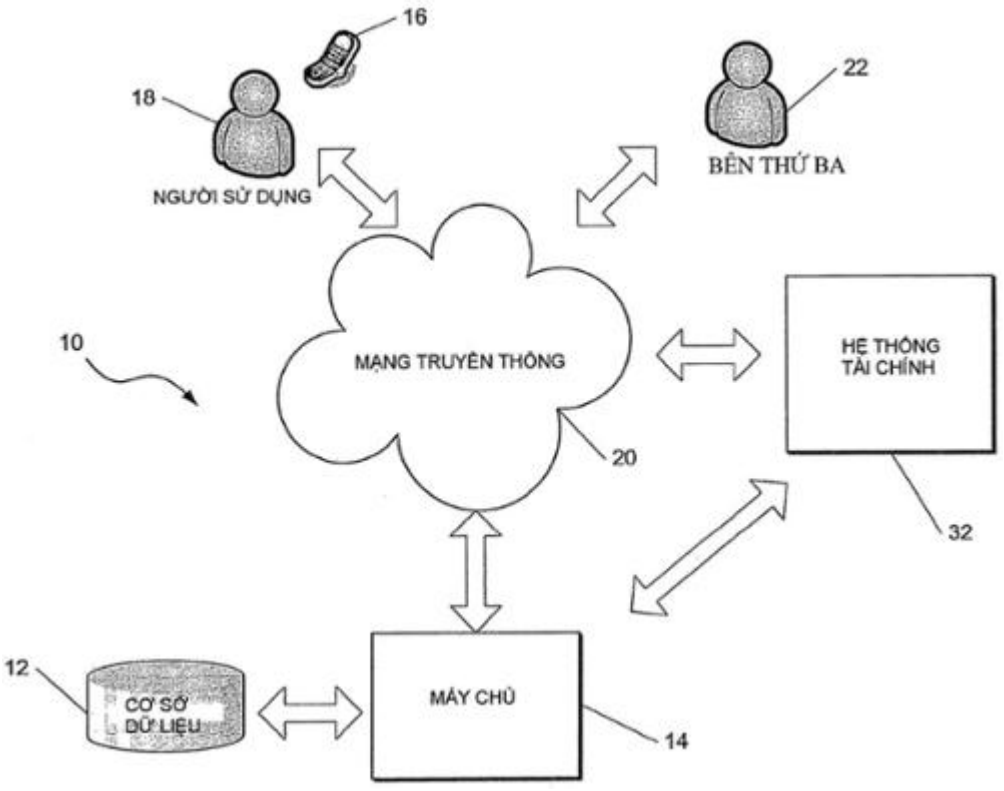
(12) BẢN MÔ TẢ SÁNG CHẾ THUỘC BẰNG ĐỘC QUYỀN SÁNG CHẾ
(19) **Cộng hòa xã hội chủ nghĩa Việt Nam (VN)**
CỤC SỞ HỮU TRÍ TUỆ
(11) **1-0023630**
(51)[7] **G06Q 20/00**
(13) **B**

(21) 1-2011-01822
(22) 18/12/2009
(86) PCT/IB2009/055838 18/12/2009
(87) WO2010/073199 01/07/2010
(30) 2008/10835 23/12/2008 ZA
(45) 25/05/2020 386
(43) 25/10/2011 283A
(73) Mastercard Asia/Pacific Pte. Ltd. (ZA)
3 Fraser Street, DUO Tower #17-21/28, Singapore, 18935
(72) Bruynse, Dirk Marinus (ZA); Bezuidenhoudt, Schalk Johann (ZA)
(74) Công ty TNHH Tầm nhìn và Liên danh (VISION & ASSOCIATES CO.LTD.)

# (54) PHƯƠNG PHÁP VÀ HỆ THỐNG XỬ LÝ GIAO DỊCH MỘT CÁCH AN TOÀN

(57) Sáng chế đề xuất phương pháp xử lý giao dịch một cách an toàn bao gồm các bước lưu trữ nhiều mã nhận dạng phương tiện giao dịch tài chính đã được mã hoá trong bộ nhớ trong đó không có khoá giải mã cho chúng được lưu trữ trong bộ nhớ và trong đó mỗi mã nhận dạng phương tiện giao dịch tài chính được mã hoá được kết hợp với thiết bị truyền thông di động. Nhận yêu cầu ở máy chủ để xử lý giao dịch, yêu cầu này bao gồm thông tin nhận dạng của thiết bị truyền thông di động. Truy hồi từ bộ nhớ mã nhận dạng phương tiện giao dịch tài chính đã được mã hoá được kết hợp với thiết bị truyền thông di động được nhận dạng trong yêu cầu. Truyền mã nhận dạng phương tiện giao dịch tài chính được mã hoá đã được truy hồi tới thiết bị truyền thông di động. Nhận dữ liệu giao dịch từ thiết bị truyền thông di động và sử dụng dữ liệu giao dịch nhận được để thực hiện giao dịch tài chính.



**Lĩnh vực kỹ thuật được đề cập**

Sáng chế đề cập đến phương pháp và hệ thống xử lý giao dịch một cách an toàn, đặc biệt bằng cách sử dụng thiết bị truyền thông di động.

**Tình trạng kỹ thuật của sáng chế**

Có nhiều phương pháp xử lý các giao dịch bằng cách sử dụng thiết bị truyền thông di động đã được biết đến. Tuy nhiên, không có phương pháp nào đưa ra giải pháp an toàn mà dễ dàng sử dụng và hiệu quả.

Mục tiêu của sáng chế là đề xuất phương pháp và hệ thống cải tiến để xử lý giao dịch một cách an toàn.

**Bản chất kỹ thuật của sáng chế**

Theo khía cạnh thứ nhất của sáng chế, phương pháp xử lý giao dịch một cách an toàn được đề xuất bao gồm các bước:

lưu trữ nhiều mã nhận dạng phương tiện giao dịch tài chính đã được mã hoá trong bộ nhớ trong đó không có khoá giải mã cho chúng được lưu trữ trong bộ nhớ và trong đó mỗi mã nhận dạng phương tiện giao dịch tài chính được mã hoá được kết hợp với thiết bị truyền thông di động;

nhận yêu cầu ở máy chủ để xử lý giao dịch, yêu cầu này bao gồm thông tin nhận dạng của thiết bị truyền thông di động;

truy hồi từ bộ nhớ mã nhận dạng phương tiện giao dịch tài chính đã được mã hoá được kết hợp với thiết bị truyền thông di động được nhận dạng trong yêu cầu;

truyền mã nhận dạng phương tiện giao dịch tài chính được mã hoá đã được truy hồi tới thiết bị truyền thông di động;

nhận dữ liệu giao dịch từ thiết bị truyền thông di động và sử dụng dữ liệu giao dịch nhận được để thực hiện giao dịch tài chính.

Dữ liệu giao dịch nhận được từ thiết bị truyền thông di động có thể bao gồm khoá giải mã để giải mã mã nhận dạng phương tiện giao dịch tài chính đã được mã hoá, lưu trữ được kết hợp với thiết bị truyền thông di động.

Theo cách khác hoặc ngoài ra, dữ liệu giao dịch nhận được từ thiết bị truyền thông di động bao gồm mã nhận dạng phương tiện giao dịch tài chính cần được sử dụng để thực hiện giao dịch tài chính.

Tốt hơn nếu phương pháp bao gồm bước nhận PIN từ thiết bị truyền thông di động để ủy quyền giao dịch tài chính.

PIN có thể được nhận thông qua kênh truyền thông khác với dữ liệu giao dịch nhận được từ thiết bị truyền thông di động.

Dữ liệu giao dịch nhận được từ thiết bị truyền thông di động có thể bao gồm một hoặc nhiều trong số:

dữ liệu thông tin nhận dạng bên thứ ba để nhận dạng bên thứ ba mà một lượng tiền cần thanh toán cho họ; và

lượng tiền cần thanh toán cho bên thứ ba.

Phương pháp này còn có thể bao gồm bước sử dụng dữ liệu giao dịch nhận được từ thiết bị truyền thông di động để tạo ra gói dữ liệu giao dịch cần được truyền tới hệ thống tài chính sử dụng gói dữ liệu giao dịch nhằm thực hiện giao dịch tài chính.

Theo một ví dụ, gói dữ liệu giao dịch được tạo cấu trúc theo cùng định dạng với gói dữ liệu hiện hữu thẻ sao cho hệ thống tài chính có thể xử lý giao dịch tài chính như là giao dịch hiện hữu thẻ.

Theo khía cạnh thứ hai của sáng chế, hệ thống xử lý giao dịch một cách an toàn được đề xuất bao gồm:

bộ nhớ lưu trữ nhiều mã nhận dạng phương tiện giao dịch tài chính đã được mã hoá trong đó không có khoá giải mã cho chúng được lưu trữ trong bộ nhớ và

trong đó mỗi mã nhận dạng phương tiện giao dịch tài chính được mã hoá được kết hợp với thiết bị truyền thông di động;

môđun truyền thông để nhận yêu cầu xử lý giao dịch, yêu cầu này bao gồm thông tin nhận dạng của thiết bị truyền thông di động;

môđun truy hồi để truy hồi từ bộ nhớ mã nhận dạng phương tiện giao dịch tài chính đã được mã hoá được kết hợp với thiết bị truyền thông di động được nhận dạng trong yêu cầu và chuyển nó tới môđun truyền thông để truyền tới thiết bị truyền thông di động; và

môđun định dạng dữ liệu truyền thông với môđun truyền thông để nhận dữ liệu giao dịch từ thiết bị truyền thông di động và để sử dụng dữ liệu giao dịch nhận được để thực hiện giao dịch tài chính.

Môđun truyền thông còn có thể nhận dữ liệu giao dịch từ thiết bị truyền thông di động, dữ liệu giao dịch này bao gồm khoá giải mã để giải mã mã nhận dạng phương tiện giao dịch tài chính đã được mã hoá, lưu trữ được kết hợp với thiết bị truyền thông di động.

Theo cách khác hoặc ngoài ra, môđun truyền thông còn nhận dữ liệu giao dịch từ thiết bị truyền thông di động, dữ liệu giao dịch này bao gồm mã nhận dạng phương tiện giao dịch tài chính cần được sử dụng để thực hiện giao dịch tài chính.

Tốt hơn nếu, môđun truyền thông còn nhận PIN từ thiết bị truyền thông di động để ủy quyền giao dịch tài chính.

Môđun truyền thông có thể nhận PIN thông qua kênh truyền thông khác với dữ liệu giao dịch nhận được từ thiết bị truyền thông di động.

Theo một ví dụ, dữ liệu giao dịch nhận được từ thiết bị truyền thông di động bao gồm một hoặc nhiều trong số:

dữ liệu thông tin nhận dạng bên thứ ba để nhận dạng bên thứ ba mà một lượng tiền cần thanh toán cho họ; và

lượng tiền cần thanh toán cho bên thứ ba.

Môđun định dạng dữ liệu còn có thể sử dụng dữ liệu giao dịch nhận được từ thiết bị truyền thông di động để tạo ra gói dữ liệu giao dịch cần được truyền tới hệ thống tài chính sử dụng gói dữ liệu giao dịch để thực hiện giao dịch tài chính.

Tốt hơn nếu, môđun định dạng dữ liệu tạo cấu trúc cho gói dữ liệu giao dịch theo cùng định dạng với gói dữ liệu hiện hữu thẻ sao cho hệ thống tài chính có thể xử lý giao dịch tài chính như giao dịch hiện hữu thẻ.

Theo khía cạnh thứ ba của sáng chế, phương pháp xử lý giao dịch một cách an toàn được đề xuất bao gồm các bước:

lưu trữ trên thiết bị truyền thông di động khoá để giải mã mã nhận dạng phương tiện giao dịch tài chính đã được mã hoá;

nhận mã nhận dạng phương tiện giao dịch tài chính được mã hoá tại thiết bị truyền thông di động;

giải mã mã nhận dạng phương tiện giao dịch tài chính đã được mã hoá;

hiển thị cho người sử dụng thiết bị truyền thông di động mã nhận dạng phương tiện giao dịch tài chính cùng với thông tin liên quan đến giao dịch tài chính;

nhắc người sử dụng nhập vào PIN xác thực;

mã hoá PIN xác thực và truyền nó qua mạng truyền thông tới máy chủ nhờ đó lệnh cho máy chủ xử lý giao dịch tài chính được nhận dạng đối với người sử dụng.

Khoá để giải mã mã nhận dạng phương tiện giao dịch tài chính đã được mã hoá có thể giống với khoá được lưu trữ trong bộ nhớ trên thiết bị truyền thông di động và được sử dụng bởi thiết bị truyền thông di động để xác thực truyền thông qua mạng truyền thông di động.

Ngoài ra, mã nhận dạng phương tiện giao dịch tài chính và PIN xác thực có thể được truyền qua các mạng truyền thông khác nhau tới máy chủ.

Theo khía cạnh thứ hai của sáng chế, hệ thống xử lý giao dịch một cách an toàn được đề xuất bao gồm:

bộ nhớ lưu trữ trên thiết bị truyền thông di động khoá để giải mã mã nhận dạng phương tiện giao dịch tài chính đã được mã hoá;

môđun nhận để nhận mã nhận dạng phương tiện giao dịch tài chính được mã hoá ở thiết bị truyền thông di động;

môđun giải mã để giải mã mã nhận dạng phương tiện giao dịch tài chính đã được mã hoá;

màn hình để hiển thị cho người sử dụng thiết bị truyền thông di động mã nhận dạng phương tiện giao dịch tài chính cùng với thông tin liên quan đến giao dịch tài chính;

môđun đầu vào dữ liệu để nhận PIN xác thực từ người sử dụng; và

môđun mã hoá để truyền PIN qua mạng truyền thông tới máy chủ nhờ đó lệnh cho máy chủ xử lý giao dịch tài chính được nhận dạng đối với người sử dụng.

**Mô tả vắn tắt các hình vẽ**

Fig.1 là sơ đồ giản lược của hệ thống theo một phương án thực hiện làm ví dụ;

Fig.2 là sơ đồ khối chi tiết hơn của máy chủ trên Fig.1;

Fig.3 là lưu đồ của phương pháp theo một phương án thực hiện làm ví dụ;

Fig.4 là lưu đồ của phương pháp làm ví dụ dùng cho sáng chế; và

Fig.5là sơ đồ khối của thiết bị truyền thông di động làm ví dụ.

**Mô tả chi tiết sáng chế**

Trong phần mô tả sau đây, để nhằm giải thích, nhiều chi tiết cụ thể được đưa ra để giúp hiểu rõ phương án thực hiện của sáng chế. Tuy nhiên, người có hiểu biết trung bình trong lĩnh vực sẽ hiểu rõ rằng sáng chế có thể được thực hiện mà không cần các chi tiết cụ thể này.

Theo các hình vẽ kèm theo trong đó hệ thống và phương pháp theo sáng chế được thể hiện, hệ thống 10 bao gồm bộ nhớ 12 lưu trữ nhiều mã nhận dạng phương tiện giao dịch tài chính đã được mã hoá.

Điều quan trọng và điều sẽ được mở rộng chi tiết hơn sau đây là không có khoá giải mã cho các mã nhận dạng phương tiện giao dịch tài chính được mã hoá đã được lưu trữ này trong bộ nhớ 12 hoặc trong máy chủ được kết hợp 14.

Điều này có nghĩa là bộ nhớ 12 cũng như máy chủ được kết hợp 14 không thể giải mã chúng để trích xuất các mã nhận dạng phương tiện giao dịch tài chính được lưu trữ trong đó.

Ngoài ra, mỗi mã nhận dạng phương tiện giao dịch tài chính được mã hoá được kết hợp duy nhất với thiết bị truyền thông di động 16 của người sử dụng 18.

Để thuận tiện, chỉ một thiết bị truyền thông di động 16 và người sử dụng 18 được minh hoạ trên Fig.1, tuy nhiên trong thực tế, có thể có nhiều thiết bị truyền thông di động 16, mỗi thiết bị này được kết hợp duy nhất với nhiều người sử dụng 18.

Một trong các mục tiêu của sáng chế là cho phép người sử dụng 18 sử dụng thiết bị truyền thông di động 16 cho giao dịch tài chính theo cách an toàn. Theo phương pháp được mô tả sau đây giao dịch tài chính sẽ được minh hoạ là thanh toán cho hàng hoá hoặc dịch vụ nhưng cần hiểu rằng nó chỉ nhằm mục đích làm ví dụ và các loại giao dịch tài chính khác có thể được thực hiện tương đương bằng cách sử dụng hệ thống và phương pháp được mô tả ở đây.

Ngoài ra, phương tiện giao dịch tài chính có thể ví dụ là thẻ tín dụng hoặc thẻ ghi nợ.

Để thu được các mã nhận dạng phương tiện giao dịch tài chính và kết hợp chúng với các thiết bị truyền thông di động, người sử dụng 18 sẽ được yêu cầu đăng ký để sử dụng hệ thống.

Trước khi đăng ký, người sử dụng phải có mã nhận dạng phương tiện giao dịch tài chính hợp lệ như thẻ ghi nợ hoặc thẻ tín dụng được kết hợp với ví dụ tài khoản thẻ

ghi nợ hoặc thẻ tín dụng. Mặc dù việc sử dụng một thẻ ghi nợ hoặc thẻ tín dụng cho mỗi người sử dụng sẽ được mô tả sau đây, nhưng hệ thống cũng có thể cung cấp nhiều thẻ cho mỗi người sử dụng.

Sau đó, người sử dụng truy cập máy chủ 14 thông qua kênh truyền thông để tiến hành quy trình đăng ký.

Máy chủ 14 được minh hoạ chi tiết hơn trong sơ đồ khối trên Fig.2 bao gồm môđun truyền thông 24 nhằm mục đích của quy trình truyền thông này và các quy trình truyền thông khác mà máy chủ thực hiện như sẽ được mô tả chi tiết hơn sau đây.

Kênh truyền thông được sử dụng cho quy trình truyền thông có thể giống với kênh truyền thông 20 được sử dụng để xử lý các giao dịch hoặc có thể là một kênh truyền thông khác.

Theo phương án thực hiện được minh hoạ, kênh truyền thông 20 bao gồm mạng truyền thông di động.

Trong đó người sử dụng dùng thiết bị truyền thông di động 16 và kênh truyền thông 20 của họ, nhiều giao thức sẵn có bao gồm quay số vào máy chủ đáp ứng thoại tương tác (interactive voice response-IVR), tiến hành các quy trình Dữ liệu dịch vụ bổ sung phi cấu trúc (Unstructured Supplementary Service Data-USSD), sử dụng giao thức Ứng dụng không dây (Wireless Application-WAP) hoặc Cổng Internet không dây (Wireless Internet Gateway-WIG) để truy cập máy chủ 14, được nêu ra nhưng chỉ là một vài ví dụ.

Rõ ràng rằng, người sử dụng có thể sử dụng mạng và giao thức truyền thông khác để hoàn thành quy trình đăng ký như nêu trên.

Trong bất kỳ trường hợp nào, máy chủ 14 hoặc một máy chủ khác được kết hợp với máy chủ 14 sẽ bao gồm phần cứng và phần mềm để cho phép người sử dụng truy cập máy chủ và hoàn thành quy trình đăng ký.

Nhằm mục đích minh hoạ, quy trình đăng ký sẽ được mô tả như được thực hiện bởi máy chủ 14.

Máy chủ 14 nhận yêu cầu đăng ký và phát hiện mã nhận dạng của thiết bị truyền thông di động ví dụ như Số thư mục thuê bao quốc tế của trạm di động (Mobile Station International Subscriber Directory Number-MSISDN) của thiết bị.

Khi người sử dụng không sử dụng thiết bị truyền thông di động để đăng ký họ sẽ được nhắc nhập vào mã nhận dạng của thiết bị truyền thông di động 16.

Máy chủ 14 xác nhận rằng mã nhận dạng của thiết bị truyền thông di động là hợp lệ bằng cách kiểm tra mã nhận dạng với mạng truyền thông di động 20.

Người sử dụng 18 được nhắc nhập vào chi tiết thông tin nhận dạng cá nhân như số nhận dạng của họ.

Ngoài ra, người sử dụng được nhắc nhập vào chi tiết phương tiện giao dịch tài chính. Theo phương án thực hiện được minh hoạ của thẻ tín dụng hoặc thẻ ghi nợ, người sử dụng nhập vào một hoặc nhiều trong số loại thẻ, số thẻ, ngày hết hạn của thẻ, và tài khoản được kết hợp với thẻ.

Khi số tài khoản thu được từ người sử dụng, tài khoản cũng có thể được kiểm tra số dư dương của các quỹ sẵn có bởi máy chủ 14.

Một khi thông tin được nhận ở máy chủ 14, thông tin được truyền một cách an toàn trở lại cho người sử dụng để xác nhận trên thiết bị truyền thông di động 16 của họ qua mạng truyền thông 20.

Người sử dụng xác nhận rằng thông tin là đúng và sau đó được nhắc thêm từ thiết bị truyền thông di động 16 của họ để nhập vào một hoặc nhiều trong số PIN được kết hợp với thẻ và giá trị kiểm tra được hiển thị trên thẻ gọi là giá trị CV2, CVV hoặc CVC.

Sau đó, tất cả thông tin phương tiện giao dịch tài chính được mô tả ở trên được mã hoá bởi thiết bị truyền thông di động 16, được truyền qua mạng truyền thông 20 tới máy chủ 14 và được lưu trong bộ nhớ 12 được kết hợp với thông tin cá nhân và thiết bị truyền thông di động 16.

Như được mô tả ở trên, khoá giải mã không được lưu trữ trong bộ nhớ 12 hoặc trong bộ nhớ bất kỳ khác được kết hợp với máy chủ 14. Đúng hơn là khoá giải mã chỉ được lưu trong bộ nhớ thiết bị truyền thông di động 16 mà phương tiện giao dịch tài chính được kết hợp với nó. Thông thường, bộ nhớ được đặt trong SIM của thiết bị truyền thông di động 16.

Theo một phương án thực hiện làm ví dụ khoá giải mã này rất giống với các khoá được nạp vào thẻ SIM tại thời điểm sản xuất trong môi trường an toàn để cho phép thẻ SIM truyền thông một cách an toàn qua mạng truyền thông. Chức năng chính của các khoá là để ngăn việc sử dụng bất hợp pháp cơ sở hạ tầng của mạng di động và sáng chế kèm thêm các khoá này. Cần hiểu rằng các khoá được nạp sau quy trình sản xuất có thể bị gây hại một cách dễ dàng hơn.

Do đó cấu trúc hoặc khối dữ liệu an toàn được tạo ra để có thể truy cập duy nhất bởi SIM của thiết bị truyền thông di động 16 nhưng không được lưu trữ trong thiết bị truyền thông di động 16. Khối dữ liệu an toàn này chứa mã nhận dạng phương tiện giao dịch tài chính được mã hoá được lưu trữ trong máy chủ 14, máy chủ này không thể truy cập khối vì nó không có quyền truy cập khoá giải mã.

Khi người sử dụng đăng ký họ có thể tiến hành các giao dịch tài chính bằng cách sử dụng thiết bị truyền thông di động 16 của họ làm thiết bị để tiến hành giao dịch.

Theo ví dụ sau đây, giao dịch tài chính sẽ được mô tả như việc mua sản phẩm hoặc dịch vụ trong đó thiết bị truyền thông di động 16 được sử dụng tiếp theo để thanh toán sản phẩm hoặc dịch vụ. Tuy nhiên, cần hiểu rằng giao dịch tài chính có thể là loại giao dịch tài chính bất kỳ khác và không bị giới hạn vào giao dịch thanh toán.

Nhằm mục đích minh hoạ, sự thanh toán được thực hiện cho bên thứ ba 22, nhóm này có tài khoản cùng loại hoặc khác loại với tổ chức tài chính. Bên thứ ba 22 có thể được kết nối hoặc không kết nối trên mạng truyền thông 20.

Trong bất kỳ trường hợp nào, người sử dụng khởi đầu giao dịch tài chính bằng cách gửi tin nhắn yêu cầu giao dịch tới máy chủ 14. Tin nhắn có thể được gửi bằng

cách sử dụng thiết bị truyền thông di động 16 và mạng truyền thông 20 hoặc tin nhắn có thể được gửi tới máy chủ 14 bằng cách sử dụng kênh truyền thông khác. Một phương án thực hiện của quy trình khởi đầu này được thể hiện trong phần đầu của quy trình trên Fig.4.

Nếu sử dụng kênh truyền thông khác thì thông tin nhận dạng của thiết bị truyền thông di động 16 cần được gửi cùng với yêu cầu. Nếu tin nhắn được gửi từ thiết bị truyền thông di động 16 thì mã nhận dạng của thiết bị truyền thông di động 16 thường có thể được trích xuất từ tin nhắn. Ví dụ, việc này thường được thực hiện bằng cách phát hiện Số thư mục thuê bao quốc tế của trạm di động (Mobile Station International Subscriber Directory Number-MSISDN) của thiết bị.

Trong bất kỳ trường hợp nào, yêu cầu được nhận ở máy chủ 14. Yêu cầu này có vai trò như sự kích hoạt để bắt đầu quy trình giao dịch tài chính.

Đáp lại sự kích hoạt, môđun truy hồi 26 của máy chủ 14 truy hồi từ bộ nhớ 12 mã nhận dạng phương tiện giao dịch tài chính được mã hoá được kết hợp với thiết bị truyền thông di động 16 mà yêu cầu đã được nhận từ đó hoặc được nhận dạng trong yêu cầu nhận được.

Bằng cách sử dụng môđun truyền thông 24, mã nhận dạng phương tiện giao dịch tài chính được mã hoá đã được truy hồi được truyền tới thiết bị truyền thông di động được nhận dạng 16 qua mạng truyền thông 20.

Như được mô tả ở trên, thiết bị truyền thông di động 16 đã lưu trữ trong đó khoá để giải mã mã nhận dạng phương tiện giao dịch tài chính đã được mã hoá nhận được từ máy chủ 14.

Theo một phương án thực hiện làm ví dụ, ít nhất một số thông tin trong các thông tin về phương tiện giao dịch tài chính được hiển thị cho người sử dụng trên thiết bị truyền thông di động 16 để người sử dụng xác nhận phương tiện giao dịch tài chính đúng cần được sử dụng.

Thông tin này thường được hiển thị cho người sử dụng cùng với một số thông tin liên quan đến giao dịch tài chính cụ thể sao cho người sử dụng có thể xác nhận thêm là phương tiện giao dịch tài chính này sẽ được sử dụng cho giao dịch tài chính này.

Sau đó, người sử dụng được yêu cầu nhập PIN của họ vào để xác thực giao dịch, PIN được truyền trở lại máy chủ 14 như sẽ được mô tả chi tiết hơn sau đây.

Tiếp theo, PIN và các thành phần khác cần thiết để thực hiện giao dịch được mã hoá theo cách sao cho chỉ có máy chủ 14 có thể truy cập và sau đó được gửi qua mạng truyền thông 20 tới máy chủ 14.

Một số thông tin thu được từ mã nhận dạng phương tiện giao dịch tài chính đã được giải mã được kết hợp trong thiết bị truyền thông di động 16 với các thông tin giao dịch khác bao gồm một hoặc nhiều trong số dữ liệu thông tin nhận dạng bên thứ ba để nhận dạng bên thứ ba mà lượng tiền là để thanh toán cho họ và lượng tiền để thanh toán cho bên thứ ba.

Theo cách khác, các thông tin khác bao gồm chi tiết về bên thứ ba và lượng tiền cần thanh toán có thể được truyền tới máy chủ 14 một cách riêng rẽ mặc dù điều này sẽ làm giảm mức độ an toàn đối với giao dịch do sự tách riêng thông tin khỏi thời điểm xác thực dẫn tới sự ghép nối giao dịch và theo đó là sự thao túng giao dịch.

Do đó, thiết bị truyền thông di động 16 tạo ra gói dữ liệu giao dịch được mã hoá và gửi nó cho máy chủ 14.

Gói dữ liệu giao dịch được mã hoá không phải là giao dịch tài chính đầy đủ mà chỉ bao gồm các thành phần của chúng và theo đó máy chủ 14 tiếp tục tạo ra giao dịch và gửi nó tới ngân hàng để xác thực. Sau đây là một ví dụ về các thành phần mà gói dữ liệu có thể bao gồm:

<u>Tập hợp dữ liệu thứ nhất</u>

MSISDN của người gửi

MSIADN của người nhận (trong ví dụ này là mã nhận dạng của người nhận)

Lượng giao dịch

Các khoá MSISDN

Tập hợp dữ liệu thứ hai

MSISDN của người gửi

Các khoá MSISDN

PIN

CVV

Theo một phương án thực hiện làm ví dụ, dữ liệu được truyền trở lại từ thiết bị di động nằm trong gói dữ liệu được mã hoá được gửi tới máy chủ 14 qua một kênh truyền thông trong khi PIN được nhập bởi người sử dụng được gửi tới máy chủ 14 qua một kênh truyền thông khác, đó là lý do tại sao ví dụ trên có hai tập hợp dữ liệu.

Cần hiểu rằng việc này tăng thêm sự an toàn cho giao dịch do gói dữ liệu được mã hoá không thể sử dụng mà không có PIN và PIN là vô dụng với gói dữ liệu được mã hoá.

Hai kênh khác nhau đều có thể là kênh an toàn hoặc một hoặc cả hai kênh có thể là kênh không an toàn.

Theo một phương án thực hiện được minh hoạ, gói dữ liệu được mã hoá được gửi qua kênh USSD là một ví dụ về kênh tương đối không an toàn trong khi PIN được gửi qua kênh WIG là kênh tương đối an toàn.

Điều này là vì kênh WIG sử dụng các khoá được gắn trong bộ nhớ của thiết bị truyền thông như được mô tả ở trên để xác thực quy trình truyền thông. Một ví dụ khác về kênh an toàn là SAD, kênh này cũng sử dụng các khoá xác thực.

Do đó, theo một phương án thực hiện làm ví dụ, PIN xác thực được truyền từ thiết bị truyền thông di động 16 qua kênh an toàn theo cách sao cho mỗi lần truyền là duy nhất và máy chủ 14 trong khi xác thực cho PIN còn đảm bảo tính duy nhất của lần

truyền để đảm bảo rằng toàn bộ khối giao dịch hoặc PIN không được gửi lại. Điều này được thực hiện để chặn sự tấn công lặp lại và tái sử dụng PIN.

Khi máy chủ 14 nhận khối PIN xác thực từ thiết bị truyền thông di động 16, nó kiểm tra rằng khối PIN là đúng bằng cách sử dụng môđun kiểm tra PIN 28. Khối PIN này sẽ có thể được gửi sau đó tới tổ chức tài chính để kiểm tra thêm.

Nếu PIN đúng, máy chủ 14 sẽ giải mã gói dữ liệu giao dịch an toàn nhận được.

Máy chủ 14 sử dụng mã nhận dạng của thiết bị truyền thông di động để truy cập toàn bộ chi tiết mã nhận dạng phương tiện giao dịch tài chính mà vẫn được mã hoá và không thể truy cập vào máy chủ 14 mà không có khối dữ liệu giao dịch an toàn nhận được từ thiết bị truyền thông di động.

Khối dữ liệu từ thiết bị di động cho phép máy chủ trích xuất các chi tiết mã nhận dạng phương tiện giao dịch tài chính được mã hoá để đóng gói lại.

Theo một phương án thực hiện làm ví dụ, các khoá nhận được từ thiết bị truyền thông di động cho phép máy chủ giải mã các chi tiết mã nhận dạng phương tiện giao dịch tài chính được lưu trữ được kết hợp với MSISDN và tạo ra giao dịch tài chính để truyền tới ngân hàng.

Theo một phương án thực hiện khác, mã nhận dạng phương tiện giao dịch tài chính được truyền trở lại máy chủ bởi thiết bị truyền thông di động để được sử dụng bởi máy chủ.

Theo đó, máy chủ 14 sử dụng dữ liệu nhận được, cùng với mã nhận dạng phương tiện giao dịch tài chính để tạo ra gói dữ liệu cần được truyền tới hệ thống tài chính 32, hệ thống này sử dụng gói dữ liệu để thực hiện giao dịch tài chính.

Theo một ví dụ, dữ liệu nhận được từ thiết bị truyền thông di động 16 được nhận theo định dạng đúng để được chuyển tiếp tới hệ thống tài chính 32.

Theo một phương án thực hiện làm ví dụ khác, dữ liệu nhận được từ thiết bị truyền thông di động 16 không được nhận theo định dạng đúng để được chuyển tiếp

tới hệ thống tài chính và được định dạng lại bởi môđun định dạng dữ liệu 30 trước khi được gửi tới hệ thống tài chính 32.

Trong trường hợp khác, gói dữ liệu được tạo cấu trúc theo cùng định dạng với gói dữ liệu hiện hữu thẻ sao cho hệ thống tài chính có thể xử lý giao dịch tài chính như giao dịch hiện hữu thẻ.

Cần hiểu rằng "môđun" trong ngữ cảnh của bản mô tả bao gồm phần mã có thể nhận dạng, các lệnh tính toán hoặc có thể chạy được, dữ liệu, hoặc đối tượng tính toán để thu được chức năng, hoạt động, xử lý, hoặc thủ tục cụ thể. Môđun không cần được cài đặt chỉ trong phần mềm mà môđun có thể được cài đặt trong phần mềm và/hoặc phần sụn và/hoặc phần cứng.

Theo một ví dụ được minh hoạ trên Fig.4, phương pháp và hệ thống được sử dụng để mua thời gian phát sóng nhờ đó yêu cầu mua thời gian phát sóng được tập hợp bởi người sử dụng thường bằng cách sử dụng thiết bị truyền thông di động 16 của họ và được truyền tới máy chủ 14 hoặc máy chủ kết hợp – phần thứ nhất trên Fig.4.

Yêu cầu được xác nhận tính hợp hệ và người sử dụng sau đó được nhắc nhập vào số thiết bị truyền thông di động của người nhận. Cần hiểu rằng người sử dụng có thể nhập vào đây số của họ và mua thời gian phát sóng cho họ.

Số nhận được do người sử dụng đã nhập vào được kiểm tra để xem nó có tồn tại hay không.

Tiếp theo, toàn bộ dữ liệu giao dịch và mã nhận dạng phương tiện giao dịch tài chính được mã hoá được gửi từ máy chủ 14 qua mạng truyền thông 20 tới thiết bị truyền thông di động được nhận dạng 16 trong đó người sử dụng được nhắc nhập vào PIN của họ.

Sau đó, thiết bị truyền thông 16 thao tác dữ liệu giao dịch và mã nhận dạng phương tiện giao dịch tài chính được mã hoá và PIN, như được mô tả ở trên, và trả lại khối dữ liệu giao dịch an toàn, mã nhận dạng phương tiện giao dịch tài chính được mã hoá đã cập nhật và PIN an toàn qua mạng truyền thông 20 cho máy chủ 14.

Quy trình thanh toán được xử lý như được mô tả ở trên, trong lúc này PIN được xác nhận tính hợp lệ bởi ngân hàng.

Cần hiểu rằng để quy trình trên được cài đặt trên thiết bị truyền thông di động 16, thiết bị sẽ được thay đổi như được mô tả dưới đây thông qua Fig.5 minh hoạ thiết bị dưới dạng giản lược. Sự thay đổi này sẽ được cài đặt thành các môđun khác nhau trên thiết bị truyền thông di động 16. Chúng có thể được cài đặt như phần mã có thể nhận dạng, các lệnh tính toán hoặc có thể chạy được, dữ liệu, hoặc đối tượng tính toán để thu được chức năng, hoạt động, xử lý, hoặc thủ tục cụ thể. Môđun không cần được cài đặt chỉ trong phần mềm mà môđun có thể được cài đặt trong phần mềm và/hoặc phần sụn và/hoặc phần cứng.

Trong bất kỳ trường hợp nào, thiết bị truyền thông di động bao gồm bộ nhớ 34 đang lưu trữ trong đó một hoặc nhiều khoá để được sử dụng cho các giao thức truyền thông khác nhau và để giải mã mã nhận dạng phương tiện giao dịch tài chính đã được mã hoá. Ví dụ, bộ nhớ 34 có thể được cài đặt trên chính thiết bị truyền thông di động hoặc có thể tạo thành một phần của thẻ SIM.

Môđun nhận thường được kết hợp vào môđun truyền thông di động 36 được sử dụng để nhận mã nhận dạng phương tiện giao dịch tài chính được mã hoá ở thiết bị truyền thông di động và môđun mã hoá/giải mã 42 để giải mã mã nhận dạng phương tiện giao dịch tài chính đã được mã hoá.

Màn hình 38 hiển thị cho người sử dụng thiết bị truyền thông di động mã nhận dạng phương tiện giao dịch tài chính cùng với thông tin liên quan đến giao dịch tài chính.

Môđun đầu vào dữ liệu 48, ví dụ vùng phím của thiết bị được sử dụng để nhận PIN xác thực từ người sử dụng và môđun mã hoá/giải mã 42 ít nhất mã hoá lại mã nhận dạng phương tiện giao dịch tài chính và PIN xác thực.

Sau đó chúng được truyền qua mạng truyền thông bởi môđun truyền thông di động 36 tới máy chủ nhờ đó chỉ thị cho máy chủ xử lý giao dịch tài chính được nhận dạng đối với người sử dụng.

Cần hiểu rằng các môđun khác nhau được minh hoạ trên Fig.5 còn được làm thích hợp để thực hiện các phương pháp nêu trên.

Cần hiểu rằng đây chỉ là một ví dụ trong số nhiều ứng dụng mà phương pháp và hệ thống theo sáng chế có thể được áp dụng.

Sáng chế được mô tả trên đây đề xuất một cách mới và an toàn để xử lý giao dịch tài chính.

Hệ thống và phương pháp cho người sử dụng khả năng sử dụng các thẻ ngân hàng đã được phát hành của họ thông qua thiết bị truyền thông di động của họ. Các thẻ được đăng ký và thông tin được lưu trữ an toàn và chỉ có thể sử dụng được đối với người sử dụng thiết bị truyền thông 16, nên khách hàng không cần thiết phải mang theo người thẻ vật lý.

## Yêu cầu bảo hộ

1. Phương pháp xử lý giao dịch một cách an toàn bao gồm các bước:

nhận yêu cầu tại máy chủ để xử lý giao dịch, yêu cầu này bao gồm thông tin nhận dạng của thiết bị truyền thông di động;

truy hồi từ bộ nhớ máy chủ mã nhận dạng phương tiện giao dịch tài chính được mã hoá được kết hợp với thiết bị truyền thông di động được nhận dạng trong yêu cầu;

nhận dữ liệu giao dịch của thiết bị truyền thông di động;

nhận PIN từ thiết bị truyền thông di động để ủy quyền giao dịch tài chính, trong đó PIN được nhận thông qua một kênh truyền thông khác với dữ liệu giao dịch nhận được từ thiết bị truyền thông di động; và

sử dụng dữ liệu giao dịch nhận được từ thiết bị truyền thông di động và mã nhận dạng phương tiện giao dịch tài chính đã được truy hồi để tạo ra gói dữ liệu giao dịch cần được truyền tới hệ thống tài chính mà sử dụng gói dữ liệu giao dịch nhằm thực hiện giao dịch tài chính.

2. Phương pháp theo điểm 1, trong đó dữ liệu giao dịch nhận được từ thiết bị truyền thông di động bao gồm một hoặc nhiều trong số:

dữ liệu nhận dạng bên thứ ba để nhận dạng bên thứ ba mà một lượng tiền cần thành toán cho họ; và

lượng tiền cần thanh toán cho bên thứ ba.

3. Phương pháp theo điểm 1, trong đó gói dữ liệu giao dịch được tạo cấu trúc theo theo cùng định dạng với gói dữ liệu hiện hữu thẻ sao cho hệ thống tài chính có thể xử lý giao dịch tài chính như giao dịch hiện hữu thẻ.

4. Hệ thống xử lý giao dịch bao gồm:

bộ nhớ lưu trữ nhiều mã nhận dạng phương tiện giao dịch tài chính đã được mã hoá trong đó mỗi mã nhận dạng phương tiện giao dịch tài chính đã được mã hoá được kết hợp với thiết bị truyền thông di động;

môđun truyền thông để nhận yêu cầu để xử lý giao dịch, yêu cầu này bao gồm thông tin nhận dạng của thiết bị truyền thông di động và để nhận PIN từ thiết bị truyền thông di động để ủy quyền giao dịch tài chính, trong đó PIN được nhận thông qua một kênh truyền thông khác với dữ liệu giao dịch nhận được từ thiết bị truyền thông di động;

môđun truy hồi để truy hồi từ bộ nhớ mã nhận dạng phương tiện giao dịch tài chính đã được mã hoá được kết hợp với thiết bị truyền thông di động được nhận dạng trong yêu cầu; và

môđun định dạng dữ liệu truyền thông với môđun truyền thông để nhận từ thiết bị truyền thông di động dữ liệu giao dịch và để sử dụng dữ liệu giao dịch nhận được để tạo ra gói dữ liệu giao dịch cần được truyền tới hệ thống tài chính mà sử dụng gói dữ liệu giao dịch nhằm thực hiện giao dịch tài chính.

5. Hệ thống theo điểm 4, trong đó dữ liệu giao dịch nhận được từ thiết bị truyền thông di động bao gồm một hoặc nhiều trong số:

dữ liệu nhận dạng bên thứ ba để nhận dạng bên thứ ba mà một lượng tiền cần thanh toán cho họ; và

lượng tiền cần thanh toán cho bên thứ ba.

6. Hệ thống theo điểm 5, trong đó môđun định dạng dữ liệu tạo cấu trúc cho gói dữ liệu giao dịch theo cùng định dạng với gói dữ liệu hiện hữu thẻ sao cho hệ thống tài chính có thể xử lý giao dịch tài chính như giao dịch hiện hữu thẻ.

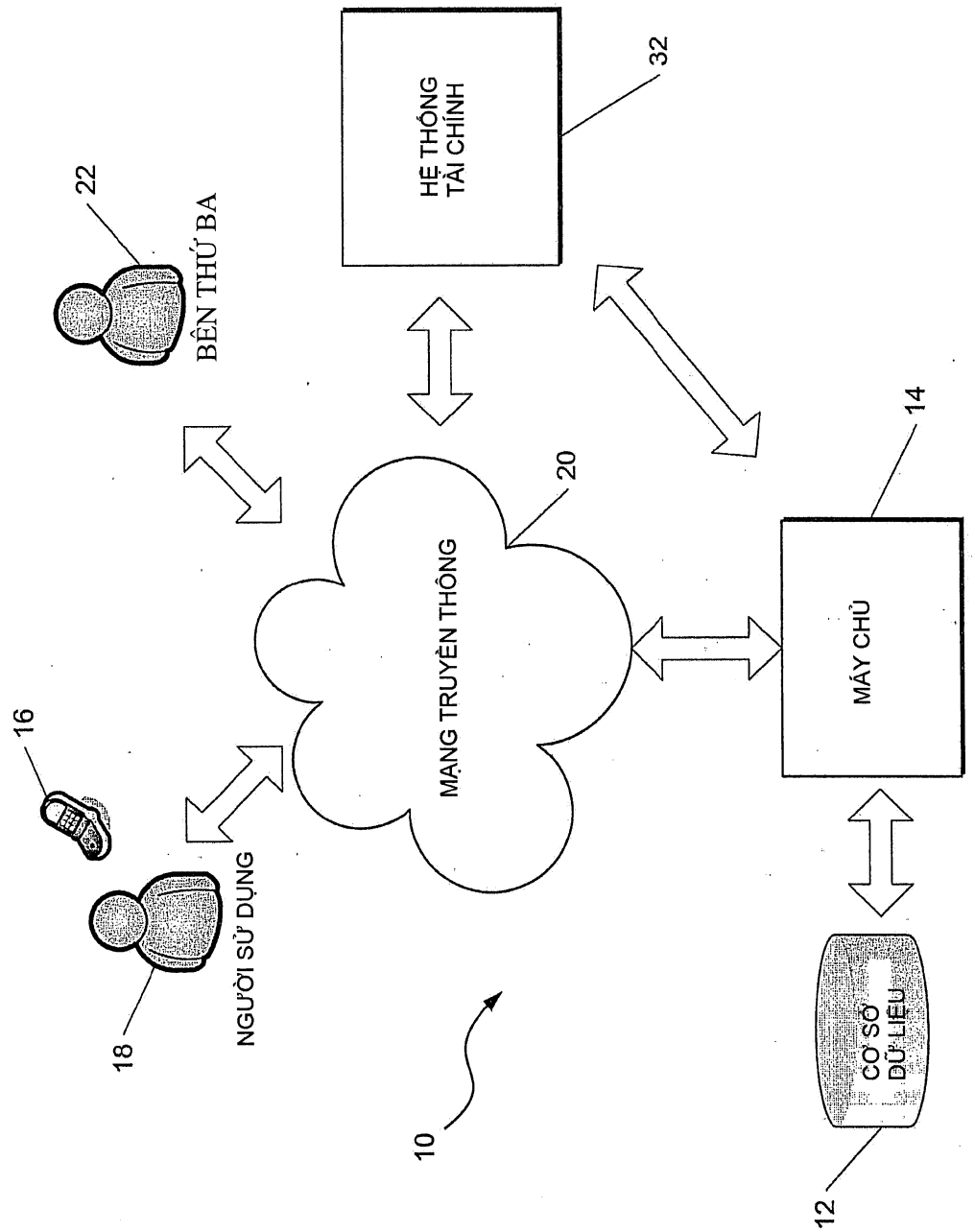

HỆ THỐNG TÀI CHÍNH
32
22
BÊN THỨ BA
MẠNG TRUYỀN THÔNG
20
MÁY CHỦ
14
16
NGƯỜI SỬ DỤNG
18
10
CƠ SỞ DỮ LIỆU
12

FIG.1

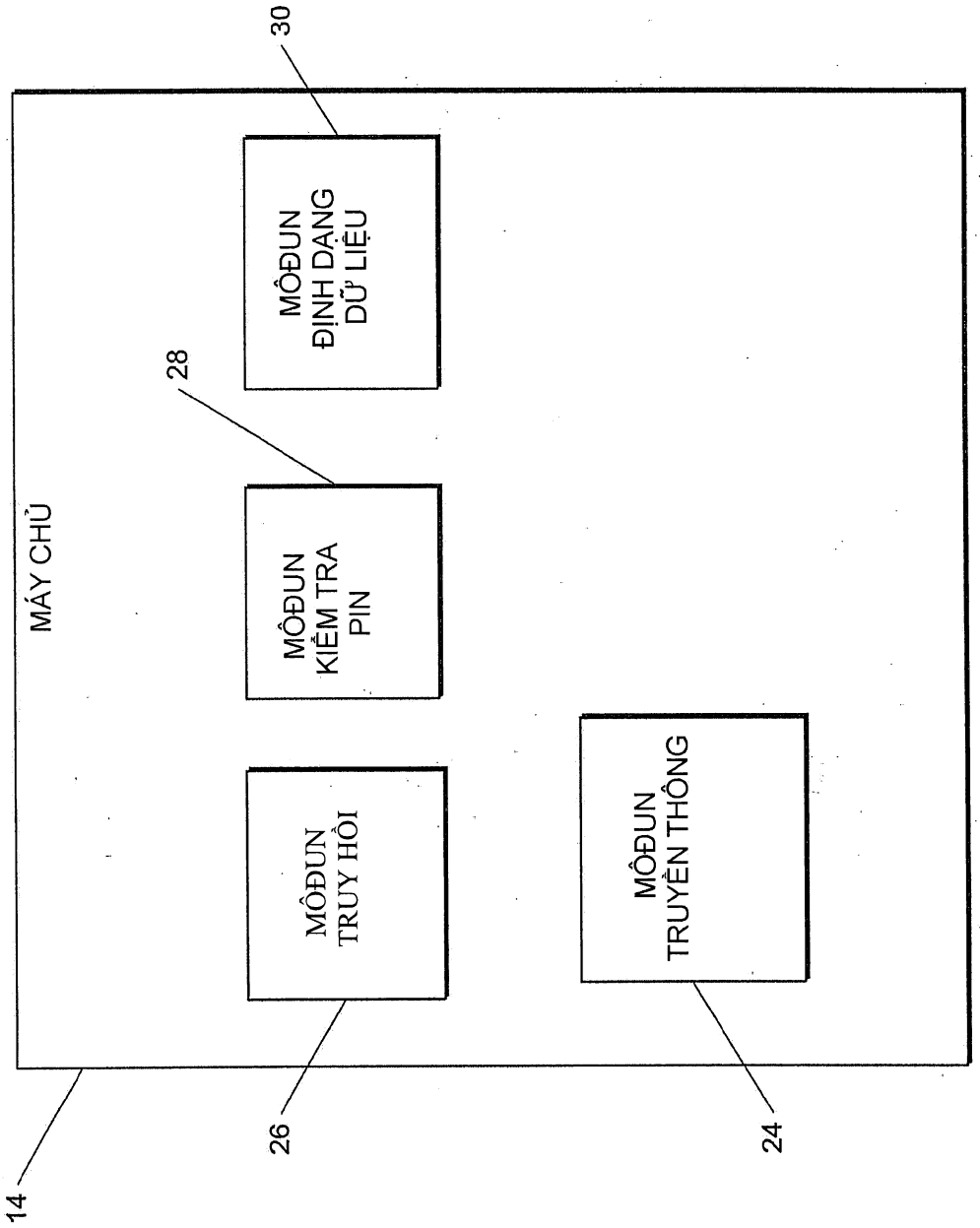

30
MÔĐUN
ĐỊNH DẠNG
DỮ LIỆU
28
MÔĐUN
KIỂM TRA
PIN
MÔĐUN
TRUY HỒI
MÔĐUN
TRUYỀN THÔNG
MÁY CHỦ
14
26
24

FIG. 2


BẮT ĐẦU
LƯU TRỮ NHIỀU MÃ NHẬN DẠNG PHƯƠNG TIỆN GIAO DỊCH TÀI CHÍNH ĐƯỢC MÃ HÓA TRONG BỘ NHỚ TRONG ĐÓ KHÔNG CÓ KHÓA GIẢI MÃ CHO CHÚNG ĐƯỢC LƯU TRỮ TRONG BỘ NHỚ VÀ TRONG ĐÓ MỖI MÃ NHẬN DẠNG PHƯƠNG TIỆN GIAO DỊCH TÀI CHÍNH ĐƯỢC MÃ HÓA ĐƯỢC KẾT HỢP VỚI THIẾT BỊ TRUYỀN THÔNG DI ĐỘNG
NHẬN YÊU CẦU TẠI MÁY CHỦ ĐỂ XỬ LÝ GIAO DỊCH, YÊU CẦU NÀY BAO GỒM THÔNG TIN NHẬN DẠNG CỦA THIẾT BỊ TRUYỀN THÔNG DI ĐỘNG
TRUYỀN MÃ NHẬN DẠNG PHƯƠNG TIỆN GIAO DỊCH TÀI CHÍNH ĐƯỢC MÃ HÓA ĐÃ ĐƯỢC TRUY HỒI TỚI THIẾT BỊ TRUYỀN THÔNG DI ĐỘNG
NHẬN DỮ LIỆU GIAO DỊCH TỪ THIẾT BỊ TRUYỀN THÔNG DI ĐỘNG VÀ SỬ DỤNG DỮ LIỆU GIAO DỊCH NHẬN ĐƯỢC ĐỂ THỰC HIỆN GIAO DỊCH TÀI CHÍNH
KẾT THÚC

**FIG. 3**

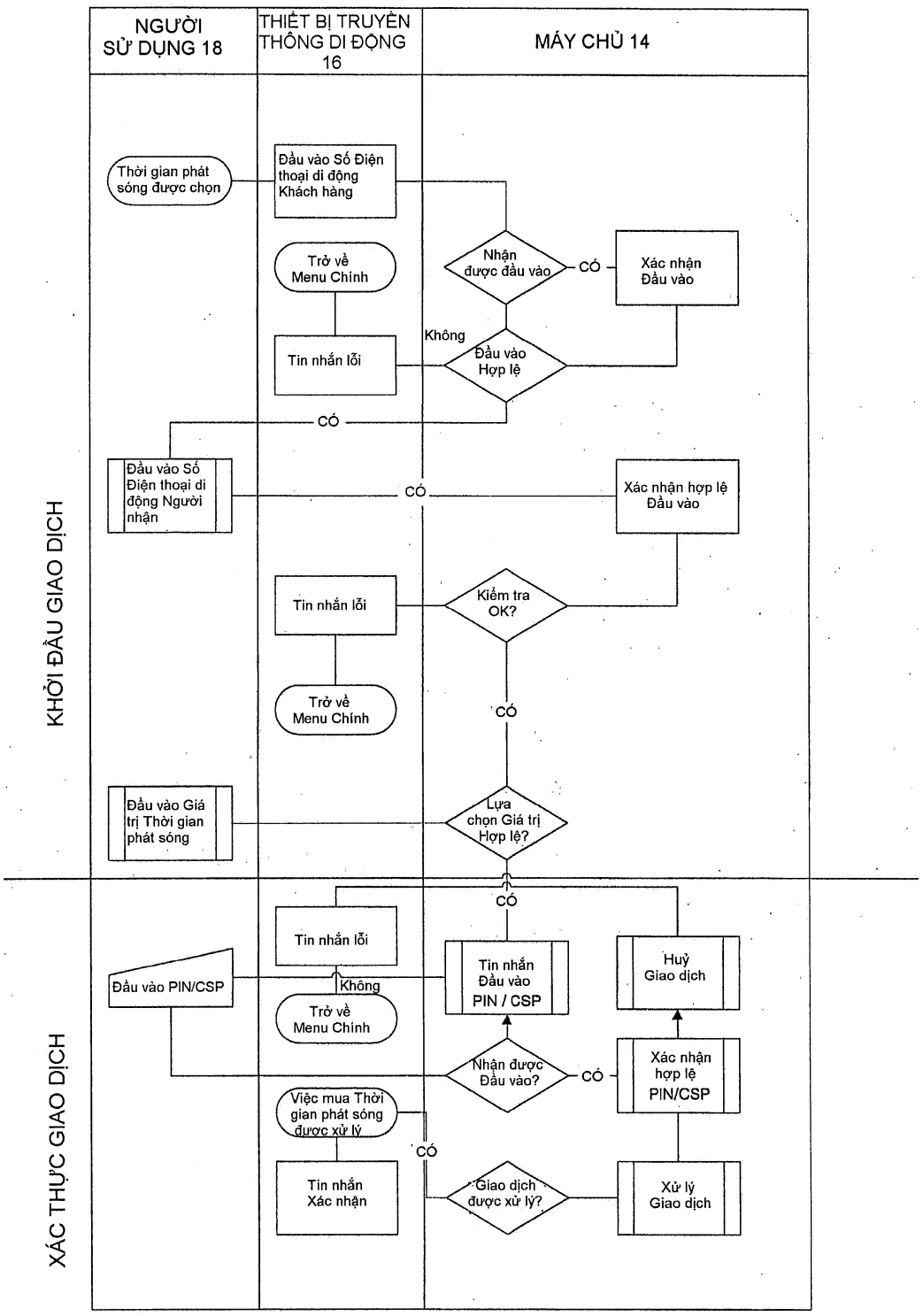

NGƯỜI SỬ DỤNG 18
THIẾT BỊ TRUYỀN THÔNG DI ĐỘNG 16
MÁY CHỦ 14
KHỞI ĐẦU GIAO DỊCH
XÁC THỰC GIAO DỊCH
Thời gian phát sóng được chọn
Đầu vào Số Điện thoại di động Khách hàng
Trở về Menu Chính
Tin nhắn lỗi
Nhận được đầu vào
CÓ
Xác nhận Đầu vào
Không
Đầu vào Hợp lệ
CÓ
Đầu vào Số Điện thoại di động Người nhận
CÓ
Xác nhận hợp lệ Đầu vào
Tin nhắn lỗi
Kiểm tra OK?
Trở về Menu Chính
CÓ
Đầu vào Giá trị Thời gian phát sóng
Lựa chọn Giá trị Hợp lệ?
CÓ
Tin nhắn lỗi
Đầu vào PIN/CSP
Không
Trở về Menu Chính
Tin nhắn Đầu vào PIN / CSP
Huỷ Giao dịch
Nhận được Đầu vào?
CÓ
Xác nhận hợp lệ PIN/CSP
Việc mua Thời gian phát sóng được xử lý
CÓ
Tin nhắn Xác nhận
Giao dịch được xử lý?
Xử lý Giao dịch

FIG. 4

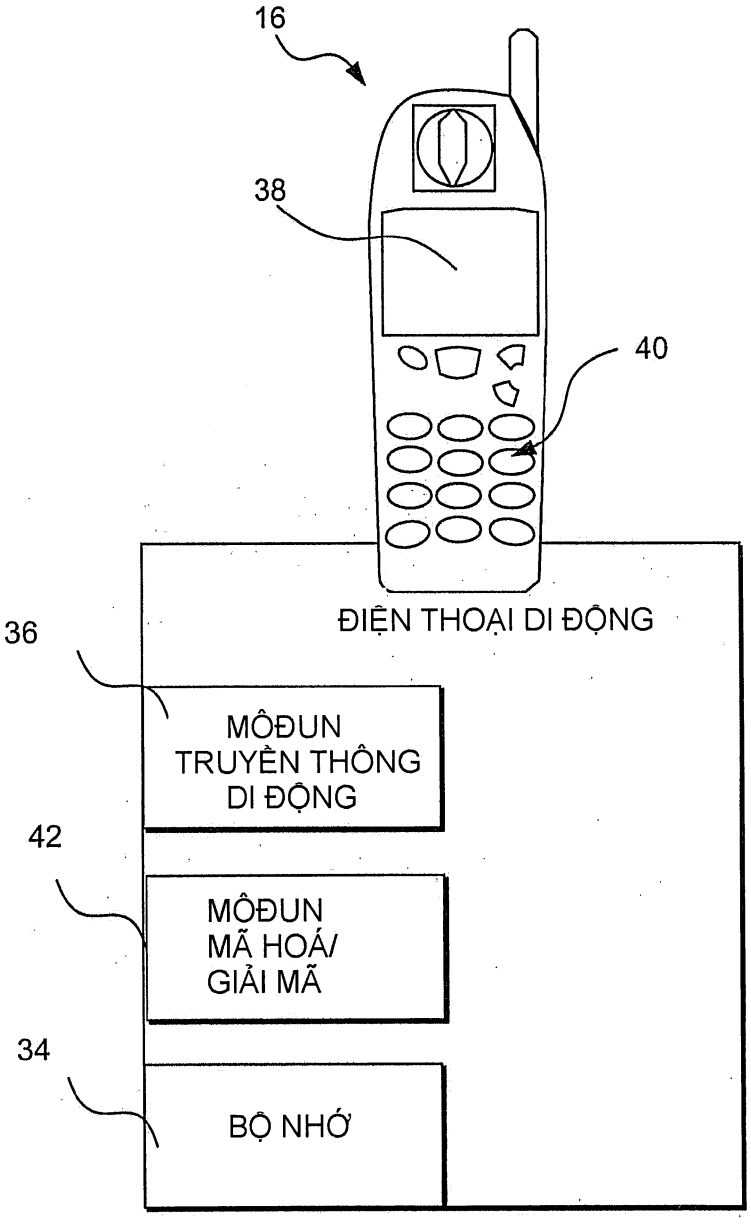

16
38
40
ĐIỆN THOẠI DI ĐỘNG
36
MÔĐUN
TRUYỀN THÔNG
DI ĐỘNG
42
MÔĐUN
MÃ HOÁ/
GIẢI MÃ
34
BỘ NHỚ

**FIG. 5**