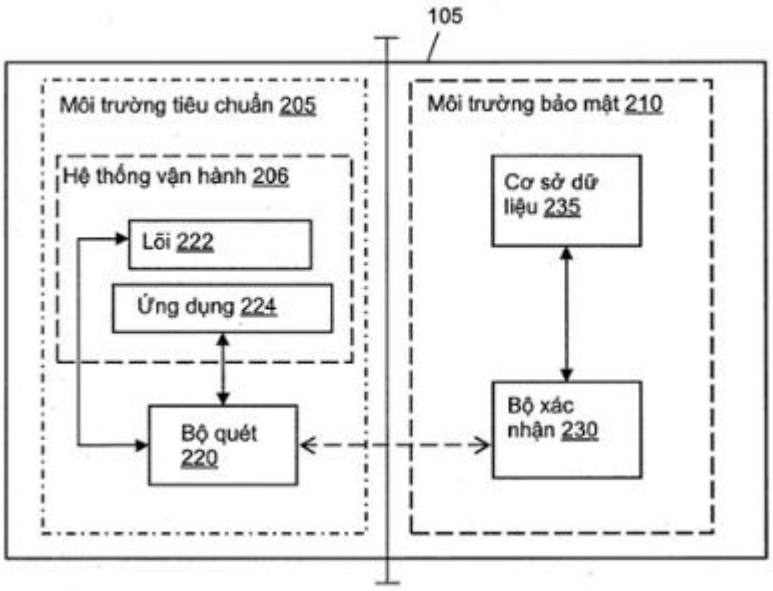
(12) BẢN MÔ TẢ SÁNG CHẾ THUỘC BẰNG ĐỘC QUYỀN SÁNG CHẾ
(19) **Cộng hòa xã hội chủ nghĩa Việt Nam (VN)**
CỤC SỞ HỮU TRÍ TUỆ
(11) **1-0032068**
(51)[8] **G06F 21/70**
(13) **B**

(21) 1-2017-04405
(22) 03/03/2017
(86) PCT/SG2017/050102 03/03/2017
(87) WO 2017/171634 05/10/2017
(30) 10201602449P 29/03/2016 SG
(45) 25/05/2022 410
(43) 25/01/2019 370A
(73) HUAWEI INTERNATIONAL PTE. LTD. (SG)
51 Changi Business Park Central 2 #07, The Signature, Singapore 486066
(72) WU, Yongzheng (SG); WEN, Xuejun (CN); FANG, Chengfang (CN); LI, Tieyan (SG).
(74) Công ty Luật TNHH Phạm và Liên danh (PHAM & ASSOCIATES)

(54) HỆ THỐNG VÀ PHƯƠNG PHÁP XÁC NHẬN TÍNH NGUYÊN VẸN CỦA THIẾT BỊ ĐIỆN TỬ

(57) Sáng chế đề cập đến hệ thống và phương pháp xác nhận tính nguyên vẹn hệ thống của thiết bị điện tử. Thiết bị điện tử này bao gồm môđun xác nhận được bố trí trong môi trường bảo mật của thiết bị điện tử và môđun quét được bố trí trong môi trường tiêu chuẩn của thiết bị điện tử nhờ đó môi trường bảo mật có phần cứng mà được cách ly với phần cứng trong môi trường tiêu chuẩn, nghĩa là hai môi trường này được cách ly với phần cứng.



Lĩnh vực kỹ thuật được đề cập

Sáng chế đề cập đến hệ thống và phương pháp xác nhận tính nguyên vẹn hệ thống của thiết bị điện tử. Thiết bị điện tử này bao gồm môđun xác nhận được bố trí trong môi trường bảo mật của thiết bị điện tử và môđun quét được bố trí trong môi trường tiêu chuẩn của thiết bị điện tử do đó môi trường bảo mật bao gồm phần cứng mà được cách ly với phần cứng trong môi trường tiêu chuẩn, nghĩa là hai môi trường này là phần cứng được phân cách. Trong quá trình xác nhận tính nguyên vẹn của thiết bị điện tử, môđun xác nhận xác nhận tính nguyên vẹn của cả môđun quét và hệ thống vận hành lắp đặt trong môi trường tiêu chuẩn.

Tình trạng kỹ thuật của sáng chế

Các sửa đổi trái phép được tạo ra cho thiết bị điện tử nhằm mục đích đạt được việc truy cập siêu người dùng và/hoặc người quản trị hoặc loại bỏ tất cả các giới hạn người dùng ra khỏi thiết bị điện tử, ví dụ, việc chiếm quyền điều khiển đối với các hệ thống vận hành android hoặc phá khoá đối với hệ thống vận hành iphone, kết xuất lỗ hổng thiết bị điện tử đối với lỗ thủng bảo mật và làm tổn hại toàn bộ hệ thống bảo mật của thiết bị này. Các môđun quan trọng hoặc đặc quyền trong các thiết bị điện tử có các quy trình quan trọng của hệ thống hoặc các trình nền quản lý hệ thống mà được thực hiện bên trong lõi hệ thống vận hành (Operating System-OS) của thiết bị hoặc bên trong hệ thống của thiết bị.

Hầu hết các sửa đổi trái phép đối với thiết bị điện tử sẽ để lại một số dấu vết trong hệ thống vận hành của thiết bị này. Ví dụ, trong các thiết bị Linux, khi thiết bị như vậy bị chiếm quyền điều khiển, quy trình chiếm quyền điều khiển này sẽ tạo ra môđun lệnh SU (nghĩa là, môđun mà cho phép các ứng dụng trái phép thu được các đặc quyền cao hơn) hoặc sẽ leo thang các đặc quyền theo các quy trình nhất định. Do đó, phương pháp xác nhận xem liệu thiết bị đã bị

chiếm quyền điều khiển hay chưa bao gồm việc quét thiết bị đối với các môđun lệnh SU hoặc đối với sự leo thang các đặc quyền của các quy trình nhất định. Các cách khác xác nhận tính nguyên vẹn của thiết bị bao gồm việc kiểm tra hệ thống tệp của thiết bị, kiểm tra các vị trí của bộ nhớ cố định đối với các mã lõi nhất định hoặc kiểm tra phần động của bộ nhớ của thiết bị đối với các quy trình chưa biết mà có các đặc quyền chiếm quyền điều khiển/hệ thống. Điều không ngạc nhiên là, các kẻ tấn công hiểm độc sẽ làm thích ứng với các kỹ thuật quét này và sẽ liên tục tạo ra các phương pháp mới để che các dấu vết của chúng do đó tránh bị phát hiện.

Các giải pháp chống phần mềm độc hại đã phải đối mặt với vấn đề chung là các chương trình phát hiện/bảo vệ thường được lắp đặt trong hệ thống vận hành mà cần phải được bảo vệ. Do đó, nếu nhận biết được về sự tồn tại của các giải pháp chống phần mềm độc hại như vậy đang chạy trong hệ thống này, kẻ tấn công có thể thực hiện việc tấn công mà khiến cho giải pháp chống phần mềm độc hại phải được sửa đổi do đó ngăn chặn một cách có hiệu quả sự hữu ích của giải pháp này. Tóm lại, các giải pháp chống phần mềm độc hại lắp đặt bên trong khoảng trống vận hành thông thường thường dễ bị các tấn công đã được thiết kế.

Phương pháp đã được đề xuất để xác định tính nguyên vẹn của thiết bị bao gồm việc kiểm tra theo định kỳ các dữ liệu lõi của thiết bị với các dữ liệu chứa trong lõi ban đầu. Môđun mà thực hiện phương pháp này được bố trí ở trạng thái bảo mật của thiết bị này. Các môđun xác nhận thường được lắp đặt bên trong các khu vực bảo mật như vậy vì theo lý thuyết, chỉ có những siêu người dùng hoặc người quản trị hệ thống có thể truy cập hoặc tạo ra các sửa đổi cho các môđun được bố trí trong khu vực này. Việc này đảm bảo rằng các môđun lắp đặt trong các khu vực bảo mật như vậy sẽ được cách ly với sự tấn công và các sửa đổi trái phép.

Giải pháp đã biết trong lĩnh vực này mà thực hiện việc đó là giải pháp vùng an toàn dựa vào kiến trúc đo lượng độ tin cậy (Trust Zone-based Integrity Measurement Architecture-TIMA). Giải pháp TIMA chạy trong môi trường tin cậy hoàn toàn, không có sự tấn công nào có thể sửa đổi được cơ chế TIMA.

Tuy nhiên, do các ứng dụng được lắp đặt bên trong hệ thống vận hành thông thường không được sử dụng trong giải pháp TIMA, điều này có nghĩa là giải pháp TIMA chỉ có thể kiểm tra đối với các dấu vết tấn công đơn giản. Ví dụ, giải pháp này chỉ có thể kiểm tra xem liệu mã lõi đã bị sửa đổi hay chưa (nghĩa là, bằng cách tính toán mã băm kỹ thuật số của vùng nhớ đã biết và so sánh kết quả này với trị số định trước) và chỉ có thể xác nhận dấu hiệu của các môđun với khoá bảo mật được lưu trữ trong môi trường tin cậy. Kết quả là, không thể phát hiện các thay đổi phức tạp đối với thiết bị hoặc hệ thống vận hành của thiết bị như dữ liệu mà đã được sửa đổi, đặc quyền của quy trình mà đã được thay đổi và v.v.. Trên thực tế, có một số công cụ tấn công đã biết, ví dụ, "towelroot", "pingpong root" và "kingroot" mà có thể được sử dụng để tấn công các thiết bị được thực hiện bởi TIMA mà không bị phát hiện. Ngoài ra, sẽ khó hơn nhiều để thực hiện việc cập nhật đối với các ứng dụng hoặc các môđun mà được lắp đặt bên trong môi trường tin cậy. Kết quả là, các môđun này trong môi trường tin cậy sẽ không có khả năng xử lý các tấn công sau cùng do không hiệu quả và khó cập nhật các môđun này.

Các phương pháp đã được đề xuất khác để xác nhận tính nguyên vẹn của thiết bị hoặc ngăn không cho thiết bị bị tấn công bao gồm việc sử dụng các thông tin mà được cập nhật liên tục bởi máy chủ từ xa. Bằng cách phân tích các mẫu tấn công, máy chủ từ xa có thể cải thiện độ chính xác và tính hiệu quả của các quy trình xác nhận/bảo vệ và các thông tin được cập nhật này được cập nhật theo định kỳ vào trong thiết bị. Giải pháp khởi động/tin cậy khởi động/dm-xác nhận bảo mật là các giải pháp khác mà dựa vào ý tưởng là, nếu chỉ có các thành phần được xác nhận được phép để được nạp lên và chạy trong hệ thống, hầu hết, nếu không phải tất cả, các tấn công đều có thể được phát hiện và được giải quyết. Để đạt được điều này, các giải pháp đó cần phải có các môđun đã được nạp cần được xác nhận bởi môđun đã được lắp đặt trước; do đó môđun đã được lắp đặt trước ban đầu được xác nhận bởi các môđun xác nhận phần cứng. Ngoài ra, giải pháp khởi động bảo mật cũng đảm bảo rằng các thành phần tốt nhất sẽ được thực hiện khi hệ thống khởi động, bằng cách sử dụng kỹ thuật đã biết như "khởi động-chuỗi". Ví dụ, trong các hệ thống vận

hành Linux, giải pháp khởi động-chuỗi bảo mật đã được đề xuất thực hiện trình tự khởi động sau khi thiết bị ban đầu khởi động:

1) Bộ xử lý của thiết bị sẽ nạp chương trình bộ nạp khởi động từ vị trí định trước mà không thể hiệu chỉnh sau khi thiết bị này đã được sản xuất;

2) Chương trình của bộ nạp khởi động sẽ xác nhận và nạp "u-khởi động" hoặc bộ nạp khởi động chung, mà xử lý các quy trình xử lý đầu vào và đầu ra cơ bản của thiết bị, tương tự với cách mà BIOS thực hiện đối với các máy tính cá nhân; và

3) Tiếp theo, u-khởi động sẽ nạp lõi, mà nạp hệ thống Android.

Giải pháp khởi động bảo mật được đề xuất nêu trên cho phép việc xác nhận cần được thực hiện bằng cách sử dụng các thành phần phần cứng. Tuy nhiên, các việc xác nhận này chỉ được thực hiện khi các môđun ban đầu được nạp và không còn bước xác nhận nào nữa được thực hiện thêm. Kết quả là, giải pháp này không bảo vệ hệ thống vận hành chống lại các tấn công theo thời gian chạy như các công cụ tấn công nêu trên.

Vì các lý do nêu trên, chuyên gia trong lĩnh vực này đang nỗ lực tạo ra hệ thống và phương pháp xác nhận tính nguyên vẹn hệ thống của thiết bị điện tử theo cách có hiệu quả và tin cậy.

Bản chất kỹ thuật của sáng chế

Các vấn đề nêu trên và các vấn đề khác được giải quyết và một tiến bộ trong lĩnh vực này được tạo ra bởi các hệ thống và phương pháp được đề xuất bởi các phương án theo sáng chế.

Ưu điểm thứ nhất của các hệ thống và phương pháp theo các phương án của sáng chế là trước khi xác nhận tính nguyên vẹn của hệ thống thiết bị điện tử, tính nguyên vẹn của môđun quét được bố trí trong hệ thống vận hành tiêu chuẩn của thiết bị này sẽ được xác nhận nhờ môđun xác nhận lắp đặt trong môi trường bảo mật của thiết bị này. Lớp xác nhận bổ sung này đảm bảo độ tin cậy của hệ thống không bị huỷ hoại.

Ưu điểm thứ hai của các hệ thống và phương pháp theo các phương án của sáng chế là việc xác nhận tính nguyên vẹn của môđun quét (do đó, môđun này

được bố trí trong hệ thống vận hành tiêu chuẩn) có thể được kết hợp với bước xác nhận tính nguyên vẹn hệ thống của thiết bị do đó loại bỏ nhu cầu về các bước xác nhận tốn thêm thời gian.

Ưu điểm thứ ba của các hệ thống và phương pháp theo các phương án của sáng chế là sự phản hồi được tạo ra bởi môđun quét có thể không bị làm giả, không bị xâm nhập hoặc không bị sửa đổi do sự phản hồi được mã hoá bằng cách sử dụng phương pháp mã hoá mà chỉ có thể được giải mã bởi môđun xác nhận.

Ưu điểm thứ tư của các hệ thống và phương pháp theo các phương án của sáng chế là việc xác nhận tính nguyên vẹn hệ thống của thiết bị có thể được thực hiện theo chu kỳ và không bị giới hạn chỉ thiết bị này cấp nguồn hoặc khởi động.

Ưu điểm thứ năm của các hệ thống và phương pháp theo các phương án của sáng chế là không giống như môđun xác nhận, khi môđun quét được lắp đặt trong môi trường tiêu chuẩn, môđun quét này có thể được cập nhật một cách dễ dàng và ổn định với các chương trình chống phần mềm độc hại mới nhất, chống chiếm quyền điều khiển hoặc chống bẻ khoá.

Các ưu điểm nêu trên được tạo ra bởi phương pháp theo các phương án của sáng chế vận hành theo cách sau.

Theo khía cạnh thứ nhất của sáng chế, phương pháp xác nhận tính nguyên vẹn hệ thống của thiết bị điện tử bao gồm các bước: tạo ra, bởi môđun xác nhận được bố trí trong môi trường bảo mật trong thiết bị điện tử, đòi hỏi; truyền đòi hỏi từ môđun xác nhận đến môđun quét được bố trí trong môi trường tiêu chuẩn trong thiết bị điện tử, trong đó đòi hỏi hướng dẫn môđun quét thực hiện chức năng xác nhận tính nguyên vẹn trong môi trường tiêu chuẩn để tạo ra phản hồi; mã hoá, bởi môđun quét, phản hồi và truyền phản hồi được mã hoá này đến môđun xác nhận; và xác nhận, bởi môđun xác nhận, tính nguyên vẹn của môđun quét do đó đáp lại sự xác nhận rằng tính nguyên vẹn của môđun quét được xác nhận, xác định, bởi môđun xác nhận, xem liệu phản hồi này có hợp lệ hay không, do đó đáp lại sự xác nhận rằng phản hồi này là không hợp lệ, thực hiện hoạt động làm giảm.

Theo khía cạnh thứ nhất, theo cách có thể thực hiện thứ nhất của khía cạnh thứ nhất, bước xác nhận tính nguyên vẹn của môđun quét bao gồm việc giải mã, bởi môđun xác nhận, phản hồi được mã hoá, do đó phản hồi sự giải mã thành công của phản hồi được mã hoá, xác nhận tính nguyên vẹn của môđun quét.

Theo khía cạnh thứ nhất hoặc cách có thể thực hiện thứ nhất của khía cạnh thứ nhất, theo cách có thể thực hiện thứ hai của khía cạnh thứ nhất, môi trường bảo mật trong thiết bị điện tử bao gồm bộ xử lý ảo thế giới bảo mật dùng cho thiết bị điện tử.

Theo khía cạnh thứ nhất, cách có thể thực hiện thứ nhất hoặc thứ hai của khía cạnh thứ nhất, theo cách có thể thực hiện thứ ba của khía cạnh thứ nhất, môi trường tiêu chuẩn trong thiết bị điện tử bao gồm bộ xử lý ảo thế giới tiêu chuẩn dùng cho thiết bị điện tử.

Theo khía cạnh thứ nhất, cách có thể thực hiện thứ nhất, thứ hai hoặc thứ ba của khía cạnh thứ nhất, theo cách có thể thực hiện thứ tư của khía cạnh thứ nhất, chức năng xác nhận bao gồm việc quét mã lõi; quét danh mục xử lý; quét bảng trang nhớ; hoặc kiểm tra trạng thái và tham số của cơ chế bảo vệ lõi.

Theo khía cạnh thứ nhất, cách có thể thực hiện thứ nhất, thứ hai, thứ ba hoặc thứ tư của khía cạnh thứ nhất, theo cách có thể thực hiện thứ năm của khía cạnh thứ nhất, bước mã hoá phản hồi bao gồm việc mã hoá với khoá riêng hoặc khoá công cộng, trong đó khoá riêng hoặc khoá công cộng được bố trí trong bộ quét và môđun xác nhận.

Theo khía cạnh thứ nhất hoặc cách có thể thực hiện thứ nhất, thứ hai, thứ ba, thứ tư hoặc thứ năm của khía cạnh thứ nhất, theo cách có thể thực hiện thứ sáu của khía cạnh thứ nhất, bước xác định nếu phản hồi là hợp lệ bao gồm việc so khớp phản hồi này với dữ liệu chứa trong cơ sở dữ liệu bảo mật được bố trí trong môi trường bảo mật, trong đó khi sự phù hợp không được tìm thấy, phản hồi được xác định là không hợp lệ.

Theo khía cạnh thứ nhất hoặc cách có thể thực hiện thứ nhất, thứ hai, thứ ba, thứ tư, thứ năm hoặc thứ sáu của khía cạnh thứ nhất, theo cách có thể thực hiện thứ bảy của khía cạnh thứ nhất, trong đó trước bước tạo ra đòi hỏi bằng cách sử dụng môđun xác nhận, phương pháp bao gồm bước xác nhận, bởi môđun xác

nhận, tính nguyên vẹn của môđun quét được bố trí trong môi trường tiêu chuẩn.

Theo cách có thể thực hiện thứ bảy của khía cạnh thứ nhất, theo cách có thể thực hiện thứ tám của khía cạnh thứ nhất, bước xác nhận tính nguyên vẹn của môđun quét được bố trí trong môi trường tiêu chuẩn bao gồm việc tạo ra, bởi môđun xác nhận, yêu cầu đáp lại sự xác nhận và truyền yêu cầu đáp lại sự xác nhận này từ môđun xác nhận đến môđun quét, trong đó yêu cầu đáp lại sự xác nhận hướng dẫn môđun quét tạo ra sự đáp lại sự xác nhận được mã hoá và truyền sự đáp lại sự xác nhận được mã hoá đến môđun xác nhận; và xác định, bởi môđun xác nhận, xem liệu sự đáp lại sự xác nhận được mã hoá có hợp lệ hay không, do đó đáp lại sự xác nhận rằng phản hồi này là không hợp lệ, thực hiện hoạt động làm giảm.

Theo cách có thể thực hiện thứ tám của khía cạnh thứ nhất, theo cách có thể thực hiện thứ chín của khía cạnh thứ nhất, bước xác định xem liệu sự đáp lại sự xác nhận được mã hoá có hợp lệ hay không bao gồm việc giải mã, bởi môđun xác nhận, sự đáp lại sự xác nhận được mã hoá, do đó đáp lại sự xác nhận rằng sự đáp lại sự xác nhận này được giải mã, so khớp sự đáp lại sự xác nhận được giải mã này với dữ liệu xác nhận có trong cơ sở dữ liệu bảo mật được bố trí trong môi trường bảo mật, trong đó khi sự phù hợp không được tìm thấy, sự đáp lại sự xác nhận này được xác định là không hợp lệ.

Theo khía cạnh thứ nhất hoặc cách có thể thực hiện thứ nhất, thứ hai, thứ ba, thứ tư, thứ năm, thứ sáu hoặc thứ bảy của khía cạnh thứ nhất, theo cách có thể thực hiện thứ mười của khía cạnh thứ nhất, hoạt động làm giảm bao gồm việc ngăn không cho thực hiện các môđun phần mềm được bố trí trong môi trường tiêu chuẩn.

Theo khía cạnh thứ nhất của sáng chế, theo cách có thể thực hiện thứ mười một của khía cạnh thứ nhất, môi trường bảo mật là phần cứng được cách ly với môi trường tiêu chuẩn.

Theo khía cạnh thứ nhất hoặc cách có thể thực hiện thứ nhất, thứ hai, thứ ba hoặc thứ tư của khía cạnh thứ nhất, theo cách có thể thực hiện thứ mười hai của khía cạnh thứ nhất, chức năng xác nhận trong môđun quét được bỏ qua.

Theo khía cạnh thứ nhất của sáng chế, theo cách có thể thực hiện thứ mười

ba của khía cạnh thứ nhất, trong đó trước bước tạo ra đòi hỏi bằng cách sử dụng môđun xác nhận, phương pháp bao gồm bước phát hiện, bởi thiết bị điện tử, bật nguồn thiết bị điện tử; và nạp môđun xác nhận trong môi trường bảo mật trong thiết bị điện tử.

Theo khía cạnh thứ nhất của sáng chế hoặc cách có thể thực hiện thứ mười ba của khía cạnh thứ nhất, theo cách có thể thực hiện thứ mười bốn của khía cạnh thứ nhất, phương pháp còn bao gồm bước xác định xem liệu khoảng thời gian thiết lập trước đã trôi qua hay chưa; và lặp lại phương pháp xác nhận tính nguyên vẹn hệ thống của thiết bị điện tử khi khoảng thời gian thiết lập trước đã trôi qua.

Theo khía cạnh thứ hai của sáng chế, hệ thống A dùng để xác nhận tính nguyên vẹn hệ thống của thiết bị điện tử, hệ thống này bao gồm: bộ xử lý có môi trường bảo mật và môi trường tiêu chuẩn; và vật ghi không tạm thời đọc được bởi bộ xử lý, vật ghi lưu trữ các hướng dẫn mà khi được thực hiện bởi bộ xử lý khiến cho bộ xử lý:

tạo ra đòi hỏi bằng cách sử dụng môđun xác nhận được bố trí trong môi trường bảo mật;

truyền đòi hỏi từ môđun xác nhận đến môđun quét được bố trí trong môi trường tiêu chuẩn, trong đó đòi hỏi hướng dẫn môđun quét thực hiện chức năng xác nhận tính nguyên vẹn trong môi trường tiêu chuẩn để tạo ra phản hồi;

mã hoá phản hồi này bằng cách sử dụng môđun quét và truyền phản hồi được mã hoá này đến môđun xác nhận; và

xác nhận tính nguyên vẹn của môđun quét bằng cách sử dụng môđun xác nhận, do đó đáp lại sự xác nhận rằng tính nguyên vẹn của môđun quét được xác nhận, để xác định bằng cách sử dụng môđun xác nhận xem liệu phản hồi này có hợp lệ hay không, do đó đáp lại sự xác nhận rằng phản hồi này là không hợp lệ, để thực hiện hoạt động làm giảm.

Theo khía cạnh thứ hai, theo cách có thể thực hiện thứ nhất của khía cạnh thứ hai, trong đó các hướng dẫn để xác nhận tính nguyên vẹn của môđun quét bao gồm:

các hướng dẫn để chỉ dẫn bộ xử lý nhằm:

giải mã phản hồi được mã hoá bằng cách sử dụng môđun xác nhận, do đó phản hồi lại việc giải mã thành công phản hồi được mã hoá, để xác nhận tính nguyên vẹn của môđun quét.

Theo khía cạnh thứ hai hoặc cách có thể thực hiện thứ nhất của khía cạnh thứ hai, theo cách có thể thực hiện thứ hai của khía cạnh thứ hai, trong đó môi trường bảo mật trong bộ xử lý bao gồm bộ xử lý ảo thế giới bảo mật.

Theo khía cạnh thứ hai, cách có thể thực hiện thứ nhất hoặc thứ hai của khía cạnh thứ hai, theo cách có thể thực hiện thứ ba của khía cạnh thứ hai, trong đó môi trường tiêu chuẩn trong bộ xử lý bao gồm bộ xử lý ảo thế giới tiêu chuẩn.

Theo khía cạnh thứ hai, cách có thể thực hiện thứ nhất, thứ hai hoặc thứ ba của khía cạnh thứ hai, theo cách có thể thực hiện tứ tư của khía cạnh thứ hai, trong đó chức năng xác nhận bao gồm:

các hướng dẫn để chỉ dẫn bộ xử lý nhằm:

quét mã lõi; quét danh mục xử lý; quét bảng trang nhớ; hoặc kiểm tra trạng thái và tham số của cơ chế bảo vệ lõi.

Theo khía cạnh thứ hai, cách có thể thực hiện thứ nhất, thứ hai, thứ ba hoặc thứ tư của khía cạnh thứ hai, theo cách có thể thực hiện thứ năm của khía cạnh thứ hai, trong đó các hướng dẫn mã hoá phản hồi bao gồm:

các hướng dẫn để chỉ dẫn bộ xử lý nhằm:

mã hoá phản hồi với khoá riêng hoặc khoá công cộng, trong đó khoá riêng hoặc khoá công cộng được bố trí trong bộ quét và môđun xác nhận.

Theo khía cạnh thứ hai hoặc cách có thể thực hiện thứ nhất, thứ hai, thứ ba, thứ tư hoặc thứ năm của khía cạnh thứ hai, theo cách có thể thực hiện thứ sáu của khía cạnh thứ hai, trong đó các hướng dẫn xác định nếu phản hồi là hợp lệ bao gồm:

các hướng dẫn để chỉ dẫn bộ xử lý nhằm:

so khớp phản hồi với dữ liệu chứa trong cơ sở dữ liệu bảo mật được bố trí trong môi trường bảo mật, trong đó khi sự phù hợp không được tìm thấy, phản hồi được xác định là không hợp lệ.

Theo khía cạnh thứ hai hoặc cách có thể thực hiện thứ nhất, thứ hai, thứ ba,

thứ tư, thứ năm hoặc thứ sáu của khía cạnh thứ hai, theo cách có thể thực hiện thứ bảy của khía cạnh thứ hai, trong đó trước khi các hướng dẫn tạo ra đòi hỏi bằng cách sử dụng môđun xác nhận, các hướng dẫn này bao gồm:

các hướng dẫn để chỉ dẫn bộ xử lý nhằm:

xác nhận tính nguyên vẹn của môđun quét được bố trí trong môi trường tiêu chuẩn bằng cách sử dụng môđun xác nhận được bố trí trong môi trường bảo mật.

Theo cách có thể thực hiện thứ bảy của khía cạnh thứ hai, theo cách có thể thực hiện thứ tám của khía cạnh thứ hai, trong đó các hướng dẫn xác nhận tính nguyên vẹn của môđun quét được bố trí trong môi trường tiêu chuẩn bao gồm:

các hướng dẫn để chỉ dẫn bộ xử lý nhằm:

tạo ra yêu cầu đáp lại sự xác nhận bằng cách sử dụng môđun xác nhận và truyền yêu cầu đáp lại sự xác nhận từ môđun xác nhận đến môđun quét, trong đó yêu cầu đáp lại sự xác nhận hướng dẫn môđun quét để tạo ra sự đáp lại sự xác nhận được mã hoá và truyền sự đáp lại sự xác nhận được mã hoá đến môđun xác nhận; và

xác định xem liệu sự đáp lại sự xác nhận được mã hoá có hợp lệ hay không bằng cách sử dụng môđun xác nhận, do đó đáp lại sự xác nhận rằng phản hồi không hợp lệ, để thực hiện hoạt động làm giảm.

Theo cách có thể thực hiện thứ tám của khía cạnh thứ hai, theo cách có thể thực hiện thứ chín của khía cạnh thứ hai, trong đó các hướng dẫn xác định nếu sự đáp lại sự xác nhận được mã hoá hợp lệ bao gồm:

các hướng dẫn để chỉ dẫn bộ xử lý nhằm:

giải mã sự đáp lại sự xác nhận được mã hoá bằng cách sử dụng môđun xác nhận, do đó đáp lại sự xác nhận rằng sự đáp lại sự xác nhận này được giải mã, để so khớp sự đáp lại sự xác nhận được giải mã với dữ liệu xác nhận chứa trong cơ sở dữ liệu bảo mật được bố trí trong môi trường bảo mật, trong đó khi sự phù hợp không được tìm thấy, sự đáp lại sự xác nhận được xác định là không hợp lệ.

Theo khía cạnh thứ hai hoặc cách có thể thực hiện thứ nhất, thứ hai, thứ ba, thứ tư, thứ năm, thứ sáu hoặc thứ bảy của khía cạnh thứ hai, theo cách có thêr

thực hiện thứ mười của khía cạnh thứ hai, trong đó hoạt động làm giảm bao gồm:

các hướng dẫn để chỉ dẫn bộ xử lý để ngăn không cho thực hiện các môđun phần mềm được bố trí trong môi trường tiêu chuẩn.

Theo khía cạnh thứ hai của sáng chế, theo cách có thể thực hiện thứ mười một của khía cạnh thứ hai, trong đó môi trường bảo mật là phần cứng được cách ly với môi trường tiêu chuẩn.

Theo khía cạnh thứ hai hoặc cách có thể thực hiện thứ nhất, thứ hai, thứ ba hoặc thứ tư của khía cạnh thứ hai, theo cách có thể thực hiện thứ mười hai của khía cạnh thứ hai, trong đó chức năng xác nhận trong môđun quét được bỏ qua.

Theo khía cạnh thứ hai của sáng chế, theo cách có thể thực hiện thứ mười ba của khía cạnh thứ hai, trong đó trước khi hướng dẫn tạo ra đòi hỏi bằng cách sử dụng môđun xác nhận, hệ thống bao gồm:

các hướng dẫn để chỉ dẫn bộ xử lý nhằm:

phát hiện việc bật thiết bị điện tử; và

nạp môđun được xác nhận trong môi trường bảo mật trong thiết bị điện tử.

Theo khía cạnh thứ hai của sáng chế hoặc cách có thể thực hiện thứ mười ba của khía cạnh thứ hai, theo cách có thể thực hiện thứ mười bốn của khía cạnh thứ hai, môđun quét được bỏ qua.

Mô tả vắn tắt các hình vẽ

Các ưu điểm và dấu hiệu kỹ thuật của sáng chế sẽ được mô tả trong phần mô tả chi tiết sau và được thể hiện trên các hình vẽ kèm theo:

Fig.1 minh hoạ sơ đồ khối biểu thị các thành phần trong thiết bị điện tử để thực hiện các phương pháp theo các phương án của sáng chế;

Fig.2 minh hoạ sơ đồ khối làm ví dụ thể hiện môi trường bảo mật và môi trường tiêu chuẩn của bộ xử lý theo các phương án của sáng chế;

Fig.3 minh hoạ sơ đồ định thời để xác nhận tính nguyên vẹn của thiết bị điện tử theo các phương án của sáng chế;

Fig.4 minh hoạ lưu đồ thể hiện quy trình được thực hiện trên môđun xác nhận để xác nhận tính nguyên vẹn của thiết bị điện tử theo các phương án của

sáng chế;

Fig.5 minh hoạ lưu đồ thể hiện quy trình xác nhận tính nguyên vẹn của môđun quét được bố trí trong môi trường tiêu chuẩn theo các phương án của sáng chế; và

Fig.6 minh hoạ lưu đồ thể hiện quy trình được thực hiện trên môđun quét để tạo ra sự phản hồi đã được mã hoá để xác nhận môđun quét và tính nguyên vẹn của thiết bị điện tử theo các phương án của sáng chế.

Mô tả chi tiết sáng chế

Sáng chế đề cập đến hệ thống và phương pháp xác nhận tính nguyên vẹn hệ thống của thiết bị điện tử. Thiết bị điện tử được trang bị môđun xác nhận được lắp đặt bên trong môi trường bảo mật của thiết bị điện tử và môđun quét được lắp đặt bên trong môi trường tiêu chuẩn của thiết bị điện tử do đó môi trường bảo mật bao gồm phần cứng mà được cách ly với phần cứng trong môi trường tiêu chuẩn, nghĩa là hai môi trường này là phần cứng cách ly.

Fig.1 minh hoạ sơ đồ khối thể hiện hệ thống xử lý và các thành phần của hệ thống xử lý mà có thể có trong thiết bị điện tử 100 để thực hiện các phương án theo các phương án của sáng chế. Thiết bị điện tử 100 có thể bao gồm, nhưng không chỉ giới hạn ở, thiết bị bất kỳ mà có khả năng thực hiện các chức năng truyền thông như điện thoại thông minh, máy tính bảng, máy tính di động, máy tính cầm tay, thiết bị điện tử xách tay như đồng hồ thông minh và v.v. Chuyên gia trong lĩnh vực này sẽ nhận biết được rằng cấu hình chính xác của mỗi thiết bị điện tử có thể là khác nhau và cấu hình chính xác của mỗi thiết bị điện tử có thể thay đổi và Fig.1 được đưa ra chỉ bằng cách ví dụ.

Theo các phương án của sáng chế, thiết bị điện tử 100 bao gồm bộ điều khiển 101 và giao diện người dùng 102. Giao diện người dùng 102 được bố trí để cho phép các tương tác bằng tay giữa người dùng và thiết bị điện tử 100 và nhằm mục đích bao gồm các thành phần đầu vào/đầu ra cần thiết để người dùng nhập các hướng dẫn để điều khiển thiết bị điện tử 100. Chuyên gia trong lĩnh vực này sẽ nhận biết được rằng các thành phần của giao diện người dùng 102 có thể thay đổi từ phương án đến phương án nhưng thường sẽ bao gồm

một hoặc nhiều màn hình 140, bàn phím 135 và đệm theo dõi 136.

Bộ điều khiển 101 trong quá trình truyền thông dữ liệu với giao diện người dùng 102 thông qua bus 115 và bao gồm bộ nhớ 120, bộ xử lý trung tâm (CPU) 105 được lắp vào bảng mạch mà xử lý các hướng dẫn và các dữ liệu để thực hiện phương pháp theo phương án này, hệ thống vận hành 106, giao diện đầu vào/đầu ra (I/O) 130 để truyền thông với giao diện người dùng 102 và giao diện truyền thông, theo phương án này ở dạng thẻ nối mạng 150. Thẻ nối mạng 150 có thể, ví dụ, được dùng để gửi dữ liệu từ thiết bị điện tử 100 thông qua mạng có dây hoặc không dây với thiết bị xử lý khác hoặc để thu dữ liệu thông qua mạng có dây hoặc không dây. Các mạng không dây mà có thể được sử dụng bởi thẻ nối mạng 150 bao gồm, nhưng không chỉ giới hạn ở, kết nối mạng không dây (Wireless-Fidelity-Wi-Fi), Bluetooth, truyền thông trường gần (Near Field Communication-NFC), các mạng tế bào, các mạng vệ tinh, các mạng viễn thông, các mạng diện rộng (Wide Area Network-WAN) và v.v..

Bộ nhớ 120 và hệ thống vận hành 106 trong quá trình truyền thông dữ liệu với CPU 105 thông qua bus 110. Các thành phần của bộ nhớ bao gồm cả bộ nhớ khả biến và không khả biến và nhiều hơn một trong số mỗi dạng bộ nhớ, bao gồm bộ nhớ truy cập ngẫu nhiên (Random Access Memory-RAM) 120, bộ nhớ chỉ đọc (Read Only Memory-ROM) 125 và thiết bị lưu trữ khối 145, thiết bị này bao gồm một hoặc nhiều ổ cứng thể rắn (solid-state drive-SSD). Chuyên gia trong lĩnh vực này sẽ nhận biết được rằng các thành phần của bộ nhớ bao gồm vật ghi đọc được bằng máy tính không tạm thời và sẽ được xem là bao gồm tất cả vật ghi đọc được bằng máy tính ngoại trừ đối với tín hiệu lan truyền tạm thời. Thông thường, các hướng dẫn được lưu trữ như mã chương trình trong các thành phần của bộ nhớ nhưng cũng có thể được truyền hữu tuyến. Bộ nhớ 120 có thể bao gồm các môđun lõi và/hoặc lập trình như ứng dụng phần mềm mà có thể được lưu trữ trong bộ nhớ khả biến hoặc không khả biến.

Trong bản mô tả này, thuật ngữ "CPU" được dùng để chỉ theo cách khái quát thiết bị hoặc thành phần bất kỳ mà có thể xử lý các hướng dẫn như vậy và có thể bao gồm: bộ vi xử lý, bộ vi điều khiển, thiết bị logic lập trình được hoặc thiết bị tính toán khác. Tức là, CPU 105 có thể được tạo ra với mạch logic thích

hợp bất kỳ để thu dữ liệu đầu vào, xử lý chúng theo các hướng dẫn được lưu trữ trong bộ nhớ và tạo ra dữ liệu đầu ra (ví dụ, đối với các thành phần bộ nhớ hoặc trên màn hình 140). Theo phương án này, CPU 105 có thể là bộ xử lý một lõi duy nhất hoặc bộ xử lý nhiều lõi với khoảng trống có thể lập địa chỉ bộ nhớ. Trong một ví dụ, CPU 105 có thể là CPU nhiều lõi, bao gồm-ví dụ-8 lõi.

Fig.2 minh hoạ sơ đồ khối làm ví dụ của bộ xử lý 105 mà đã được tạo cấu hình để tạo ra bộ xử lý ảo của môi trường bảo mật 210 (dưới đây được gọi là "môi trường bảo mật) và bộ xử lý ảo của môi trường tiêu chuẩn 205 (dưới đây được gọi là "môi trường tiêu chuẩn) theo các phương án của sáng chế. Môi trường tiêu chuẩn 205 có thể bao gồm hệ thống vận hành 206, lõi 222, ứng dụng 224 và bộ quét 220 mà đã được tạo cấu hình để vận hành theo chế độ tiêu chuẩn với các thiết lập bảo mật tối thiểu. Ngược lại, môi trường bảo mật 210 có thể được trang bị hệ thống vận hành bảo mật, lõi bảo mật, cơ sở dữ liệu bảo mật 235 và môđun xác nhận bảo mật 230.

Môi trường bảo mật 210 có thể là phần cứng được cách ly với môi trường tiêu chuẩn 205 do đó đảm bảo rằng các ứng dụng, các lõi, các môđun và các hệ thống vận hành được đặt bên trong môi trường tiêu chuẩn có thể không truy cập các ứng dụng, các lõi, các môđun và hệ thống vận hành được bố trí trong môi trường bảo mật. Sự tách biệt dựa vào phần cứng như vậy có thể được tạo ra bởi, nhưng không chỉ giới hạn ở, các kết cấu của bộ xử lý được tạo ra bởi máy RISC tiến bộ (Advanced RISC Machines-ARM). Trong bộ xử lý ARM, sự cách ly dựa vào phần cứng như vậy được thực hiện như kỹ thuật vùng tin cậy. Kỹ thuật vùng tin cậy của các bộ xử lý ARM cho phép cách ly dựa vào phần cứng để chia quá trình thực hiện mã trên một lõi bộ xử lý vật lý duy nhất thành hai môi trường, môi trường bảo mật và môi trường tiêu chuẩn. Chuyên gia trong lĩnh vực này sẽ nhận biết được rằng phần mềm hoặc môđun được minh hoạ trên Fig.2, như các môđun được lắp đặt trong các môi trường bảo mật 210 và môi trường tiêu chuẩn 205, có thể được ghi bằng cách sử dụng các mã phát triển dùng cho các hệ thống vận hành như vậy hoặc có thể được sửa đổi từ các nhóm hoặc các thành phần hiện có được mã hoá dùng cho các hệ thống vận hành như vậy để thực hiện các quy trình cần thiết cho mỗi môđun như được mô

tả dưới đây và các dữ liệu hoặc các thông tin đó có thể được truyền giữa các môđun này, nếu cần.

Các thành phần được lắp đặt trong môi trường bảo mật là đối tượng để giới hạn các yêu cầu bảo mật và kết quả là, có thể thực hiện các chức năng giới hạn và chỉ có thể được truy cập hoặc được sửa đổi bởi nhà sản xuất thiết bị hoặc siêu người dùng của thiết bị. Điều này khiến cho việc cập nhật các ứng dụng, các môđun hoặc các lõi bên trong môi trường bảo mật lựa chọn thiếu hấp dẫn và không thực tế.

Hệ thống vận hành 206 mà được bố trí trong môi trường tiêu chuẩn 205 có thể bao gồm các hệ thống vận hành tuỳ ý như Android, Linux, iPhone OS (iOS) hoặc hệ thống vận hành khác bất kỳ thích hợp để sử dụng trong thiết bị điện tử 100 hoặc các thiết bị di động. Lõi 222 và/hoặc ứng dụng 224 có thể thực hiện các hướng dẫn để quản lý các tài nguyên của thiết bị điện tử 100. Môđun quét 220 mà được bố trí trong môi trường tiêu chuẩn 205 có thể được tạo cấu hình để tạo ra các hướng dẫn hoặc các lệnh cho hệ thống vận hành 206, lõi 222 hoặc ứng dụng 224 cũng có thể được tạo cấu hình để thu các đáp lại từ mỗi thành phần trong số các thành phần này. Tuy nhiên, cần phải lưu ý rằng các thành phần trong môi trường tiêu chuẩn 205 không thể truy cập hoặc điều khiển các thành phần mà được bố trí trong môi trường bảo mật 210 như các cơ sở dữ liệu 235 hoặc bộ xác nhận 230. Tuy nhiên, các thành phần được lắp đặt trong môi trường tiêu chuẩn có thể truyền các dữ liệu hoặc thu các hướng dẫn từ các thành phần được lắp đặt trong môi trường bảo mật 210. Các dữ liệu được truyền từ các thành phần của môi trường tiêu chuẩn 205 không thể bao gồm các lệnh hoặc các hướng dẫn do dữ liệu có bản chất như vậy sẽ không được xử lý bởi các thành phần trong môi trường bảo mật 210.

Fig.3 minh hoạ sơ đồ định thời để xác nhận tính nguyên vẹn của thiết bị điện tử 100 theo các phương án của sáng chế. Như được minh hoạ trên đây trên Fig.2, môđun xác nhận 230 được bố trí trong môi trường bảo mật 210. Môđun xác nhận 210 có thể bao gồm ứng dụng hoặc chương trình bảo mật được tạo cấu hình để tạo ra các hướng dẫn (dưới đây được gọi là "đòi hỏi") hoặc các dạng yêu cầu khác nhau, như yêu cầu xác nhận, mà sau đó được truyền đến các

thành phần trong môi trường tiêu chuẩn 205. Hệ thống được minh hoạ trên Fig.2 vận thành theo cách sau. Bộ xác nhận 230 trước tiên sẽ tạo ra đòi hỏi mà chứa các hướng dẫn cụ thể mà cần phải được thực hiện bởi môđun quét 220. Theo các phương án của sáng chế, đòi hỏi này có thể được mã hoá bằng cách sử dụng quá trình mã hoá khoá công cộng hoặc khoá riêng do đó khoá công cộng hoặc khoá riêng tương ứng đã được bố trí trước cho môđun quét 220. Tiếp theo, đòi hỏi được truyền đến môđun quét 220 ở bước 305. Khi thu đòi hỏi, môđun quét 220 sẽ thực hiện các hướng dẫn chứa trong đòi hỏi. Nếu đòi hỏi đã được mã hoá, môđun quét 220 sẽ giải mã đòi hỏi bằng cách sử dụng khoá giải mã phù hợp và tiếp theo sẽ thực hiện các hướng dẫn chứa trong đó. Điều này đảm bảo đòi hỏi đó, các hướng dẫn chứa trong đòi hỏi và các chức năng/các đích quét được xác định trong các hướng dẫn này vẫn đáng tin cậy với tất cả các môđun và/hoặc quy trình khác.

Các hướng dẫn có thể chứa các lệnh dùng cho môđun quét 220 để thực hiện các bước xác nhận tính nguyên vẹn của hệ thống vận hành 206 và việc này có thể được thực hiện bằng cách sử dụng các dấu hiệu và chức năng mặc định được cung cấp bởi hệ thống vận hành 206. Theo các phương án của sáng chế, các hướng dẫn có thể bao gồm, nhưng không chỉ giới hạn ở, các lệnh dùng cho môđun quét 220 để thực hiện các thuật toán để quét mã trong lõi 222 đối với các mã độc đã biết, để quét danh mục quy trình, để kiểm tra bộ nhớ 120 để chiếm quyền điều khiển hoặc bẻ khoá, để quét bảng trang của bộ nhớ 120, để kiểm tra trạng thái và các tham số đặc quyền của lõi 222 hoặc ứng dụng 224. Tất cả các thuật toán xác nhận tính nguyên vẹn này có thể được lưu trữ trong môđun quét 220. Theo các phương án của sáng chế, các thuật toán xác nhận tính nguyên vẹn chứa trong môđun quét 220 và/hoặc môđun quét 220 có thể được bỏ qua do đó ngăn không cho môđun quét 220 và các mã này bị truy cập và/hoặc bị phân tích bởi các kẻ tấn công độc. Cần phải lưu ý rằng môđun quét 220 được bỏ qua vẫn có thể thực hiện các hướng dẫn thu được từ môđun xác nhận 210. Nói cách khác, môđun đã được quét 220 không cần phải không được bỏ qua trước khi môđun quét 220 có khả năng thực hiện các hướng dẫn thu được. Do đó, môđun quét được bỏ qua 220 sẽ luôn cần phải được bỏ qua mọi

lúc. Nhờ có các hướng dẫn xác nhận được mã hoá và nhờ có môđun quét 220 được bỏ qua, việc này đảm bảo rằng that môđun quét 220, mà được bố trí trong môi trường vận hành tiêu chuẩn 205, được che chắn hai lần không bị truy cập trái phép từ các môđun khác trong môi trường tiêu chuẩn 205. Chuyên gia trong lĩnh vực này sẽ nhận biết được rằng các thuật toán xác nhận mới có được bố trí cho môđun quét 220 khi các lần cập nhật mới được phát triển để chỉ dẫn mã độc hoặc sự tấn công được phát hiện mới mà không chệch khỏi sáng chế. Các cập nhật này có thể được lắp đặt một cách dễ dàng trong môđun quét 220 khi môđun quét được lắp đặt trong môi trường vận hành tiêu chuẩn 205. Việc thực hiện các thuật toán xác nhận tính nguyên vẹn bởi môđun quét 220 xảy ra ở bước 310.

Sau khi chức năng xác nhận được thực hiện, các kết quả và các phản hồi xác nhận từ các lõi tương ứng, các ứng dụng và/hoặc các môđun sau đó sẽ được phản hồi lại môđun quét 220. Việc này xảy ra ở bước 315. Tất cả các phản hồi được đối chiếu trên môđun quét 220 mà sau đó diễn ra mã hoá các phản hồi đối chiếu bằng cách sử dụng khoá công cộng hoặc khoá riệng được bố trí trong môđun quét 220. Chuyên gia trong lĩnh vực này sẽ nhận biết được rằng các kỹ thuật mã hoá khác hoặc thậm chí các kỹ thuật bỏ qua có thể có khác có thể được sử dụng để mã hoá phản hồi đối chiếu mà không chệch khỏi sáng chế. Sau đó, phản hồi đối chiếu được mã hoá này được truyền đến môđun xác nhận 230 ở bước 320.

Tiếp theo, môđun xác nhận 230 sẽ xác nhận tính nguyên vẹn của môđun quét 220 bằng cách sử dụng phản hồi được mã hoá. Theo các phương án của sáng chế, nếu môđun xác nhận 230 giải mã thành công phản hồi được mã hoá, điều này có nghĩa là tính nguyên vẹn của môđun quét 220 đã không bị tổn hại do cùng một khoá và/hoặc thuật toán mã hoá được sử dụng để mã hoá phản hồi. Để giải mã phản hồi được mã hoá, môđun xác nhận 230 sẽ phải truy cập khoá công cộng/khoá riêng bảo mật từ cơ sở dữ liệu bảo mật 235. Việc này xảy ra ở bước 325.

Cơ sở dữ liệu 235 sẽ phân tích yêu cầu bởi môđun xác nhận 230 để xác định xem liệu yêu cầu này có phải là yêu cầu hợp lệ hay không, nghĩa là xem liệu

khoá bảo mật được yêu cầu này có chứa trong các bản ghi của nó hay không. Nếu khoá bảo mật được yêu cầu không sẵn có, việc này có thể khởi động báo động rằng tính nguyên vẹn của hệ thống đã bị tổn hại. Trái lại, nếu khoá bảo mật có thể được truy cập một cách thành công, khoá bảo mật này tiếp theo được chuyển đến môđun xác nhận 230 ở bước 330.

Tiếp theo, môđun xác nhận 230 sẽ sử dụng khoá bảo mật để giải mã phản hồi được mã hoá. Nếu phản hồi không thể được mã hoá hoặc nếu việc giải mã này tạo ra các kết quả không cần thiết, điều này sẽ có hàm ý rằng môđun quét 220 đã bị tổn hại và hoạt động làm giảm tiếp theo sẽ được thực hiện bởi môđun xác nhận 230. Theo các phương án của sáng chế, hoạt động làm giảm có thể bao gồm việc khoá thiết bị điện tử do đó ngăn không cho các ứng dụng khác chạy, tắt thiết bị điện tử, và/hoặc gửi báo động đến máy chủ từ xa thông báo cho máy chủ rằng hoạt động làm giảm đã được bắt đầu trên thiết bị điện tử. Chuyên gia trong lĩnh vực này sẽ nhận biết được rằng các bước giảm nhẹ khác có thể được thực hiện mà không chệch khỏi sáng chế. Theo cách khác, nếu phản hồi được giải mã thành công, điều này có nghĩa là tính nguyên vẹn của môđun quét 220 là nguyên vẹn và tiếp theo phản hồi được phân tích hơn nữa bởi môđun xác nhận 230.

Dựa vào các lệnh chứa trong đòi hỏi được tạo ra trước, môđun xác nhận 230 tiếp theo sẽ truy cập tập hợp kết quả mong đợi từ cơ sở dữ liệu bảo mật 235. Tiếp theo, các kết quả được truy cập từ cơ sở dữ liệu 235 được so với các kết quả chứa trong phản hồi được giải mã. Nếu cả hai tập hợp kết hợp phù hợp hoặc thoả mãn danh sách kiểm tra nội bộ, sau đó phản hồi được xác định là hợp lệ và tiếp theo môđun xác nhận 230 xác định rằng tính nguyên vẹn của thiết bị điện tử 100 đã không bị tổn hại. Theo cách khác, nếu kết quả không phù hoặc nếu tất cả các nội dung của danh sách kiểm tra không được đáp ứng, điều này có nghĩa là tính nguyên vẹn của thiết bị điện tử 100 đã bị huỷ hoại và hoạt động làm giảm tiếp theo cần phải được thực hiện bởi môđun xác nhận 230. Như được nêu trên đây, các hoạt động làm giảm mà có thể được thực hiện bởi môđun xác nhận 230 bao gồm, nhưng không chỉ giới hạn ở, khoá thiết bị điện tử do đó ngăn không có các ứng dụng khác chạy, tắt thiết bị điện tử, và/hoặc

gửi báo động đến máy chủ từ xa thông báo cho máy chủ rằng hoạt động làm giảm đã được bắt đầu trên thiết bị điện tử.

Theo phương án làm ví dụ của sáng chế, hệ thống của sáng chế có thể được thực hiện khi hệ thống phát hiện chống chiếm quyền điều khiển dùng cho thiết bị trong hệ thống hãy mang thiết bị của mình (Bring-Your-Own-Device-BYOD). Trong các hệ thống BYOD, người lao động được cho phép nhìn dữ liệu bảo mật của công ty bằng cách sử dụng các thiết bị điện tử của chính họ. Để đảm bảo rằng tính bảo mật của các dữ liệu này không bị huỷ hoại, công ty cần phải đảm bảo rằng thiết bị điện tử có hệ thống vận hành (OS) mà là nguyên vẹn, tức là OS đã không bị chiếm quyền điều khiển hoặc bị bẻ khoá. Tóm lại, công ty cần phải đảm bảo rằng các biện pháp bảo mật được thực hiện bởi hệ thống vận hành của thiết bị vẫn còn nguyên vẹn do đó người dùng chỉ được cấp đặc quyền điều khiển truy cập bị giới hạn.

Theo phương án này của sáng chế, hai chương trình hoặc môđun trước tiên được lắp đặt trong thiết bị điện tử khi người lao đồng chèn thiết bị của họ vào hệ thống BYOD. Chương trình hoặc môđun thứ nhất là môđun xác nhận mà cần được lắp đặt trong môi thực hiện tin cậy (rusted Execution Environment-TEE) của thiết bị hoặc môi trường bảo mật tương đương của nó và chương trình thứ hai là môđun quét mà cần được lắp đặc trong môi trường thực hiện phong phú (Rich Execution Environment-REE) của thiết bị hoặc môi trường tiêu chuẩn tương đương của nó.

Môđun xác nhận có thể chứa danh mục nhiệm vụ mà môđun xác nhận có thể yêu cầu môđun quét thực hiện, ví dụ, việc quét mã lõi, quét danh mục quy trình, kiểm tra đối với môđun SU, quét bảng trang nhớ, kiểm tra trạng thái và tham số của cơ chế bảo vệ lõi và các quy trình khác. Các nhiệm vụ này có thể được chọn bằng cách sử dụng chương trình bộ gửi yêu cầu được bố trí trong môđun xác nhận do đó chương trình này gửi yêu cầu xác nhận hoặc đòi hỏi chứa trong tập hợp đối tượng/lệnh đến môđun quét. Theo các phương án của sáng chế, chương trình gửi yêu cầu có thể được trang bị bộ định thời và bộ xử lý gọi lại chức năng, sao cho chương trinh gửi yêu cầu này có thể bắt đàu theo chu kỳ và/hoặc sau đó chức năng BYOD tốt nhất để bắt đầu.

Môđun xác nhận cũng có thể chứa khoá riêng (nó cũng có thể là khoá giải mã đối xứng) mà có thể được sử dụng bởi thuật toán nhận biết để giải mã và phê chuẩn phản hồi được gửi trở lại bởi môđun quét. Ngoài môđun nêu trên, môđun xác nhận cũng bao gồm bộ xử lý phản hồi mà được tạo cấu hình để thực hiện các hoạt động làm giảm như khoá điện thoại, tắt điện thoại và/hoặc thông báo quyền phản hồi phản hồi để thu phản hồi không hợp lệ hoặc sự giải mã không thành công phản hồi.

Môđun quét mà được lắp đặt trong môi trường REE bao gồm khoá công cộng (cũng có thể là khoá mã hoá đối xứng) mà có thể được sử dụng để mã hoá phản hồi mà cần được gửi đến môđun xác nhận và khoá công cộng có thể được bảo vệ nhờ bỏ qua và các kỹ thuật hộp trắng. Môđun quét cũng chứa tập hợp thuật toán quét mà được sử dụng để thực hiện các hướng dẫn hoặc các lệnh thu được từ môđun xác nhận và các thuật toán này cũng có thể được bỏ qua. Môđun quét cũng bao gồm thuật toán phản hồi mà sử dụng khoá công cộng để mã hoá các kết quả của các thuật toán quét trước khi gửi các kết quả được mã hoá trở lại bộ xác nhận. Theo các phương án của sáng chế, môđun quét được thực hiện như môđun hệ thống của hệ thống vận hành, ví dụ nếu hệ thống vận hành là hệ thống vận hành Android; môđun quét sẽ được thực hiện như môđun hệ thống Android mà có thể được nạp bởi lõi Android.

Theo các phương án của sáng chế, môđun xác nhận có thể được nạp một cách tự động mỗi lần thiết bị điện tử khởi động hoặc bật lên (trước hoặc ngay sau khi việc khởi động toàn bộ được nạp). Trình tự khởi động này tương tự với kỹ thuật chuỗi khởi động bảo mật đã biết trong lĩnh vực này. Sau khi môđun xác nhận đã được nạp, nó vẫn ở trong TEE của thiết bị và do đó được che chắn không bị các ứng dụng được lắp đặt trong REE nhờ phân cứng phần cứng. Điều này có nghĩa là các kẻ tấn công độc hại không thể nạp lên môđun hoặc sửa đổi các thiết lập của nó khi môđun xác nhận đang chạy. Tương tự, chuỗi khởi động bảo mật sẽ nạp môđun quét trong REE hoặc môi trường tiêu chuẩn sau khi nạp lõi trong REE. Ngay sau khi môđun quét được nạp và trước khi hệ thống vận hành được nạp, môđun quét sẽ quét lõi và gửi đến bộ xác nhận tham chiếu của lõi hiệu chỉnh. Sau đó, hệ thống vận hành trong REE được nạp và thực hiện

như thông thường.

Theo phương án khác của sáng chế, môđun xác nhận có thể được thực hiện theo chu kỳ với khoảng thời gian ngẫu nhiên nằm trong khoảng từ 5 phút đến 1 giờ. Điều này có nghĩa là môđun xác nhận sẽ yêu cầu theo chu kỳ môđun quét để thực hiện việc quét tính nguyên vẹn của hệ thống. Các bước 305-330 như được thể hiện trên Fig.3 được thực hiện trong khi quét tính nguyên vẹn của hệ thống này. Khoảng thời gian ngẫu nhiên được điều chỉnh để đạt dược sự cân bằng giữa tính năng của thiết bị và tính bảo mật của thiết bị. Để cải thiện hơn nữa hiệu quả, môđun xác nhận có thể điều chỉnh khoảng thời gian thực hiện dựa vào trạng thái hoạt động của thiết bị, trạng thái nạp điện của thiết bị, nạp làm việc CPU của thiết bị, thời gian một ngày, v.v.. Cần phải lưu ý rằng tất cả các thông tin cần thiết được yêu cầu bởi môđun xác nhận có thể thu được từ lõi và các ứng dụng chứa trong TEE hoặc môi trường bảo mật của thiết bị.

Theo phương án làm ví dụ khác của sáng chế, hệ thống của sáng chế có thể được thực hiện như hệ thống giao dịch tiền trực tuyến mà chấp thuận tính nguyên vẹn của thiết bị trước khi các ứng dụng giao dịch trực tiếp có thể được thực hiện giữa thiết bị điện tử và viện tài chính. Theo phương án này, hệ thống đảm bảo rằng dữ liệu nhạy cảm như dữ liệu tài chính chứa trong thiết bị được bảo vệ trong quá trình giao dịch trực truyến. Hơn nữa, hệ thống cũng sẽ đảm bảo rằng quá trình giao dịch thực vậy được cho phép bởi người dùng. Hơn nữa, theo phương án này, hệ thống cũng sẽ xác nhận rằng ứng dụng ghi khoá không phải đang chạy trong hệ thống của thiết bị đang nỗ lực lấy cắp mật lệnh của người dùng hoặc các thông tin nhạy cảm khác bất kỳ.

Tương tự, môđun xác nhận được lắp đặt trong môi trường thực hiện tin cậy (TEE) của thiết bị hoặc môi trường bảo mật tương đương của nó và môđun quét được lắp đặt trong môi trường thực hiện phong phú (REE) của thiết bị hoặc môi trường tiêu chuẩn tương đương của nó.

Theo phương án này, trước khi bộ nhận biết tạo ra và truyền đòi hỏi đến môđun quét, nghĩa là trước bước 305, môđun xác nhận trước tiên sẽ xác nhận tính nguyên vẹn của môđun quét. Việc này có thể được thực hiện bằng cách xác nhận tín hiệu số của môđun quét hoặc bằng cách kiểm tra nội dung của bộ nhớ

của môđun quét. Ví dụ, viện tài chính tương ứng sẽ có khoá riêng mà được sử dụng để tính toán tín hiệu số của các môđun quét được chấp thuận và môđun xác nhận sẽ có khoá công cộng tương ứng mà được sử dụng để xác nhận rằng môđun quét thực vậy hiệu chỉnh phiên bản mà đã được ký hiệu về mặt kỹ thuật số bởi ngân hàng. Thông thường, khoá công cộng được lưu trữ trong cơ sở dữ liệu bảo mật được trang bị trong TEE. Mỗi khi chương trình kết hợp với viện tài chính yêu cầu môđun quét cần được cập nhật (ví dụ, để trợ giúp chức năng mới hoặc để biên tập danh mục quy trình được cho phép, v.v.), viện tài chính sẽ giải phóng phiên bản mới của môđun quét cùng với ký hiệu số tương ứng (ví dụ, thông qua cổng trực tuyến). Tiếp theo, người dùng sẽ phải tải xuống và lắp đặt các cập nhật trên thiết bị của mình. Bộ xác nhận sẽ kiểm tra theo chu kỳ tính nguyên vẹn của môđun quét bằng cách sử dụng ký hiệu số của môđun để ngăn không cho các liệu tin bảo mật của người dùng (ví dụ, mật lệnh) bị truy nhập hoặc được chụp thông qua các chương trình/các tấn công độc hại mới. Do môđun xác nhận khó cập nhật hơn nhiều, các đối tượng phiên bản mới được bổ sung vào môđun quét theo cách sao cho môđun xác nhận ban đầu vẫn có khả năng phê chuẩn phản hồi của các hoạt động quét được cập nhật được thực hiện bởi môđun quét. Một ví dụ về cách mà việc này có thể đạt được là, các phản hồi từ môđun quét sẽ chứa các kết quả mong đợi mà đã được ký hiệu về mặt kỹ thuật số bằng cách sử dụng hoá riêng của ngân hàng.

Trong trường hợp tính nguyên vẹn của môđun quét đã bị tổn hại hoặc nếu các phản hồi được tạo ra bởi môđun quét không được phê chuẩn, nghĩa là hệ thống này đã bị huỷ hoại, môđun xác nhận sẽ thực hiện các hoạt động làm giảm như thông báo cho viện tài chính rằng tính nguyên vẹn của môđun hoặc hệ thống tương ứng đã bị tổn hại. Trong một số kịch bản, thậm chí khi thu thông báo như vậy từ thiết bị, quá trình giao dịch vẫn có thể được cho phép diễn ra nếu tiện tài chính xác định rằng nguy cơ này có thể chấp nhận được. Do đó, để cho viện tài chính thực hiện việc phân tích đánh giá mối đe doạ chính xác, môđun xác nhận cũng sẽ phải cung cấp các chi tiết về lỗi xác nhận tính nguyên vẹn, ví dụ các chi tiết về các ứng dụng mà đang chạy, các đối tượng mà không được đáp ứng, các kết quả mà được phản hồi từ môđun quét, v.v.., khi truyền

thông báo đến viện tài chính.

Theo phương án của sáng chế, phương pháp xác nhận tính nguyên vẹn hệ thống của thiết bị điện tử bao gồm bốn bước sau:

Bước 1, tạo ra, bởi môđun xác nhận được bố trí trong môi trường bảo mật trong thiết bị điện tử, đòi hỏi;

Bước 2, truyền đòi hỏi này từ môđun xác nhận đến môđun quét được bố trí trong môi trường tiêu chuẩn trong thiết bị điện tử, trong đó đòi hỏi hướng dẫn môđun quét thực hiện bước xác nhận tính nguyên vẹn trong môi trường tiêu chuẩn để tạo ra phản hồi;

Bước 3, mã hoá, bởi môđun quét, phản hồi và truyền phản hồi được mã hoá đến môđun xác nhận; và

Bước 4, xác nhận, bởi môđun xác nhận, tính nguyên vẹn của môđun quét nhờ đó đáp lại sự xác nhận rằng tính nguyên vẹn của môđun quét được xác nhận, xác định, bởi môđun xác nhận, nếu phản hồi là hợp lệ, nhờ đó đáp lại sự xác nhận rằng phản hồi là không hợp lệ, thực hiện hoạt động làm giảm.

Để tạo ra hệ thống hoặc phương pháp như vậy, quy trình cần phải xác nhận tính nguyên vẹn hệ thống của thiết bị điện tử bằng cách sử dụng môđun xác nhận được lắp đặt trong môi trường bảo mật của thiết bị và môđun quét được lắp đặt trong môi trường tiêu chuẩn của thiết bị. Phần mô tả sau và các hình vẽ Fig.4 đến Fig.6 mô tả các quy trình theo các phương án mà đề xuất các quy trình theo sáng chế.

Fig.4 minh hoạ quy trình 400 mà được thực hiện bởi môđun xác nhận được lắp đặt trong môi trường bảo mật của thiết bị điện tử để xác nhận tính nguyên vẹn hệ thống của thiết bị theo các phương án của sáng chế. Quy trình 400 bắt đầu ở bước 405 bằng cách tạo ra đòi hỏi mà cần được truyền đến môđun quét được bố trí trong môi trường tiêu chuẩn của thiết bị điện tử. Đòi hỏi sẽ chứa các hướng dẫn cụ thể mà cần được thực hiện bởi môđun quét để phê chuẩn tính nguyên vẹn của hệ thống. Một khi đòi hỏi được tạo ra, đòi hỏi sau đó được truyền và được thực hiện bởi môđun quét. Tiếp theo, quy trình 400 thu phản hồi được mã hoá từ môđun quét ở bước 410. Tiếp theo, phản hồi được giải mã bởi quy trình 400 ở bước 415. Quy trình 400 có thể giải mã phản hồi được mã hoá

bằng cách sử dụng khoá riêng và/hoặc công cộng được lưu trữ trong môđun xác nhận hoặc quy trình 400 có thể truy cập khoá bảo mật cần thiết từ cơ sở dữ liệu bảo mật được bố trí trong môi trường bảo mật. Nếu phản hồi được mã hoá không được giải mã thành công, quy trình 400 diễn ra đến bước 420 do đó quy trình 400 tiếp theo diễn ra để thực hiện các hoạt động làm giảm cần thiết. Sau đó, quy trình 400 kết thúc.

Theo cách khác, nếu phản hồi đã được giải mã thành công ở bước 415, quy trình 400 sẽ diễn ra đến bước 425. Ở bước 425, quy trình 400 sẽ sửa đổi phản hồi để xác định các dữ liệu yêu cầu hoặc dánh sách kiểm tra mà cần được truy cập từ cơ sở dữ liệu bảo mật. Tiếp theo, quy trình 400 sẽ so sánh dữ liệu được truy cập với dữ liệu chứa trong phản hồi được giải mã để xác định tính hợp lệ của phản hồi. Việc này xảy ra ở bước 430. Nếu quy trình 400 xác định rằng phản hồi là hợp lệ, điều này có nghĩa là tính nguyên vẹn của hệ thống là nguyên vẹn và quy trình 400 diễn ra đến bước A. Trái lại, nếu phản hồi được xác định là không hợp lệ, quy trình 400 diễn ra đến bước 420 để thay thế do đó hoạt động làm giảm được thực hiện bởi quy trình 400. Tiếp theo, quy trình 400 kết thúc.

Theo phương án khác của sáng chế, nếu môđun xác nhận thu sự biểu thị ở bước A mà thiết bị điện tử đã được tắt và đang bật lên (nghĩa là, khởi động), môđun xác nhận trước tiên sẽ bắt đầu, trước khi các quy trình khác bất kỳ được thực hiện và sẽ thực hiện quy trình 400. Tiếp theo, quy trình 400 sẽ khiến cho các bước 405-430 cần được lặp lại trước khi lõi hoặc hệ thống vận hành trong môi trường tiêu chuẩn có thể được bắt đầu. Theo phương án khác nữa của sáng chế, ở bước A, sau khi khoảng thời gian thiết lập lại hoặc khoảng thời gian đã trôi qua, quy trình 400 sẽ khiến cho các bước 405-430 cần được lặp lại để xác nhận tính nguyên vẹn hệ thống của thiết bị điện tử.

Theo phương án khác của sáng chế, trước khi bước 400 tạo ra đòi hỏi ở bước 405, quy trình 400 thứ nhất sẽ xác nhận tính nguyên vẹn của môđun quét mà được lắp đặt trong môi trường tiêu chuẩn. Bước xác nhận trước đòi hỏi này diễn ra ở bước B trên Fig.4. Fig.5 minh hoạ quy trình 500 mà được thực hiện bởi môđun xác nhận để xác nhận tính nguyên vẹn của môđun quét theo các

phương án của sáng chế. Quy trình 500 bắt đầu ở bước 505 do đó yêu cầu đáp lại sự xác nhận được tạo ra. Yêu cầu đáp lại sự xác nhận sẽ khiến cho môđun quét tạo ra phản hồi được mã hoá bằng cách sử dụng khoá bảo mật (ví dụ khoá riêng hoặc công cộng) đã biết đối với cả bộ xác nhận và môđun quét. Một khi yêu cầu được tạo ra, yêu cầu sẽ được truyền đến môđun quét. Sau đó, môđun quét sẽ thực hiện các hướng dẫn chứa trong yêu cầu thu đượ. Tiếp theo, quy trình 500 thu sự đáp lại sự xác nhận được mã hoá từ môđun quét ở bước 510. Tiếp theo, quy trình 500 diễn ra để phê chuẩn sự đáp lại thu được ở bước 515. Sự phê chuẩn phản hồi có thể bao gồm việc mã hoá phản hồi được mã hoá do đó nếu phản hồi được giải mã thành công, việc này ngụ ý là quy trình 500 mà phản hồi là hợp lệ. Trái lại, nếu phản hồi không thể được giải mã thành công, việc này biểu thị rằng phản hồi không hợp lệ. Nếu phản hồi được xác định bởi quy trình 500 để là hợp lệ ở bước 515, sau đó quy trình 500 kết thúc. Tuy nhiên, nếu phản hồi được xác định để là không hợp lệ ở bước 515, quy trình 500 sẽ diễn ra đến bước 520 do đó các hoạt động làm giảm sẽ được thực hiện. Sau đó, quy trình 500 kết thúc.

Fig.6 minh hoạ quy trình 600 mà được thực hiện bởi môđun quét được lắp đặt trong môi trường tiêu chuẩn của thiết bị điện tử để tạo ra phản hồi được mã hoá để xcas nhận môđun quét và tính nguyên vẹn của thiết bị điện tử theo các phương án của sáng chế. Quy trình 600 bắt đầu ở bước 605 do đó quy trình 600 thu đòi hỏi từ môđun xác nhận. Để lắp mới, đòi hỏi sẽ có tất cả các bước xác nhận mà cần được thực hiện bởi quy trình 600. Tiếp theo, quy trình 600 diễn ra để thực hiện tất cả các chức năng xác nhận như được biểu thị trong đòi hỏi ở bước 610. Sau khi mỗi chức năng đã hoàn thành, quy trình 600 sẽ đối chiếu phản hồi được tạo ra đối với mỗi chức năng cụ thể và đối chiếu tất cả các phản hồi thành một phản hồi duy nhất. Tiếp theo, các phản hồi duy nhất được mã hoá bằng cách sử dụng khoá bảo mật (ví dụ, khoá riêng hoặc khoá công cộng) ở bước 615. Tiếp theo, phản hồi được mã hoá này được truyền đến môđun xác nhận ở bước 620 và tiếp theo quy trình 600 kết thúc.

Hệ thống và quy trình theo các phương án của sáng chế đã được mô tả trên đây như được nêu trong các điểm yêu cầu bảo hộ sau. Cần phải hiểu rằng

các phương án khác có thể và sẽ được tạo ra đều nằm trong phạm vi bảo hộ của sáng chế.

YÊU CẦU BẢO HỘ

1. Phương pháp xác nhận tính nguyên vẹn hệ thống của thiết bị điện tử, trong đó phương pháp bao gồm các bước:

tạo, bằng môđun xác nhận được đặt trong môi trường bảo mật trong thiết bị điện tử, đòi hỏi;

truyền đòi hỏi từ môđun xác nhận đến môđun quét được đặt trong môi trường bình thường trong thiết bị điện tử;

thực thi, bằng môđun quét, chức năng xác nhận tính nguyên vẹn trong môi trường bình thường để tạo đáp ứng, trong đó môđun quét được ra lệnh bởi đòi hỏi để thực thi chức năng xác nhận tính nguyên vẹn;

mật mã hóa, bằng môđun quét, sự đáp lại và truyền đáp lại được mật mã hóa đến môđun xác nhận; và

xác nhận, bằng môđun xác nhận, tính nguyên vẹn của môđun quét;

xác định, đáp lại việc xác định rằng tính nguyên vẹn của môđun quét được xác nhận, bằng môđun xác nhận, liệu sự đáp lại là hợp lệ; và

thực hiện, đáp lại việc xác định rằng sự đáp lại là không hợp lệ, hoạt động làm giảm.

2. Phương pháp theo điểm 1, trong đó việc xác nhận tính nguyên vẹn của môđun quét bao gồm bước:

giải mật mã, bằng môđun xác nhận, đáp lại được mật mã hóa, và đáp lại việc giải mật mã thành công sự đáp lại được mật mã hóa, xác nhận tính nguyên vẹn của môđun quét.

3. Phương pháp theo điểm 1 hoặc 2, trong đó chức năng xác nhận bao gồm ít nhất một trong:

quét mã lõi;

quét danh mục xử lý;

quét bảng trang nhớ; và

kiểm tra trạng thái và tham số của cơ cấu bảo vệ lõi.

4. Phương pháp theo điểm bất kỳ trong số các điểm từ 1 đến 3 trong đó việc xác định liệu sự đáp lại là hợp lệ bao gồm bước:

so khớp sự đáp lại với dữ liệu được chứa trong cơ sở dữ liệu bảo mật được đặt trong môi trường bảo mật, trong đó khi không tìm thấy so khớp, sự đáp lại được xác định là không hợp lệ.

5. Phương pháp theo điểm bất kỳ trong số các điểm từ 1 đến 4, trong đó trước bước tạo đòi hỏi nhờ sử dụng môđun xác nhận, phương pháp bao gồm bước:

xác nhận, bằng môđun xác nhận, tính toàn vẹn của môđun quét được đặt trong môi trường bình thường.

6. Phương pháp theo điểm 5 trong đó việc xác nhận tính nguyên vẹn của môđun quét được đặt trong môi trường bình thường bao gồm các bước:

tạo, bằng môđun xác nhận, yêu cầu đáp lại xác nhận và truyền yêu cầu đáp lại xác nhận từ môđun xác nhận đến môđun quét, trong đó yêu cầu đáp lại xác nhận ra lệnh môđun quét tạo đáp ứng xác nhận được mật mã hóa, và truyền đáp ứng xác nhận được mật mã hóa đến môđun xác nhận;

xác định, bằng môđun xác nhận, liệu đáp ứng xác nhận được mật mã hóa là hợp lệ; và

thực hiện, đáp lại việc xác định rằng sự đáp lại là không hợp lệ, hoạt động làm giảm.

7. Phương pháp theo điểm 6, trong đó việc xác định liệu đáp ứng xác nhận được mật mã hóa là hợp lệ bao gồm các bước:

giải mật mã, bằng môđun xác nhận, đáp ứng xác nhận được mật mã hóa;

so khớp, đáp lại việc xác định rằng đáp ứng xác nhận được giải mã, đáp ứng xác nhận được giải mã với dữ liệu xác nhận được chứa trong cơ sở dữ liệu bảo mật được đặt trong môi trường bảo mật, trong đó khi không tìm thấy so khớp, đáp ứng xác nhận được xác định là không hợp lệ.

8. Phương pháp theo điểm bất kỳ trong số các điểm từ 1 đến 7, trong đó hoạt động làm giảm bao gồm:

ngăn ngừa thực thi các môđun phần mềm được đặt trong môi trường bình thường.

9. Phương pháp theo điểm bất kỳ trong số các điểm từ 1 đến 8, trong đó môi trường bảo mật trong thiết bị điện tử bao gồm bộ xử lý ảo thế giới bảo mật cho thiết bị điện tử, môi trường bình thường trong thiết bị điện tử bao gồm bộ xử lý ảo thế giới thông thường cho thiết bị điện tử, và môi trường bảo mật là phần cứng được cô lập khỏi môi trường bình thường.

10. Phương pháp theo điểm bất kỳ trong số các điểm từ 1 đến 9, trong đó phương pháp còn bao gồm:

xác định liệu khoảng thời gian định trước đã trôi qua; và

lặp lại phương pháp xác nhận tính toàn vẹn hệ thống của thiết bị điện tử khi khoảng thời gian định trước đã trôi qua.

11. Hệ thống xác nhận tính toàn vẹn hệ thống của thiết bị điện tử, hệ thống bao gồm:

khối xử lý có môi trường bảo mật và môi trường bình thường; và

vật ghi máy tính đọc được bất biến bởi khối xử lý, vật ghi lưu trữ lệnh trên khối xử lý khiến khối xử lý:

tạo đòi hỏi nhờ sử dụng môđun xác nhận được đặt trong môi trường bảo mật;

truyền đòi hỏi từ môđun xác nhận đến môđun quét được đặt trong môi trường bình thường;

thực thi, chức năng xác nhận tính nguyên vẹn nhờ sử dụng máy quét trong môi trường bình thường để tạo đáp ứng, trong đó máy quét được ra lệnh bởi đòi hỏi để thực thi chức năng xác nhận tính nguyên vẹn;

mật mã hóa sự đáp lại nhờ sử dụng môđun quét, và truyền đáp lại được mật mã hóa đến môđun xác nhận; và

xác nhận tính toàn vẹn của môđun quét nhờ sử dụng môđun xác nhận, nhờ đó đáp lại việc xác định rằng tính nguyên vẹn của môđun quét được xác nhận, để xác định sử dụng môđun xác nhận liệu sự đáp lại là hợp lệ, nhờ đó đáp lại việc xác định rằng sự đáp lại là không hợp lệ, để thực hiện hoạt động làm giảm.

12. Hệ thống theo điểm 11, trong đó các lệnh xác nhận tính nguyên vẹn của môđun quét bao gồm:

các lệnh ra lệnh khối xử lý:

giải mật mã đáp lại được mật mã hóa nhờ sử dụng môđun xác nhận, nhờ đó đáp lại việc giải mật mã thành công đáp lại được mật mã hóa, để xác nhận tính nguyên vẹn của môđun quét.

13. Hệ thống theo điểm 11 hoặc 12, trong đó chức năng xác nhận bao gồm:

các lệnh ra lệnh khối xử lý:

quét mã lõi;

quét danh mục xử lý;

quét bảng trang nhớ; và

kiểm tra trạng thái và tham số của cơ cấu bảo vệ lõi.

14. Hệ thống theo điểm bất kỳ trong số các điểm từ 11 đến 13, trong đó các lệnh để xác định nếu sự đáp lại là hợp lệ bao gồm:

các lệnh ra lệnh khối xử lý:

so khớp sự đáp lại với dữ liệu được chứa trong cơ sở dữ liệu bảo mật được đặt trong môi trường bảo mật, trong đó khi không tìm thấy so khớp, sự đáp lại được xác định là không hợp lệ.

15. Hệ thống theo điểm bất kỳ trong số các điểm từ 11 đến14 trong đó trước khi các lệnh tạo đòi hỏi nhờ sử dụng môđun xác nhận, các lệnh bao gồm:

các lệnh ra lệnh khối xử lý:

xác nhận tính toàn vẹn của môđun quét được đặt trong môi trường bình thường nhờ sử dụng môđun xác nhận được đặt trong môi trường bảo mật.

16. Hệ thống theo điểm 15 trong đó các lệnh để xác nhận tính nguyên vẹn của môđun quét được đặt trong môi trường bình thường bao gồm: các lệnh ra lệnh khối xử lý: tạo yêu cầu đáp lại xác nhận nhờ sử dụng môđun xác nhận và truyền yêu cầu đáp lại xác nhận từ môđun xác nhận đến môđun quét, trong đó yêu cầu đáp lại xác nhận ra lệnh môđun quét tạo đáp ứng xác nhận được mật mã hóa, và truyền đáp ứng xác nhận được mật mã hóa đến môđun xác nhận; và xác định liệu đáp ứng xác nhận được mật mã hóa là hợp lệ nhờ sử dụng môđun xác nhận, nhờ đó đáp lại việc xác định rằng sự đáp lại là không hợp lệ, để thực hiện hoạt động làm giảm.

17. Hệ thống theo điểm 16, trong đó các lệnh để xác định nếu đáp ứng xác nhận được mật mã hóa là hợp lệ bao gồm: các lệnh ra lệnh khối xử lý: giải mật mã đáp ứng xác nhận được mật mã hóa nhờ sử dụng môđun xác nhận, nhờ đó đáp lại việc xác định rằng đáp ứng xác nhận được giải mã, để so khớp đáp ứng xác nhận được giải mã với dữ liệu xác nhận được chứa trong cơ sở dữ liệu bảo mật được đặt trong môi trường bảo mật, trong đó khi không tìm thấy so khớp, đáp ứng xác nhận được xác định là không hợp lệ.

18. Hệ thống theo điểm bất kỳ trong số các điểm từ 11 đến 17, trong đó hoạt động làm giảm bao gồm: các lệnh ra lệnh khối xử lý ngăn ngừa thực thi của các môđun phần mềm được đặt trong môi trường bình thường.

19. Hệ thống theo điểm bất kỳ trong số các điểm từ 11 đến 18, trong đó môi trường bảo mật trong thiết bị điện tử bao gồm bộ xử lý ảo thế giới bảo mật cho thiết bị điện tử, môi trường bình thường trong thiết bị điện tử bao gồm bộ xử lý ảo thế giới thông thường cho thiết bị điện tử, và môi trường bảo mật là phần cứng được cô lập khỏi môi trường bình thường.

20. Hệ thống theo điểm bất kỳ trong số các điểm từ 11 đến 19, trong đó hệ thống còn bao gồm: các lệnh ra lệnh khối xử lý: xác định liệu khoảng thời gian định trước đã trôi qua; và lặp lại hệ thống để xác nhận tính toàn vẹn hệ thống của thiết bị điện tử khi khoảng thời gian định trước đã trôi qua.

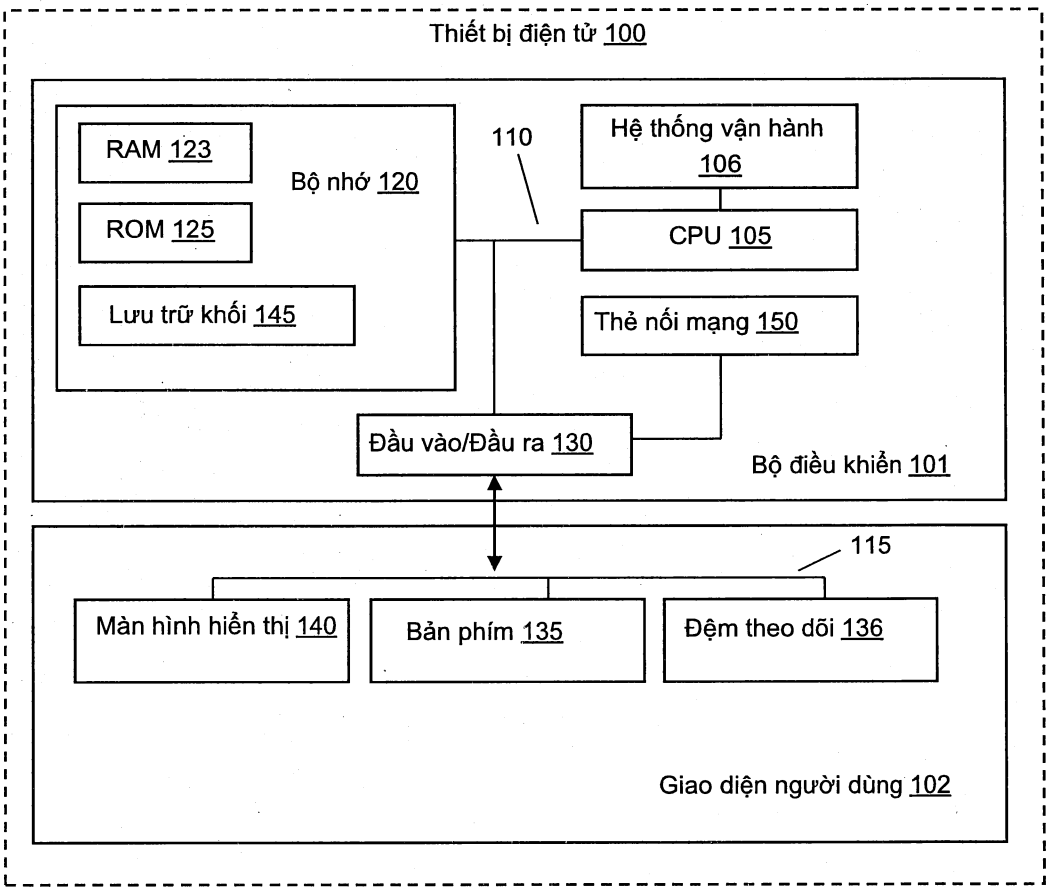

Thiết bị điện tử 100
RAM 123
ROM 125
Lưu trữ khối 145
Bộ nhớ 120
110
Hệ thống vận hành 106
CPU 105
Thẻ nối mạng 150
Đầu vào/Đầu ra 130
Bộ điều khiển 101
115
Màn hình hiển thị 140
Bản phím 135
Đệm theo dõi 136
Giao diện người dùng 102

Fig.1

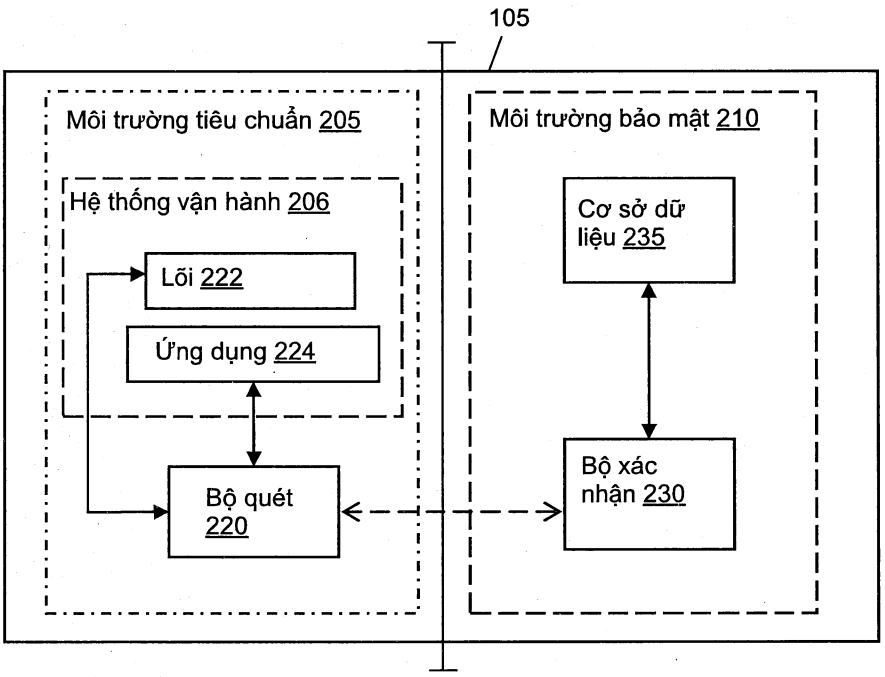

105
Môi trường tiêu chuẩn 205
Môi trường bảo mật 210
Hệ thống vận hành 206
Lõi 222
Ứng dụng 224
Bộ quét 220
Cơ sở dữ liệu 235
Bộ xác nhận 230

Fig.2

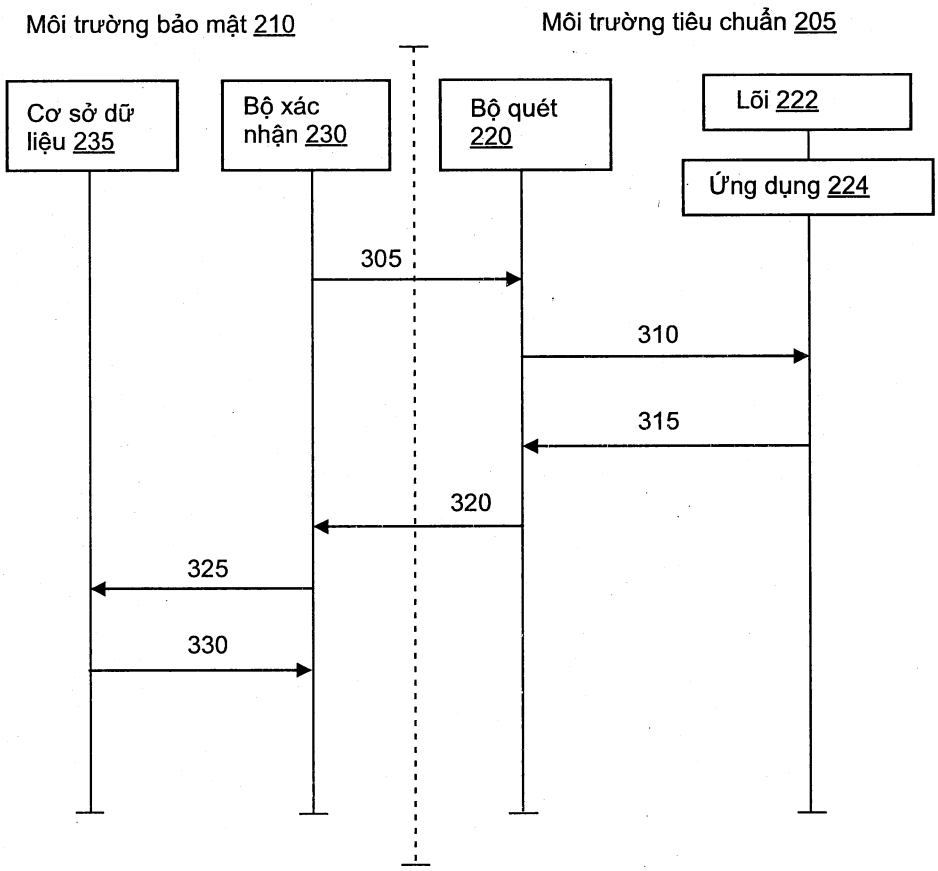

Môi trường bảo mật 210
Môi trường tiêu chuẩn 205
Cơ sở dữ liệu 235
Bộ xác nhận 230
Bộ quét 220
Lõi 222
Ứng dụng 224
305
310
315
320
325
330

Fig.3

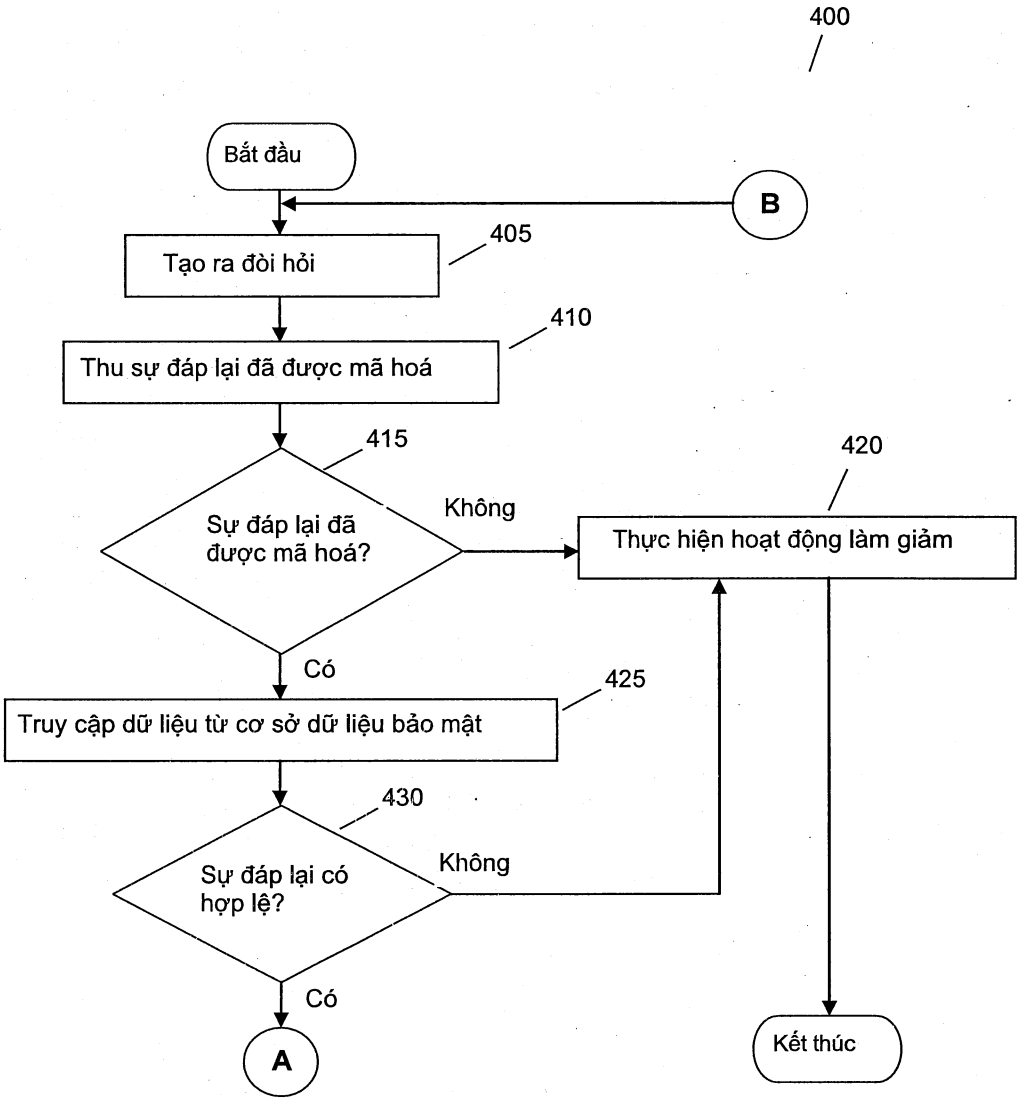

400
Bắt đầu
B
405
Tạo ra đòi hỏi
410
Thu sự đáp lại đã được mã hoá
415
Sự đáp lại đã được mã hoá?
Không
420
Thực hiện hoạt động làm giảm
Có
425
Truy cập dữ liệu từ cơ sở dữ liệu bảo mật
430
Sự đáp lại có hợp lệ?
Không
Có
A
Kết thúc

Fig.4

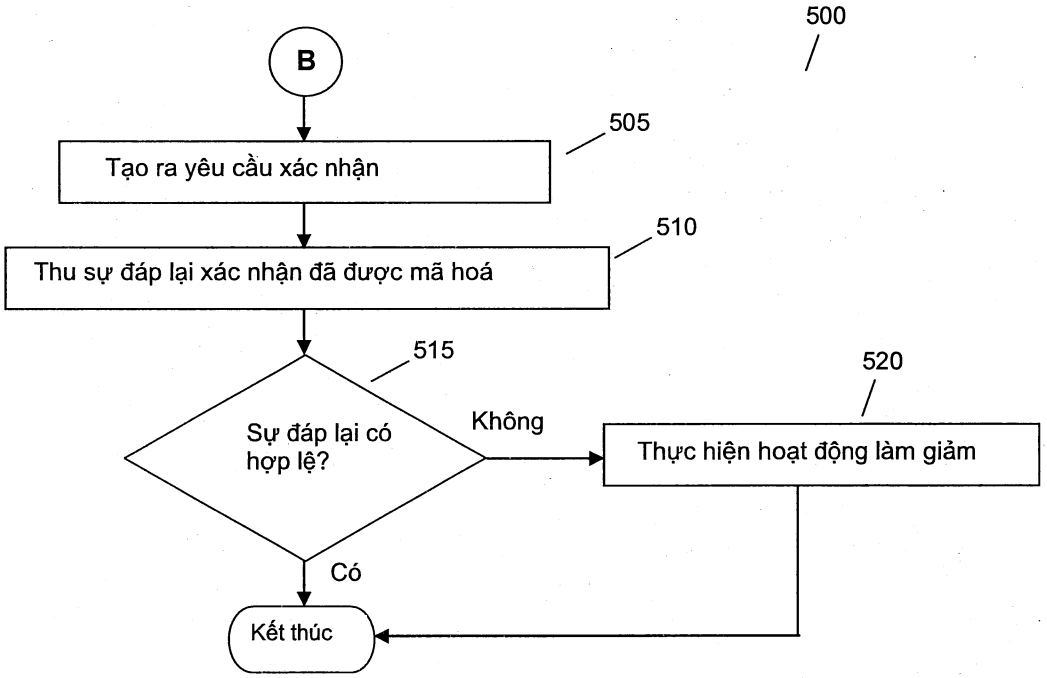

500
B
505
Tạo ra yêu cầu xác nhận
510
Thu sự đáp lại xác nhận đã được mã hoá
515
Sự đáp lại có hợp lệ?
Không
520
Thực hiện hoạt động làm giảm
Có
Kết thúc

Fig.5

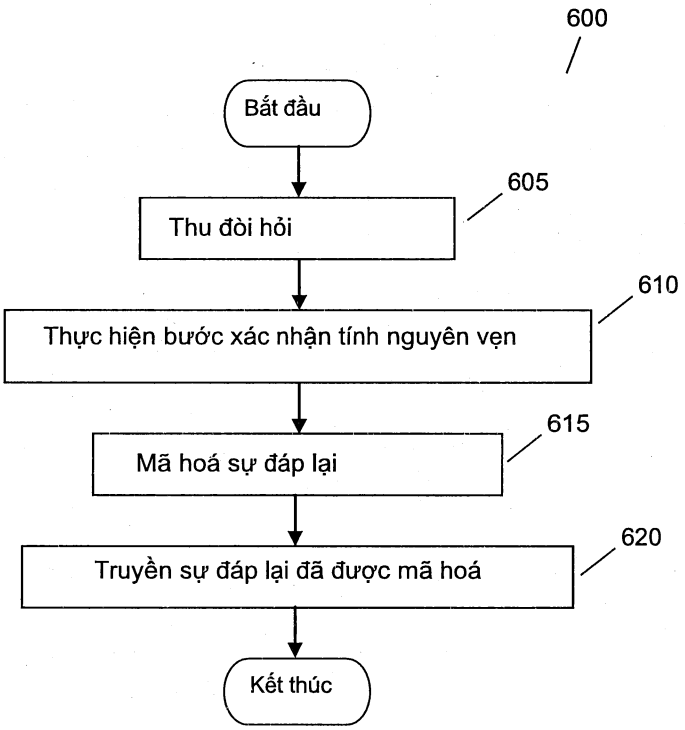

600
Bắt đầu
605
Thu đòi hỏi
610
Thực hiện bước xác nhận tính nguyên vẹn
615
Mã hoá sự đáp lại
620
Truyền sự đáp lại đã được mã hoá
Kết thúc

Fig.6