(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) **1-0022147**

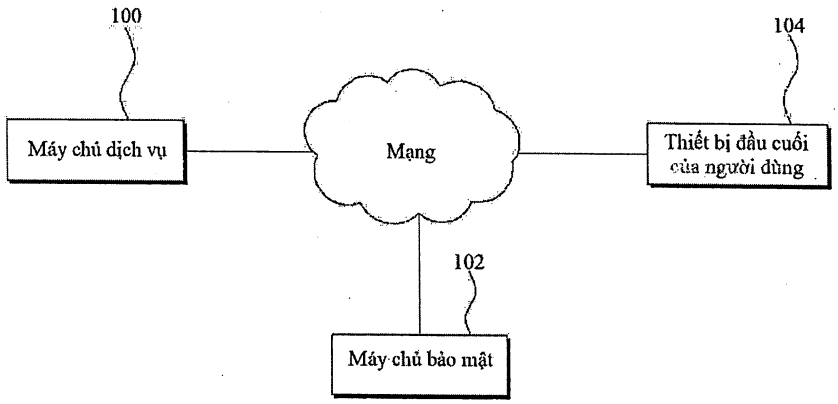
(51)[7] **H04N 21/433**, 21/2343

(13) **B**

(21) 1-2015-02841
(22) 25.06.2013
(86) PCT/KR2013/005614 25.06.2013
(87) WO2014/123283 14.08.2014
(30) 10-2013-0012900 05.02.2013 KR
(45) 25.11.2019 380
(43) 26.10.2015 331
(73) ALTICAST CORPORATION (KR)
(Seocho-dong, Park Bldg.) 6th floor, 16, Banpo-daero 27-gil, Seocho-gu, Seoul 137-952, Republic of Korea
(72) CHO, Mi-Sung (KR), SHIN, YoungMi (KR), EOM, TaeIn (KR), LEE, SuYong (KR), SEO, EunJung (KR), KIM, Eunwoo (KR)
(74) Công ty TNHH Trà và cộng sự (TRA & ASSOCIATES CO.,LTD)

(54) PHƯƠNG PHÁP KIỂM SOÁT VIỆC TẢI XUỐNG MÔĐUN BẢO MẬT CHO DỊCH VỤ QUẢNG BÁ VÀ THIẾT BỊ MÁY CHỦ BẢO MẬT

(57) Sáng chế đề cập đến phương pháp và thiết bị kiểm soát việc tải xuống môđun bảo mật cho dịch vụ quảng bá. Trong phương pháp kiểm soát việc tải xuống môđun bảo mật cho dịch vụ quảng bá trong thiết bị đầu cuối của người dùng kết nối với máy chủ dịch vụ và máy chủ bảo mật qua mạng, bộ tải được tải xuống bằng cách cho phép thiết bị đầu cuối của người dùng được kết nối với máy chủ dịch vụ. Thiết bị đầu cuối của người dùng được kết nối với máy chủ bảo mật qua bộ tải. Bộ khởi động được tải xuống từ máy chủ bảo mật. Môđun bảo mật được tải xuống từ máy chủ bảo mật bằng cách chạy bộ khởi động.



Lĩnh vực kỹ thuật được đề cập

Sáng chế đề cập đến phương pháp và thiết bị kiểm soát việc tải xuống môđun bảo mật cho dịch vụ quảng bá, và cụ thể hơn sáng là chế đề cập đến phương pháp và thiết bị có khả năng tải xuống một cách an toàn môđun bảo mật cho các dịch vụ quảng bá.

Tình trạng kỹ thuật của sáng chế

Việc chuyển đổi quảng bá kỹ thuật số được thực hiện trên toàn thế giới, và đã hoàn thành việc chuyển đổi công nghệ kỹ thuật số công nghệ và hệ thống kỹ thuật số liên quan đến sản phẩm quảng bá.

Không giống như các nội dung tương tự, các nội dung kỹ thuật số có thể được sao chép hoàn hảo và biên tập dễ dàng và phân phát theo đặc tính của phương tiện truyền thông. Do đó, việc giới hạn truy cập nội dung và bảo vệ nội dung là cần thiết.

Vì lý do này, hệ thống truy cập có điều kiện (sau đây gọi là 'CAS – conditional access system') và quản lý quyền kỹ thuật số được đề xuất (DRM – digital rights mângement) cho phép chỉ các thuê bao hợp pháp truy cập vào nội dung tương ứng.

Cùng với hệ thống quản lý thuê bao (SMS – subscriber management system), CAS cho phép chỉ các thuê bao được phép nhận và sao chép một chương trình cụ thể.

Trong CAS nói chung, đầu cuối của nhà cung cấp quảng bá trộn nội dung bằng cách dùng từ kiểm soát (CW control word). Trong trường hợp này, CW được mã hóa như một khóa xác thực, và khóa xác thực được mã hóa như một khóa phân phối.

Sau đó, CW, khóa xác thực, và khóa tương tự được chứa trong tin nhắn xác định trước (ví dụ, tin nhắn kiểm soát định tính hoặc tin nhắn quản lý định tính) được chuyển đến máy thu quảng bá.

Ở đây, máy thu quảng bá có thể là hộp đầu (một thiết bị giải mã tín hiệu truyền) thông thường.

Khi nhận dòng truyền đã trộn (nội dung đã trộn), hộp đầu giải mã khóa xác thực làm một khóa phân phối, và thu được CW với khóa xác thực đã giải mã. Hộp đầu giải

trộn dòng truyền đã trộn qua CW đã thu và đưa ra dòng truyền đã giải trộn làm tín hiệu dưới dạng nhìn thấy và nghe được.

Thông thường, môđun hỗ trợ chức năng CAS được thiết kế trong hộp đầu bằng cách nhúng. Tuy nhiên, gần đây người ta đề xuất hệ thống truy cập có điều kiện tải xuống được (DCAS – downloadable CAS) để cung cấp cho khách hàng CAS từ máy chủ theo cách tải xuống.

Mặc dù áp dụng DCAS, môđun liên quan đến chứng nhận chẳng hạn trong phạm vi bảo mật nên được thiết kế trong DCAS trong quy trình sản xuất hộp đầu.

Gần đây, các dịch vụ quảng bá đã được dùng không chỉ qua các hộp đầu lắp trong nhà mà còn trong các thiết bị di động như thiết bị đầu cuối truyền thông di động (điện thoại thông minh) và máy tính bảng.

Trong môi trường N-màn hình, khó để cung cấp trước môđun bảo mật. Do vậy, cần cung cấp môđun bảo mật ở dạng tải xuống.

Tuy nhiên, khi môđun bảo mật cho dịch vụ quảng bá, đặc biệt dịch vụ quảng bá đã thanh toán được cung cấp ở dạng tải xuống mà không có bất kỳ giới hạn, môđun bảo mật có thể bị sao chép bất hợp pháp.

Đặc biệt, trong những năm gần đây, thiết bị đầu cuối dựa vào nguồn mở thường được cung cấp. Trong trường hợp này, nhiều li-xăng khác nhau có trong mã nguồn mở, nhưng khái niệm cơ bản của mã nguồn mở là công bố tự do và phân phối loại bản đồ thiết kế được tham chiếu khi tạo ra phần mềm.

Tuy nhiên, khi môđun bảo mật cho dịch vụ quảng bá được cung cấp dựa vào mã nguồn mở, môđun bảo mật có thể được thực hiện và phân phối bất hợp pháp với việc tham chiếu đến bản đồ thiết kế của nó. Vì vậy, cần ngăn chặn việc mở môđun bảo mật và phần mềm hỗ trợ.

Bản chất kỹ thuật của sáng chế

Phương án ưu tiên của sáng chế đề cập đến phương pháp và thiết bị kiểm soát việc tải xuống môđun bảo mật cho dịch vụ quảng bá, phương pháp và thiết bị này cho phép môđun bảo mật được tải xuống an toàn trong thiết bị đầu cuối trong đó môđun bảo mật không được thiết kế theo cách nhúng.

Theo một khía cạnh của sáng chế, sáng chế đề xuất phương pháp kiểm soát việc

tải xuống môđun bảo mật cho dịch vụ quảng bá trong thiết bị đầu cuối của người dùng kết nối với máy chủ dịch vụ và máy chủ bảo mật qua mạng, phương pháp bao gồm các bước: tải xuống một bộ tải bằng cách cho phép thiết bị đầu cuối của người dùng kết nối với máy chủ dịch vụ; kết nối thiết bị đầu cuối của người dùng với máy chủ dịch vụ qua bộ tải; tải xuống bộ khởi động từ máy chủ bảo mật; và tải xuống một môđun bảo mật từ máy chủ bảo mật bằng cách chạy bộ khởi động.

Môđun bảo mật có thể bao gồm ít nhất một khách hàng CAS, khách hàng DRM, chính sách bảo mật và một thẻ chứng nhận.

Máy chủ dịch vụ có thể bao gồm ít nhất một máy chủ web và máy chủ kho ứng dụng di động.

Bộ tải có thể bao gồm thông tin địa chỉ của máy chủ bảo mật, và liên kết với máy chủ bảo mật bằng cách dùng thông tin địa chỉ.

Bộ khởi động có thể xác định liệu tồn tại mỗi khách hàng CAS, khách hàng DRM, chính sách bảo mật, và thẻ chứng nhận và liệu mỗi khách hàng CAS, khách hàng DRM, chính sách bảo mật, và thẻ chứng nhận đã được cập nhật.

Bộ khởi động có thể xác định liệu bộ khởi động mới được tải xuống có tham chiếu đến chính sách bảo mật.

Bộ khởi động và môđun bảo mật có thể thực hiện việc giải mã nội dung đã mã hóa.

Theo một khía cạnh khác của sáng chế, sáng chế đề xuất phương tiện ghi đọc được bằng máy tính ghi chương trình để thực hiện phương pháp.

Theo khía cạnh khác của sáng chế, sáng chế đề xuất thiết bị máy chủ bảo mật kết nối với thiết bị đầu cuối của người dùng qua mạng, thiết bị máy chủ bảo mật bao gồm: bộ phận giao tiếp được cấu tạo để nhận yêu cầu của bộ khởi động từ thiết bị đầu cuối của người dùng kết nối với máy chủ dịch vụ để điều khiển bộ tải; bộ phận lưu trữ được cấu tạo để lưu bộ khởi động và môđun bảo mật được yêu cầu bởi thiết bị đầu cuối của người dùng để bộ khởi động được tải xuống; và thiết bị kiểm soát được cấu tạo để kiểm soát bộ khởi động và môđun bảo mật được truyền qua bộ phận giao tiếp.

Nên hiểu rằng các phương án ưu tiên khác nhau của sáng chế, bao gồm các phương án ưu tiên được mô tả dưới các khía cạnh khác nhau của sáng chế, có nghĩa là

được áp dụng chung cho tất cả các khía cạnh của sáng chế. Bất kỳ phương án ưu tiên nào có thể được kết hợp với bất kỳ phương án ưu tiên khác trừ khi không thích hợp. Tất cả các ví dụ là để minh họa và không nhằm giới hạn.

Ưu điểm của sáng chế

Theo sáng chế, bộ khởi động có thể được tải xuống qua bộ tải được cung cấp từ máy chủ dịch vụ, sao cho có thể ngăn bộ khởi động chứa môđun bảo mật mở.

Mô tả vắn tắt các hình vẽ

Fig.1 là lược đồ minh họa hệ thống cung cấp môđun bảo mật cho dịch vụ quảng bá theo một phương án ưu tiên của sáng chế.

Fig.2 là lược đồ minh họa cấu hình chi tiết của máy chủ bảo mật theo một phương án ưu tiên của sáng chế.

Fig.3 là lược đồ minh họa cấu hình chi tiết của thiết bị đầu cuối của người dùng theo một phương án ưu tiên của sáng chế.

Fig.4 là sơ đồ trình tự minh họa quy trình tải xuống môđun bảo mật theo một phương án ưu tiên của sáng chế.

Fig.5 là lưu đồ minh họa quy trình kiểm soát việc tải xuống môđun bảo mật trong thiết bị đầu cuối của người dùng theo một phương án ưu tiên của sáng chế.

Mô tả chi tiết sáng chế

Các phương án ưu tiên của sáng chế sẽ được mô tả chi tiết hơn dưới đây cùng với việc tham chiếu đến các hình vẽ kèm theo. Tuy nhiên, sáng chế có thể được thể hiện ở các hình thức khác nhau và không nên hiểu là giới hạn ở các phương án ưu tiên nêu ra ở đây. Thay vào đó, các phương án ưu tiên này được đề xuất sao cho việc bộc lộ này sẽ toàn diện và đầy đủ và sẽ chuyển tải đầy đủ phạm vi của sáng chế cho những người có hiểu biết trung bình về lĩnh vực kỹ thuật tương ứng. Thông qua việc bộc lộ, các số tham chiếu giống nhau đề cập đến các phần giống nhau ở tất cả các hình vẽ và các phương án ưu tiên khác nhau của sáng chế.

Fig.1 là lược đồ minh họa hệ thống cung cấp môđun bảo mật cho dịch vụ quảng bá theo một phương án ưu tiên của sáng chế.

Như minh họa trên Fig.1, hệ thống theo phương án ưu tiên của sáng chế bao

gồm máy chủ dịch vụ 100 để cung cấp môđun bảo mật cho dịch vụ quảng bá, máy chủ bảo mật 102, và thiết bị đầu cuối của người dùng 104 kết nối với các máy chủ 100 và 102 qua mạng.

Ở đây, mạng có thể bao gồm internet có dây/không dây, các mạng quảng bá, các mạng vệ tinh, và mạng tương tự.

Thiết bị đầu cuối của người dùng 104 theo phương án ưu tiên của sáng chế có thể bao gồm hộp đầu trong đó môđun bảo mật cho các dịch quảng bá không được thiết kế bằng cách nhúng, hoặc thiết bị đầu cuối di động như thiết bị đầu cuối truyền thông di động và máy tính bảng.

Ngoài ra, thiết bị đầu cuối của người dùng 104 có thể bao gồm tất cả các thiết bị đầu cuối có thể được kết nối qua mạng, và tải xuống và chạy môđun bảo mật.

Môđun bảo mật theo phương án ưu tiên của sáng chế là tập tin ứng dụng và cấu hình cho phép chỉ những người dùng hợp pháp dùng nội dung đã mã hóa như chương trình trực tiếp đã thanh toán hoặc chương trình theo yêu cầu. Môđun bảo mật có thể bao gồm thẻ chứng nhận, chính sách bảo mật, khách hàng CAS, khách hàng DRM, khách hàng bảo mật, và tương tự. Việc tải xuống và quản lý môđun bảo mật được thực hiện bởi bộ khởi động.

Theo phương án ưu tiên của sáng chế, bộ khởi động và môđun bảo mật có thể được cung cấp cho thiết bị đầu cuối của người dùng 104 ở trạng thái không mở.

Khi có kết nối của thiết bị đầu cuối của người dùng 104, máy chủ dịch vụ 100 theo phương án ưu tiên của sáng chế cung cấp bộ tải cho thiết bị đầu cuối của người dùng 104.

Ở đây, máy chủ dịch vụ 100 có thể là máy chủ web thông thường hoặc kho ứng dụng di động.

Thiết bị đầu cuối của người dùng 104 theo phương án ưu tiên của sáng chế có thể là thiết bị đầu cuối dựa vào bộ trình duyệt. Trong môi trường của bộ trình duyệt, thiết bị đầu cuối của người dùng 104 có thể được kết nối với máy chủ web qua bộ trình duyệt, và máy chủ web truyền bộ tải đến thiết bị đầu cuối của người dùng 104.

Bộ tải có thể là một ứng dụng chạy ở dạng thêm vào. Máy chủ web có thể cho phép bộ tải có trong trang web và truyền trang web đến thiết bị đầu cuối của người

dùng 104.

Khi không cài đặt bất kỳ bộ tải nào trong thiết bị đầu cuối của người dùng 104, thiết bị đầu cuối của người dùng 104 cho phép bộ tải cung cấp từ máy chủ web được cài đặt trong đó và chạy bộ tải.

Bộ tải theo phương án ưu tiên của sáng chế có thể được cung cấp thậm chí trong môi trường ứng dụng di động. Thiết bị đầu cuối của người dùng 104 có thể được kết nối với máy chủ kho ứng dụng di động và có thể tải xuống bộ tải.

Tốt hơn, khi người dùng tải xuống một ứng dụng di động để dùng cho dịch vụ quảng bá trong môi trường ứng dụng di động, bộ tải có thể có trong ứng dụng di động tương ứng được tải xuống.

Bộ tải theo phương án ưu tiên của sáng chế bao gồm thông tin địa chỉ của máy chủ bảo mật 102, và giao tiếp với máy chủ bảo mật 102 bằng cách dùng thông tin địa chỉ.

Khi thiết bị đầu cuối của người dùng 104 được kết nối với máy chủ bảo mật 102 qua bộ tải, máy chủ bảo mật 102 truyền bộ khởi động đến thiết bị đầu cuối của người dùng 104.

Bộ khởi động theo phương án ưu tiên của sáng chế kiểm soát việc tải xuống một thẻ chứng nhận, khách hàng bảo mật, và chính sách bảo mật, và xác định liệu có môđun bảo mật và liệu môđun bảo mật được cập nhật có liên quan với máy chủ bảo mật 102.

Theo đó, trong phương án ưu tiên của sáng chế, bộ khởi động thực hiện chức năng bảo mật nội dung không được cung cấp từ máy chủ dịch vụ 100 nhưng được cung cấp qua máy chủ bảo mật 102 kết nối được bằng bộ tải, sao cho bộ khởi động và môđun bảo mật có thể được cung cấp an toàn ở trạng thái không mở.

Fig.2 là lưu đồ minh họa cấu hình chi tiết của máy chủ bảo mật theo phương án ưu tiên của sáng chế.

Như minh họa trên Fig.2, máy chủ bảo mật 102 bao gồm bộ phận giao tiếp 200, thiết bị kiểm soát 202, và bộ phận lưu 204.

Bộ phận giao tiếp 200 liên lạc với thiết bị đầu cuối của người dùng 104 trong bộ tải được chạy.

Khi nhận yêu cầu của bộ khởi động từ thiết bị đầu cuối của người dùng 104 qua bộ phận giao tiếp 200, thiết bị kiểm soát 202 kiểm soát bộ khởi động được lưu trong bộ phận lưu 204 được truyền đến thiết bị đầu cuối của người dùng 104.

Trong trường hợp này, thiết bị đầu cuối của người dùng 104 chạy bộ khởi động được nhận từ bộ phận giao tiếp 200 của máy chủ bảo mật 102, và yêu cầu máy chủ bảo mật 102 của môđun bảo mật bao gồm thẻ chứng nhận, khách hàng bảo mật, và chính sách bảo mật qua bộ khởi động.

Khi nhận yêu cầu, bộ phận giao tiếp 200 truyền môđun bảo mật lưu trong bộ phận lưu 204 đến thiết bị đầu cuối của người dùng 104.

Khi tải xuống bộ khởi động và môđun bảo mật xong, thiết bị đầu cuối của người dùng 104 có thể được kết nối với máy chủ nội dung (không được minh họa) để nhận nội dung đã mã hóa, và giải mã nội dung đã mã hóa.

Fig.3 là lưu đồ minh họa cấu hình chi tiết của thiết bị đầu cuối của người dùng theo phương án ưu tiên của sáng chế.

Như minh họa trên Fig.3, thiết bị đầu cuối của người dùng 104 theo phương án ưu tiên của sáng chế có thể bao gồm bộ tải 300, bộ khởi động 302, lõi 304, khách hàng CAS 306, khách hàng DRM 308, bộ phận lưu thẻ chứng nhận 310, và bộ phận lưu chính sách bảo mật 312.

Bộ tải 300 được cung cấp từ máy chủ dịch vụ 100 như máy chủ web hoặc máy chủ kho ứng dụng di động được cài đặt trong thiết bị đầu cuối của người dùng 104. Bộ tải 300 liên lạc với máy chủ bảo mật 102 qua thông tin địa chỉ của máy chủ bảo mật.

Bộ tải 300 yêu cầu máy chủ bảo mật 102 của bộ khởi động và theo đó bộ khởi động có thể tải xuống để được cài đặt và chạy trong thiết bị đầu cuối của người dùng 104.

Bộ khởi động 302 theo phương án ưu tiên của sáng chế quản lý thẻ chứng nhận, chính sách bảo mật và khách hàng bảo mật.

Cụ thể hơn, bộ khởi động 302 theo phương án ưu tiên của sáng chế xác định liệu có thẻ chứng nhận hay không. Khi không có bất kỳ thẻ chứng nhận nào, bộ khởi động 302 yêu cầu máy chủ bảo mật 102 về thẻ chứng nhận.

Bộ khởi động 302 giám sát giai đoạn khả dụng của thẻ chứng nhận. Khi giai

đoạn khả dụng hết hạn, bộ khởi động 302 yêu cầu máy chủ bảo mật 102 về thẻ chứng nhận mới.

Thẻ chứng nhận được cung cấp từ máy chủ bảo mật 102 được lưu trong bộ phận lưu thẻ chứng nhận 310.

Bộ khởi động 302 xác định liệu có chính sách bảo mật hay không. Khi không có bất kỳ chính sách bảo mật hoặc khi phiên bản của chính sách bảo mật được cập nhật, bộ khởi động 302 yêu cầu máy chủ bảo mật 102 về chính sách bảo mật. Chính sách bảo mật được lưu trong bộ phận lưu chính sách bảo mật 312.

Ở đây, chính sách bảo mật bao gồm thông tin về giai đoạn khả dụng của bộ khởi động, các giai đoạn khả dụng của khách hàng CAS và khách hàng DRM, và giai đoạn khả dụng của chính sách bảo mật, và có thể được cung cấp làm tập tin cấu hình.

Khi cập nhật bộ khởi động 302 được yêu cầu bởi chính sách bảo mật, bộ khởi động 302 có thể yêu cầu máy chủ bảo mật 102 về bộ khởi động mới.

Bộ khởi động 302 theo phương án ưu tiên của sáng chế yêu cầu máy chủ bảo mật 102 của khách hàng CAS 306 được yêu cầu để thu được từ kiểm soát khi sử dụng nội dung và khách hàng DRM 308 để ngăn các bản sao bất hợp pháp.

Lõi 304 thực hiện chức năng giải mã nội dung đã mã hóa kết hợp với khách hàng CAS 306 và khách hàng DRM 308.

Ví dụ, thiết bị đầu cuối của người dùng 104 nhận, từ máy chủ nội dung, tin nhắn quản lý quyền (EMM) và tin nhắn kiểm soát quyền (ECM) cùng với nội dung đã mã hóa (nội dung đã trộn).

Khách hàng CAS 306 tách thông tin (ví dụ từ kiểm soát) để giải trộn nội dung đã trộn bằng cách sử dụng thông tin có trong EMM và ECM. Lõi 304 giải trộn nội dung đã mã hóa bằng cách sử dụng từ kiểm soát đã tách, và truyền nội đung đã giải trộn vào bộ phận hiển thị (không được minh họa).

Fig.4 là sơ đồ trình tự minh họa quy trình tải xuống môđun bảo mật theo phương án ưu tiên của sáng chế.

Tham chiếu đến Fig.4, thiết bị đầu cuối của người dùng 104 chạy bộ tải được tải xuống từ máy chủ dịch vụ 100 (bước S400).

Bộ tải theo phương án ưu tiên của sáng chế bao gồm thông tin địa chỉ của máy chủ bảo mật 102. Thiết bị đầu cuối của người dùng 104 được kết nối với máy chủ bảo mật 102 qua bộ tải, và yêu cầu máy chủ bảo mật 102 về bộ khởi động (bước 402).

Máy chủ bảo mật 102 truyền bộ khởi động đến thiết bị đầu cuối của người dùng 104 (bước S404).

Thiết bị đầu cuối của người dùng 104 chạy bộ khởi động (bước S406), và yêu cầu máy chủ bảo mật 102 về môđun bảo mật bao gồm thẻ chứng nhận, chính sách bảo mật, và khách hàng bảo mật qua bộ khởi động (bước S408).

Máy chủ bảo mật 102 truyền môđun bảo mật đã yêu cầu đến thiết bị đầu cuối của người dùng (bước S410).

Fig.5 là lưu đồ minh họa quy trình kiểm soát việc tải xuống môđun bảo mật trong thiết bị đầu cuối của người dùng theo phương án ưu tiên của sáng chế.

Tham chiếu đến Fig.5, thiết bị đầu cuối của người dùng 104 xác định liệu có bộ khởi động trong chương trình mồi hay không (bước S500). Khi không có bất kỳ bộ khởi động nào, thiết bị đầu cuối của người dùng 104 được kết nối với máy chủ bảo mật 102 để tải xuống bộ khởi động (bước S502).

Trong khi đó, khi có bộ khởi động, bộ khởi động được điều khiển (bước S504). Bộ khởi động xác định liệu có thẻ chứng nhận hay không (bước S506). Khi không có bất kỳ thẻ chứng nhận nào, thiết bị đầu cuối của người dùng 104 tải xuống một thẻ chứng nhận từ máy chủ bảo mật 102 (bước S508).

Khi có thẻ chứng nhận, bộ khởi động 302 xác định liệu có chính sách bảo mật (bước S510). Khi có chính sách bảo mật, bộ khởi động 302 kiểm tra phiên bản chính sách bảo mật (bước S512).

Khi không có bất kỳ chính sách bảo mật nào hoặc khi phiên bản của chính sách bảo mật không tương ứng với phiên bản hiện thời, bộ khởi động 302 tải xuống chính sách bảo mật từ máy chủ bảo mật 102 (bước S514).

Khi phiên bản chính sách bảo mật tương ứng với phiên bản hiện thời, bộ khởi động 302 xác định liệu có khách hàng bảo mật hay không (bước S516).

Như mô tả ở trên, khách hàng bảo mật có thể bao gồm khách hàng CAS 306 để giải trộn nội dung đã trộn và khách hàng DRM 308.

Khi không có bất kỳ khách hàng bảo mật nào, bộ khởi động 302 tải xuống một khách hàng bảo mật từ máy chủ bảo mật 102 (bước S518).

Trong khi đó, mặc dù có khách hàng bảo mật, bộ khởi động 302 kiểm tra phiên bản khách hàng bảo mật (bước S520). Khi phiên bản khách hàng bảo mật không tương ứng với phiên bản hiện thời, thực hiện bước S518.

Khi phiên bản khách hàng bảo mật tương ứng với phiên bản hiện thời, khách hàng bảo mật được điều khiển (bước S522)

Các phương án ưu tiên của sáng chế có thể được thực hiện ở dạng lệnh chương trình có khả năng được thực hiện qua các phương tiện máy tính khác nhau được ghi lại trong phương tiện ghi đọc được bằng máy tính. Phương tiện ghi đọc được bằng máy tính có thể bao gồm lệnh chương trình, tập tin dữ liệu, cấu trúc dữ liệu và tương tự riêng biệt hoặc kết hợp. Lệnh chương trình ghi trong phương tiện ghi có thể là lệnh được thiết kết hoặc cấu hình đặc biệt theo sáng chế, hoặc người có hiểu biết trung bình về lĩnh vực phần mềm máy tính biết để dùng được. Các ví dụ về phương tiện ghi đọc được bằng máy tính bao gồm phương tiện từ tính như đĩa cứng, đĩa mềm, và băng từ, đĩa quang như CD-ROM và DVD, phương tiện quang-từ như đĩa mềm quang học, và thiết bị phần cứng như ROM, RAM và bộ nhớ cực nhanh, được cấu tạo để lưu và thực hiện các lệnh chương trình. Các ví dụ về các lệnh chương trình bao gồm mã ngôn ngữ máy thực hiện bởi trình biên dịch và mã ngôn ngữ trình cao được thực hiện bằng cách sử dụng bộ diễn dịch của máy tính. Thiết bị phần cứng có thể được cấu tạo ít nhất như một môđun phần mềm để tiến hành thao tác các phương án ưu tiên của sáng chế, và ngược lại.

Trong khi sáng chế đã được mô tả đối với các phương án ưu tiên cụ thể, sáng chế sẽ rõ ràng với người có hiểu biết trung bình về lĩnh vực kỹ thuật tương ứng rằng các thay đổi và sửa đổi khác nhau có thể được thực hiện mà không rời khỏi phạm vi của sáng chế như được xác định trong các điểm yêu cầu bảo hộ dưới đây.

Yêu cầu bảo hộ

1. Phương pháp kiểm soát việc tải xuống môđun bảo mật cho dịch vụ quảng bá trong thiết bị đầu cuối của người dùng kết nối với máy chủ dịch vụ và máy chủ bảo mật qua mạng, phương pháp nay bao gồm các bước:

tải xuống bộ tải bằng cách cho phép thiết bị đầu cuối của người dùng kết nối với máy chủ dịch vụ;

kết nối thiết bị đầu cuối của người dùng với máy chủ bảo mật qua bộ tải;

tải xuống bộ khởi động từ máy chủ bảo mật; và

tải xuống môđun bảo mật từ máy chủ bảo mật bằng cách chạy bộ khởi động.

2. Phương pháp theo điểm 1, trong đó môđun bảo mật bao gồm ít nhất một khách hàng CAS, khách hàng DRM, chính sách bảo mật, và thẻ chứng nhận.

3. Phương pháp theo điểm 1, trong đó máy chủ dịch vụ bao gồm ít nhất một máy chủ web và máy chủ kho ứng dụng di động.

4. Phương pháp theo điểm 1, trong đó bộ tải bao gồm thông tin địa chỉ của máy chủ bảo mật, và liên lạc với máy chủ bảo mật bằng cách sử dụng thông tin địa chỉ.

5. Phương pháp theo điểm 1, trong đó bộ khởi động xác định liệu có khách hàng CAS, khách hàng DRM, chính sách bảo mật, và thẻ chứng nhận hay không và liệu khách hàng CAS, khách hàng DRM, chính sách bảo mật, và thẻ chứng nhận đã được cập nhật.

6. Phương pháp theo điểm 5, trong đó bộ khởi động xác định liệu bộ khởi động mới được tải xuống với sự tham chiếu đến chính sách bảo mật.

7. Phương pháp theo điểm 1, trong đó bộ khởi động và môđun bảo mật thực hiện giải mã nội dung đã mã hóa.

8. Phương tiện ghi đọc được bằng máy tính ghi chương trình để thực hiện phương pháp theo theo điểm 1.

9. Thiết bị máy chủ bảo mật kết nối với thiết bị đầu cuối của người dùng qua mạng, thiết bị máy chủ bảo mật này bao gồm:

bộ phận giao tiếp được cấu tạo để nhận yêu cầu về bộ khởi động từ thiết bị đầu cuối của người dùng được kết nối với máy chủ dịch vụ để điều khiển bộ tải;

bộ phận lưu được cấu tạo để lưu bộ khởi động sẽ được tải xuống thiết bị đầu cuối của người dùng và môđun bảo mật được yêu cầu bởi thiết bị đầu cuối của người dùng; và

bộ phận kiểm soát được cấu tạo để kiểm soát bộ khởi động và môđun bảo mật sẽ được truyền qua bộ phận giao tiếp.

10. Thiết bị máy chủ bảo mật theo điểm 9, trong đó môđun bảo mật bao gồm ít nhất một khách hàng CAS, khách hàng DRM, chính sách bảo mật và thẻ chứng nhận.

Fig. 1

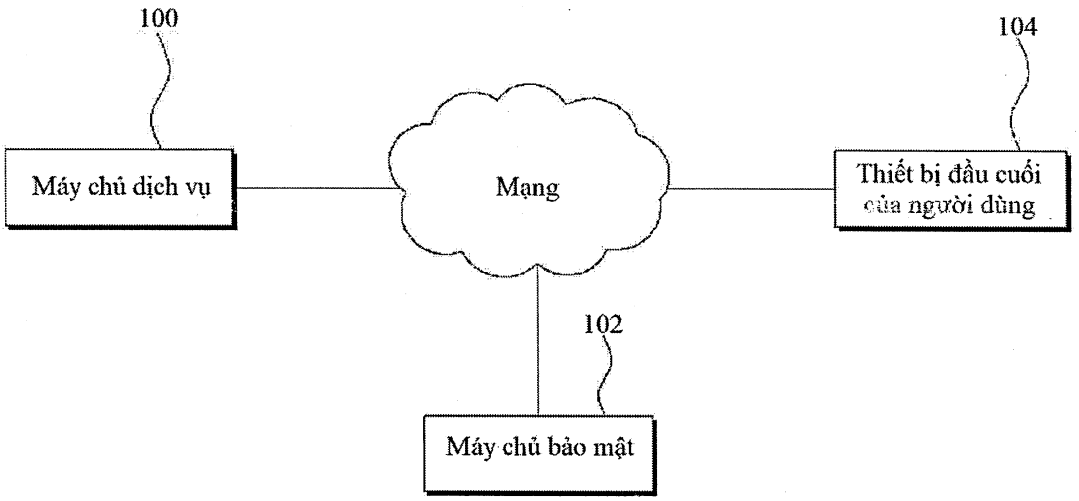

100
104
Máy chủ dịch vụ
Mạng
Thiết bị đầu cuối của người dùng
102
Máy chủ bảo mật

Fig. 2

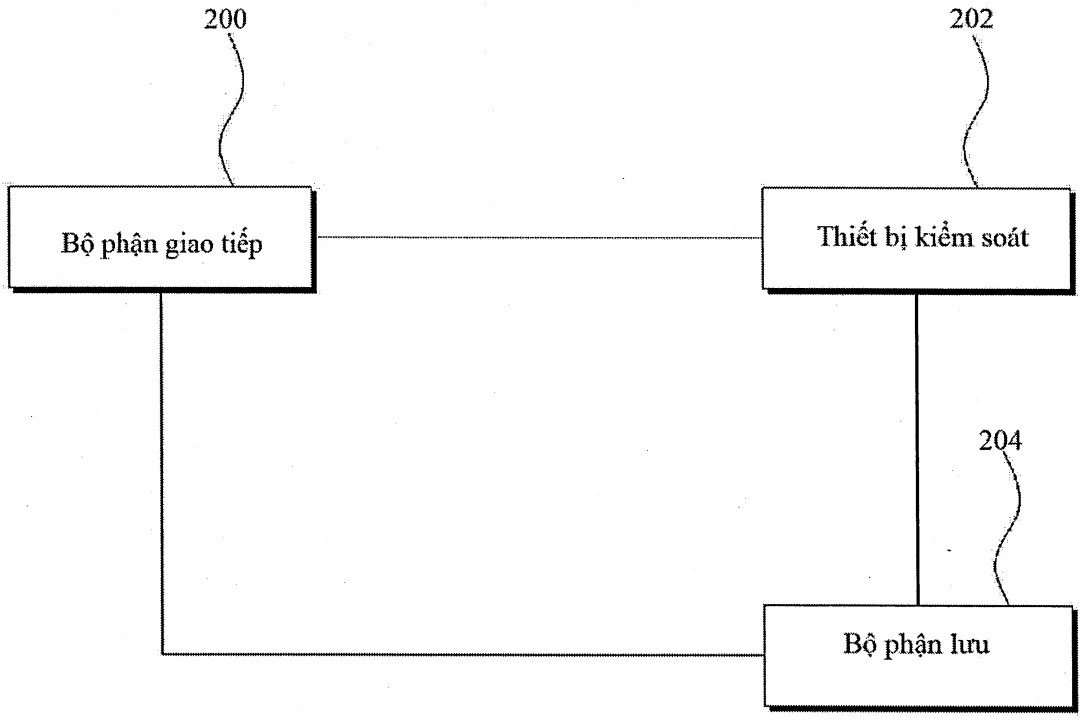

200
202
Bộ phận giao tiếp
Thiết bị kiểm soát
204
Bộ phận lưu

Fig. 3

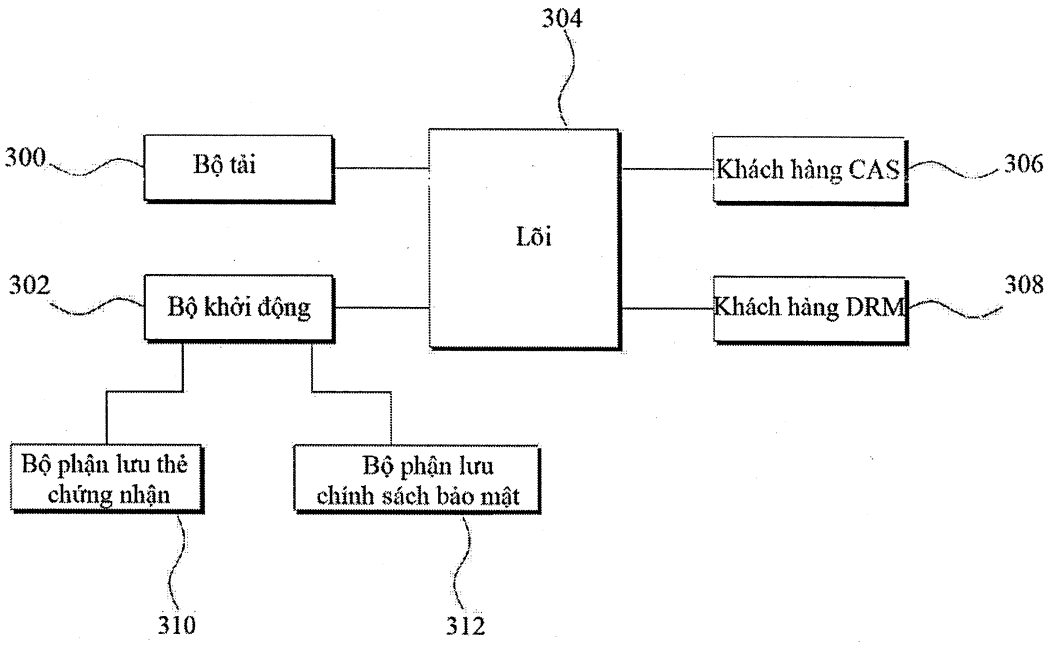

304
300
Bộ tải
Lõi
Khách hàng CAS
306
302
Bộ khởi động
Khách hàng DRM
308
Bộ phận lưu thẻ chứng nhận
Bộ phận lưu chính sách bảo mật
310
312

Fig. 4

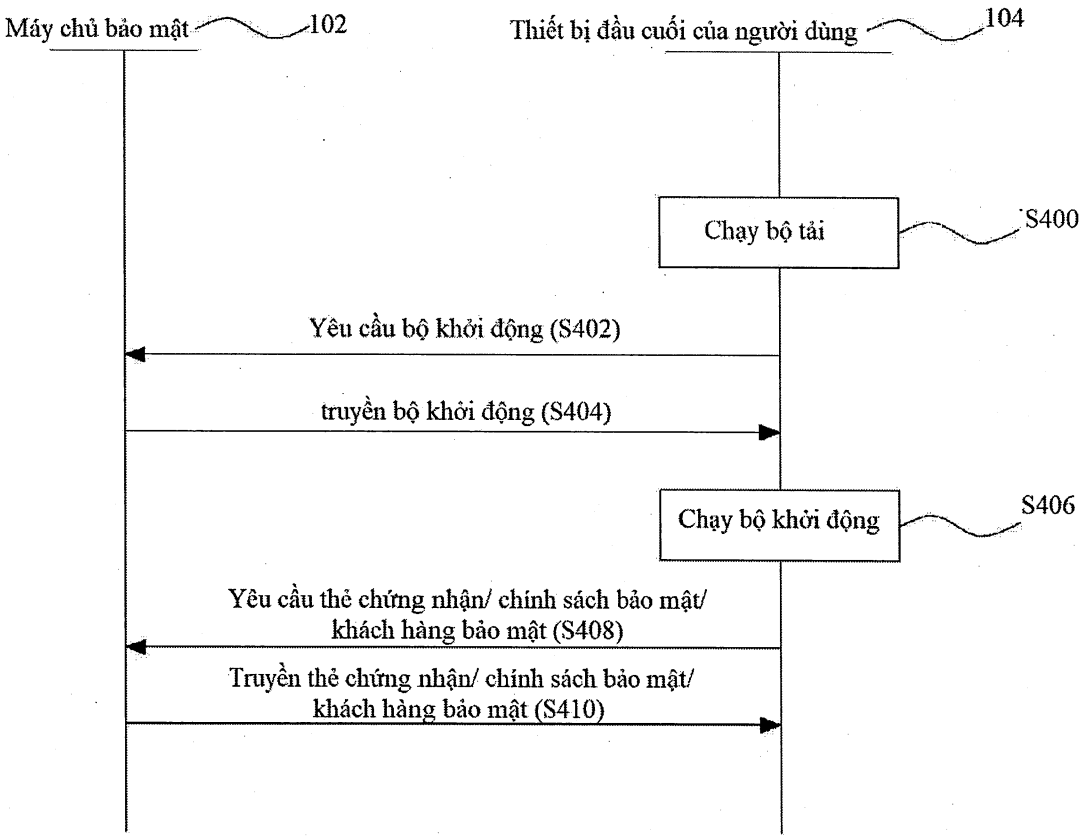
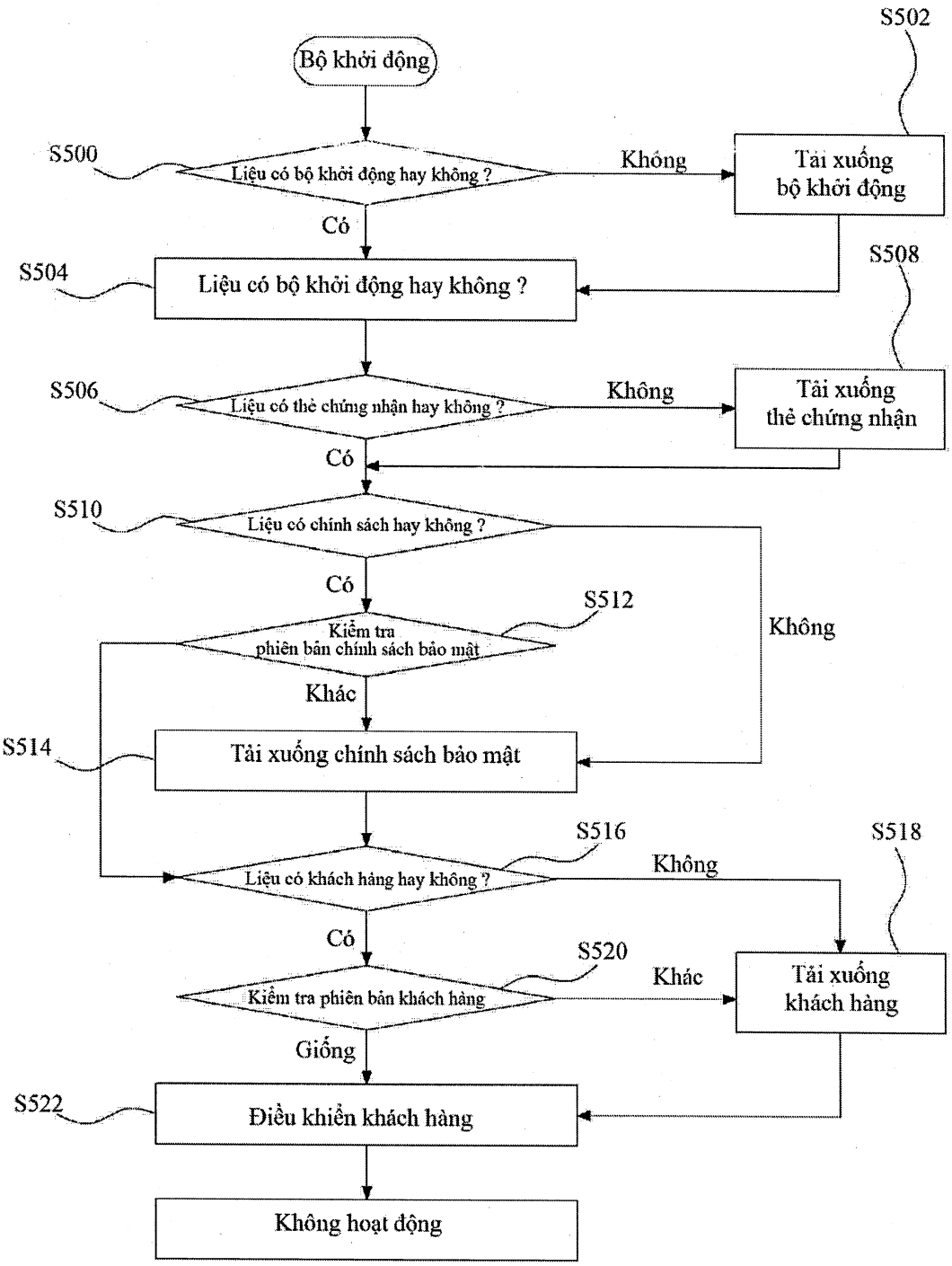

Máy chủ bảo mật
102
Thiết bị đầu cuối của người dùng
104
Chạy bộ tải
S400
Yêu cầu bộ khởi động (S402)
truyền bộ khởi động (S404)
Chạy bộ khởi động
S406
Yêu cầu thẻ chứng nhận/ chính sách bảo mật/ khách hàng bảo mật (S408)
Truyền thẻ chứng nhận/ chính sách bảo mật/ khách hàng bảo mật (S410)

Fig. 5


Bộ khởi động
S500
Liệu có bộ khởi động hay không ?
Không
Tải xuống bộ khởi động
S502
Có
S504
Liệu có bộ khởi động hay không ?
S508
S506
Liệu có thẻ chứng nhận hay không ?
Không
Tải xuống thẻ chứng nhận
Có
S510
Liệu có chính sách hay không ?
Có
Không
S512
Kiểm tra phiên bản chính sách bảo mật
Khác
S514
Tải xuống chính sách bảo mật
S516
S518
Liệu có khách hàng hay không ?
Không
Có
S520
Kiểm tra phiên bản khách hàng
Khác
Tải xuống khách hàng
Giống
S522
Điều khiển khách hàng
Không hoạt động