo cách cục bộ trong thiết bị đầu cuối, nhưng thông tin dấu vân tay có thể không phải là thông tin dấu vân tay của người dùng. Để nâng cao hơn nữa độ bảo mật thông tin khi người dùng sử dụng dịch vụ, theo sáng chế, trước khi danh tính người dùng được đăng ký với máy chủ dựa vào thông tin đặc điểm sinh trắc học cần được xác minh, người dùng có thể được nhắc để nhập vào mật khẩu cho dịch vụ. Khi mật khẩu được nhập vào bởi người dùng nhận được, thì thiết bị đầu cuối xác minh xem mật khẩu có chính xác hay không. Nếu mật khẩu là chính xác, thì danh tính người dùng có thể được đăng ký với máy chủ dựa vào thông tin đặc điểm sinh trắc học cần được xác minh. Nếu mật khẩu là không chính xác, thì danh tính người dùng không được đăng ký với máy chủ dựa vào thông tin đặc điểm sinh trắc học cần được xác minh, và người dùng được thông báo là việc xử lý dịch vụ thất bại.

Ngoài ra, đáng lưu ý trong bản mô tả này rằng khi thiết bị đầu cuối không xác định khóa bí mật tương ứng với mã nhận dạng, thiết bị đầu cuối có thể thông báo trực tiếp cho người dùng rằng việc xử lý dịch vụ thất bại. Trong trường hợp này, người dùng có thể nhập vào mật khẩu cho dịch vụ để tiếp tục sử dụng dịch vụ. Thiết bị đầu cuối có thể nhận mật khẩu được nhập vào bởi người dùng và xác minh xem mật khẩu có chính xác hay không, và nếu có, thì đăng ký danh tính người dùng với máy chủ dựa vào thông tin đặc điểm sinh trắc học cần được xác minh.

Tiếp tục với ví dụ được mô tả trước đó, giả sử rằng điện thoại di động đã không xác định khóa bí mật tương ứng với mã nhận dạng. Điện thoại di động nhắc người dùng sử dụng mật khẩu cho dịch vụ truy vấn thông tin. Giả sử rằng người dùng nhập vào mật khẩu xxxx. Sau khi nhận mật khẩu xxxx mà được nhập vào bởi người dùng, nếu thiết bị đầu cuối xác minh rằng mật khẩu là chính xác, thì thiết bị đầu cuối tạo ra khóa bí mật và khóa công khai tương ứng với mã nhận dạng, trong đó mã nhận dạng này tương ứng với thông tin dấu vân tay chuẩn mà khớp với thông tin dấu vân tay cần được xác minh dựa vào mã nhận dạng, lưu trữ mối quan hệ ánh xạ giữa mã nhận dạng

và khóa bí mật đã tạo ra trong điện thoại di động, và gửi mối quan hệ ánh xạ giữa mã nhận dạng và khóa công khai đã tạo ra đến máy chủ để lưu trữ.

Theo phương pháp nêu trên, bất kể thông tin đặc điểm sinh trắc học được sử dụng bởi người dùng để đăng ký, miễn là thiết bị đầu cuối có thể xác định thông tin đặc điểm sinh trắc học chuẩn phù hợp với thông tin đặc điểm sinh trắc học cần được xác minh, ngay cả khi khóa bí mật tương ứng với mã nhận dạng không được xác định trong thiết bị đầu cuối dựa vào mã nhận dạng tương ứng với thông tin đặc điểm sinh trắc học chuẩn, thì thiết bị đầu cuối có thể đăng ký trực tiếp danh tính người dùng dựa vào thông tin đặc điểm sinh trắc học cần được xác minh, để hoàn thành việc xử lý dịch vụ, tạo ra sự thuận tiện tuyệt vời cho người dùng sử dụng dịch vụ, và cũng nâng cao một cách hiệu quả tỷ lệ thành công của việc sử dụng dịch vụ.

Hơn nữa, trong các ứng dụng thực tế, yêu cầu xử lý dịch vụ có thể được gửi đến máy chủ dựa vào thông tin đặc điểm sinh trắc học cần được xác minh sau khi danh tính người dùng được đăng ký với máy chủ. Như vậy, máy chủ thực hiện việc xử lý dịch vụ dựa vào khóa công khai tương ứng với thông tin đặc điểm sinh trắc học cần được xác minh.

Ở bước S304, khóa bí mật và khóa công khai tương ứng với mã nhận dạng của thông tin dấu vân tay (nghĩa là, thông tin đặc điểm sinh trắc học) đã được tạo ra lại dựa vào thông tin dấu vân tay cần được xác minh, và khóa công khai được gửi đến máy chủ để lưu trữ. Do đó, trong quy trình gửi yêu cầu xử lý dịch vụ đến máy chủ dựa vào thông tin dấu vân tay cần được xác minh, sáng chế có thể bao gồm các bước sau: ký thông tin dịch vụ dựa vào khóa bí mật đã tạo ra và gửi yêu cầu xử lý dịch vụ mà bao gồm thông tin dịch vụ đã ký và mã nhận dạng đến máy chủ, vì vậy máy chủ xác định khóa công khai tương ứng với mã nhận dạng có trong yêu cầu xử lý dịch vụ dựa vào mã nhận dạng, xác minh chữ ký của thông tin dịch vụ có trong yêu cầu xử lý dịch vụ dựa vào khóa công khai đã xác định để xác minh danh tính người dùng, và thực hiện việc xử lý dịch vụ đối với thông tin dịch vụ.

Tiếp tục với ví dụ được mô tả trước đó, điện thoại di động ký thông tin đăng nhập dựa vào khóa bí mật đã tạo ra của mã nhận dạng, và gửi yêu cầu xử lý đăng nhập mà bao gồm thông tin đăng nhập đã ký và mã nhận dạng đến máy chủ. Máy chủ xác định khóa công khai tương ứng với mã nhận dạng dựa vào mã nhận dạng có trong yêu

cầu xử lý đăng nhập, xác minh chữ ký của thông tin đăng nhập có trong yêu cầu xử lý đăng nhập bằng cách sử dụng khóa công khai, và hoàn thành việc đăng nhập của người dùng.

Trong các ứng dụng thực tế, việc thanh toán đối với hàng hóa được mua bằng cách sử dụng ứng dụng thanh toán đã trở nên ngày càng phổ biến. Theo sáng chế, phần sau mô tả sáng chế một cách chi tiết bằng cách sử dụng một ví dụ trong đó yêu cầu xử lý dịch vụ là yêu cầu thanh toán.

Ví dụ, giả sử rằng người dùng A đã đăng ký thông tin dấu vân tay (nghĩa là, thông tin nhận dạng) trong ứng dụng thanh toán. Khi người dùng A thanh toán cho hàng hóa được mua bằng cách sử dụng ứng dụng thanh toán, thì người dùng A mở ứng dụng thanh toán trên điện thoại di động (nghĩa là, thiết bị đầu cuối) và nhấn bằng dấu vân tay. Sau khi nhận thông tin dấu vân tay của người dùng mà cần được xác minh, điện thoại di động so khớp theo cách cục bộ thông tin dấu vân tay chuẩn phù hợp với thông tin dấu vân tay cần được xác minh. Giả sử rằng thông tin dấu vân tay chuẩn phù hợp với thông tin dấu vân tay cần được xác minh được xác định. Điện thoại di động tìm kiếm đối với khóa bí mật tương ứng với mã nhận dạng dựa vào mã nhận dạng tương ứng với thông tin dấu vân tay chuẩn. Nếu điện thoại di động không xác định khóa bí mật tương ứng với mã nhận dạng, thì điện thoại di động nhắc trực tiếp người dùng nhập vào mật khẩu thanh toán. Điện thoại di động nhận mật khẩu thanh toán cccc được nhập vào bởi người dùng và xác minh xem mật khẩu này có chính xác hay không. Nếu có, điện thoại di động tạo ra khóa bí mật và khóa công khai tương ứng với mã nhận dạng, trong đó mã nhận dạng tương ứng với thông tin dấu vân tay chuẩn mà khớp với thông tin dấu vân tay cần được xác minh dựa vào mã nhận dạng, lưu trữ mối quan hệ ánh xạ giữa mã nhận dạng và khóa bí mật đã tạo ra trong điện thoại di động, và gửi mối quan hệ ánh xạ giữa mã nhận dạng và khóa công khai đã tạo ra đến máy chủ để lưu trữ.

Trong quy trình xử lý dịch vụ thanh toán sau đây, điện thoại di động ký thông tin thanh toán dựa vào khóa bí mật đã tạo ra tương ứng với mã nhận dạng và gửi yêu cầu xử lý thanh toán mà bao gồm thông tin thanh toán đã ký và mã nhận dạng đến máy chủ. Máy chủ xác định khóa công khai tương ứng với mã nhận dạng dựa vào mã nhận dạng có trong yêu cầu xử lý thanh toán, xác minh chữ ký của thông tin thanh toán bằng cách sử dụng khóa công khai, và hoàn thành việc thanh toán một cách thành công.

Được mô tả ở trên là phương pháp đăng ký danh tính được đề xuất theo một phương án thực hiện của sáng chế. Như được thể hiện trên Fig.4, dựa vào cùng ý tưởng, sáng chế còn đề xuất thiết bị đăng ký danh tính tương ứng.

Fig.4 là sơ đồ cấu trúc sơ lược minh họa thiết bị đăng ký danh tính, theo một phương án thực hiện của sáng chế. Thiết bị này bao gồm các bộ phận sau: môđun nhận 401, được tạo cấu hình để nhận thông tin đặc điểm sinh trắc học của người dùng mà cần được xác minh; môđun so khớp 402, được tạo cấu hình để so khớp thông tin đặc điểm sinh trắc học chuẩn phù hợp với thông tin đặc điểm sinh trắc học cần được xác minh trong thông tin đặc điểm sinh trắc học được lưu trữ trước; môđun tìm kiếm 403, được tạo cấu hình để tìm kiếm đối với khóa bí mật tương ứng với mã nhận dạng dựa vào mã nhận dạng tương ứng với thông tin đặc điểm sinh trắc học chuẩn sau khi so khớp thành công; và môđun đăng ký 404, được tạo cấu hình để đăng ký danh tính người dùng với máy chủ dựa vào thông tin đặc điểm sinh trắc học cần được xác minh khi môđun tìm kiếm 403 không xác định khóa bí mật tương ứng với mã nhận dạng, vì vậy máy chủ lưu trữ khóa công khai tương ứng với thông tin đặc điểm sinh trắc học cần được xác minh.

Thiết bị này còn bao gồm bộ phận sau: môđun xác minh mật khẩu 405, được tạo cấu hình để nhận mật khẩu được nhập vào bởi người dùng và xác minh rằng mật khẩu là chính xác trước khi môđun đăng ký 404 đăng ký danh tính người dùng với máy chủ dựa vào thông tin đặc điểm sinh trắc học cần được xác minh.

Môđun đăng ký 404 được tạo cấu hình để tạo ra khóa bí mật và khóa công khai tương ứng với mã nhận dạng dựa vào mã nhận dạng tương ứng với thông tin đặc điểm sinh trắc học chuẩn mà khớp với thông tin đặc điểm sinh trắc học cần được xác minh; lưu trữ mối quan hệ ánh xạ giữa mã nhận dạng và khóa bí mật đã tạo ra trong thiết bị đầu cuối; và gửi mối quan hệ ánh xạ giữa mã nhận dạng và khóa công khai đã tạo ra đến máy chủ để lưu trữ.

Thiết bị này còn bao gồm bộ phận sau: môđun xử lý 406, được tạo cấu hình để gửi yêu cầu xử lý dịch vụ đến máy chủ dựa vào thông tin đặc điểm sinh trắc học cần được xác minh sau khi môđun đăng ký 404 đăng ký danh tính người dùng với máy chủ, vì vậy máy chủ thực hiện việc xử lý dịch vụ dựa vào khóa công khai tương ứng với thông tin đặc điểm sinh trắc học cần được xác minh.

Môđun xử lý 406 được tạo cấu hình để ký thông tin dịch vụ dựa vào khóa bí mật đã tạo ra và gửi yêu cầu xử lý dịch vụ mà bao gồm thông tin dịch vụ đã ký và mã nhận dạng đến máy chủ, vì vậy máy chủ xác định khóa công khai tương ứng với mã nhận dạng có trong yêu cầu xử lý dịch vụ đã nhận và thực hiện việc xử lý dịch vụ dựa vào khóa công khai đã xác định và thông tin dịch vụ đã ký.

Yêu cầu xử lý dịch vụ bao gồm yêu cầu thanh toán.

Trong cấu hình điển hình, thiết bị tính toán bao gồm một hoặc nhiều bộ xử lý (CPU), giao diện đầu vào/đầu ra, giao diện mạng và bộ nhớ.

Bộ nhớ có thể bao gồm bộ nhớ không ổn định, bộ nhớ truy nhập ngẫu nhiên (random access memory, RAM) và/hoặc bộ nhớ không khả biến, v.v. trong vật ghi đọc được bằng máy tính, chẳng hạn như bộ nhớ chỉ đọc (read-only memory, ROM) hoặc bộ nhớ chớp (flash RAM). Bộ nhớ là một ví dụ về vật ghi đọc được bằng máy tính.

Vật ghi đọc được bằng máy tính bao gồm các vật ghi ổn định, không ổn định, di chuyển được, không thể di chuyển được mà có thể lưu trữ thông tin bằng cách sử dụng phương pháp hoặc công nghệ bất kỳ. Thông tin có thể là lệnh đọc được bằng máy tính, cấu trúc dữ liệu, môđun chương trình hoặc dữ liệu khác. Các ví dụ về vật ghi lưu trữ bằng máy tính bao gồm nhưng không bị giới hạn ở bộ nhớ truy cập ngẫu nhiên đổi pha (phase change random access memory, PRAM), RAM tĩnh (static RAM, SRAM), RAM động (dynamic RAM, DRAM), RAM của kiểu khác, bộ nhớ chỉ đọc (ROM), bộ nhớ chỉ đọc lập trình được xóa được bằng điện (electrically erasable programmable read-only memory, EEPROM), bộ nhớ chớp hoặc công nghệ bộ nhớ khác, bộ nhớ chỉ đọc đĩa nén (compact disc read-only memory, CD-ROM), đĩa đa năng kỹ thuật số (digital versatile disc, DVD) hoặc hoặc bộ lưu trữ quang khác, băng từ, bộ lưu trữ đĩa từ, một thiết bị lưu trữ từ khác hoặc vật ghi không truyền dẫn khác bất kỳ. Vật ghi lưu trữ bằng máy tính có thể được sử dụng để lưu trữ thông tin mà có thể được truy nhập bởi thiết bị tính toán. Như được mô tả trong bản mô tả này, vật ghi đọc được bằng máy tính không bao gồm các vật ghi tạm thời, ví dụ, tín hiệu dữ liệu được điều biến và sóng mang.

Đáng lưu ý thêm là, thuật ngữ "bao gồm", "chứa" hoặc biến thể khác bất kỳ nhằm bao gồm sự bao hàm không loại trừ sao cho quy trình, phương pháp, sản phẩm hoặc thiết bị mà bao gồm một loạt phần tử không chỉ bao gồm các phần tử này, mà còn

bao gồm các phần tử khác mà không được liệt kê một cách rõ ràng, hoặc còn bao gồm các phần tử vốn có đối với quy trình, phương pháp, sản phẩm hoặc thiết bị này. Phần tử đứng trước bởi cụm từ "bao gồm ..." không, mà không có nhiều ràng buộc hơn, loại trừ sự tồn tại của các phần tử giống nhau bổ sung trong quy trình, phương pháp, sản phẩm hoặc thiết bị mà bao gồm phần tử này.

Người có hiểu biết trung bình trong lĩnh vực sẽ hiểu rằng các phương án thực hiện của sáng chế có thể được đề xuất dưới dạng phương pháp, hệ thống hoặc sản phẩm chương trình máy tính. Do đó, sáng chế có thể sử dụng dạng các phương án thực hiện chỉ về phần cứng, các phương án thực hiện chỉ về phần mềm hoặc các phương án thực hiện với sự kết hợp của phần mềm và phần cứng. Ngoài ra, sáng chế có thể sử dụng dạng sản phẩm chương trình máy tính được thực hiện trên một hoặc nhiều vật ghi lưu trữ sử dụng được bằng máy tính (bao gồm nhưng không bị giới hạn ở bộ nhớ đĩa từ, CD-ROM và bộ nhớ quang) mà bao gồm mã chương trình sử dụng được bằng máy tính.

Các phần mô tả nêu trên chỉ là các phương án thực hiện của sáng chế, và không nhằm làm giới hạn sáng chế. Người có hiểu biết trung bình trong lĩnh vực kỹ thuật có thể thực hiện các cải biến và thay đổi khác nhau đối với sáng chế. Các cải biến, thay thế tương đương, cải tiến, v.v. bất kỳ được thực hiện nằm trong mục đích và nguyên lý của sáng chế sẽ nằm trong phạm vi bảo hộ của các điểm yêu cầu bảo hộ của sáng chế.

YÊU CẦU BẢO HỘ

1. Phương pháp đăng ký danh tính người dùng, phương pháp này bao gồm các bước:

nhận (S301), bởi thiết bị đầu cuối, thông tin đặc điểm sinh trắc học của người dùng, người mà cần được xác minh, trong đó người dùng có tài khoản được đăng ký với dịch vụ được cung cấp bởi máy chủ;

so khớp (S302), bởi thiết bị đầu cuối, đoạn thông tin đặc điểm sinh trắc học chuẩn được lưu trữ cục bộ mà phù hợp với thông tin đặc điểm sinh trắc học đã nhận của người dùng, người mà cần được xác minh, trong đó mỗi đoạn thông tin đặc điểm sinh trắc học chuẩn được lưu trữ cục bộ được cấp phát mã nhận dạng đặc điểm sinh trắc học tương ứng và được sử dụng để xác định xem người dùng tương ứng có thể được xác minh khi sử dụng dịch vụ hay không;

xác định, bởi thiết bị đầu cuối, xem khóa bí mật tương ứng với mã nhận dạng đặc điểm sinh trắc học của đoạn thông tin đặc điểm sinh trắc học chuẩn được lưu trữ cục bộ có được lưu trữ ở thiết bị đầu cuối hay không, bao gồm bước tìm kiếm (S303), bởi thiết bị đầu cuối và sau khi so khớp thành công, đối với khóa bí mật tương ứng với mã nhận dạng đặc điểm sinh trắc học của đoạn thông tin đặc điểm sinh trắc học chuẩn được lưu trữ cục bộ; và

đáp lại việc xác định rằng khóa bí mật tương ứng với mã nhận dạng đặc điểm sinh trắc học của đoạn thông tin đặc điểm sinh trắc học chuẩn được lưu trữ cục bộ không được lưu trữ ở thiết bị đầu cuối, thì xác định rằng thông tin đặc điểm sinh trắc học đã nhận của người dùng, người mà cần được xác minh thuộc về người dùng nhưng không phải là thông tin đặc điểm sinh trắc học được cung cấp bởi người dùng trong quá trình đăng ký ban đầu với máy chủ và đăng ký trực tiếp (S304) danh tính người dùng với máy chủ dựa vào thông tin đặc điểm sinh trắc học đã nhận của người dùng, người mà cần được xác minh và khóa bí mật và khóa công khai đã tạo lại tương ứng, trong đó máy chủ lưu trữ khóa công khai đã tạo ra tương ứng với thông tin đặc điểm sinh trắc học đã nhận của người dùng, người mà cần được xác minh (S304) và mối quan hệ ánh xạ giữa mã nhận dạng đặc điểm sinh trắc học tương ứng và khóa công khai đã tạo ra.

2. Phương pháp theo điểm 1, trong đó trước khi đăng ký danh tính người dùng với máy chủ dựa vào thông tin đặc điểm sinh trắc học đã nhận của người dùng, người mà cần

được xác minh, phương pháp này còn bao gồm các bước:

nhận mật khẩu được nhập bởi người dùng; và

xác minh rằng mật khẩu này là chính xác.

3. Phương pháp theo điểm 1, trong đó bước đăng ký danh tính người dùng với máy chủ dựa vào thông tin đặc điểm sinh trắc học đã nhận của người dùng, người mà cần được xác minh bao gồm các bước:

tạo ra khóa bí mật và khóa công khai tương ứng với mã nhận dạng đặc điểm sinh trắc học của đoạn thông tin đặc điểm sinh trắc học chuẩn được lưu trữ cục bộ dựa vào mã nhận dạng đặc điểm sinh trắc học của đoạn thông tin đặc điểm sinh trắc học chuẩn được lưu trữ cục bộ mà khớp với thông tin đặc điểm sinh trắc học đã nhận của người dùng, người mà cần được xác minh;

lưu trữ mối quan hệ ánh xạ giữa mã nhận dạng đặc điểm sinh trắc học của đoạn thông tin đặc điểm sinh trắc học chuẩn được lưu trữ cục bộ và khóa bí mật đã tạo ra trong thiết bị đầu cuối; và

gửi mối quan hệ ánh xạ giữa mã nhận dạng của đoạn thông tin đặc điểm sinh trắc học chuẩn được lưu trữ cục bộ và khóa công khai đã tạo ra đến máy chủ để lưu trữ.

4. Phương pháp theo điểm 1, trong đó sau khi đăng ký danh tính người dùng với máy chủ, phương pháp này còn bao gồm bước:

gửi yêu cầu xử lý dịch vụ đến máy chủ dựa vào thông tin đặc điểm sinh trắc học đã nhận của người dùng, người mà cần được xác minh, trong đó máy chủ thực hiện việc xử lý dịch vụ dựa vào khóa công khai tương ứng với thông tin đặc điểm sinh trắc học đã nhận của người dùng, người mà cần được xác minh.

5. Phương pháp theo điểm 4, trong đó bước gửi yêu cầu xử lý dịch vụ đến máy chủ dựa vào thông tin đặc điểm sinh trắc học đã nhận của người dùng, người mà cần được xác minh bao gồm bước:

ký thông tin dịch vụ dựa vào khóa bí mật đã tạo ra và gửi yêu cầu xử lý dịch vụ mà bao gồm thông tin dịch vụ đã ký và mã nhận dạng của đoạn thông tin sinh trắc học chuẩn đã lưu trữ cục bộ đến máy chủ, trong đó máy chủ tìm kiếm khóa công khai tương ứng với mã nhận dạng có trong yêu cầu xử lý dịch vụ đã nhận và thực hiện việc

xử lý dịch vụ dựa vào khóa công khai đã xác định và thông tin dịch vụ đã ký.

6. Phương pháp theo điểm 4 hoặc điểm 5, trong đó yêu cầu xử lý dịch vụ bao gồm yêu cầu thanh toán.

7. Phương pháp theo điểm 4 hoặc điểm 5, trong đó phương pháp này còn bao gồm bước:

tạo ra yêu cầu đối với đầu vào người dùng bao gồm mật khẩu cho dịch vụ truy vấn thông tin.

8. Phương pháp theo điểm bất kỳ trong số các điểm từ 1 đến 6, trong đó thông tin đặc điểm sinh trắc học thể hiện danh tính người dùng và biểu thị đặc điểm vật lý của người dùng.

9. Phương pháp theo điểm 8, trong đó đặc điểm vật lý của người dùng bao gồm mống mắt của mắt hoặc dấu vân tay của ngón tay.

10. Thiết bị đăng ký danh tính, thiết bị này bao gồm các môđun được tạo cấu hình để thực hiện phương pháp theo điểm bất kỳ trong số các điểm từ 1 đến 9.

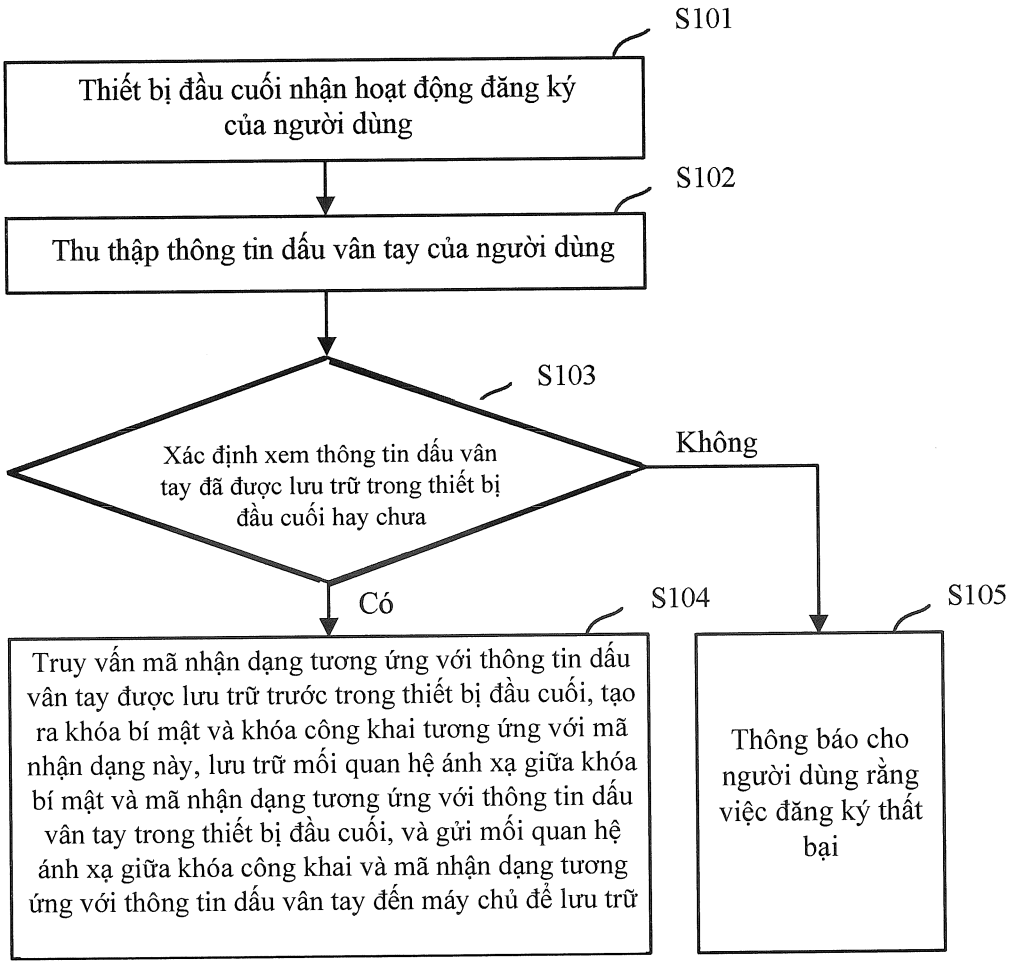

S101
Thiết bị đầu cuối nhận hoạt động đăng ký của người dùng
S102
Thu thập thông tin dấu vân tay của người dùng
S103
Xác định xem thông tin dấu vân tay đã được lưu trữ trong thiết bị đầu cuối hay chưa
Không
Có
S104
Truy vấn mã nhận dạng tương ứng với thông tin dấu vân tay được lưu trữ trước trong thiết bị đầu cuối, tạo ra khóa bí mật và khóa công khai tương ứng với mã nhận dạng này, lưu trữ mối quan hệ ánh xạ giữa khóa bí mật và mã nhận dạng tương ứng với thông tin dấu vân tay trong thiết bị đầu cuối, và gửi mối quan hệ ánh xạ giữa khóa công khai và mã nhận dạng tương ứng với thông tin dấu vân tay đến máy chủ để lưu trữ
S105
Thông báo cho người dùng rằng việc đăng ký thất bại

FIG. 1

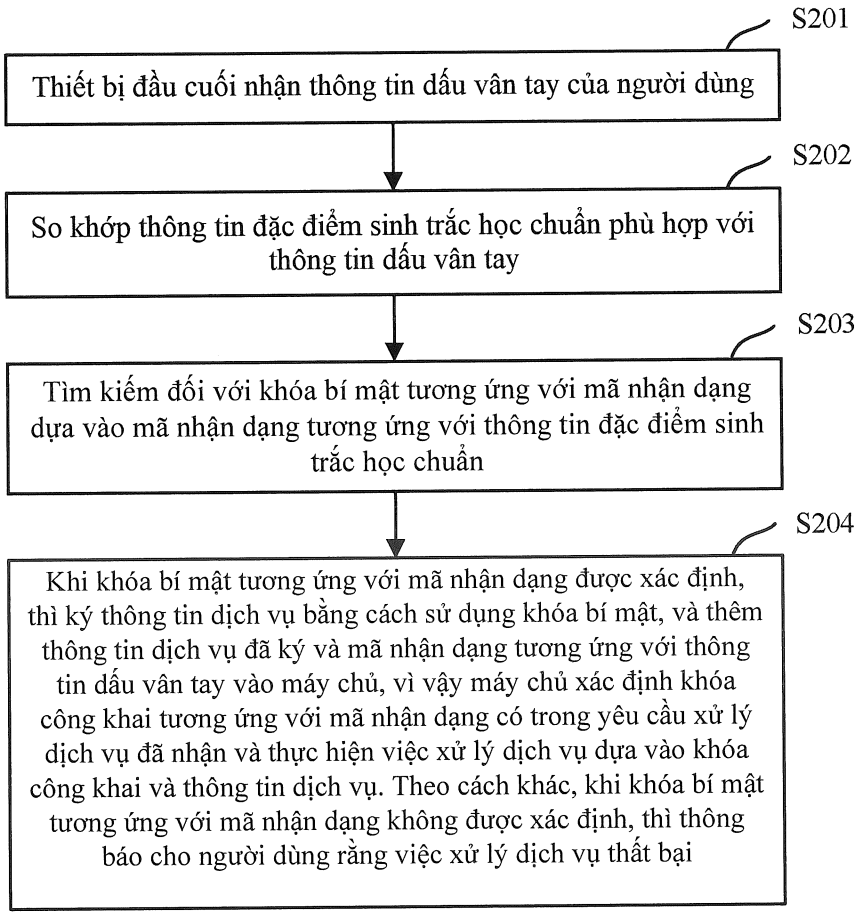

S201
Thiết bị đầu cuối nhận thông tin dấu vân tay của người dùng
S202
So khớp thông tin đặc điểm sinh trắc học chuẩn phù hợp với thông tin dấu vân tay
S203
Tìm kiếm đối với khóa bí mật tương ứng với mã nhận dạng dựa vào mã nhận dạng tương ứng với thông tin đặc điểm sinh trắc học chuẩn
S204
Khi khóa bí mật tương ứng với mã nhận dạng được xác định, thì ký thông tin dịch vụ bằng cách sử dụng khóa bí mật, và thêm thông tin dịch vụ đã ký và mã nhận dạng tương ứng với thông tin dấu vân tay vào máy chủ, vì vậy máy chủ xác định khóa công khai tương ứng với mã nhận dạng có trong yêu cầu xử lý dịch vụ đã nhận và thực hiện việc xử lý dịch vụ dựa vào khóa công khai và thông tin dịch vụ. Theo cách khác, khi khóa bí mật tương ứng với mã nhận dạng không được xác định, thì thông báo cho người dùng rằng việc xử lý dịch vụ thất bại

FIG. 2

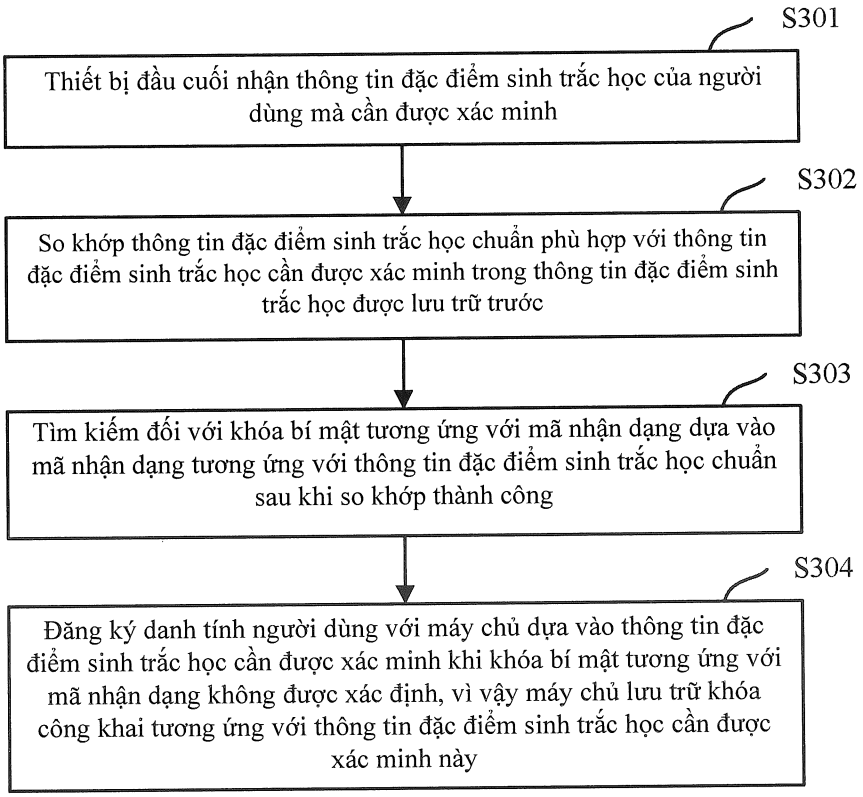

S301
Thiết bị đầu cuối nhận thông tin đặc điểm sinh trắc học của người dùng mà cần được xác minh
S302
So khớp thông tin đặc điểm sinh trắc học chuẩn phù hợp với thông tin đặc điểm sinh trắc học cần được xác minh trong thông tin đặc điểm sinh trắc học được lưu trữ trước
S303
Tìm kiếm đối với khóa bí mật tương ứng với mã nhận dạng dựa vào mã nhận dạng tương ứng với thông tin đặc điểm sinh trắc học chuẩn sau khi so khớp thành công
S304
Đăng ký danh tính người dùng với máy chủ dựa vào thông tin đặc điểm sinh trắc học cần được xác minh khi khóa bí mật tương ứng với mã nhận dạng không được xác định, vì vậy máy chủ lưu trữ khóa công khai tương ứng với thông tin đặc điểm sinh trắc học cần được xác minh này

FIG. 3

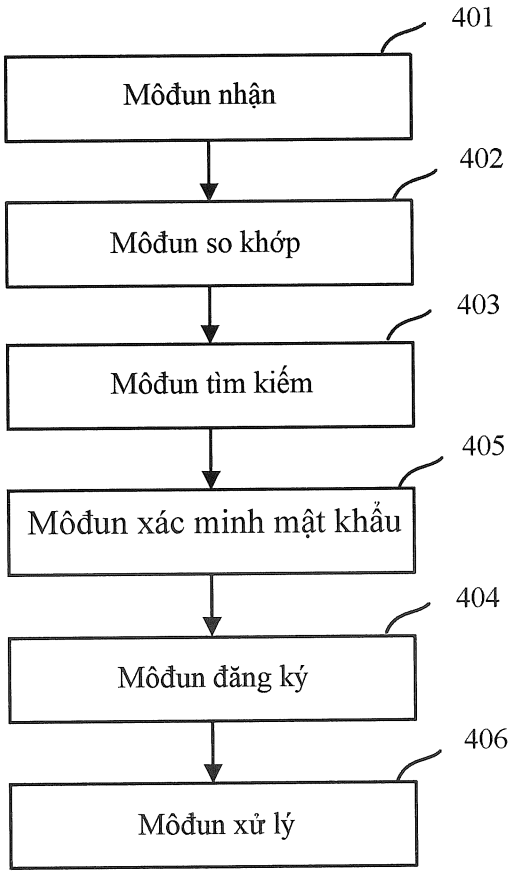

401
Môđun nhận
402
Môđun so khớp
403
Môđun tìm kiếm
405
Môđun xác minh mật khẩu
404
Môđun đăng ký
406
Môđun xử lý

FIG. 4