(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) **1-0027393**

(51)[7] **G06F 21/32**; G06F 21/64; G06F 21/62

(13) **B**

(21) 1-2017-00937

(22) 15/06/2015

(86) PCT/HU2015/000055 15/06/2015

(87) WO2016/027111 25/02/2016

(30) P 14 00392 18/08/2014 HU; P 15 00259 29/05/2015 HU

(45) 25/02/2021 395

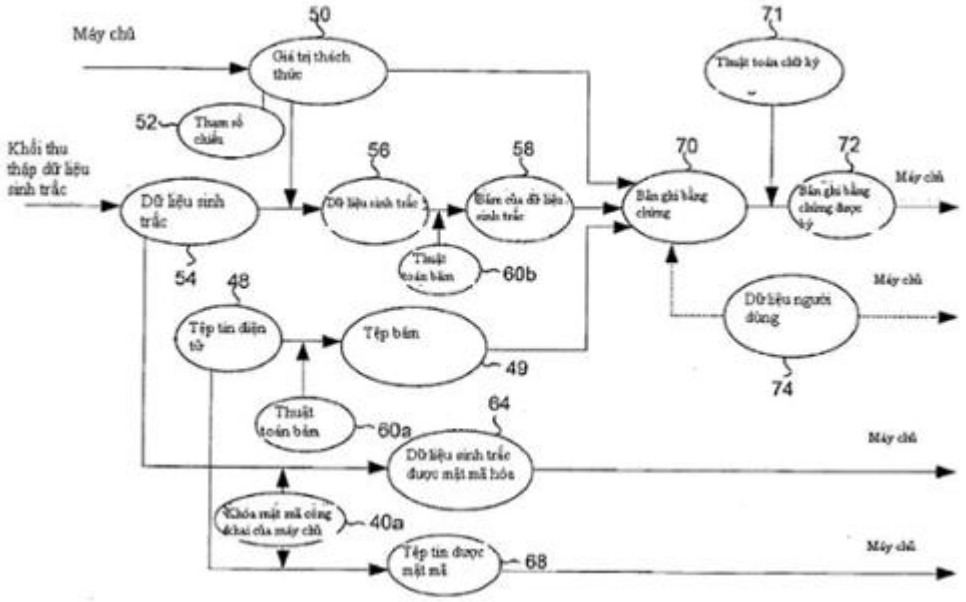
(43) 26/06/2017 351A

(76) 1. CSÍK, Balázs (HU)
Királyi Pál u. 18, I. emelet 6, H-1053 Budapest, Hungary
2. LENGYEL, Csaba (HU)
Madách u. 77, H-2461 Tárnok, Hungary
3. ROGÁN, Antal (HU)
Hankóczy Jenö u. 4-6, D lépcsöház, III/6 H-1022 Budapest, Hungary

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

(54) PHƯƠNG PHÁP KÝ SỐ TỆP TIN ĐIỆN TỬ VÀ PHƯƠNG PHÁP XÁC THỰC

(57) Sáng chế đề xuất phương pháp ký số tệp tin điện tử (48), bao gồm các bước được thực thi bởi máy chủ: tạo giá trị thử thách (50) bao gồm tham số chiếu (52), truyền giá trị thử thách (50) đến thiết bị máy khách qua kênh truyền thông, tiếp nhận, qua kênh truyền thông, bản ghi chứng cứ (70), tệp tin điện tử (48) được ký, và dữ liệu sinh trắc của người dùng (54) từ thiết bị máy khách, tạo dữ liệu kiểm chứng sinh học rút gọn bằng cách áp dụng phép chiếu sử dụng tham số chiếu (52), tạo bản ghi chứng cứ kiểm chứng và so sánh nó với bản ghi chứng cứ (70) được gửi bởi thiết bị máy khách, tạo chứng nhận máy chủ, ký chứng nhận máy chủ áp dụng khóa ký riêng tư của máy chủ, nhờ đó tạo chứng nhận máy chủ được ký, tạo chữ ký số bằng cách liên kết ít nhất chứng nhận máy chủ được ký và băm (49) của tệp tin điện tử (48), và liên kết chữ ký số với tệp tin điện tử (48), nhờ đó tạo tệp tin điện tử được ký số. Sáng chế còn đề xuất phương pháp xác thực.



Lĩnh vực kỹ thuật được đề cập

Sáng chế liên quan đến các phương pháp ký số tệp tin điện tử và đến phương pháp xác thực dựa vào sinh trắc học.

Tình trạng kỹ thuật của sáng chế

Có nhiều phương pháp khác nhau để xác thực và ký các tệp tin điện tử. Công bố đơn quốc tế WO 2007/034255 bộc lộ phương pháp trong đó hệ thống cung cấp chữ ký số tập trung hóa được áp dụng để ký số các tệp tin điện tử được đệ trình cho nó thay mặt các người dùng từ xa sử dụng các chữ ký số gồm dữ liệu sinh trắc của người dùng. Nhờ dữ liệu sinh trắc (chẳng hạn, dữ liệu liên quan chữ ký viết bằng tay) chữ ký số có thể được liên kết với người ký tên, trong khi sáng chế đề xuất việc chữ ký số có thể chỉ được áp dụng cho tệp tin điện tử theo cách thức được xác thực và được giám sát. Phương pháp có nhược điểm là việc kiểm chứng dữ liệu được gửi lại bởi người dùng từ xa, cũng như việc quản lý dữ liệu sinh trắc, không đủ bảo mật.

Ở bằng Mỹ số US 6,735,695 B1, giải pháp được bộc lộ trong đó thực hiện xác thực bằng cách sử dụng chỉ một phần của dữ liệu sinh trắc thay vì toàn bộ sinh trắc học. Đối với độ bảo mật tăng cường, nhờ đó giả sử rằng mẫu sinh trắc học đầy đủ được truyền. Mẫu sinh trắc học bán phần được áp dụng để xác thực có thể còn được lựa chọn bằng cách sử dụng số ngẫu nhiên. Nhược điểm của giải pháp đã biết này chính là không thực thi rút gọn dữ liệu (biến đổi), và do vậy bằng cách nghe trộm trên các tuyến truyền thông đối với các sinh trắc học bán phần, các cá nhân không được ủy quyền có thể không sớm thì muộn bắt được thông tin sinh trắc đầy đủ. Ưu điểm khác của giải pháp chính là bộ cảm biến sinh trắc ghi nhận mẫu

sinh trắc đầy đủ, và các sinh trắc học bán phần được lựa chọn từ mẫu đầy đủ. Việc ghi nhận mẫu sinh trắc đầy đủ tạo điểm yếu đáng kể.

Công bố đơn số US 2008/0209227 A1 bộc lộ giải pháp trong đó phiên bản rút gọn biến đổi của mẫu sinh trắc được tạo. Dữ liệu sinh trắc rút gọn hoặc tóm tắt sinh trắc rút gọn có thể chứa các dấu hiệu đặc trưng khác nhau của mẫu sinh trắc, chẳng hạn các đoạn tuyến tính. Ở công bố đơn số US 2010/0066493 A1, giải pháp liên quan biến đổi phép chiếu ngẫu nhiên của dữ liệu sinh trắc được bộc lộ. Các giải pháp đã biết này có các nhược điểm nêu trên.

Bản chất kỹ thuật của sáng chế

Mục đích của sáng chế là đề xuất các phương pháp ký số và xác thực mà loại trừ các nhược điểm của các giải pháp kỹ thuật đã biết ở mức độ lớn nhất có thể.

Sáng chế đề cập đến phương pháp ký số tệp tin điện tử, bao gồm các bước sau được thực thi bởi máy chủ: tạo giá trị thử thách bao gồm tham số chiếu; truyền giá trị thử thách đến thiết bị máy khách qua kênh truyền thông; tiếp nhận, qua kênh truyền thông, bản ghi chứng cứ, tệp tin điện tử được ký, và dữ liệu sinh trắc của người dùng từ thiết bị máy khách, bản ghi chứng cứ được tạo bởi thiết bị máy khách bằng cách liên kết giá trị thử thách, băm của dữ liệu sinh trắc rút gọn, dữ liệu sinh trắc rút gọn được tạo từ dữ liệu sinh trắc áp dụng phép chiếu sử dụng tham số chiếu, và băm của tệp tin điện tử; tạo dữ liệu kiểm chứng sinh học rút gọn từ dữ liệu sinh trắc áp dụng phép chiếu sử dụng tham số chiếu; tạo băm của dữ liệu kiểm chứng sinh học rút gọn; tạo băm của tệp tin điện tử; tạo bản ghi chứng cứ kiểm chứng bằng cách liên kết giá trị thử thách, băm của dữ liệu kiểm chứng sinh học rút gọn, và băm của tệp tin điện tử, và so sánh nó với bản ghi chứng cứ được gửi bởi thiết bị máy khách và chỉ tiếp tục quá trình chữ ký số nếu bản ghi chứng cứ kiểm chứng giống hệt với bản

ghi chứng cứ được gửi bởi thiết bị máy khách; nhận diện người dùng của thiết bị máy khách và định nghĩa ít nhất một mục dữ liệu người dùng; tạo chứng nhận máy chủ bằng cách liên kết ít nhất băm của tệp tin điện tử, ít nhất một mục dữ liệu người dùng, và dữ liệu chữ ký liên quan ít nhất đến thời gian của chữ ký; ký chứng nhận máy chủ áp dụng khóa ký riêng tư của máy chủ, nhờ đó tạo chứng nhận máy chủ được ký; tạo chữ ký số bằng cách liên kết ít nhất chứng nhận máy chủ được ký và băm của tệp tin điện tử, và liên kết chữ ký số với tệp tin điện tử, nhờ đó tạo tệp tin điện tử được ký số.

Sáng chế đề cập đến phương pháp ký số tệp tin điện tử bao gồm các bước: tạo bởi máy chủ giá trị thử thách bao gồm tham số chiếu; truyền bởi máy chủ giá trị thử thách đến thiết bị máy khách qua kênh truyền thông; ghi nhận dữ liệu sinh trắc bởi khối thu thập dữ liệu sinh trắc; bằng cách áp dụng phép chiếu sử dụng tham số chiếu, tạo dữ liệu sinh trắc rút gọn từ dữ liệu sinh trắc nhờ thiết bị máy khách; tạo băm của dữ liệu sinh trắc rút gọn nhờ thiết bị máy khách; tạo băm của tệp tin điện tử nhờ thiết bị máy khách; tạo bởi thiết bị máy khách bản ghi chứng cứ bằng cách liên kết ít nhất giá trị thử thách, băm của dữ liệu sinh trắc rút gọn, và băm của tệp tin điện tử; truyền bởi thiết bị máy khách bản ghi chứng cứ, tệp tin điện tử được ký và dữ liệu sinh trắc đến máy chủ qua kênh truyền thông; tạo bởi máy chủ dữ liệu kiểm chứng sinh học rút gọn từ dữ liệu sinh trắc áp dụng phép chiếu sử dụng tham số chiếu; tạo bởi máy chủ băm của dữ liệu kiểm chứng sinh học rút gọn; tạo bởi máy chủ băm của tệp tin điện tử; tạo bởi máy chủ bản ghi chứng cứ kiểm chứng bằng cách liên kết giá trị thử thách, băm của dữ liệu kiểm chứng sinh học rút gọn, và băm của tệp tin điện tử, và để so sánh nó với bản ghi chứng cứ được gửi bởi thiết bị máy khách và chỉ tiếp tục quá trình chữ ký số nếu bản ghi chứng cứ kiểm chứng giống hệt với bản ghi chứng cứ được gửi bởi thiết bị máy khách; nhận diện bởi máy chủ người dùng của thiết bị máy khách, và

định nghĩa ít nhất một mục dữ liệu người dùng; tạo bởi máy chủ chứng nhận máy chủ bằng cách liên kết ít nhất băm của tệp tin điện tử, ít nhất một mục dữ liệu người dùng, và dữ liệu chữ ký liên quan ít nhất đến thời gian của chữ ký; ký bởi máy chủ chứng nhận máy chủ áp dụng khóa ký riêng tư của máy chủ, nhờ đó tạo chứng nhận máy chủ được ký; tạo bởi máy chủ chữ ký số bằng cách liên kết ít nhất chứng nhận máy chủ được ký và băm của tệp tin điện tử, và liên kết bởi máy chủ chữ ký số với tệp tin điện tử, nhờ đó tạo tệp tin điện tử được ký số.

Sáng chế đề cập đến phương pháp ký số tệp tin điện tử, bao gồm các bước được thực thi bởi máy chủ: tạo giá trị thử thách bao gồm tham số chiếu; truyền giá trị thử thách đến thiết bị máy khách qua kênh truyền thông; tiếp nhận từ thiết bị máy khách, qua kênh truyền thông, bản ghi chứng cứ, tệp tin điện tử được ký, và dữ liệu sinh trắc rút gọn của người dùng được rút gọn theo tham số chiếu, bản ghi chứng cứ được tạo bởi thiết bị máy khách bằng cách liên kết giá trị thử thách, băm của dữ liệu sinh trắc rút gọn, và băm của tệp tin điện tử; tạo băm của dữ liệu sinh trắc rút gọn; tạo băm của tệp tin điện tử; tạo bản ghi chứng cứ kiểm chứng bằng cách liên kết giá trị thử thách, băm của dữ liệu sinh trắc rút gọn, và băm của tệp tin điện tử, và so sánh nó với bản ghi chứng cứ được gửi bởi thiết bị máy khách và chỉ tiếp tục quá trình chữ ký số nếu bản ghi chứng cứ kiểm chứng giống hệt với bản ghi chứng cứ được gửi bởi thiết bị máy khách; nhận diện người dùng của thiết bị máy khách, và định nghĩa ít nhất một mục dữ liệu người dùng; tạo chứng nhận máy chủ bằng cách liên kết ít nhất băm của tệp tin điện tử, ít nhất một mục dữ liệu người dùng, và dữ liệu chữ ký liên quan ít nhất đến thời gian của chữ ký; ký chứng nhận máy chủ áp dụng khóa ký riêng tư của máy chủ, nhờ đó tạo chứng nhận máy chủ được ký; tạo chữ ký số bằng cách liên kết ít nhất chứng nhận máy chủ được ký và băm của tệp tin điện tử, và liên kết chữ ký số với tệp tin điện tử, nhờ đó tạo tệp tin điện tử được ký số.

Sáng chế đề cập đến phương pháp ký số tệp tin điện tử, bao gồm các bước: tạo bởi máy chủ giá trị thử thách bao gồm tham số chiếu; truyền bởi máy chủ giá trị thử thách đến thiết bị máy khách qua kênh truyền thông; nhờ khối thu thập dữ liệu sinh trắc được nối với thiết bị máy khách, ghi nhận dữ liệu sinh trắc rút gọn áp dụng phép chiếu sử dụng tham số chiếu; tạo băm của dữ liệu sinh trắc rút gọn nhờ thiết bị máy khách; tạo bởi thiết bị máy khách băm của tệp tin điện tử; tạo bởi thiết bị máy khách bản ghi chứng cứ bằng cách liên kết ít nhất giá trị thử thách, băm của dữ liệu sinh trắc rút gọn, và băm của tệp tin điện tử; truyền bởi thiết bị máy khách bản ghi chứng cứ, tệp tin điện tử được ký và dữ liệu sinh trắc rút gọn đến máy chủ qua kênh truyền thông; tạo bởi máy chủ băm của dữ liệu sinh trắc rút gọn; tạo bởi máy chủ băm của tệp tin điện tử; tạo bởi máy chủ bản ghi chứng cứ kiểm chứng bằng cách liên kết giá trị thử thách, băm của dữ liệu sinh trắc rút gọn, và băm của tệp tin điện tử, và so sánh nó với bản ghi chứng cứ được gửi bởi thiết bị máy khách và chỉ tiếp tục quá trình chữ ký số nếu bản ghi chứng cứ kiểm chứng giống hệt với bản ghi chứng cứ được gửi bởi thiết bị máy khách; nhận diện người dùng của thiết bị máy khách nhờ máy chủ và định nghĩa ít nhất một mục dữ liệu người dùng; tạo bởi máy chủ chứng nhận máy chủ bằng cách liên kết ít nhất băm của tệp tin điện tử, ít nhất một mục dữ liệu người dùng, và dữ liệu chữ ký liên quan ít nhất đến thời gian của chữ ký; ký bởi máy chủ chứng nhận máy chủ áp dụng khóa ký riêng tư của máy chủ, nhờ đó tạo chứng nhận máy chủ được ký; tạo chữ ký số bởi máy chủ bằng cách liên kết ít nhất chứng nhận máy chủ được ký và băm của tệp tin điện tử, và liên kết bởi máy chủ chữ ký số với tệp tin điện tử, nhờ đó tạo tệp tin điện tử được ký số.

Sáng chế đề cập đến phương pháp xác thực bao gồm các bước: truyền từ máy chủ giá trị thử thách bao gồm tham số chiếu đến thiết bị máy khách qua kênh truyền thông; nhờ khối thu thập dữ liệu sinh trắc

được nối với thiết bị máy khách, ghi nhận dữ liệu sinh trắc rút gọn áp dụng phép chiếu sử dụng tham số chiếu; truyền bởi thiết bị máy khách dữ liệu sinh trắc rút gọn đến máy chủ qua kênh truyền thông; nhận diện bởi máy chủ người dùng của thiết bị máy khách; tạo, từ mẫu gốc sinh trắc của người dùng, dữ liệu kiểm chứng mẫu gốc sinh trắc rút gọn áp dụng phép chiếu bao gồm tham số chiếu, và thực hiện xác thực bằng cách so sánh dữ liệu sinh trắc rút gọn với dữ liệu kiểm chứng mẫu gốc sinh trắc rút gọn.

Mô tả vắn tắt các hình vẽ

Sáng chế được giải thích chi tiết hơn nhờ các phương án thực hiện được ưu tiên được minh họa trong các hình vẽ đi kèm, trong đó

Fig.1 là sơ đồ khối của các thiết bị công nghệ thông tin chính được áp dụng trong phương pháp theo sáng chế;

Fig.2 là sơ đồ luồng tổng quan của phương pháp theo sáng chế;

Fig.3 là sơ đồ luồng của các bước phía máy khách của phương pháp theo phương án thực hiện thứ nhất của sáng chế;

Fig.4 là sơ đồ luồng của các bước xác thực và kiểm chứng phía máy chủ của phương pháp theo phương án thực hiện thứ nhất của sáng chế;

Fig.5 là sơ đồ luồng thu được nhờ chỉnh sửa phương án thực hiện sáng chế theo phương án thực hiện khác được minh họa trên Fig.3;

Fig.6 là sơ đồ luồng phía máy chủ liên quan đến Fig.5, thu được nhờ chỉnh sửa phương án thực hiện được minh họa trên Fig.4;

Fig.7 là sơ đồ luồng sơ lược mật mã hóa tệp tin điện tử bởi máy chủ, và

Fig.8 là sơ đồ luồng sơ lược tạo và ký bản ghi chứng cứ máy chủ.

Mô tả chi tiết sáng chế

Các thiết bị công nghệ thông tin chính và các thành phần chính ở phương pháp theo sáng chế được thể hiện trên Fig.1. Phương pháp theo

sáng chế được làm thích ứng để ký bởi máy chủ 20 tệp tin điện tử được làm khả dụng hoặc được tạo trên thiết bị máy khách 10. Thiết bị máy khách 10 có thể được nối đến máy chủ 20 qua kênh truyền thông 30. Kênh truyền thông điện tử 30 này có thể được thiết lập chẳng hạn trong mạng truyền thông điện tử 32, chẳng hạn thông qua ví dụ áp dụng LAN (local area network, mạng cục bộ) không dây và/hoặc có dây, mạng IT toàn cầu, cụ thể là mạng Internet, cũng như mạng viễn thông di động tương ứng với các chuẩn 3G hoặc 4G, mạng GSM, v.v..

Thiết bị máy khách 10 có thể được triển khai dưới dạng thiết bị truyền thông người dùng bất kỳ mà bao gồm một hoặc nhiều bộ xử lý 12, bộ lưu trữ dữ liệu 14, khối truyền thông máy khách 16, và các thiết bị ngoại vi 18. Thông qua ví dụ, thiết bị máy khách 10 có thể là máy tính để bàn, máy tính xách tay hoặc máy tính notebook, điện thoại tế bào (điện thoại di động) – cụ thể là điện thoại thông minh, máy tính tablet, v.v..

Theo phương án thực hiện, bộ lưu trữ dữ liệu 14 được thể hiện dưới dạng phần tích hợp của thiết bị máy khách 10, nhưng bộ lưu trữ dữ liệu 14 có thể còn là phương tiện lưu trữ ngoài, tức là thành phần ở đây được gọi là bộ lưu trữ dữ liệu 14 nghĩa là bao gồm phương tiện lưu trữ dữ liệu trong và ngoài bất kỳ mà thiết bị máy khách 10 truy nhập được. Bộ lưu trữ dữ liệu 14 có thể được triển khai dưới dạng loại bất kỳ trong các phương tiện lưu trữ dữ liệu quang, từ tính hoặc điện tử (chẳng hạn bộ nhớ, thẻ nhớ, đĩa cứng, đĩa ngoài, v.v.) Bộ lưu trữ dữ liệu 14 tốt hơn là được áp dụng để lưu trữ các khóa PKI (Public Key Infrastructure, hạ tầng cơ sở khóa công khai), ít nhất khóa mã hóa công khai của máy chủ 40a tương ứng với máy chủ 20. Có thể còn cân nhắc phương án thực hiện trong đó khóa mã hóa công khai của máy chủ 40a không được lưu trữ trong bộ lưu trữ dữ liệu 14 nhưng được tạo khả dụng tạm thời cho thiết bị máy khách 10, được tải xuống tạm thời từ Internet nhằm các mục đích của quá trình mã hóa.

Thành phần được gọi là khối truyền thông máy khách 16 nghĩa là bao gồm các thành phần phần cứng và phần mềm bất kỳ (tức là, thẻ mạng, kết nối mạng, bộ điều hợp WiFi, anten, v.v.) nhờ thiết bị máy khách 10 nào có thể thiết lập kênh truyền thông điện tử 30 ít nhất với máy chủ 20, mà trên kênh đó có thể trao đổi dữ liệu điện tử.

Thiết bị máy khách 10 bao gồm – hoặc dưới dạng thành phần của nó hoặc được kết nối với nó dưới dạng thiết bị ngoại vi 18 hoặc dưới dạng khối bên ngoài khác (tức là, được kết nối theo cách bất kỳ với thiết bị máy khách 10) – khối thu thập dữ liệu sinh trắc 18a và tốt hơn là ít nhất một giao diện đầu vào 18b và ít nhất một giao diện đầu ra 18c.

Thông qua ví dụ, khối thu thập dữ liệu sinh trắc 18a có thể là máy tính bảng bộ số hóa có thể tiếp nhận và ghi nhận chữ ký viết tay dưới dạng dữ liệu sinh trắc. Máy tính bảng số hóa có thể được bổ sung bằng bút số, nhưng ở các trường hợp cụ thể ngón tay của người dùng có thể còn được áp dụng dưới dạng "thiết bị viết" được dò bởi máy tính bảng số hóa.

Khối thu thập dữ liệu sinh trắc 18a có thể, thông qua ví dụ, được triển khai dưới dạng máy quét mống mắt, nhờ đó ảnh mống mắt được nhận, và dữ liệu số biểu thị ảnh mống mắt được lưu trữ dưới dạng dữ liệu sinh trắc.

Khối thu thập dữ liệu sinh trắc 18a có thể còn là máy đọc vân tay, áp dụng việc nhận vân tay và dữ liệu số biểu thị vân tay được lưu trữ dưới dạng dữ liệu sinh trắc.

Ngoài ra, khối thu thập dữ liệu sinh trắc 18a có thể là thiết bị loại bất kỳ được áp dụng để đo lường/đăng ký định danh sinh trắc học (chẳng hạn mẫu hình ven gan tay, DNS) và để ghi nhận dữ liệu thu được này.

Có thể còn xem xét phương án thực hiện trong đó khối thu thập dữ liệu sinh trắc 18a cùng lúc có chức năng như là giao diện đầu vào 18b. Chẳng hạn, bên cạnh tiếp nhận các chữ ký viết tay, máy tính bảng số hóa

có thể còn được áp dụng để nhập vào lệnh người dùng để vận hành các chương trình phần mềm chạy trên thiết bị máy khách 10.

Thiết bị máy khách 10 tốt hơn là bao gồm ít nhất một màn hình được sử dụng làm giao diện đầu ra 18c. Bên cạnh đó, các giao diện đầu ra 18c khác có thể được xem xét, thông qua ví dụ, các máy in hoặc thiết bị được làm thích ứng để viết các phương số khác (chẳng hạn CD, DVD, đĩa mềm, thẻ nhớ v.v.).

Ít nhất một giao diện đầu vào 18b có thể được triển khai, thông qua ví dụ, dưới dạng bàn phím, chuột, hoặc thiết bị đầu vào thông thường khác. Giao diện đầu ra 18c có thể đồng thời cũng là giao diện đầu vào 18b, chẳng hạn màn hình cảm ứng. Tương tự, thiết bị viết phương tiện mang dữ liệu có thể đồng thời có chức năng như là giao diện đầu vào 18b giả sử có thể đọc và viết phương tiện. Bàn phím có thể được triển khai dưới dạng bàn phím ảo, chẳng hạn trong trường hợp màn hình cảm ứng được áp dụng như là màn hình, bàn phím ảo có thể được hiển thị trên đó, có thể áp dụng như là giao diện đầu vào 18b.

Trong trường hợp màn hình cảm ứng được áp dụng như là giao diện đầu vào 18b và giao diện đầu ra 18c, màn hình cảm ứng có thể còn thực hiện các chức năng của khối thu thập dữ liệu sinh trắc 18a, tức là trong các trường hợp cụ thể, thiết bị ngoại vi đơn có thể thực hiện ba chức năng.

Máy chủ 20 nghĩa là bao gồm các thiết bị IT khác (chẳng hạn các máy tính xách tay hoặc máy tính để bàn) có thể có chức năng như là máy chủ. Máy chủ 20 còn bao gồm một hoặc bộ xử lý 22, bộ lưu trữ dữ liệu 24 và khối truyền thông máy chủ 26.

Bộ lưu trữ dữ liệu 24 có thể được triển khai dưới dạng loại phương tiện lưu trữ dữ liệu khác bất kỳ, điện tử, từ tính hoặc quang học. Theo phương án thực hiện, bộ lưu trữ dữ liệu 24 được thể hiện dưới dạng phần tích hợp của máy chủ 20, nhưng bộ lưu trữ dữ liệu 24 có thể còn bao gồm

phương tiện lưu trữ dữ liệu ngoài mà máy chủ 20 có thể truy nhập, chẳng hạn HSM 24' (hardware security module, môđun bảo mật phần cứng) được thể hiện trên Fig.1. Do vậy, bộ lưu trữ dữ liệu 24 có nghĩa bao gồm phương tiện lưu trữ dữ liệu trong và ngoài (chẳng hạn ROM và RAM cài sẵn, HSM bên ngoài, phương tiện lưu trữ ngoài khác, v.v.) mà máy chủ 20 truy nhập được trực tiếp hoặc gián tiếp.

Tốt hơn là, máy chủ 20 sở hữu các khóa PKI và các khóa ký khác, chẳng hạn khóa mật mã hóa riêng tư của máy chủ 40b và các khóa ký riêng tư của máy chủ 41 tương ứng với máy chủ 20, cũng như các khóa ký riêng tư của người dùng 42 tương ứng với người dùng, có thể được lưu trữ trong cơ sở dữ liệu khóa 43 trong bộ lưu trữ dữ liệu 24, và tốt hơn nữa là trong HSM 24'. Tốt hơn là, bộ lưu trữ dữ liệu 24 có thể còn lưu trữ cơ sở dữ liệu người dùng 44, và được bao gồm hoặc tách riêng, cơ sở dữ liệu sinh trắc 45 được làm thích ứng để lưu trữ các mẫu gốc sinh trắc 45a của các người dùng.

Khóa ký riêng tư của người dùng 42 có thể, thông qua ví dụ, còn là khóa mật mã hóa riêng tư dựa trên cơ sở hạ tầng PKI có thể được áp dụng bởi bất kỳ ai để giải mã dữ liệu được mật mã hóa bằng cách sử dụng khóa mã hóa công khai, nhưng đã biết đến các thuật toán ký khác bất kỳ không dựa trên mật mã hóa. Chẳng hạn, các thuật toán loại HMAC (hash-based message authentication code, mã xác thực tin nhắn dựa vào băm) có thể còn được sử dụng để ký. Các thuật toán này liên quan đến việc tạo giá trị băm tổ hợp từ giá trị của khóa và chính tin nhắn. Băm có chức năng kép: một mặt nó bảo vệ định danh tin nhắn, và mặt khác chứng tỏ rằng nó chỉ có thể được tạo bởi ai có khóa. Khác biệt chính được so sánh với các quá trình ký loại PKI (RSA) chính là quá trình này chủ yếu liên quan đến một loại khóa, tức là khóa ký riêng tư của người dùng 42, nhưng không liên quan khóa ký công khai của người dùng, và thuật toán ký gồm việc tạo băm thay vì mật mã hóa.

Như trên, thành phần được gọi là khối truyền thông máy chủ 26 nghĩa là bao gồm các thành phần phần cứng và phần mềm bất kỳ (tức là thẻ mạng, kết nối mạng, bộ điều hợp WiFi, anten, v.v.) nhờ nó mà máy chủ 20 có thể thiết lập kênh truyền thông điện tử 30 ít nhất với thiết bị máy khách 10, trên đó dữ liệu điện tử kênh có thể được trao đổi.

Dưới đây, phương pháp theo hai phương án thực hiện sáng chế sẽ được trình bày có dựa vào các thành phần phần cứng lấy làm ví dụ được mô tả trên đây.

Trên Fig.2 thể hiện sơ đồ luồng tổng quan của phương pháp theo sáng chế. Các bước của phương pháp, cũng như các tài liệu, dữ liệu, các thuật toán và các tệp tin được sử dụng hoặc được tạo trong quá trình của nó được minh họa trên chi tiết hơn trên các hình vẽ từ Fig.2 đến Fig.8.

Mặc dù để đơn giản, các bước được đánh số liên tiếp, thứ tự các bước có thể được thay đổi trong nhiều trường hợp, hoặc các bước cụ thể có thể được thực thi đồng thời, có thể được hợp lại hoặc phân chia phụ, cũng như các bước khác có thể được bao gồm giữa các bước được trình bày ở đây, do nó rõ ràng với chuyên gia trong lĩnh vực.

Phương pháp theo sáng chế được đứng trước một cách linh hoạt bằng cách thiết lập kênh truyền thông 30 giữa thiết bị máy khách 10 và máy chủ 20. Tốt hơn là, kênh truyền thông 30 là kênh bảo mật có thể được thiết lập bằng cách áp dụng thông qua ví dụ các giao thức SSL, TLS, SNPv3, VPN, HTTPS, FTPS, TelnetS, IMAPS, IPSec, v.v., như chuyên gia trong lĩnh vực đã biết. Trong quá trình của phương pháp kênh truyền thông 30 – là kênh dữ liệu ảo – có thể bị gián đoạn và thiết lập lại, với tùy chọn nhiều hơn một kênh dữ liệu ảo được thiết lập giữa thiết bị máy khách 10 và máy chủ 20, nhưng để đơn giản được gọi chung là kênh truyền thông 30.

Việc cung cấp tệp tin điện tử 48 được ký có thể còn được gọi là điểm bắt đầu của phương pháp theo sáng chế. Tệp tin điện tử 48 có thể được

tạo nhờ sử dụng thiết bị máy khách 10, và do vậy nó có thể chẳng hạn là tài liệu được tạo trên thiết bị máy khách 10 hoặc tệp tin ảnh được chụp bằng camera của thiết bị máy khách 10 được áp dụng dưới dạng giao diện đầu vào 18b. Có thể còn cân nhắc việc tệp tin điện tử 48 được ký bởi người dùng của thiết bị máy khách 10 không được tạo bởi chính thiết bị máy khách 10 nhưng được tiếp nhận bởi thiết bị máy khách 10 từ nguồn bên ngoài, chẳng hạn qua thư điện tử, hoặc tệp tin điện tử 48 được tải xuống từ mạng Internet hoặc được đọc từ phương tiện lưu trữ dữ liệu (chẳng hạn, CD, DVD, thẻ nhớ, v.v.) áp dụng thiết bị (viết)/đọc làm giao diện đầu vào 18b, hoặc được nhận từ máy chủ 20 hoặc từ chỗ khác.

Các bước từ 1 đến 8 của phương pháp theo biến thể thứ nhất/phương án thực hiện của sáng chế được nêu trên Fig.2 được minh họa chi tiết trên Fig.3.

Như là bước 1 của phương pháp theo sáng chế, giá trị thử thách 50 được tạo nhờ sử dụng máy chủ 20. Giá trị thử thách 50 bao gồm một hoặc nhiều tham số chiếu 52 (thông thường là các số). Giá trị thử thách 50 có thể tùy chọn chứa nhãn thời gian được tạo bởi chính máy chủ 20, hoặc – theo yêu cầu của máy chủ 20 – bởi máy chủ nhãn thời gian bên ngoài, chẳng hạn theo giao thức RFC3161.

Ở bước 2 giá trị thử thách 50 được truyền bởi máy chủ 20 đến thiết bị máy khách 10 qua kênh truyền thông 30.

Ở bước 3 thiết bị máy khách 10 được áp dụng để trích rút một hoặc nhiều tham số chiếu 52 từ giá trị thử thách 50. Dĩ nhiên, bước này có thể được thực hiện thời gian bất kỳ trước khi sử dụng các tham số chiếu 52, hoặc đồng thời với nó.

Ở bước 4, dữ liệu sinh trắc của người dùng 54 được ghi nhận ở phía máy khách 10 sử dụng khối thu thập dữ liệu sinh trắc 18a, dữ liệu sinh trắc có thể bao gồm một hoặc nhiều mục dữ liệu động hoặc tĩnh (các nhóm dữ liệu) được ghi nhận dựa trên các đặc tính vật lý của người dùng.

Chẳng hạn, trong trường hợp máy tính bảng bộ số hóa được áp dụng dưới dạng khối thu thập dữ liệu sinh trắc 18a, chữ ký viết tay được tạo bằng cách sử dụng bút số hoặc ngón tay của người dùng dưới dạng thiết bị viết được nhận và được ghi lại dưới dạng dữ liệu sinh trắc 54. Trong trường hợp này, dữ liệu sinh trắc 54 có thể chẳng hạn là các tọa độ vị trí ấn thiết bị viết với bề mặt máy tính bảng, các tọa độ vị trí nhấc thiết bị viết từ bề mặt máy tính bảng, hàm thời gian của các tọa độ thiết bị viết, hàm thời gian của tốc độ thiết bị viết, hàm thời gian của gia tốc thiết bị viết, hàm thời gian của lực nhấn thiết bị viết, hoặc tổ hợp của nhiều hơn một dữ liệu này.

Theo phương án thực hiện được ưu tiên, trong quá trình nhập vào chữ ký viết tay, ảnh chữ ký được hiển thị trên màn hình của thiết bị máy khách 10, được áp dụng dưới dạng thiết bị đầu vào 18c, nhờ đó cung cấp phản hồi trực quan cho người dùng. Điều này đặc biệt hiệu quả trong trường hợp khối thu thập dữ liệu sinh trắc 18a cùng lúc còn có chức năng như là màn hình, như với các PDA, các máy tính bảng, các điện thoại tế bào màn hình cảm ứng, v.v..

Nếu khối thu thập dữ liệu sinh trắc được triển khai dưới dạng máy quét mống mắt, ảnh mống mắt được nhận, và dữ liệu số đại diện ảnh mống mắt được ghi nhận dưới dạng dữ liệu sinh trắc 54. Trong trường hợp khối thu thập dữ liệu sinh trắc là máy đọc vân tay, vân tay được ghi nhận và dữ liệu số biểu thị vân tay được lưu trữ dưới dạng dữ liệu sinh trắc 54.

Ở bước 5, thiết bị máy khách 10 được áp dụng để tạo bản ghi chứng cứ 70. Trong quá trình đó, thiết bị máy khách 10 được áp dụng để tạo băm 49 của tệp tin điện tử 48 sử dụng thuật toán băm bảo mật một chiều 60a, mà thông qua ví dụ là thuật toán SHA-256, SHA-512, v.v.. Băm 49 được tạo nhờ sử dụng thuật toán băm 60a đại diện dữ liệu được cô đọng mà từ nó không thể suy ra tệp tin điện tử gốc 48. Dấu hiệu đặc trưng của

các thuật toán băm 60a chính là việc chỉnh sửa phần bất kỳ của tệp tin điện tử gốc 48 gây ra hiệu ứng tuyết lở trong băm 49, mà do nó băm trở nên khác biệt hoàn toàn. Bằng cách tạo băm 49 một lần nữa, có thể kiểm tra xem liệu các thay đổi (không hợp pháp) có thể được thực hiện cho tệp tin điện tử 48, hoặc liệu tệp tin có bị can thiệp hay không. Đặc trưng quan trọng khác của thuật toán băm 60a chính là không thể tạo các tệp dữ liệu từ đó mà thuật toán sẽ tạo băm 49 tương tự.

Việc tạo bản ghi chứng cứ 70 còn liên quan việc tạo dữ liệu sinh trắc rút gọn 56 từ dữ liệu sinh trắc của người dùng 54 với thuật toán chiếu áp dụng cho một hoặc nhiều tham số chiếu 52. Theo sáng chế, thuật ngữ "phép chiếu" được sử dụng để đề cập đến các phép ánh xạ toán học một chiều, hoặc các phép rút gọn khác, của dữ liệu mà thu được dữ liệu rút gọn này không thể được sử dụng để phục hồi dữ liệu gốc, trong khi cùng lúc dữ liệu rút gọn có thể chỉ được tạo bởi người có dữ liệu gốc và biết các tham số chiếu. Các thuật toán chiếu áp dụng các tham số chiếu (hoặc, nói theo cách khác, rút gọn dữ liệu) được biết đối với các chuyên gia trong lĩnh vực, các thuật toán đưa vào, thông qua ví dụ, phép chiếu dữ liệu được ghi nhận trên mặt phẳng hoặc trục định trước, hoặc xử lý dữ liệu nhờ mạng nơ ron. Trong trường hợp này, chẳng hạn, ảnh chữ ký tĩnh (dữ liệu sinh trắc rút gọn 56) có thể được tạo từ dữ liệu chữ ký động được ghi nhận bằng chữ ký viết tay được ghi nhận dưới dạng dữ liệu sinh trắc 54.

Dữ liệu sinh trắc rút gọn 56 đặc trưng cho người dùng nhưng không thể được áp dụng để khôi phục dữ liệu sinh trắc gốc 54. Dữ liệu sinh trắc rút gọn 56 dùng làm bằng chứng cho bộ tạo của nó – trong trường hợp này, thiết bị máy khách 10 – có sở hữu dữ liệu sinh trắc gốc 54 và các tham số chiếu 52 được gửi với giá trị thử thách 50.

Tiếp theo, thiết bị máy khách 10 được áp dụng để tạo băm 58 của dữ liệu sinh trắc rút gọn 56 sử dụng thuật toán băm bảo mật một chiều 60b có thể giống hệ hoặc khác thuật toán băm 60a.

Sau đó, bản ghi chứng cứ 70 được tạo bởi thiết bị máy khách 10 bằng cách liên kết giá trị thử thách 50, băm 58 của dữ liệu sinh trắc rút gọn 56, và băm 49 của tệp tin điện tử 48. Việc liên kết dữ liệu có thể được thực hiện bằng cách áp dụng phương pháp thích hợp đã biết bất kỳ, chẳng hạn toán tử XOR theo bit mà kết hợp ba dữ liệu theo cách sao cho chúng không thể được suy ra từ kết quả này, mà giữ lại khả năng kiểm chứng được. Như nêu trên, chức năng băm được làm thích hợp để băm (bản ghi chứng cứ 70) bằng cách nối ba dữ liệu có thể còn được áp dụng ở đây.

Ngoài ra, bản ghi chứng cứ 70 có thể chứa dữ liệu khác.

Bản ghi chứng cứ 70 chứng tỏ rằng tệp tin điện tử 48 và dữ liệu sinh trắc 54 xuất phát từ thiết bị máy khách 10 cụ thể. Trong trường hợp, kẻ tấn công bên ngoài cố gắng truyền dữ liệu sinh trắc 54 được ghi nhận trước đó vào hệ thống với tài liệu được ký, kẻ đó không thể tạo bản ghi chứng cứ 70 tương ứng với nó do nó không sở hữu giá trị thử thách 50 (một cách tùy chọn có thể còn chứa nhãn thời gian để ngăn ngừa can thiệp). Do giá trị thử thách 50 chứa các tham số duy nhất được tạo cho mỗi sự kiện ký, dữ liệu sinh trắc 54 không thể được sử dụng hai lần, tình cờ hoặc có chủ ý.

Tiếp theo, ở bước 6 bản ghi chứng cứ 70 tốt hơn là được ký bằng cách áp dụng thuật toán ký số 71 sử dụng thiết bị máy khách 10. Thuật toán ký 71 có thể chẳng hạn là giải pháp dựa vào mật khẩu sử dụng một lần, dựa vào mật khẩu, dựa vào PKI (chẳng hạn RSA) có thể được làm thích ứng để phù hợp tình trạng cho trước. Quá trình ký dẫn đến bản ghi chứng cứ được ký 72.

Ở bước 7, dữ liệu sinh trắc 54 và/hoặc tệp tin điện tử 48 được ký tốt hơn là được ký bởi thiết bị máy khách 10, có thể được thực hiện bằng

cách áp dụng mật mã hóa dựa vào PKI bằng cách sử dụng khóa mật mã hóa công khai của máy chủ 40a, sao cho dữ liệu sinh trắc được mật mã hóa 64 và tệp tin điện tử được mật mã hóa 68 do vậy được tạo có thể chỉ được giải mã bằng cách sử dụng khóa mật mã hóa riêng tư của máy chủ 40b được lưu trữ trong cơ sở dữ liệu khóa 43 của máy chủ 20.

Dĩ nhiên, các phương pháp khác có thể còn được áp dụng để mật mã hóa dữ liệu sinh trắc 54 và/hoặc tệp tin điện tử 48 được ký. Thông qua ví dụ, cụ thể là đối với các tệp tin lớn mật mã hóa có thể linh hoạt tạo khóa đối xứng duy nhất cho mỗi sự kiện mật mã hóa *và* mật mã hóa tệp tin bằng cách sử dụng khóa (chẳng hạn với thuật toán đối xứng AES), với khóa đối xứng được mật mã hóa sử dụng khóa mật mã hóa công khai PKI 40a của máy chủ và còn được truyền đến máy chủ 20 bởi thiết bị máy khách 10. Nhờ đó, ở bước thứ nhất ở phía máy chủ, khóa mật mã hóa đối xứng phải được giải mật mã bằng cách sử dụng khóa mật mã hóa riêng tư 40b của máy chủ, và các tệp tin được mật mã hóa có thể được giải mã bằng cách sử dụng khóa đối xứng này. Ưu điểm của quá trình mật mã hóa hai giai đoạn này chính là thuật toán đối xứng nhanh hơn các thuật toán mật mã hóa bất đối xứng, với chi phí bổ sung kích thước nhỏ hơn trên các tệp tin dữ liệu được mật mã hóa, do vậy các tệp tin có kích thước lớn thậm chí có thể được mật mã hóa nhanh chóng.

Ở bước 8, bản ghi chứng cứ được ký 72, dữ liệu sinh trắc tốt hơn là được mật mã hóa 64 và tệp tin điện tử tốt hơn là được mật mã hóa 68 được truyền bởi thiết bị máy khách 10 đến máy chủ 20 qua kênh truyền thông 30. Bên cạnh đó, tốt hơn là các mục dữ liệu người dùng 74 (chẳng hạn định danh người dùng, PIN người dùng, v.v.) được gửi đến máy chủ 20 bởi thiết bị máy khách 10 trước khi, trong quá trình hoặc sau khi hoàn thành phương pháp nêu trên. Thông qua ví dụ, trong quá trình tạo bản ghi chứng cứ 70, dữ liệu người dùng 74 còn được liên kết với các thành phần được liệt kê phía trên. Tuy nhiên, dữ liệu người dùng 74 có thể được gửi

đến máy chủ 20 (tốt hơn là được mật mã hóa) tách riêng khỏi bản ghi chứng cứ 70, thông thường để nhận diện người dùng, yêu cầu ít nhất dữ liệu nhận diện này dựa vào việc máy chủ 20 có thể, chẳng hạn, tìm ra khóa ký riêng tư 42 của người dùng nào được sử dụng của các khóa được lưu trữ trong cơ sở dữ liệu khóa 43, hoặc, chẳng hạn, thiết lập dữ liệu người dùng 74 của người dùng được sử dụng để tạo chữ ký số (được mô tả chi tiết dưới đây) của dữ liệu được lưu trữ trong cơ sở dữ liệu người dùng 44, hoặc, chẳng hạn, thiết lập mẫu gốc sinh trắc của người dùng 45a – mẫu sinh trắc duy nhất (bản mẫu) tương ứng với người dùng cụ thể – được truy xuất từ cơ sở dữ liệu sinh trắc 45. Thông tin khác được tạo khả dụng đến máy chủ 20 bằng cách truyền thông dữ liệu có thể còn thực hiện chức năng định danh người dùng – có chức năng như là dữ liệu người dùng 74 – chẳng hạn số điện thoại (nếu điện thoại thông minh được áp dụng làm thiết bị máy khách 10), hoặc địa chỉ IP tĩnh (trong trường hợp máy tính để bàn được áp dụng làm thiết bị máy khách 10), v.v..

Các bước từ 9 đến 11 của phương pháp theo biến thể thứ nhất của sáng chế được thể hiện trên Fig.2 được minh họa chi tiết trên Fig. 4.

Ở bước 9, máy chủ 20 được áp dụng để nhận diện người dùng của thiết bị máy khách 10 và để định nghĩa ít nhất một mục dữ liệu người dùng 74. Mục sau có thể là dữ liệu người dùng 74 được gửi bởi thiết bị máy khách 10, hoặc ngoài các mục dữ liệu người dùng 74 được truy xuất từ cơ sở dữ liệu người dùng 44 dựa trên dữ liệu người dùng 74 được gửi bởi thiết bị máy khách.

Sự kiện liên quan đến bước 9 có thể là xác thực người dùng, mà qua đó, thông qua ví dụ, chữ ký của bản ghi chứng cứ 72 được ký bởi thiết bị máy khách 10 được kiểm chứng, và người dùng được xác thực tương ứng.

Theo phương án thực hiện được ưu tiên cụ thể, tuy nhiên, thực hiện xác thực dựa trên dữ liệu sinh trắc 54. Để thực hiện xác thực, ở bước 10

trước hết dữ liệu sinh trắc được mật mã hóa 64 được gửi bởi thiết bị máy khách 10 được giải mật mã với khóa mã hóa riêng tư của máy chủ 40b (hoặc, một cách tùy chọn, việc sử dụng khóa đối xứng được giải mật mã với khóa mã hóa riêng tư của máy chủ 40b). Tiếp theo, mẫu gốc sinh trắc 45a tương ứng với người dùng được xác định bởi dữ liệu người dùng 74 được truy xuất từ cơ sở dữ liệu sinh trắc 45, mẫu gốc sinh trắc 45a sau đó được so sánh bởi máy chủ 20 với dữ liệu sinh trắc 54 được giải mã nhờ sử dụng chương trình phần mềm thích hợp (thông qua ví dụ, chương trình phần mềm bao gồm các thuật toán dựa vào CRC, dựa vào phép chiếu, dựa vào mạng nơron hoặc tương tự khác). Chẳng hạn, tính xác thực của chữ ký viết tay được kiểm chứng bởi chương trình chạy trên máy chủ 20 sử dụng các chữ ký mẫu ban đầu của người dùng cụ thể làm mẫu sinh trắc 45a. Trong trường hợp xác thực thành công, tức là, dữ liệu sinh trắc 54 được truyền so khớp với một hoặc nhiều mẫu sinh trắc 45a được lưu trữ cho người dùng cụ thể, quá trình tiếp tục, ngược lại yêu cầu cho ký tệp tin điện tử 48 bị từ chối hoặc quá trình bị dừng lại.

Ưu điểm xác thực được thực hiện bằng cách sử dụng dữ liệu sinh trắc 54 chính là người dùng không phải ghi nhớ các mã PIN bất kỳ. Xác thực được thực hiện bằng cách sử dụng chữ ký bằng tay dưới dạng dữ liệu sinh trắc 54 được ưu tiên đặc biệt do nó là thứ gần nhất với việc ký tài liệu giấy theo cách quen thuộc.

Tốt hơn là, tất cả dữ liệu sinh trắc 54 được gửi đến máy chủ 20 được lưu trữ trong cơ sở dữ liệu sinh trắc 45 dưới dạng các mẫu sinh trắc 45a lần lượt tương ứng với những người dùng cụ thể, trong khi máy chủ 20 còn kiểm tra xem liệu dữ liệu sinh trắc 54 hiện được đệ trình có giống với các mẫu sinh trắc 45a được lưu trữ trước đó, hoặc các phần của nó, nhờ đó bảo vệ việc đệ trình lại dữ liệu sinh trắc 54 ban đầu.

Ở bước 11, bản ghi chứng cứ kiểm chứng 70' được tạo nhờ sử dụng máy chủ 20 theo phần sau (xem Fig.4):

Máy chủ 20 được sử dụng để tạo dữ liệu kiểm chứng sinh học rút gọn 56' từ dữ liệu sinh trắc 54 áp dụng phép chiếu sử dụng tham số chiếu 52 được gửi trong giá trị thử thách 50, với thuật toán chiếu tương tự được sử dụng ở phía máy khách để tạo dữ liệu sinh trắc rút gọn 56. Tiếp theo, băm 58' của dữ liệu kiểm chứng sinh học rút gọn 56' được tạo với thuật toán băm 60b tương tự được áp dụng ở phía máy khách để tạo băm 58 của dữ liệu sinh trắc rút gọn 56.

Tiếp theo, máy chủ 20 được sử dụng để tạo băm 49' của tệp tin điện tử 48 với thuật toán băm tương tự 60a được sử dụng để tạo băm 49 của tệp tin điện tử 48 ở phía máy khách.

Sau đó, bản ghi chứng cứ kiểm chứng 70' được tạo bởi máy chủ 20, liên kết giá trị thử thách 50, băm 58' của dữ liệu kiểm chứng sinh học rút gọn 56', và băm 49' của tệp tin điện tử 48, và được so sánh với bản ghi chứng cứ 70 được gửi bởi thiết bị máy khách 10. Trong trường hợp bản ghi chứng cứ kiểm chứng 70' giống hệt bản ghi chứng cứ 70 được gửi bởi thiết bị máy khách 10, quá trình chữ ký số được tiếp tục, ngược lại yêu cầu bị từ chối và quá trình bị dừng lại.

Các bước tương ứng của phương pháp theo biến thể thứ hai của sáng chế được minh họa trên Fig.5 và Fig.6, lần lượt tương ứng các phiên bản chỉnh sửa của Fig.3 và Fig 4.

Liên quan đến việc bảo vệ chống trộm cắp và tái sử dụng dữ liệu sinh trắc, tốt hơn là nếu các tham số chiếu được đệ trình với giá trị thử thách được áp dụng không chỉ để giảm tuần tự các sinh trắc học rút gọn, mà thực hiện ghi nhận dữ liệu rút gọn theo phép rút gọn tương ứng với các tham số. Thực tế, các sinh trắc học rút gọn có thể được tạo từ dữ liệu sinh trắc được ghi nhận cho các giá trị tham số bất kỳ, nếu dữ liệu sinh trắc được lưu trữ có thể truy nhập được. Tuy nhiên, trong trường hợp chính các giá trị tham số ảnh hưởng quá trình ghi nhận, dữ liệu sinh trắc rút gọn

được ghi nhận không thể được sử dụng sau này để tạo phép rút gọn tương ứng với các giá trị tham số khác nhau.

Trong trường hợp các chữ ký bằng tay, giải pháp lấy làm ví dụ là ở nơi một phần tham số gồm văn bản sẽ được viết tay bởi người ký tên, và trong trường hợp văn bản tương tự không bao giờ được viết hai lần, đảm bảo rằng không viết tay tương ứng với giá trị tham số khác nhau (văn bản) có thể được tạo sau nhờ sử dụng văn bản cố định được ghi nhận trước đó.

Việc triển khai tham số chiếu và rút gọn dữ liệu sinh trắc tương ứng với nó có thể được phân loại thành ba phân loại chính. Mỗi phân loại liên quan phép biến đổi được thực hiện tùy thuộc vào tham số (ba phân loại này có thể còn được áp dụng cho biến thể thứ nhất của sáng chế, được thể hiện trên Fig.3 và Fig.4).

1. Các sinh trắc học rút gọn, trong đó xác định biến đổi trực tiếp bằng tham số cụ thể. Các ví dụ:

- phép chiếu vận tốc trên đường thẳng theo hướng cụ thể (chữ ký),
- phép chiếu gia tốc trên đường thẳng theo hướng cụ thể (chữ ký),
- lấy mẫu sử dụng các giá trị X, Y, Z cụ thể (chữ ký),
- thông tin ảnh được truy xuất từ các vị trí cụ thể được xác định bởi tham số (chữ ký, vân tay, mống mắt),
- các điểm đặc trưng phép chiếu trên đường thẳng theo hướng cụ thể (vân tay, mống mắt).

2. Các sinh trắc học rút gọn, trong đó tham số để lựa chọn thuật toán xác thực (hoặc nhiều hơn một thuật toán cùng lúc). Trong trường hợp này, kết quả kiểm chứng dữ liệu sinh trắc gồm các kết quả kiểm chứng riêng rẽ của nhiều dấu hiệu đặc trưng. Chẳng hạn, thay đổi tạm thời các vận tốc hướng X và Y và các góc vectơ tiếp tuyến được kiểm tra; và quyết định cuối cùng được lấy dựa trên các điểm số thu được nhờ các phép so sánh riêng rẽ. Trong trường hợp này tham số rút gọn xác định chỉ

loại rút gọn sẽ được thực hiện bởi thiết bị ghi nhận. Nếu, chẳng hạn, tham số chỉ báo rằng thực hiện xác thực nhờ sử dụng gia tốc hướng X và thay đổi góc vectơ tiếp tuyến, thì hai chuỗi dữ liệu này (= các sinh trắc học rút gọn) sẽ được ghi nhận, từ đó không thể khôi phục sinh trắc học ban đầu. Các ví dụ:

- vectơ tiếp tuyến (chữ ký),
- các vận tốc và gia tốc hướng X và Y (chữ ký),
- áp lực (chữ ký).

3. Các sinh trắc học rút gọn, trong đó xác định biến đổi trực tiếp nhờ tham số cho trước. Thông qua ví dụ, các giải pháp được triển khai nhờ sử dụng các mạng nơ ron nằm trong phân loại này. Chẳng hạn, mạng nơ ron được áp dụng để xác thực có thể gồm ba lớp. Mạng nơ ron cụ thể có cấu trúc cố định, và mạng tương tự – được định nghĩa bởi cấu trúc và trọng lượng của nó – luôn được áp dụng để xác thực người cụ thể. Mạng nơ ron duy nhất được đào tạo cho mỗi người để được xác thực, mạng này có thể chỉ được áp dụng để nhận dạng người cụ thể. Giá trị tham số nhanh chóng chứa các trọng số và các thiết lập tùy chọn khác của lớp thứ nhất của mạng nơ ron. Trong quá trình đăng ký, tất cả các tham số đầu vào của lớp thứ hai được tính toán dựa trên tham số chiếu 52 được gửi bởi máy chủ, một cách hiệu quả bao gồm các sinh trắc học rút gọn từ đó không thể khôi phục chữ ký. Môđun xác thực không phải tính toán lại mạng nơ ron dựa trên giá trị tham số (mạng đã được biết đối với môđun do nó được xây dựng trong quá trình đăng ký chữ ký), và do vậy tất cả máy chủ phải làm là đảm bảo rằng lớp thứ nhất được định nghĩa bởi tham số giống hệt với lớp thứ nhất của mạng nơ ron đã được biết, và nếu vậy, các lớp thứ hai và thứ ba sẽ được chạy trong môđun xác thực.

Nếu mạng có 5 lớp và tham số đệ trình chứa dữ liệu của hai lớp thứ nhất, thì các đầu vào của lớp thứ ba sẽ được nhận từ phía khách hàng

dưới dạng các sinh trắc học rút gọn, và máy chủ sẽ vận hành các lớp thứ ba, thứ tư và thứ năm trong môđun xác thực.

Các mẫu gốc sinh trắc được áp dụng trong trường hợp ba phân loại nêu trên như sau.

Trong trường hợp phân loại 1 cơ sở dữ liệu sinh trắc 45 và các mẫu gốc sinh trắc 45a chứa trong nó chủ yếu gồm chính các mẫu sinh trắc được ghi ban đầu (chẳng hạn, các chữ ký), do chúng có thể được áp dụng để tính toán tất cả thông tin cần trong quá trình xác thực. Các tham số rút gọn dữ liệu, chẳng hạn tham số hóa tuyến chiếu hoặc các tham số của các quyết định lựa chọn khác sẽ khác đối với mỗi phiên, và các phép ánh xạ rút gọn sẽ có thể được tính toán lại cũng cho các mẫu/các chữ ký được chứa bởi bản mẫu. Trường hợp phụ đặc biệt có thể là khi số lượng hữu hạn các "phép chiếu" được ghi trước đó, tức là các sinh trắc học rút gọn được áp dụng (chẳng hạn, các phép chiếu trên ba tuyến định trước), trong trường hợp mà các chuỗi dữ liệu tham chiếu không cần được tính lại bởi môđun xác thực bằng cách sử dụng nhóm dữ liệu sinh trắc đầy đủ (được ghi nhận ở thời gian đăng ký), do dữ liệu có thể được tính toán trước, trong quá trình đăng ký. Nhờ đó, thậm chí các phương án thực hiện này có thể được triển khai trong đó mẫu sinh trắc đầy đủ không được biết đến bởi chính môđun xác thực.

Trong trường hợp các phân loại 1 và 2, do vậy, mẫu gốc sinh trắc của người cụ thể có thể bao gồm chuỗi dữ liệu rút gọn được tính toán trước, do các dữ liệu này có thể được tạo ở thời điểm người được đăng ký.

Đối với biến thể mạng nơ ron của phân loại 3, tuy nhiên, mẫu gốc sinh trắc của một người được tạo bởi các giá trị trọng số và các thiết lập của mạng nơ ron được đào tạo cụ thể cho người cụ thể. Mạng nơ ron phải tồn tại ở thời điểm giá trị tham số được đệ trình (do tham số được tạo bởi các lớp thứ nhất của mạng), và – do bản chất – mạng không thể được tạo

lại (được đào tạo) chính xác theo cách tương tự như trước đó. Do vậy, các thiết lập của mạng nơ ron nên được lưu trữ ở mẫu gốc sinh trắc.

Kết luận, do vậy có thể xem xét rằng mẫu gốc sinh trắc có thể:

- gồm các mẫu sinh trắc đầy đủ được ghi nhận trong quá trình đăng ký,

- gồm chỉ các chuỗi dữ liệu được tính toán trước đó cụ thể (các sinh trắc học rút gọn), trong trường hợp đó không thể áp dụng các phép chiếu tùy ý, hoặc

- gồm tổ hợp các mẫu sinh trắc học đầy đủ và các chuỗi dữ liệu được tính toán trước.

Dĩ nhiên, trong quá trình kiểm chứng định danh sinh trắc, tất cả các tổ hợp khả thi của các tham số nêu trên có thể xuất hiện, tức là có thể xuất hiện việc, như được xác định bởi tham số chiếu 52 của giá trị thử thách 50, để xác thực phép chiếu cụ thể gia tốc hướng X, các giá trị thu được nhờ thuật toán cụ thể (chẳng hạn dựa trên áp lực), và các giá trị đầu vào của lớp thứ hai của mạng nơ ron tương ứng với người cụ thể được yêu cầu. Sau đó, cuối cùng cấp xác thực bằng các kết hợp các xác thực một phần này.

Fig.5 thể hiện lưu đồ gồm các bước phía khách hàng theo biến thể thứ hai của sáng chế. Bằng cách so sánh Fig.3 và Fig.5, nhận thấy rằng biến thể thứ hai này của sáng chế khác phương án thực hiện được mô tả trên đây trong đó, để bảo mật tăng cường, toàn bộ dữ liệu sinh trắc không được ghi nhận ở phía khách hàng, nhưng thay vào đó tham số chiếu 52 được mang bởi giá trị thử thách 50 đã xác định cách thức trong đó dữ liệu sinh trắc được ghi nhận, tức là thay cho sinh trắc học toàn phần chỉ dữ liệu sinh trắc rút gọn 56 được ghi ở phía máy khách. Dữ liệu rút gọn có thể được ghi nhận theo các cách khác nhau. Trong trường hợp ví dụ, có thể xem xét việc, cân nhắc tham số chiếu 52, khối thu thập dữ liệu sinh trắc 18a lưu trữ trong bộ nhớ và tiếp tục đưa qua để xử lý thêm chỉ dữ

liệu sinh trắc rút gọn 56. Biến thể này có thể còn được xem xét trong đó toàn bộ dữ liệu sinh trắc tạm thời có trong bộ nhớ của khối thu thập dữ liệu sinh trắc 18a nhưng chỉ một phần nội dung được xác định bởi tham số chiếu 52 được ghi nhận và đệ trình.

Bên cạnh đó, phương án thực hiện theo Fig.5 khác phương án thực hiện được minh họa trên Fig.3 trong đó ở tiến trình của phương pháp chỉ dữ liệu sinh trắc rút gọn 56 khả dụng để đệ trình cho máy chủ 20, tốt hơn là ở dạng mật mã hóa, tức là dưới dạng dữ liệu sinh trắc được mật mã hóa rút gọn 65.

Theo phần nêu trên – theo phương pháp theo phương án bất kỳ hoặc tất cả các phương án thực hiện sáng chế – nội dung dữ liệu của tham số chiếu 52 được gồm trong giá trị thử thách 50 có thể thay đổi rộng rãi. Có thể xem xét trường hợp trong đó giá trị thử thách 50 được tạo bởi chính tham số chiếu 52, gồm chỉ một tham số. Có thể còn xem xét rằng giá trị thử thách 50 chứa dữ liệu khác bên cạnh tham số chiếu 52, mà dữ liệu không tham gia quá trình rút gọn dữ liệu. Tham số chiếu 52 có thể là một tham số hoặc thậm chí nhóm tham số, như được yêu cầu đối với lớp đầu vào, các trọng số của các lớp, và một cách tùy chọn các tham số khác của mạng trong trường hợp xử lý dữ liệu bởi mạng nơ ron. Theo sáng chế, bởi tham số chiếu 52, theo nghĩa rộng nhất là tham số bất kỳ hoặc nhóm tham số nêu trên. Thuật ngữ "phép chiếu" trong ngữ cảnh này không nghĩa là chỉ có thể thực hiện rút gọn bằng phép chiếu được hiểu theo nghĩa hẹp, nhưng nhờ tham số chiếu 52, tham số bất kỳ có nghĩa là nhờ đó có thể thực hiện rút gọn dữ liệu mẫu sinh trắc. Do vậy, nhờ tham số chiếu 52, loại tham số rút gọn dữ liệu hoặc nhóm tham số được hiểu theo nghĩa rộng nhất có thể.

Trên Fig.6 các quá trình liên quan đến các bước phía máy chủ theo biến thể thứ hai của sáng chế, được thể hiện trên Fig.5, được minh họa. Bằng cách so sánh Fig.6 và Fig.4, có thể thấy rằng theo phương án thực

hiện thứ hai toàn bộ nhóm dữ liệu sinh trắc không được nhận ở phía của máy chủ, tốt hơn là chỉ dữ liệu sinh trắc được mật mã hóa rút gọn 65. Từ dữ liệu này – trong trường hợp áp dụng mật mã hóa – dữ liệu sinh trắc rút gọn 56 được giải mã bằng cách sử dụng khóa mật mã hóa riêng tư của máy chủ 40b, và sau đó có thể được áp dụng để tạo bản ghi chứng cứ kiểm chứng 70' hoặc tốt hơn là cho các quá trình xác thực.

Trong quá trình theo Fig.6, dữ liệu sinh trắc rút gọn 56 khả dụng ở phía máy chủ, mà không cần tham số chiếu 52 để tạo chúng. Như có thể thấy, phương án thực hiện sáng chế bảo mật hơn các phương án thực hiện theo Fig.3 và Fig.4 do ở đây mẫu sinh trắc đầy đủ không được truyền thông, thậm chí không có dạng mật mã hóa.

Theo phương án thực hiện dữ liệu sinh trắc rút gọn 56 có thể được sử dụng để xác thực ở phía máy chủ. Mẫu gốc sinh trắc 45a tương ứng với người dùng cụ thể được nhận diện trong các mẫu gốc sinh trắc 45a được lưu trữ trong cơ sở dữ liệu sinh trắc 45 sử dụng dữ liệu người dùng 74 tương ứng, và sau đó dữ liệu kiểm chứng mẫu gốc sinh trắc rút gọn 56'' được tạo từ mẫu sinh trắc 45a cụ thể nhờ tham số chiếu 52 được mang bởi giá trị thử thách 50. Do vậy, có thể thực hiện xác thực bằng cách so sánh dữ liệu sinh trắc rút gọn 56 (được nhận từ phía máy khách ở dạng mật mã hóa và sau đó được giải mã) và dữ liệu kiểm chứng mẫu gốc sinh trắc rút gọn 56''.

Các bước từ 12 đến 16 của phương pháp theo sáng chế được minh họa chi tiết trên Fig.7. Ở bước 12, máy chủ 20 được áp dụng để tạo chứng nhận máy chủ 80 bằng cách liên kết ít nhất băm 49 của tệp tin điện tử 48, ít nhất một mục dữ liệu người dùng 74, và ít nhất dữ liệu chữ ký 78 liên quan đến thời gian của chữ ký.

Ít nhất một mục dữ liệu người dùng 74 có thể là dữ liệu người dùng 74 được gửi bởi thiết bị máy khách 10, hoặc dữ liệu khác được truy xuất từ cơ sở dữ liệu người dùng 44 dựa trên dữ liệu người dùng 74 được gửi

bởi thiết bị máy khách. Dữ liệu người dùng 74 được áp dụng để tạo chứng nhận máy chủ 80 thông thường bao gồm một hoặc nhiều mục dữ liệu sau: tên của người dùng (của người ký tên), dữ liệu sinh, nơi sinh, tên của mẹ, địa chỉ, số thẻ ID, v.v.

Dữ liệu chữ ký 78 là siêu dữ liệu mô tả các "trường hợp" của sự kiện chữ ký, bao gồm thông thường một hoặc nhiều dữ liệu sau: ngày ký, thông tin trên thiết bị máy khách 10, thông tin trên máy chủ 20, tên của tệp tin điện tử 48 được ký, v.v..

Ở bước 13, chứng nhận máy chủ 80 tốt hơn là được ký bởi máy chủ 20 với khóa ký riêng tư của máy chủ 41, để tạo chứng nhận máy chủ 82 được ký mà sau đó có thể được sử dụng để thiết lập chắc chắn rằng chữ ký xuất phát từ máy chủ 20. Khóa ký riêng tư của máy chủ 41 có thể giống hệt khóa mật mã hóa riêng tư của máy chủ 40b được áp dụng trong suốt các bước trước đó. Tuy nhiên, chứng nhận máy chủ được ký 82 có thể được tạo nhờ sử dụng khóa khác, hoặc thuật toán ký khác, các thuật toán ký áp dụng được gồm các thuật toán loại HMAC (hash-based message authentication code, mã xác thực tin nhắn dựa vào băm).

Ở bước 14 (có thể đứng trước các bước 12 và 13), máy chủ 20 được sử dụng để tạo dữ liệu sinh trắc họa hiển thị được trực quan 54a một cách tùy chọn từ dữ liệu sinh trắc 54 (hoặc trong trường hợp phương án thực hiện theo Fig.5 và Fig.6, từ dữ liệu sinh trắc rút gọn 56) với thuật toán ánh xạ một chiều 84. Chẳng hạn, ảnh chữ ký tĩnh được tạo từ dữ liệu động được ghi nhận của chữ ký bằng tay. Có thể còn cân nhắc việc dữ liệu sinh trắc họa hiển thị được trực quan 54a được tạo từ các loại dữ liệu sinh trắc 54 khác (chẳng hạn các vân tay, các ảnh ven bàn tay, các ảnh mống mắt), nhưng trong trường hợp các loại dữ liệu sinh trắc này, dữ liệu sinh trắc họa hiển thị được trực quan 54a thông thường không được tạo. Thuật toán ánh xạ 84 có thể một cách tùy chọn còn dựa trên thuật toán chiếu được triển khai bằng cách sử dụng tham số chiếu 52.

Ở bước 15, máy chủ 20 được sử dụng để tạo chữ ký số 85 bằng cách liên kết chứng nhận máy chủ được ký 82, băm 49 của tệp tin điện tử 48, và – trong trường hợp chúng khả dụng – dữ liệu sinh trắc họa hiển thị được trực quan 54. Trong suốt bước này, liên kết dữ liệu tốt hơn là được thực hiện nhờ đóng gói dữ liệu trong gói dữ liệu. Tiếp theo, chữ ký số 85 được liên kết với tệp tin điện tử 48, thông qua ví dụ bằng cách nhúng nó vào trong đó, hoặc bằng cách bao gồm cả theo chuẩn thông thường – chẳng hạn, tệp XML, nhờ đó tạo tệp tin điện tử 86 được ký số. Tốt hơn là thực hiện nhúng sao cho dữ liệu sinh trắc họa hiển thị được trực quan 54a có thể được xem dưới dạng ảnh chữ ký trong khi mở tệp tin điện tử được ký số 86. Dĩ nhiên, chữ ký số 85 có thể còn chứa dữ liệu khác.

Tốt hơn là ở bước 16, tệp tin điện tử được ký số 86 còn được ký thay mặt người dùng sử dụng máy chủ 20, thông qua ví dụ áp dụng khóa ký riêng tư của người dùng 42 để có tệp tin điện tử 88 ký kép. Việc sử dụng khóa ký công khai của người dùng, bất kỳ ai có thể đảm bảo rằng tệp tin điện tử ký kép 88 được ký bằng khóa ký riêng tư của người dùng 42 tương ứng với người dùng cụ thể (người ký tên).

Bước 17 của phương pháp theo sáng chế được minh họa chi tiết trên Fig.8.

Ở bước 17, máy chủ 20 được sử dụng để tạo bản ghi chứng cứ máy chủ 90 bằng cách liên kết ít nhất giá trị thử thách 50, dữ liệu sinh trắc 54 (hoặc, theo phương án thực hiện theo Fig.5 và Fig.6, dữ liệu sinh trắc rút gọn 56) và băm 49 của tệp tin điện tử 48 (chẳng hạn bằng toán tử XOR theo bit nêu trên, hoặc với thuật toán băm), sau đó bản ghi chứng cứ máy chủ 90 được ký bằng khóa ký riêng tư của máy chủ 41, và bản ghi chứng cứ máy chủ 92 được ký thu được được lưu trữ. Các ngữ cảnh sự kiện ký, cũng như dữ liệu được sử dụng trong tiến trình của nó, có thể được biết từ bản ghi chứng cứ máy chủ 92 được ký sử dụng khóa ký công khai của máy chủ 40a. Bản ghi chứng cứ máy chủ 90 có thể được sử dụng sau

(thậm chí nhiều năm sau) để chứng tỏ rằng giao dịch ký cụ thể với nội dung cụ thể thực sự đã diễn ra. Có thể được yêu cầu chẳng hạn cho phiên tòa. Trong các trường hợp này, dữ liệu sinh trắc toàn diện 54 có thể được yêu cầu, và do vậy tốt hơn là nhóm dữ liệu sinh trắc đầy đủ được gồm trong bản ghi chứng cứ máy chủ 90 thay vì chỉ dữ liệu sinh trắc rút gọn 56, băm 58 của nó, hoặc dữ liệu sinh trắc 54a nhìn thấy được.

Quá trình nêu trên có thể được thực hiện trong trường hợp nhiều người ký, khi dĩ nhiên dữ liệu sinh trắc 54 của nhiều hơn một người dùng được ghi nhận bằng cách sử dụng khối thu thập dữ liệu sinh trắc 18a, thực hiện các hoạt động tương ứng cho mỗi nhóm dữ liệu sinh trắc 54, trong khi ở phía máy chủ, dữ liệu sinh trắc 54a thấy được sẽ được tạo từ tất cả các nhóm dữ liệu sinh trắc 54, và đều được bao gồm trong chữ ký số 85.

Như có thể được hiểu từ phần đề cập trên đây, sáng chế đi với cách tiếp cận kỹ thuật tổng quát ưu tiên đơn giản hóa. Ý nghĩa kỹ thuật thông thường nên đề cập việc chữ ký số thông thường nên được áp dụng cho dữ liệu sinh trắc và tài liệu ban đầu, nhờ đó "liên kết" cả theo cách xác thực. Trong trường hợp này, giả thiết các sinh trắc học và tài liệu đã được biết, có thể kiểm chứng liệu các sinh trắc học cụ thể tương ứng với tài liệu cụ thể. Tuy nhiên, nếu một người sở hữu sinh trắc học, thì bằng cách sao chép nó, anh ta có thể sử dụng nó để tạo tài liệu khác. Sáng chế khiến giải pháp đã biết này bảo mật hơn; để ngăn không cho sinh trắc học được bộc lộ, nó được lưu trữ và sử dụng dưới dạng mật mã hóa/rút gọn.

Theo giải pháp kỹ thuật đã biết, phép tương ứng của sinh trắc học và tài liệu chỉ có thể được kiểm chứng bởi thực thể đáng tin cậy được ủy quyền để loại bỏ mật mã của sinh trắc học. Tuy nhiên, có thể nhằm kiểm chứng vào các thực thể mà chúng không được xem là đáng tin cậy. Giải pháp theo sáng chế còn cho phép thực thể không đáng tin kiểm chứng tính xác thực của các tài liệu (mà không giải mã các sinh trắc học được mật mã hóa).

Do vậy, giải pháp theo sáng chế đi với các nguyên lý đơn giản hóa theo cách thức sau:

Giải pháp được làm thích ứng để tạo các sinh trắc học rút gọn dựa vào thách thức được bao gồm trong bản ghi chứng cứ được ký bằng cách sử dụng cả tài liệu lẫn các tham số thách thức. Bản ghi chứng cứ được ký và các sinh trắc học rút gọn có thể được chuyển giao sang thực thể không đáng tin bất kỳ do nó không thể được áp dụng để khôi phục các sinh trắc học gốc do các đặc tính của thuật toán chiếu, trong khi giá trị rút gọn sẽ là duy nhất cho mỗi chữ ký do nó chỉ có thể được tạo sử dụng các tham số khác nhau mỗi lần (tức là hai ảnh rút gọn giống hệt nhau không cần được áp dụng thậm chí trong trường hợp các sinh trắc học giống hệt). Do tính xác thực của bản ghi chứng cứ được ký có thể được kiểm chứng bởi thực thể không tin cậy, nên thực thể có thể đảm bảo rằng các sinh trắc học thích hợp được liên kết với tài liệu cụ thể.

Phương pháp xác thực theo sáng chế còn bao gồm các bước nêu trên, theo phương án bất kỳ trong các phương án thực hiện được ưu tiên nêu trên có thể áp dụng cho phương pháp xác thực. Trong tiến trình của phương pháp xác thực theo sáng chế

– giá trị thử thách 50 bao gồm tham số chiếu 52 được truyền từ máy chủ 20 đến thiết bị máy khách 10 qua kênh truyền thông 30,

– khối thu thập dữ liệu sinh trắc 18a được nối với thiết bị máy khách 10 được sử dụng để ghi nhận dữ liệu sinh trắc rút gọn 56 áp dụng phép chiếu sử dụng tham số chiếu 52,

– thiết bị máy khách 10 được sử dụng để truyền dữ liệu sinh trắc rút gọn 56 đến máy chủ 20 qua kênh truyền thông 30,

– máy chủ 20 được sử dụng để nhận diện người dùng của thiết bị máy khách 10,

– dữ liệu kiểm chứng mẫu gốc sinh trắc rút gọn 56'' được tạo từ mẫu gốc sinh trắc của người dùng 45a áp dụng phép chiếu bao gồm tham số

chiếu 52, và thực hiện xác thực bằng cách so sánh dữ liệu sinh trắc rút gọn 56 với dữ liệu kiểm chứng mẫu gốc sinh trắc rút gọn 56''.

Theo phương án thực hiện được ưu tiên, người dùng được nhận diện dựa trên dữ liệu sinh trắc rút gọn 56.

Do các bước nêu trên có thể được thấy trên Fig.5 và Fig.6, phương pháp xác thực này không được minh họa riêng rẽ. Phương pháp xác thực dựa trên kiến trúc thu thập dữ liệu sinh trắc máy khách – máy chủ trong đó giá trị thử thách, được gửi bởi máy chủ, được sử dụng bởi khối thu thập dữ liệu sinh trắc được nối với hoặc đưa vào máy khách để ghi nhận dữ liệu sinh trắc rút gọn.

Khối thu thập dữ liệu sinh trắc có thể thông qua ví dụ máy tính bảng hoặc điện thoại tế bào (điện thoại thông minh) và phần mềm chạy trên nó, tức là khối thu thập dữ liệu sinh trắc được gắn trong máy khách. Máy chủ có thể, chẳng hạn, là dịch vụ trung tâm được làm thích ứng để nhận diện người dùng dựa trên sinh trắc học được ghi nhận bởi thiết bị và để cấp truy nhập cho các dịch vụ cụ thể tùy thuộc kết quả nhận diện. Các sinh trắc học có thể chẳng hạn được tạo bởi chữ ký bằng tay trên màn hình cảm ứng, ảnh mống mắt được chụp bằng camera của thiết bị, vân tay được ghi nhận bởi thiết bị (giả sử thiết bị có khả năng cần thiết), hoặc ghi nhận cử chỉ được thực hiện bằng cách sử dụng camera của thiết bị. Trong trường hợp theo phương án thực hiện, thực hiện rút gọn nhanh chóng bằng phần mềm chạy trên máy tính bảng.

Thiết bị thu thập dữ liệu sinh trắc có thể là "đệm chữ ký" (máy tính bảng bộ số hóa có bút có thể còn có phần hiển thị riêng nó – gần như tương tự với thiết bị máy tính bảng), được nối với PC bằng bộ nối USB. Trong trường hợp này "máy chủ" thậm chí có thể là chính PC, chạy ứng dụng phần mềm được làm thích ứng để sử dụng dữ liệu chữ ký viết tay được ghi nhận. Dĩ nhiên, máy chủ từ xa có thể còn được áp dụng trong trường hợp này, khi chính PC gửi dữ liệu đến máy chủ qua liên kết truyền

thông. Theo phương án thực hiện này, thủ tục rút gọn dữ liệu đã được thực hiện nhanh chóng bên trong "đệm thiết bị", do trong trường hợp này toàn bộ sinh trắc học không lấy ra khỏi thiết bị được bảo vệ và đóng kín về mặt vật lý.

Khối thu thập dữ liệu sinh trắc có thể còn là chuột máy tính đơn giản được nối với PC. Ứng dụng phần mềm có thể được áp dụng để ghi nhận các chuyển động chuột của người dùng trong quá trình duyệt web. Các chuyển động chuột/tay có thể được đề cập dưới dạng đặc trưng dữ liệu sinh trắc cho cá nhân cụ thể. Dựa trên dữ liệu được ghi nhận, các đặc trưng tâm lý của người dùng có thể còn được thu thập, có thể được áp dụng thậm chí đối với việc hiển thị các quảng cáo tùy chỉnh nhằm vào người dùng. Như là cách khác, camera được nối với PC có thể được áp dụng để ghi nhận các chuyển động mắt của người dùng (dưới dạng dữ liệu sinh trắc). Ở các ví dụ này, thực hiện nhanh chóng rút gọn dữ liệu bởi ứng dụng phần mềm chạy trên PC.

Ở trường hợp cụ thể, hai loại thông tin có thể thu được từ thiết bị đệm chữ ký trong suốt sự kiện ký:

– các sinh trắc học rút gọn (sẽ được sử dụng sau này bởi máy chủ để nhận diện người),

– ảnh tĩnh của chữ ký (có thể được sao chép trực quan đến tài liệu, nhưng ở chính nó không thích hợp để tái tạo các sinh trắc học chữ ký).

Điều này là có lợi do dữ liệu sinh trắc quan trọng không thể thu được từ thiết bị, chỉ nhóm thông tin rút gọn cần để nhận diện, mà ảnh chữ ký vẫn có thể được tái tạo. Trong trường hợp này giá trị thử thách sẽ bao gồm

– tham số (hoặc nhóm tham số) xác định rút gọn cần để nhận diện người, và

– tham số khác được làm thích ứng để rút gọn dữ liệu sinh trắc động về các sinh trắc tĩnh (tức là, thực tế các tham số thời gian và áp lực được

xóa khỏi nhóm dữ liệu ban đầu, ảnh được vẽ từ chuỗi điểm còn lại, và tốt hơn là được biến đổi về kích thước định trước).

Trong trường hợp này các sinh trắc học rút gọn là tổng hợp của hai loại thông tin rút gọn, với hai phần được sử dụng bởi máy chủ theo hai cách khác nhau.

Phương pháp xác thực dựa trên các sinh trắc học rút gọn có ưu điểm là nó cho phép nhận diện cá nhân bởi các thực thể/dịch vụ mà

– không cho phép sở hữu toàn bộ dữ liệu sinh trắc do luật pháp ngăn cấm hoặc

– không ở mức bảo mật mà cho phép chúng bảo vệ danh tính của người; hoặc

– không được tin cậy đầy đủ, như là người cung cấp dịch vụ, bởi những người được nhận diện.

Phương pháp xác thực theo sáng chế còn có thể áp dụng để xây dựng hệ thống nhận diện vô danh, do dữ liệu sinh trắc có thể áp dụng cho việc ăn cắp danh tính không được lưu trữ ở máy khách và không được vận chuyển bên trong hệ thống. Theo phương án thực hiện được ưu tiên, nhiều camera có thể được lắp trong cửa hàng và hành lang trung tâm mua sắm. Hệ thống camera có thể thu thập thông tin chuyển động/dạng người/mặt thu gọn trên các cá nhân, truyền chỉ thông tin rút gọn này đến máy chủ. Dựa trên thông tin rút gọn máy chủ có gắng ghi nhận người này. Trong trường hợp người này không được ghi nhận, họ không được nhận diện là khách hàng mới, mẫu sinh trắc tương ứng (dữ liệu rút gọn) được lưu trữ cùng với số nhận dạng liên kết. Tiếp theo, hệ thống giám sát chuyển động của người ở khu trung tâm (cửa hàng nào mà họ đi vào, trước khi cửa sổ cửa hàng nào họ dừng lại, dành bao nhiêu thời gian ở các vị trí cụ thể, cửa hàng nào đã ăn tối, sản phẩm nào đã mua – cái sau có thể được thiết lập bằng cách sử dụng camera quầy thu ngân và thông tin máy đếm tiền), tức là, hệ thống có thể nhận diện các thói quen và sở thích

khách hàng. Dựa trên các sở thích khách hàng của người được nhận diện và ghi nhận trước đó, hệ thống có thể hiển thị các quảng cáo được cá nhân hóa ở bất kỳ đâu (chẳng hạn, trên tường TV động). Hệ thống nhận diện/ghi nhận cho phép các cửa hàng đưa ra các chương trình khuyến mãi được cá nhân hóa cho khách hàng khi đi vào cửa hàng.

Nên hiểu rằng các giải pháp đưa ra các tùy chọn cho các phương án thực hiện chi tiết nêu trên có thể được hiểu bởi người có hiểu biết trung bình trong lĩnh vực, mà nằmtrong phạm vi bảo hộ được định nghĩa bởi các điểm yêu cầu bảo hộ sau.

YÊU CẦU BẢO HỘ

1. Phương pháp ký số tệp tin điện tử, khác biệt ở các bước sau được thực thi bởi máy chủ:

- tạo giá trị thử thách (50) bao gồm tham số chiếu (52),
- truyền giá trị thử thách (50) đến thiết bị máy khách (10) qua kênh truyền thông (30),
- tiếp nhận, qua kênh truyền thông (30), bản ghi chứng cứ (70), tệp tin điện tử (48) được ký, và dữ liệu sinh trắc của người dùng (54) từ thiết bị máy khách (10), bản ghi chứng cứ (70) được tạo bởi thiết bị máy khách (10) bằng cách liên kết
  - giá trị thử thách (50),
  - băm (58) của dữ liệu sinh trắc rút gọn (56), dữ liệu sinh trắc rút gọn (56) được tạo từ dữ liệu sinh trắc (54) áp dụng phép chiếu sử dụng tham số chiếu (52), và
  - băm (49) của tệp tin điện tử (48),
- tạo dữ liệu kiểm chứng sinh học rút gọn (56') từ dữ liệu sinh trắc (54) áp dụng phép chiếu sử dụng tham số chiếu (52),
- tạo băm (58') của dữ liệu kiểm chứng sinh học rút gọn (56'),
- tạo băm (49) của tệp tin điện tử (48),
- tạo bản ghi chứng cứ kiểm chứng (70') bằng cách liên kết giá trị thử thách (50), băm (58') của dữ liệu kiểm chứng sinh học rút gọn (56'), và băm (49) của tệp tin điện tử (48), và so sánh nó với bản ghi chứng cứ (70) được gửi bởi thiết bị máy khách (10) và chỉ tiếp tục quá trình chữ ký số nếu bản ghi chứng cứ kiểm chứng (70') giống hệt với bản ghi chứng cứ (70) được gửi bởi thiết bị máy khách (10),
- nhận diện người dùng của thiết bị máy khách (10) và định nghĩa ít nhất một mục dữ liệu người dùng (74),

- tạo chứng nhận máy chủ (80) bằng cách liên kết ít nhất băm (49) của tệp tin điện tử (48), ít nhất một mục dữ liệu người dùng (74), và dữ liệu chữ ký (78) liên quan ít nhất đến thời gian của chữ ký,
- ký chứng nhận máy chủ (80) áp dụng khóa ký riêng tư của máy chủ (41), nhờ đó tạo chứng nhận máy chủ được ký (82),
- tạo chữ ký số (85) bằng cách liên kết ít nhất chứng nhận máy chủ được ký (82) và băm (49) của tệp tin điện tử (48), và
- liên kết chữ ký số (85) với tệp tin điện tử (48), nhờ đó tạo tệp tin điện tử được ký số (86).

2. Phương pháp theo điểm 1, khác biệt ở chỗ, ký tệp tin điện tử được ký số (86) thay mặt người dùng, tốt hơn là với khóa ký riêng tư của người dùng (42).

3. Phương pháp theo các điểm 1 hoặc 2, khác biệt ở chỗ, tạo dữ liệu sinh trắc họa hiển thị được trực quan (54a) từ dữ liệu sinh trắc (54) nhờ ánh xạ một chiều, trong đó dữ liệu sinh trắc họa hiển thị được trực quan (54a) còn được liên kết với chứng nhận máy chủ (80) và với băm (49) của tệp tin điện tử (48) để tạo chữ ký số (85).

4. Phương pháp theo điểm bất kỳ trong số các điểm từ 1 đến 3, khác biệt ở chỗ, người dùng được xác thực dựa trên dữ liệu sinh trắc (54).

5. Phương pháp theo điểm 4, khác biệt ở chỗ, trong quá trình xác thực dữ liệu sinh trắc (54) được so sánh với mẫu gốc sinh trắc (45a).

6. Phương pháp theo điểm bất kỳ trong số các điểm từ 1 đến 5, khác biệt ở chỗ, tiếp nhận, như là bản ghi chứng cứ (70), bản ghi chứng cứ (70') được ký bởi thiết bị máy khách (10) và kiểm chứng chữ ký.

7. Phương pháp theo điểm bất kỳ trong số các điểm từ 1 đến 6, khác biệt ở chỗ, tiếp nhận, dưới dạng dữ liệu sinh trắc (54) và/hoặc dưới dạng tệp tin điện tử (48), dữ liệu sinh trắc (64) và/hoặc tệp tin điện tử (68) được mật mã hóa bởi thiết bị máy khách (10), và giải mã dữ liệu sinh trắc được mật mã hóa (64) và/hoặc tệp tin điện tử được mật mã hóa (68) trước khi tạo dữ liệu sinh trắc rút gọn (56).

8. Phương pháp theo điểm 7, khác biệt ở chỗ, tiếp nhận dữ liệu sinh trắc được mật mã hóa (64) và/hoặc tệp tin điện tử được mật mã hóa (68) được mật mã hóa với khóa mã hóa công khai của máy chủ (40a) và giải mã nó với khóa mã hóa riêng tư của máy chủ (40b), hoặc tiếp nhận dữ liệu sinh trắc được mật mã hóa (64) và/hoặc tệp tin điện tử được mật mã hóa được mật mã hóa với khóa mã hóa công khai của máy chủ (40a) và giải mã khóa đối xứng được mật mã hóa với khóa mã hóa riêng tư của máy chủ (40b), tuần tự giải mã dữ liệu sinh trắc được mật mã hóa (64) và/hoặc tệp tin điện tử (68) với khóa đối xứng.

9. Phương pháp theo điểm bất kỳ trong số các điểm từ 1 đến 8, khác biệt ở chỗ, tạo, bằng cách liên kết ít nhất giá trị thử thách (50), dữ liệu sinh trắc (54) và băm (49) của tệp tin điện tử (48), bản ghi chứng cứ máy chủ (90), ký bản ghi chứng cứ máy chủ (90) tốt hơn là với khóa ký riêng tư của máy chủ (41), và lưu trữ bản ghi chứng cứ máy chủ được ký thu được (92).

10. Phương pháp theo điểm bất kỳ trong số các điểm từ 1 đến 9, khác biệt ở chỗ, ghi nhận dữ liệu sinh trắc của người dùng (54) nhờ khối thu thập dữ liệu sinh trắc (18a), và nhờ thiết bị máy khách (10):

- tạo, áp dụng phép chiếu sử dụng tham số chiếu (52), dữ liệu sinh trắc rút gọn (56) từ dữ liệu sinh trắc (54),

- tạo băm (58) của dữ liệu sinh trắc rút gọn (56),
- tạo băm (49) của tệp tin điện tử (48),
- tạo bản ghi chứng cứ (70) bằng cách liên kết ít nhất giá trị thử thách (50), băm (58) của dữ liệu sinh trắc rút gọn (56), và băm (49) của tệp tin điện tử (48), và
- truyền bản ghi chứng cứ (70), tệp tin điện tử (48) được ký và dữ liệu sinh trắc (54) đến máy chủ (20) qua kênh truyền thông (30).

11. Phương pháp theo điểm 10, khác biệt ở chỗ, ký bản ghi chứng cứ (70) bởi thiết bị máy khách (10) và kiểm chứng chữ ký bởi máy chủ (20).

12. Phương pháp theo điểm 10 hoặc 11, khác biệt ở chỗ, mật mã hóa dữ liệu sinh trắc (54) và/hoặc tệp tin điện tử (48) được ký bởi thiết bị máy khách (10) trước khi truyền dữ liệu sinh trắc (54) và/hoặc tệp tin điện tử (48) được ký.

13. Phương pháp theo điểm bất kỳ trong số các điểm từ 10 đến 12, khác biệt ở chỗ, khối thu thập dữ liệu sinh trắc (18a) là máy tính bảng bộ số hóa, nhờ đó chữ ký viết bằng tay được nhận và được ghi lại dưới dạng dữ liệu sinh trắc (54), tốt hơn là dưới dạng ít nhất một loại dữ liệu sinh trắc (54) được lựa chọn từ nhóm sau: các tọa độ vị trí ấn thiết bị viết, các tọa độ vị trí nhấc thiết bị viết, hàm thời gian của các tọa độ thiết bị viết, hàm thời gian của tốc độ thiết bị viết, hàm thời gian của gia tốc thiết bị viết, hàm thời gian của lực nhấn thiết bị viết.

14. Phương pháp theo điểm bất kỳ trong số các điểm từ 10 đến 12, khác biệt ở chỗ, khối thu thập dữ liệu sinh trắc (18a) là máy quét mống mắt, nhờ đó ảnh mống mắt được nhận, và dữ liệu số biểu thị ảnh mống mắt được lưu trữ dưới dạng dữ liệu sinh trắc (54).

15. Phương pháp theo điểm bất kỳ trong số các điểm từ 10 đến 12, khác biệt ở chỗ,khối thu thập dữ liệu sinh trắc (18a) là máy đọc vân tay, nhờ đó nhận vân tay, và dữ liệu số biểu thị vân tay được lưu trữ dưới dạng dữ liệu sinh trắc (54).

16. Phương pháp ký số tệp tin điện tử, khác biệt ở chỗ,bao gồm các bước:

- tạo bởi máy chủ (20) giá trị thử thách (50) bao gồm tham số chiếu (52),
- truyền bởi máy chủ (20) giá trị thử thách (50) đến thiết bị máy khách (10) qua kênh truyền thông (30),
- ghi nhận dữ liệu sinh trắc (54) bởi khối thu thập dữ liệu sinh trắc (18a),
- bằng cách áp dụng phép chiếu sử dụng tham số chiếu (52), tạo dữ liệu sinh trắc rút gọn (56) từ dữ liệu sinh trắc (54) nhờ thiết bị máy khách (10),
- tạo băm (58) của dữ liệu sinh trắc rút gọn (56) nhờ thiết bị máy khách (10),
- tạo băm (49) của tệp tin điện tử (48) nhờ thiết bị máy khách (10),
- tạo bởi thiết bị máy khách (10) bản ghi chứng cứ (70) bằng cách liên kết ít nhất giá trị thử thách (50), băm (58) của dữ liệu sinh trắc rút gọn (56), và băm (49) của tệp tin điện tử (48),
- truyền bởi thiết bị máy khách (10) bản ghi chứng cứ (70), tệp tin điện tử (48) được ký và dữ liệu sinh trắc (54) đến máy chủ (20) qua kênh truyền thông (30),
- tạo bởi máy chủ (20) dữ liệu kiểm chứng sinh học rút gọn (56') từ dữ liệu sinh trắc (54) áp dụng phép chiếu sử dụng tham số chiếu (52),
- tạo bởi máy chủ (20) băm (58') của dữ liệu kiểm chứng sinh học rút gọn (56'),
- tạo bởi máy chủ (20) băm (49) của tệp tin điện tử (48),

- tạo bởi máy chủ (20) bản ghi chứng cứ kiểm chứng (70') bằng cách liên kết giá trị thử thách (50), băm (58') của dữ liệu kiểm chứng sinh học rút gọn (56'), và băm (49) của tệp tin điện tử (48), và để so sánh nó với bản ghi chứng cứ (70) được gửi bởi thiết bị máy khách (10) và chỉ tiếp tục quá trình chữ ký số nếu bản ghi chứng cứ kiểm chứng (70') giống hệt với bản ghi chứng cứ (70) được gửi bởi thiết bị máy khách (10),
- nhận diện bởi máy chủ (20) người dùng của thiết bị máy khách (10), và định nghĩa ít nhất một mục dữ liệu người dùng (74),
- tạo bởi máy chủ (20) chứng nhận máy chủ (80) bằng cách liên kết ít nhất băm (49) của tệp tin điện tử (48), ít nhất một mục dữ liệu người dùng (74), và dữ liệu chữ ký (78) liên quan ít nhất đến thời gian của chữ ký,
- ký bởi máy chủ (20) chứng nhận máy chủ (80) áp dụng khóa ký riêng tư của máy chủ (41), nhờ đó tạo chứng nhận máy chủ được ký (82),
- tạo bởi máy chủ (20) chữ ký số (85) bằng cách liên kết ít nhất chứng nhận máy chủ được ký (82) và băm (49) của tệp tin điện tử (48), và
- liên kết bởi máy chủ (20) chữ ký số (85) với tệp tin điện tử (48), nhờ đó tạo tệp tin điện tử được ký số (86).

17. Phương pháp theo điểm 16, khác biệt ở chỗ, bước ký bởi máy chủ (20) tệp tin điện tử được ký số (86) thay mặt người dùng, tốt hơn là với khóa ký riêng tư của người dùng.

18. Phương pháp theo các điểm 16 hoặc 17, khác biệt ở chỗ, bước tạo bởi máy chủ (20) dữ liệu sinh trắc họa hiển thị được trực quan (54a) từ dữ liệu sinh trắc (54) nhờ ánh xạ một chiều, trong đó dữ liệu sinh trắc họa hiển thị được trực quan (54a) còn được liên kết với chứng nhận máy chủ (80) và với băm (49) của tệp tin điện tử (48) để tạo chữ ký số (85).

19. Phương pháp theo điểm bất kỳ trong số các điểm từ 16 đến 18, khác biệt ở chỗ, bước xác thực người dùng nhờ máy chủ (20) dựa trên dữ liệu sinh trắc (54), trong quá trình mà dữ liệu sinh trắc (54) tốt hơn là được so sánh với mẫu gốc sinh trắc (45a).

20. Phương pháp theo điểm bất kỳ trong số các điểm từ 16 đến 19, khác biệt ở chỗ, bước tạo, bằng cách liên kết ít nhất giá trị thử thách (50), dữ liệu sinh trắc (54) và băm (49) của tệp tin điện tử (48), bản ghi chứng cứ máy chủ (90) bởi máy chủ (20), ký bản ghi chứng cứ máy chủ (90) tốt hơn là với khóa ký riêng tư của máy chủ (41), và lưu trữ bản ghi chứng cứ máy chủ được ký thu được (92).

21. Phương pháp theo điểm bất kỳ trong số các điểm từ 16 đến 20, khác biệt ở chỗ, bước ký bản ghi chứng cứ bởi thiết bị máy khách (10) và kiểm chứng chữ ký bởi máy chủ.

22. Phương pháp theo điểm bất kỳ trong số các điểm từ 16 đến 21, khác biệt ở chỗ, bước mật mã hóa bởi thiết bị máy khách (10) dữ liệu sinh trắc (54) và/hoặc tệp tin điện tử (48) trước khi truyền chúng, nhờ đó tạo dữ liệu sinh trắc được mật mã hóa (64) và/hoặc tệp tin điện tử được mật mã hóa (68), và giải mã bởi máy chủ (20) dữ liệu sinh trắc được mật mã hóa (64) và/hoặc tệp tin điện tử được mật mã hóa (68).

23. Phương pháp ký số tệp tin điện tử, khác biệt ở chỗ, các bước được thực thi bởi máy chủ:

- tạo giá trị thử thách (50) bao gồm tham số chiếu (52),
- truyền giá trị thử thách (50) đến thiết bị máy khách (10) qua kênh truyền thông (30),

- tiếp nhận từ thiết bị máy khách (10), qua kênh truyền thông (30), bản ghi chứng cứ (70), tệp tin điện tử (48) được ký, và dữ liệu sinh trắc rút gọn của người dùng (56) được rút gọn theo tham số chiếu (52), bản ghi chứng cứ (70) được tạo bởi thiết bị máy khách (10) bằng cách liên kết
  - giá trị thử thách (50),
  - băm (58) của dữ liệu sinh trắc rút gọn (56), và
  - băm (49) của tệp tin điện tử (48),
- tạo băm (58') của dữ liệu sinh trắc rút gọn (56),
- tạo băm (49) của tệp tin điện tử (48),
- tạo bản ghi chứng cứ kiểm chứng (70') bằng cách liên kết giá trị thử thách (50), băm (58') của dữ liệu sinh trắc rút gọn (56), và băm (49) của tệp tin điện tử (48), và so sánh nó với bản ghi chứng cứ (70) được gửi bởi thiết bị máy khách (10) và chỉ tiếp tục quá trình chữ ký số nếu bản ghi chứng cứ kiểm chứng (70') giống hệt với bản ghi chứng cứ (70) được gửi bởi thiết bị máy khách (10),
- nhận diện người dùng của thiết bị máy khách (10), và định nghĩa ít nhất một mục dữ liệu người dùng (74),
- tạo chứng nhận máy chủ (80) bằng cách liên kết ít nhất băm (49) của tệp tin điện tử (48), ít nhất một mục dữ liệu người dùng (74), và dữ liệu chữ ký (78) liên quan ít nhất đến thời gian của chữ ký,
- ký chứng nhận máy chủ (80) áp dụng khóa ký riêng tư của máy chủ (41), nhờ đó tạo chứng nhận máy chủ được ký (82),
- tạo chữ ký số (85) bằng cách liên kết ít nhất chứng nhận máy chủ được ký (82) và băm (49) của tệp tin điện tử (48), và
- liên kết chữ ký số (85) với tệp tin điện tử (48), nhờ đó tạo tệp tin điện tử được ký số (86).

24. Phương pháp theo điểm 23, khác biệt ở chỗ, bước xác thực người dùng dựa trên dữ liệu sinh trắc rút gọn (56), trong quá trình xác thực mà

phép chiếu bao gồm tham số chiếu (52) được áp dụng để tạo, từ mẫu gốc sinh trắc của người dùng (45a), dữ liệu kiểm chứng mẫu gốc sinh trắc rút gọn (56''), và so sánh dữ liệu sinh trắc rút gọn (56) với dữ liệu kiểm chứng mẫu gốc sinh trắc rút gọn (56'').

25. Phương pháp theo điểm 24, khác biệt ở chỗ, bước tiếp nhận, như là dữ liệu sinh trắc rút gọn (56), dữ liệu sinh trắc được mật mã hóa rút gọn (65) được mật mã hóa bởi thiết bị máy khách (10), và giải mã dữ liệu sinh trắc được mật mã hóa rút gọn (65) trước khi xác thực.

26. Phương pháp theo điểm 23, khác biệt ở chỗ bao gồm các bước:

- ghi nhận dữ liệu sinh trắc rút gọn của người dùng (56) nhờ khối thu thập dữ liệu sinh trắc (18a),
- tạo băm (58) của dữ liệu sinh trắc rút gọn (56),
- tạo băm (49) của tệp tin điện tử (48),
- tạo bản ghi chứng cứ (70) bằng cách liên kết ít nhất giá trị thử thách (50), băm (58) của dữ liệu sinh trắc rút gọn (56), và băm (49) của tệp tin điện tử (48), và
- truyền bản ghi chứng cứ (70), tệp tin điện tử (48) được ký và dữ liệu sinh trắc rút gọn (56) đến máy chủ (20) qua kênh truyền thông (30).

27. Phương pháp ký số tệp tin điện tử, khác biệt ở chỗ, bao gồm các bước:

- tạo bởi máy chủ (20) giá trị thử thách (50) bao gồm tham số chiếu (52),
- truyền bởi máy chủ (20) giá trị thử thách (50) đến thiết bị máy khách (10) qua kênh truyền thông (30),
- nhờ khối thu thập dữ liệu sinh trắc (18a) được nối với thiết bị máy khách (10), ghi nhận dữ liệu sinh trắc rút gọn (56) áp dụng phép chiếu sử dụng tham số chiếu (52),

- tạo băm (58) của dữ liệu sinh trắc rút gọn (56) nhờ thiết bị máy khách (10),
- tạo bởi thiết bị máy khách (10) băm (49) của tệp tin điện tử (48),
- tạo bởi thiết bị máy khách (10) bản ghi chứng cứ (70) bằng cách liên kết ít nhất giá trị thử thách (50), băm (58) của dữ liệu sinh trắc rút gọn (56), và băm (49) của tệp tin điện tử (48),
- truyền bởi thiết bị máy khách (10) bản ghi chứng cứ (70), tệp tin điện tử (48) được ký và dữ liệu sinh trắc rút gọn (56) đến máy chủ (20) qua kênh truyền thông (30),
- tạo bởi máy chủ (20) băm (58') của dữ liệu sinh trắc rút gọn (56),
- tạo bởi máy chủ (20) băm (49) của tệp tin điện tử (48),
- tạo bởi máy chủ (20) bản ghi chứng cứ kiểm chứng (70') bằng cách liên kết giá trị thử thách (50), băm (58') của dữ liệu sinh trắc rút gọn (56), và băm (49) của tệp tin điện tử (48), và so sánh nó với bản ghi chứng cứ (70) được gửi bởi thiết bị máy khách (10) và chỉ tiếp tục quá trình chữ ký số nếu bản ghi chứng cứ kiểm chứng (70') giống hệt với bản ghi chứng cứ (70) được gửi bởi thiết bị máy khách (10),
- nhận diện người dùng của thiết bị máy khách (10) nhờ máy chủ (20) và định nghĩa ít nhất một mục dữ liệu người dùng (74),
- tạo bởi máy chủ (20) chứng nhận máy chủ (80) bằng cách liên kết ít nhất băm (49) của tệp tin điện tử (48), ít nhất một mục dữ liệu người dùng (74), và dữ liệu chữ ký (78) liên quan ít nhất đến thời gian của chữ ký,
- ký bởi máy chủ (20) chứng nhận máy chủ (80) áp dụng khóa ký riêng tư của máy chủ (41), nhờ đó tạo chứng nhận máy chủ được ký (82),
- tạo chữ ký số (85) bởi máy chủ (20) bằng cách liên kết ít nhất chứng nhận máy chủ được ký (82) và băm (49) của tệp tin điện tử (48), và

- liên kết bởi máy chủ (20) chữ ký số (85) với tệp tin điện tử (48), nhờ đó tạo tệp tin điện tử được ký số (86).

28. Phương pháp theo điểm 27, khác biệt ở chỗ, xác thực bởi máy chủ (20) người dùng dựa trên dữ liệu sinh trắc rút gọn (56), trong quá trình xác thực mà phép chiếu bao gồm tham số chiếu (52) được áp dụng để tạo, từ mẫu gốc sinh trắc của người dùng (45a), dữ liệu kiểm chứng mẫu gốc sinh trắc rút gọn (56''), và so sánh dữ liệu sinh trắc rút gọn (56) với dữ liệu kiểm chứng mẫu gốc sinh trắc rút gọn (56'').

29. Phương pháp theo điểm 27, khác biệt ở chỗ, mật mã hóa dữ liệu sinh trắc rút gọn (56) bởi thiết bị máy khách (10) trước khi truyền chúng, nhờ đó tạo dữ liệu sinh trắc được mật mã hóa rút gọn (65) bởi máy chủ.

30. Phương pháp xác thực khác biệt ở chỗ, bao gồm các bước:

- truyền từ máy chủ (20) giá trị thử thách (50) bao gồm tham số chiếu (52) đến thiết bị máy khách (10) qua kênh truyền thông (30),
- nhờ khối thu thập dữ liệu sinh trắc (18a) được nối với thiết bị máy khách (10), ghi nhận dữ liệu sinh trắc rút gọn (56) áp dụng phép chiếu sử dụng tham số chiếu (52),
- truyền bởi thiết bị máy khách (10) dữ liệu sinh trắc rút gọn (56) đến máy chủ (20) qua kênh truyền thông (30),
- nhận diện bởi máy chủ (20) người dùng của thiết bị máy khách (10),
- tạo, từ mẫu gốc sinh trắc của người dùng (45a), dữ liệu kiểm chứng mẫu gốc sinh trắc rút gọn (56'') áp dụng phép chiếu bao gồm tham số chiếu (52), và thực hiện xác thực bằng cách so sánh dữ liệu sinh trắc rút gọn (56) với dữ liệu kiểm chứng mẫu gốc sinh trắc rút gọn (56'').

31. Phương pháp theo điểm 30, khác biệt ở chỗ, nhận diện người dùng dựa trên dữ liệu sinh trắc rút gọn (56).

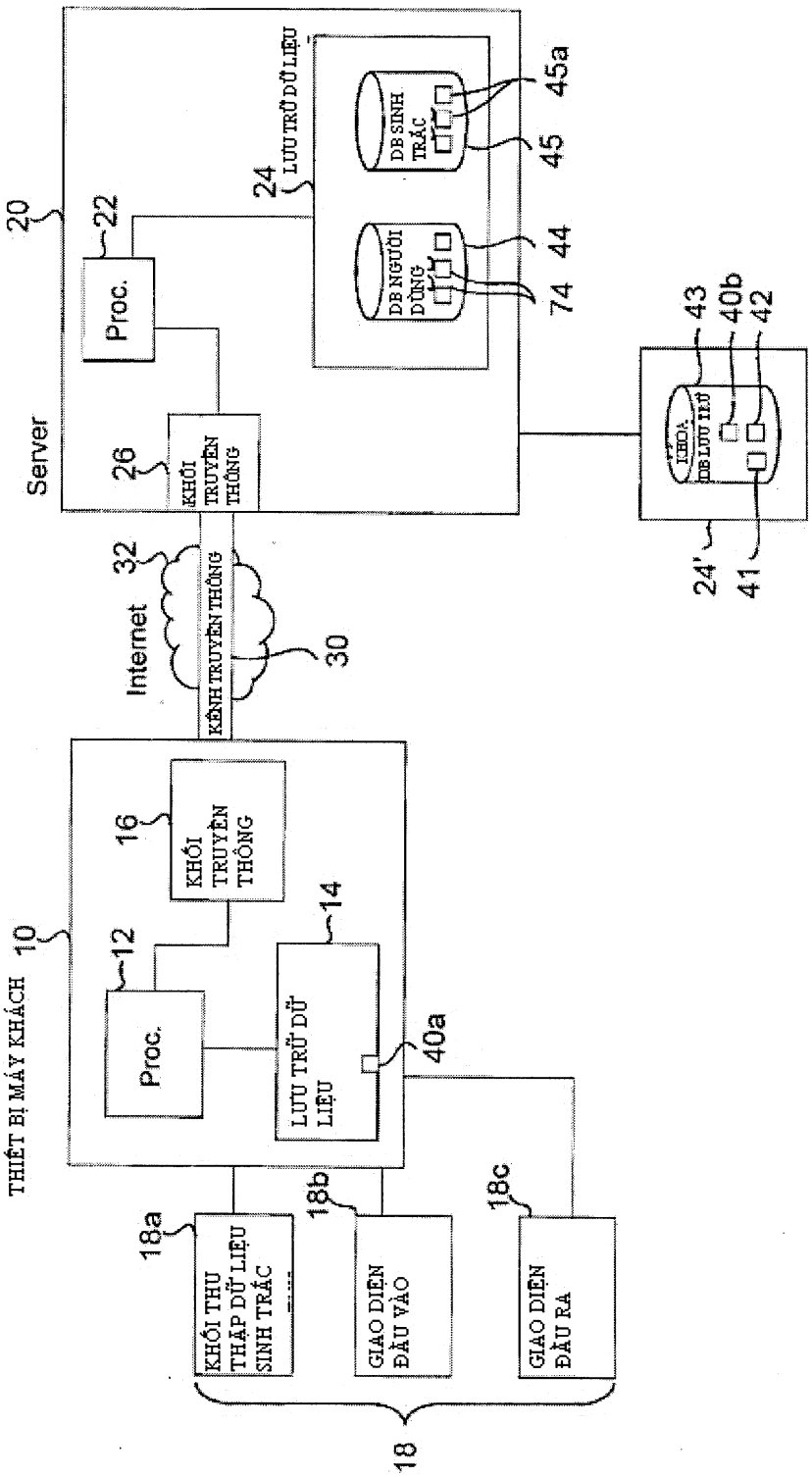

THIẾT BỊ MÁY KHÁCH
10
Proc.
12
KHỐI TRUYỀN THÔNG
16
LƯU TRỮ DỮ LIỆU
14
40a
KHỐI THU THẬP DỮ LIỆU SINH TRẮC
18a
GIAO DIỆN ĐẦU VÀO
18b
GIAO DIỆN ĐẦU RA
18c
18
Internet
32
KÊNH TRUYỀN THÔNG
30
Server
20
Proc.
22
KHỐI TRUYỀN THÔNG
26
LƯU TRỮ DỮ LIỆU
24
DB SINH TRẮC
45
45a
DB NGƯỜI DÙNG
44
74
KHÓA
43
40b
42
24'
41

Fig. 1

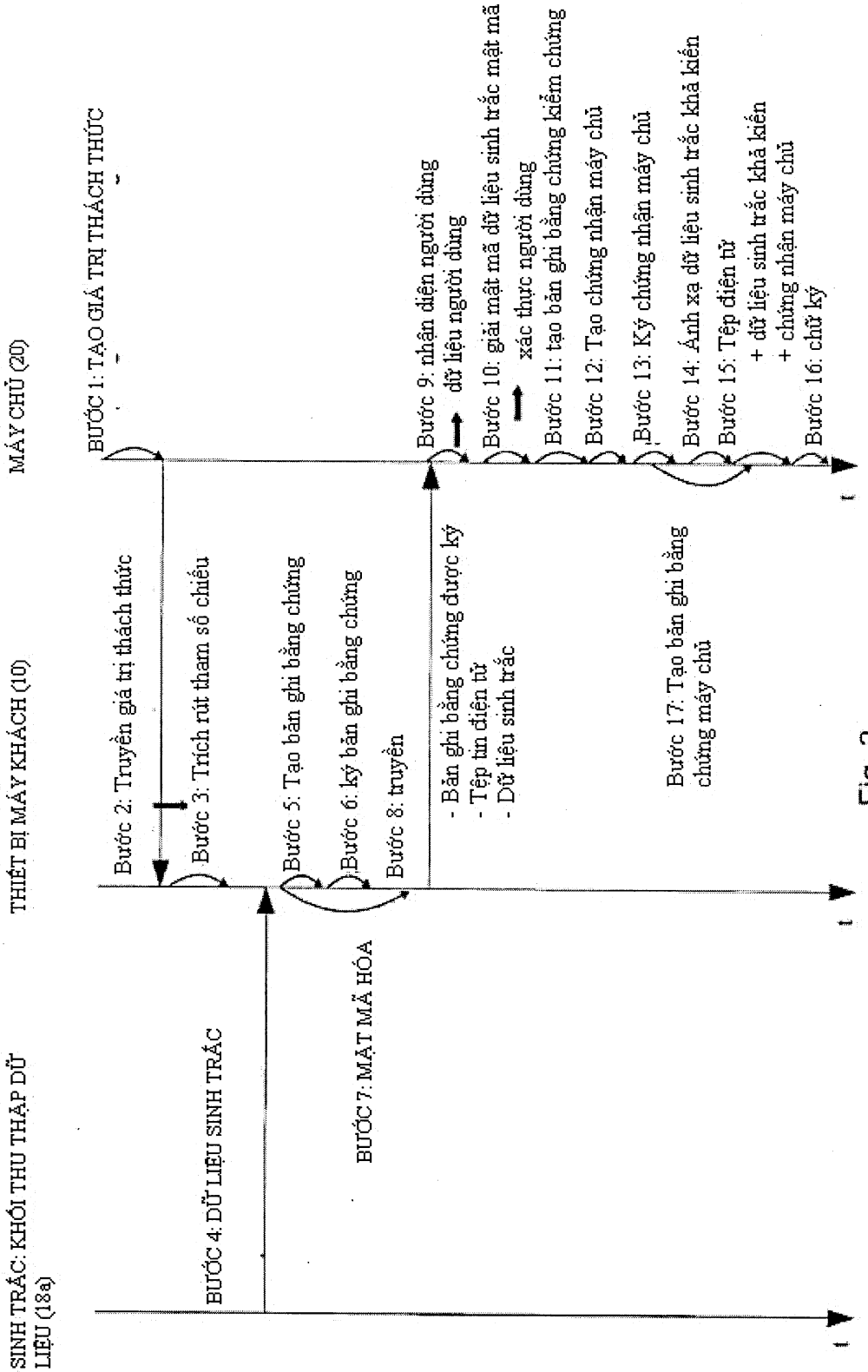

SINH TRẮC: KHỐI THU THẬP DỮ LIỆU (18a)
THIẾT BỊ MÁY KHÁCH (10)
MÁY CHỦ (20)
BƯỚC 1: TẠO GIÁ TRỊ THÁCH THỨC
Bước 2: Truyền giá trị thách thức
Bước 3: Trích rút tham số chiếu
BƯỚC 4: DỮ LIỆU SINH TRẮC
Bước 5: Tạo bản ghi bằng chứng
Bước 6: ký bản ghi bằng chứng
BƯỚC 7: MẬT MÃ HÓA
Bước 8: truyền
- Bản ghi bằng chứng được ký
- Tệp tin điện tử
- Dữ liệu sinh trắc
Bước 9: nhận diện người dùng
dữ liệu người dùng
Bước 10: giải mật mã dữ liệu sinh trắc mật mã
xác thực người dùng
Bước 11: tạo bản ghi bằng chứng kiểm chứng
Bước 12: Tạo chứng nhận máy chủ
Bước 13: Ký chứng nhận máy chủ
Bước 14: Ánh xạ dữ liệu sinh trắc khả kiến
Bước 15: Tệp điện tử
+ dữ liệu sinh trắc khả kiến
+ chứng nhận máy chủ
Bước 16: chữ ký
Bước 17: Tạo bản ghi bằng chứng máy chủ
t
t

Fig. 2

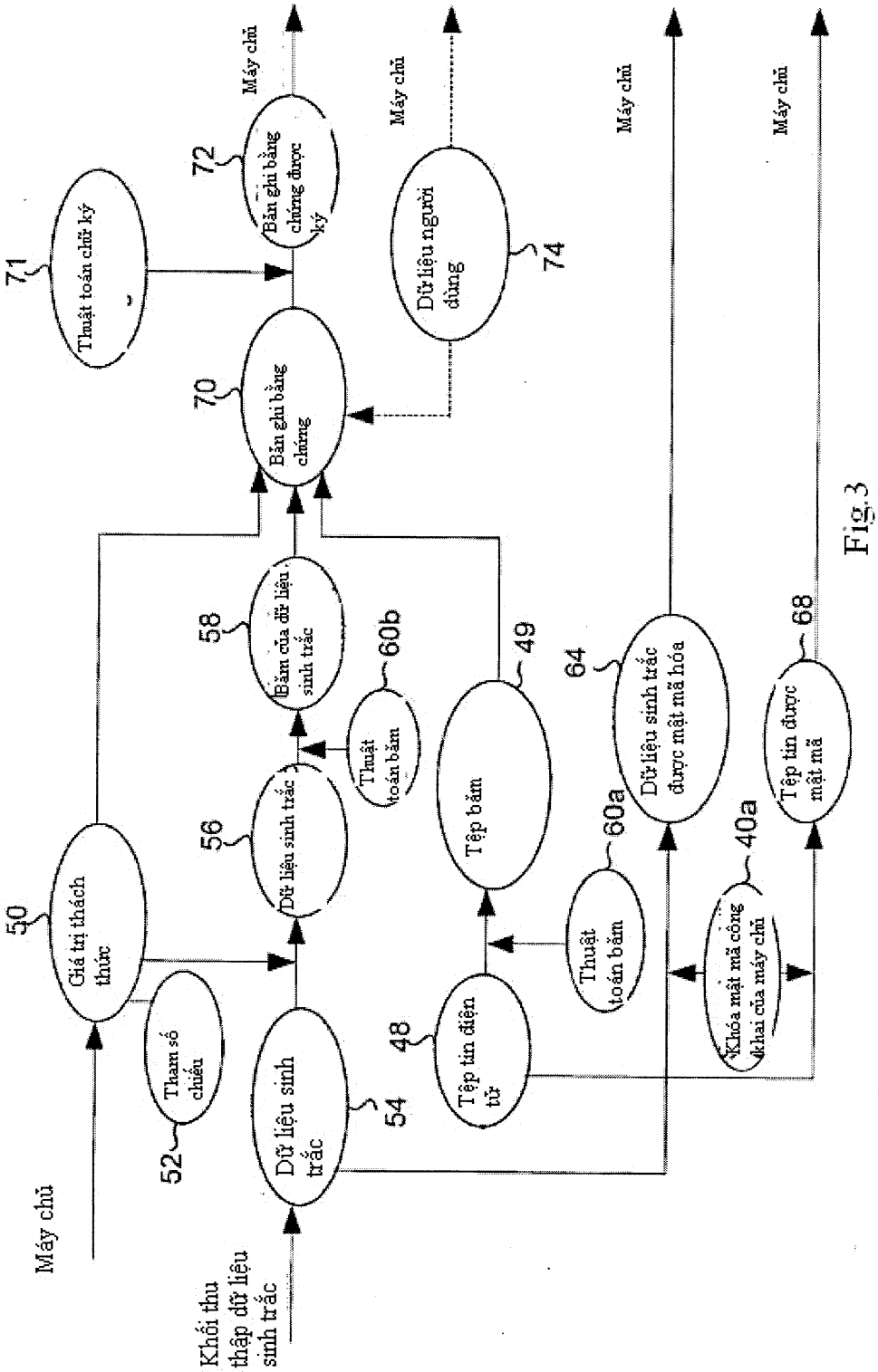

Máy chủ
Khối thu thập dữ liệu sinh trắc
Giá trị thách thức
50
Tham số chiếu
52
Dữ liệu sinh trắc
54
Dữ liệu sinh trắc
56
Thuật toán băm
60b
Băm của dữ liệu sinh trắc
58
Bản ghi bằng chứng
70
Thuật toán chữ ký
71
Bản ghi bằng chứng được ký
72
Máy chủ
Dữ liệu người dùng
74
Máy chủ
Tệp tin điện tử
48
Tệp băm
49
Thuật toán băm
60a
Khóa mật mã công khai của máy chủ
40a
Dữ liệu sinh trắc được mật mã hóa
64
Máy chủ
Tệp tin được mật mã
68
Máy chủ

Fig.3

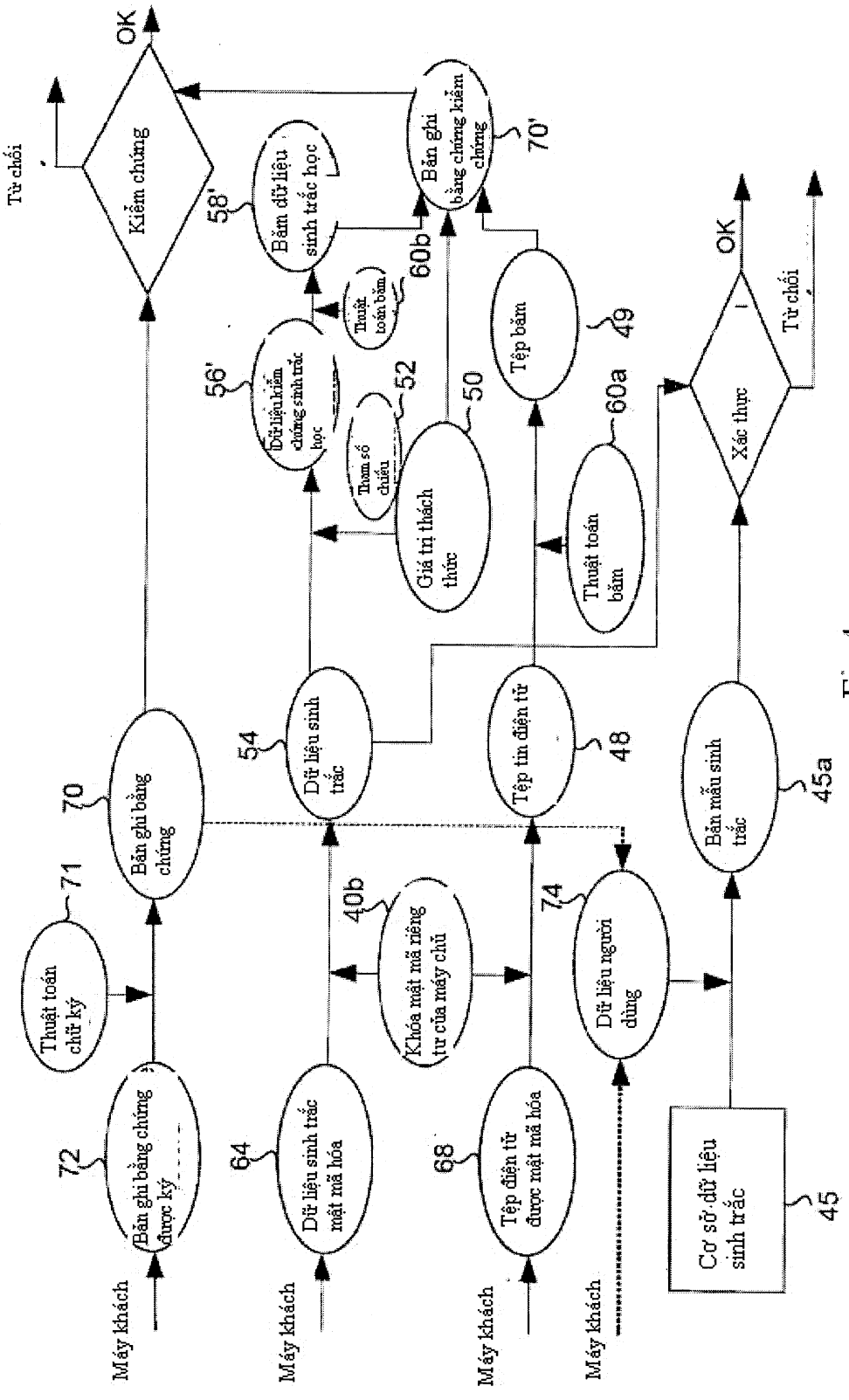

Máy khách
Bản ghi bằng chứng được ký
72
Thuật toán chữ ký
71
Bản ghi bằng chứng
70
Máy khách
Dữ liệu sinh trắc mật mã hóa
64
Khóa mật mã riêng tư của máy chủ
40b
Dữ liệu sinh trắc
54
Máy khách
Tệp tin điện tử được mật mã hóa
68
Tệp tin điện tử
48
Máy khách
Dữ liệu người dùng
74
Cơ sở dữ liệu sinh trắc
45
Bản mẫu sinh trắc
45a
Xác thực
OK
Từ chối
Thuật toán băm
60a
Tệp băm
49
Giá trị thách thức
50
Tham số chiếu
52
Dữ liệu kiểm chứng sinh trắc học
56'
Thuật toán băm
60b
Băm dữ liệu sinh trắc học
58'
Bản ghi bằng chứng kiểm chứng
70'
Kiểm chứng
OK
Từ chối

Fig.4

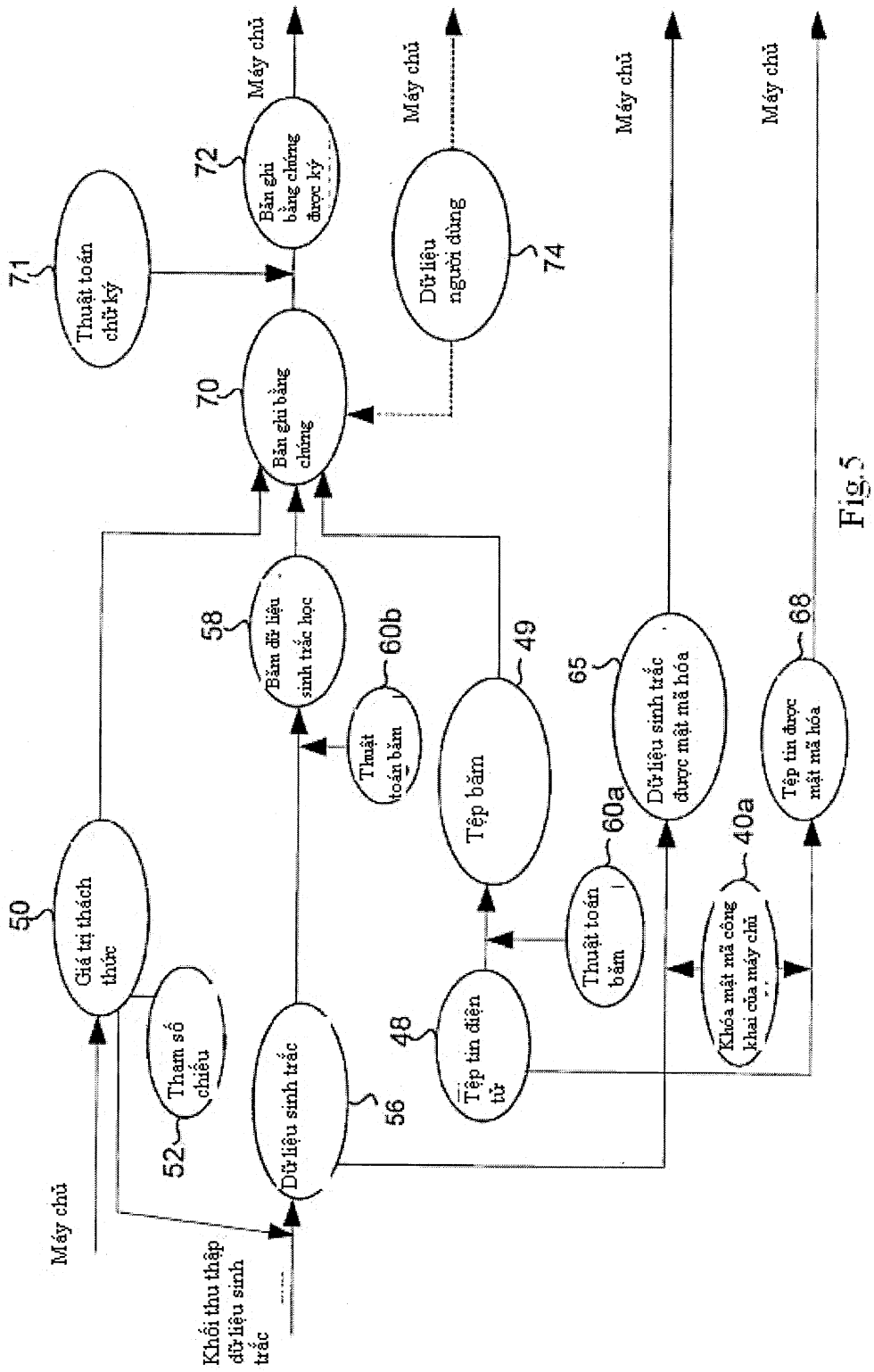

Máy chủ
Khối thu thập dữ liệu sinh trắc
Giá trị thách thức
50
Tham số chiếu
52
Dữ liệu sinh trắc
56
Tệp tin điện tử
48
Thuật toán băm
60a
Tệp băm
49
Khóa mật mã công khai của máy chủ
40a
Dữ liệu sinh trắc được mật mã hóa
65
Tệp tin được mật mã hóa
68
Máy chủ
Máy chủ
Máy chủ
Băm dữ liệu sinh trắc học
58
Thuật toán băm
60b
Bản ghi bằng chứng
70
Thuật toán chữ ký
71
Bản ghi bằng chứng được ký
72
Dữ liệu người dùng
74

Fig.5

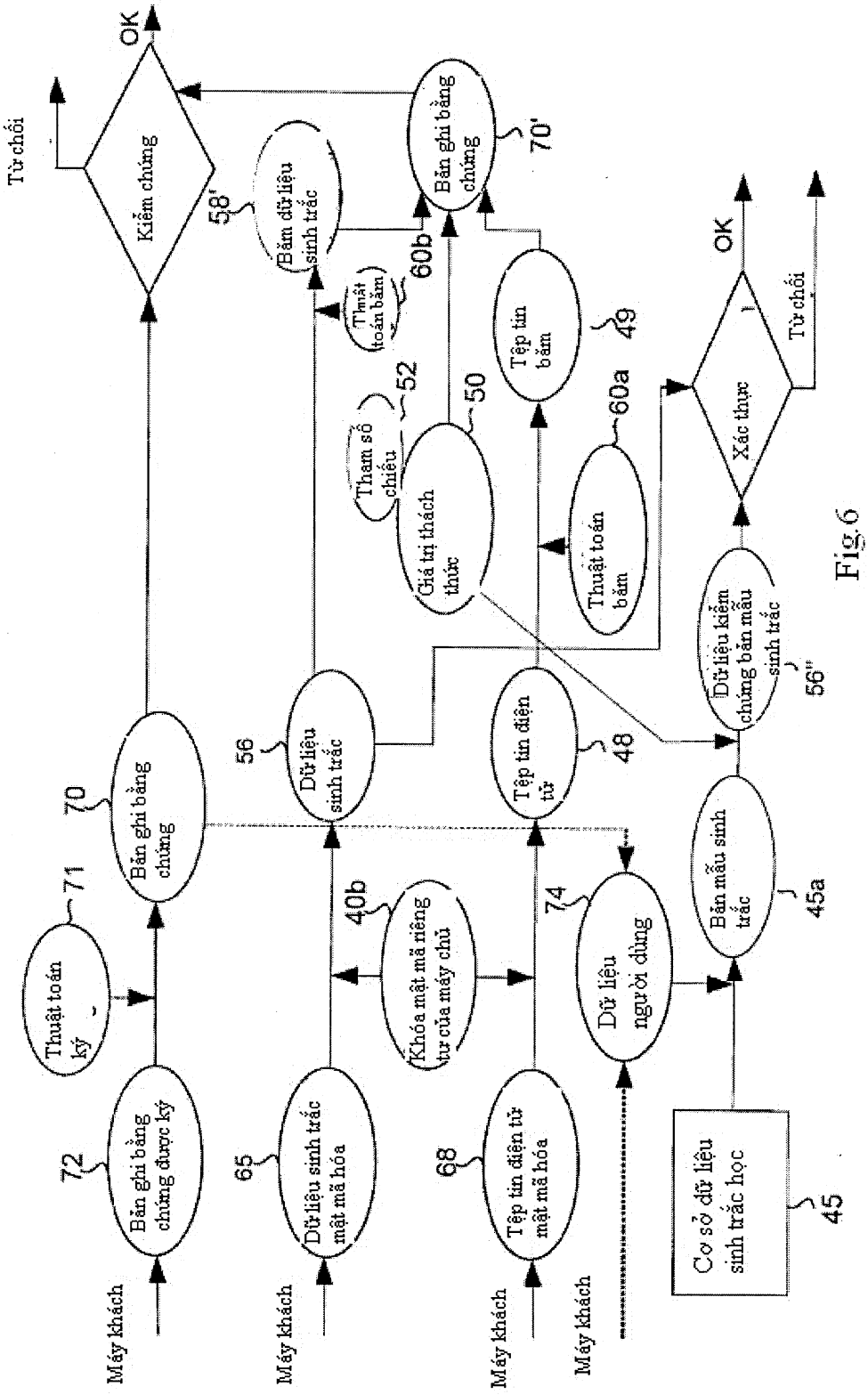

Máy khách
Bản ghi bằng chứng được ký
72
Thuật toán ký
71
Bản ghi bằng chứng
70
Máy khách
Dữ liệu sinh trắc mật mã hóa
65
Khóa mật mã riêng tư của máy chủ
40b
Dữ liệu sinh trắc
56
Máy khách
Tệp tin điện tử mật mã hóa
68
Tệp tin điện tử
48
Máy khách
Dữ liệu người dùng
74
Cơ sở dữ liệu sinh trắc học
45
Bản mẫu sinh trắc
45a
Dữ liệu kiểm chứng bản mẫu sinh trắc
56''
Xác thực
OK
Từ chối
Thuật toán bằm
Tham số chiếu
52
Giá trị thách thức
50
Thuật toán bằm
60a
Tệp tin bằm
49
Bản ghi bằng chứng
70'
Băm dữ liệu sinh trắc
58'
60b
Kiểm chứng
OK
Từ chối

Fig.6

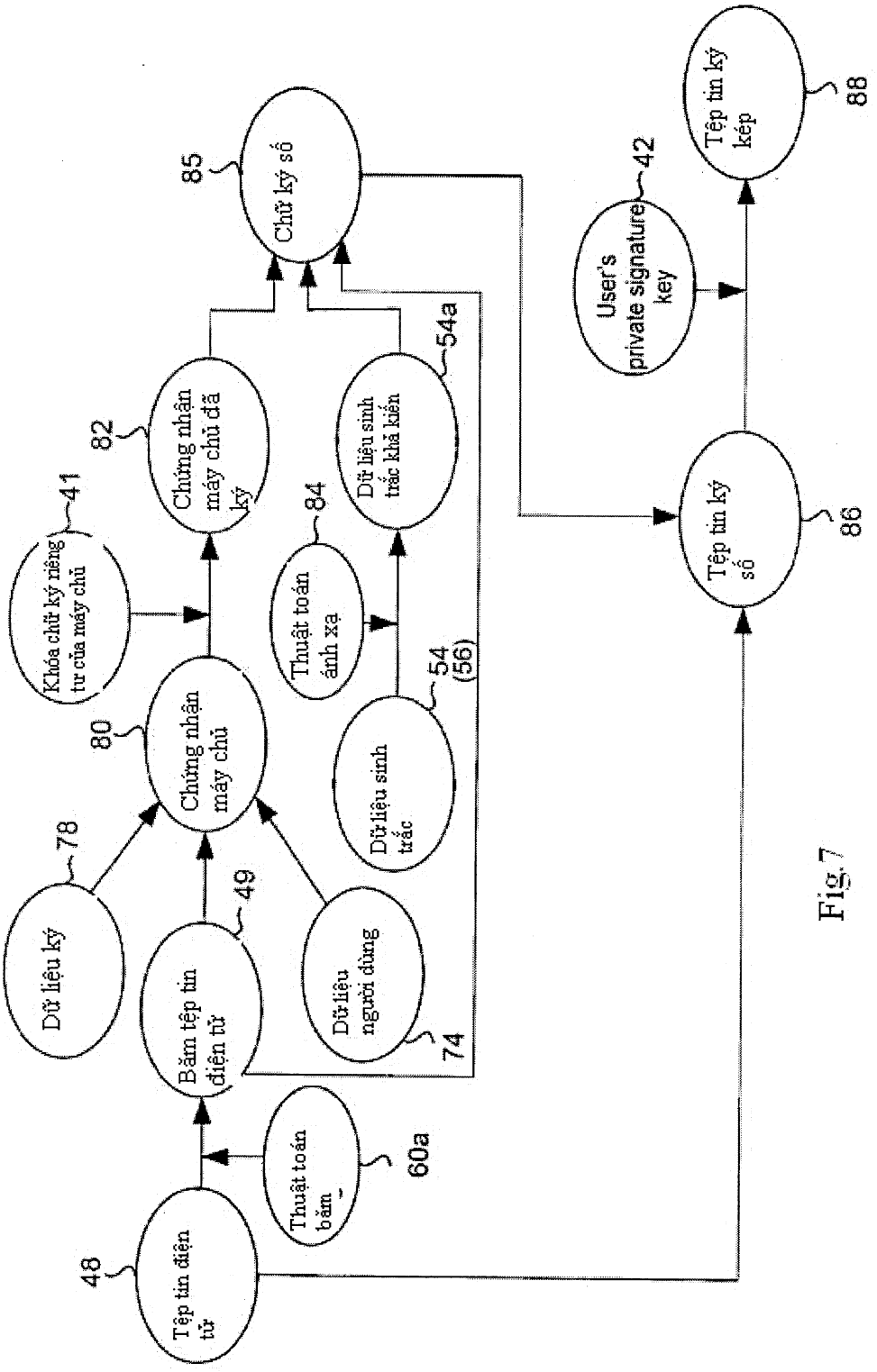

Tệp tin điện tử
48
Thuật toán băm
60a
Băm tệp tin điện tử
49
Dữ liệu ký
78
Dữ liệu người dùng
74
Chứng nhận máy chủ
80
Khóa chữ ký riêng tư của máy chủ
41
Chứng nhận máy chủ đã ký
82
Thuật toán ánh xạ
84
Dữ liệu sinh trắc
54
(56)
Dữ liệu sinh trắc khả kiến
54a
Chữ ký số
85
Tệp tin ký số
86
User's private signature key
42
Tệp tin ký kép
88

Fig 7

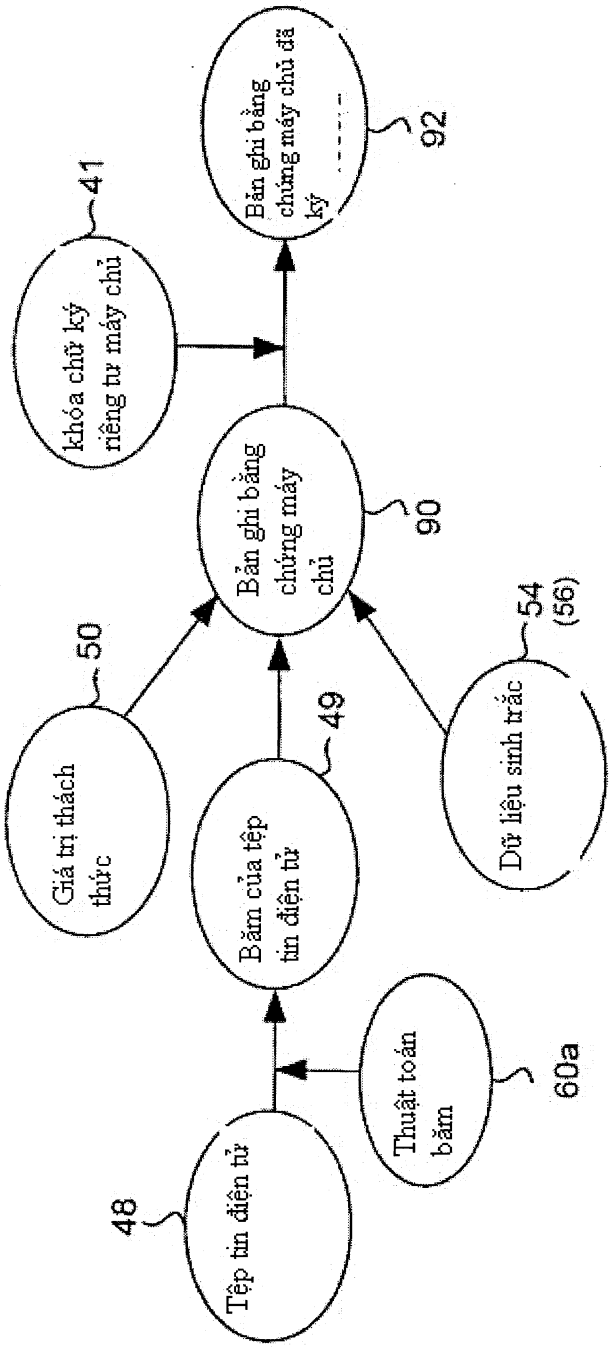

Tệp tin điện tử
48
Thuật toán băm
60a
Băm của tệp tin điện tử
49
Giá trị thách thức
50
Dữ liệu sinh trắc
54
(56)
Bản ghi bằng chứng máy chủ
90
khóa chữ ký riêng tư máy chủ
41
Bản ghi bằng chứng máy chủ đã ký
92

Fig.8