(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) **1-0025918**

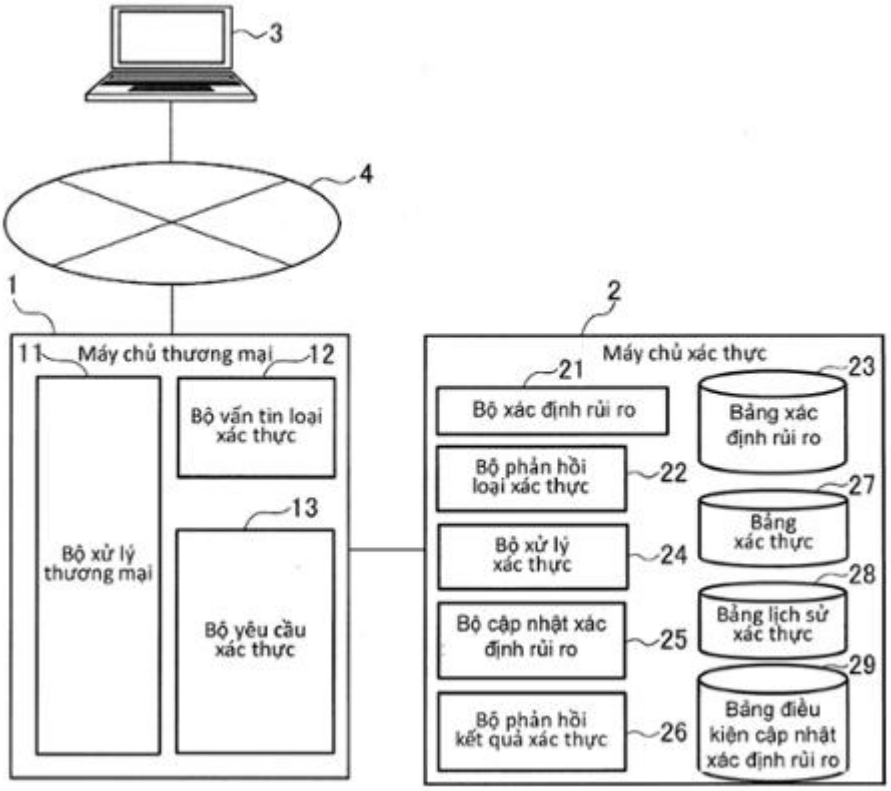
(51)[7] **G06F 21/31**; G09C 1/00

(13) **B**

(21) 1-2016-03782
(22) 09/12/2014
(86) PCT/JP2014/082492 09/12/2014
(87) WO 2015/136800 A1 17/09/2015
(30) 2014-050476 13/03/2014 JP
(45) 26/10/2020 391
(43) 27/02/2017 347A
(73) HITACHI, LTD. (JP)
6-6, Marunouchi 1-chome, Chiyoda-ku, Tokyo 1008280, Japan
(72) NAKAYAMA, Masahiro (JP); MIYAZAKI, Yoshinori (JP); HATANAKA, Hiroyuki (JP).
(74) Công ty TNHH một thành viên Sở hữu trí tuệ VCCI (VCCI-IP CO.,LTD)

(54) HỆ THỐNG XÁC THỰC

(57) Sáng chế đề cập đến thiết bị xác thực, hệ thống xác thực và phương pháp xác thực để cập nhật điều kiện xác định rủi ro dựa vào yêu cầu xác thực khả nghi. Thiết bị xác thực (2) bao gồm: bảng xác định rủi ro (23) để lưu giữ điều kiện xác định rủi ro; bộ xác định (21) để nhận thông tin truy cập của người dùng và truy vấn về loại xác thực từ thiết bị thương mại (1), mà xác định mức rủi ro dựa vào thông tin truy cập và điều kiện xác định rủi ro, và nhận dạng loại xác thực dựa vào mức rủi ro; bộ phản hồi (22) để phản hồi lại thiết bị thương mại (1) về loại xác thực được nhận dạng; bộ xử lý xác thực (24) để nhận mật khẩu người dùng nhập vào và yêu cầu xác thực từ thiết bị thương mại (1) và thực hiện quy trình xác thực người dùng dựa vào mật khẩu người dùng nhập vào; bộ phản hồi (26) để phản hồi lại thiết bị thương mại (1) về kết quả xác thực; bảng điều kiện cập nhật (29) để lưu giữ điều kiện cập nhật để cập nhật điều kiện xác định rủi ro; và bộ cập nhật (25) để cập nhật điều kiện xác định rủi ro khi yêu cầu xác thực từ thiết bị thương mại (1) thỏa mãn điều kiện cập nhật.


3
4
1
2
11
Máy chủ thương mại
12
Bộ vấn tin loại xác thực
13
Bộ xử lý thương mại
Bộ yêu cầu xác thực
Máy chủ xác thực
21
Bộ xác định rủi ro
23
Bảng xác định rủi ro
Bộ phản hồi loại xác thực
22
27
Bảng xác thực
Bộ xử lý xác thực
24
28
Bảng lịch sử xác thực
Bộ cập nhật xác định rủi ro
25
29
Bảng điều kiện cập nhật xác định rủi ro
Bộ phản hồi kết quả xác thực
26

Lĩnh vực kỹ thuật được đề cập

Sáng chế đề cập đến thiết bị xác thực, hệ thống xác thực và phương pháp xác thực để thực hiện việc xác thực người dùng trong hệ thống trực tuyến hoặc tương tự và, cụ thể là, đề cập đến thiết bị xác thực, hệ thống xác thực và phương pháp xác thực để thực hiện việc xác thực trên cơ sở rủi ro.

Tình trạng kỹ thuật của sáng chế

Các dịch vụ mua đồ và thực hiện các giao dịch chuyển tiền ở các cơ sở tài chính ví dụ như các ngân hàng thông qua Internet đã được cung cấp. Thông thường, phương pháp xác thực người dùng bằng cách nhận ID và mật khẩu từ người dùng đã được ứng dụng. Tuy nhiên, các mật khẩu dễ dàng bị chặn bởi bên thứ ba và ẩn chứa rủi ro cao về việc lộ thông tin cá nhân với người phá hoại. Do đó, các kỹ thuật đã được đề xuất để cải thiện khả năng xác thực bằng cách kết hợp phương pháp xác thực dựa vào mật khẩu với phương pháp xác thực sử dụng thông tin sinh học, phương pháp xác thực sử dụng thẻ IC, phương pháp xác thực sử dụng thẻ cứng, và các phương pháp tương tự.

Phương pháp xác thực trên cơ sở rủi ro được đề xuất, phương pháp này xác định danh tính của người dùng bằng cách thu thập thông tin ví dụ như các loại OS và trình duyệt, địa chỉ IP, vị trí sử dụng, và khe thời gian truy cập của thiết bị đầu cuối nguồn truy cập và phân tích và mô hình hóa các mẫu hành vi rời rạc của người dùng. Bằng phương pháp xác thực trên cơ sở rủi ro này, mẫu hành vi của người dùng được phân tích dựa vào biểu đồ truy cập tại thời điểm đăng nhập và tương tự, giá trị rủi ro của mỗi giao dịch chuyển tiền được tính toán, và phương pháp xác thực hoặc khả năng xác thực được thay đổi theo mức rủi ro dựa vào chính sách của nhà cung cấp dịch vụ.

Đối với hệ thống xác thực áp dụng phương pháp xác thực trên cơ sở rủi ro nêu trên, tài liệu sáng chế 1 bộc lộ hệ thống xác thực trong đó các máy chủ thương mại của nhiều doanh nghiệp chia sẻ một máy chủ xác thực mà thực hiện

việc xác thực trên cơ sở rủi ro.

Tài liệu sáng chế 2 bộc lộ hệ thống xác thực trên cơ sở rủi ro bao gồm: máy chủ xác thực để thực hiện việc phân tích quy tắc, phân tích hành vi, và ứng dụng chính sách theo quy tắc xác thực và để đánh giá mức rủi ro của truy cập đích; và máy chủ dò thông tin về rủi ro mà thường xuyên thu thập thông tin về rủi ro trên Internet từ máy chủ bên ngoài và cập nhật quy tắc xác thực trên máy chủ xác thực dựa vào thông tin về rủi ro thu thập được, trong đó kết quả đánh giá mức rủi ro được thay đổi theo sự thay đổi của thông tin về rủi ro và, theo đó, mức xác thực của việc thực hiện xác thực bổ sung được thay đổi.

Danh mục tài liệu trích dẫn

Tài liệu sáng chế

Tài liệu sáng chế 1: Đơn sáng chế Nhật Bản số 2011-215753

Tài liệu sáng chế 2: Sáng chế Nhật Bản số 5191376

Vấn đề cần được giải quyết bởi sáng chế

Với hệ thống xác thực trên cơ sở rủi ro thông thường được mô tả ở trên, quy tắc xác thực không được cập nhật chỉ trừ khi thông tin mới về rủi ro được thu thập từ máy chủ bên ngoài. Do đó, ngay cả khi có yêu cầu xác thực mà bị nghi ngờ cao là giả mạo hoặc tương tự, yêu cầu xác thực không thể ngay lập tức được phản chiếu trong quy tắc xác thực (điều kiện xác định rủi ro).

Bản chất kỹ thuật của sáng chế

Sáng chế được tạo ra để giải quyết các vấn đề nêu trên và mục đích của sáng chế là đề xuất thiết bị xác thực, hệ thống xác thực và phương pháp xác thực mà cập nhật điều kiện xác định rủi ro dựa vào yêu cầu xác thực khả nghi.

Cách thức giải quyết vấn đề

Thiết bị xác thực theo phương án thứ nhất bao gồm: bảng xác định rủi ro mà lưu giữ điều kiện xác định rủi ro để tính toán mức rủi ro của việc truy cập từ người dùng đến thiết bị thương mại; bộ xác định để nhận thông tin truy cập của

người dùng và truy vấn về loại xác thực từ thiết bị thương mại, mà xác định mức rủi ro của việc truy cập dựa vào thông tin truy cập và điều kiện xác định rủi ro, và nhận dạng loại xác thực đối với người dùng dựa vào mức rủi ro; bộ phản hồi thứ nhất để phản hồi lại thiết bị thương mại về loại xác thực được nhận dạng bởi bộ xác định; bộ xử lý xác thực để nhận mật khẩu người dùng nhập vào theo loại xác thực và yêu cầu xác thực từ thiết bị thương mại và thực hiện quy trình xác thực người dùng dựa vào mật khẩu người dùng nhập vào; bộ phản hồi thứ hai để phản hồi lại thiết bị thương mại về kết quả xác thực bằng bộ xử lý xác thực; bảng điều kiện cập nhật mà lưu giữ điều kiện cập nhật để cập nhật điều kiện xác định rủi ro; và bộ cập nhật để cập nhật điều kiện xác định rủi ro khi yêu cầu xác thực từ thiết bị thương mại thỏa mãn điều kiện cập nhật.

Tốt hơn là, thiết bị xác thực theo phương án thứ nhất ngoài ra còn bao gồm bảng lịch sử xác thực để lưu giữ yêu cầu xác thực được nhận từ thiết bị thương mại và kết quả xác thực tương ứng với yêu cầu xác thực, trong đó bộ cập nhật so sánh các yêu cầu xác thực và các kết quả xác thực được lưu giữ trong bảng lịch sử xác thực với điều kiện cập nhật.

Tốt hơn là, trong thiết bị xác thực theo phương án thứ nhất, điều kiện xác định rủi ro bao gồm danh sách địa chỉ IP mô tả ít nhất một địa chỉ IP, thông tin truy cập bao gồm địa chỉ IP của người dùng, yêu cầu xác thực bao gồm ID người dùng và địa chỉ IP của người dùng, bộ xác định phát hiện xem địa chỉ IP được bao gồm trong thông tin truy cập có được mô tả trong danh sách địa chỉ IP hay không và, khi địa chỉ IP được mô tả, tính toán mức rủi ro cao hơn so với khi địa chỉ IP không được mô tả, và khi một số lượng định trước các yêu cầu xác thực hoặc nhiều hơn với cùng một địa chỉ IP và các ID người dùng khác nhau được lưu giữ trong bảng lịch sử xác thực trong một khoảng thời gian định trước, bộ cập nhật bổ sung địa chỉ IP vào danh sách địa chỉ IP.

Tốt hơn là, thiết bị xác thực theo phương án thứ nhất ngoài ra còn bao gồm bộ xác định thứ hai để tìm kiếm bảng xác định rủi ro dựa vào ID người dùng được bao gồm trong yêu cầu xác thực, trong đó điều kiện xác định rủi ro

bao gồm danh sách ID người dùng mô tả ít nhất một ID người dùng, yêu cầu xác thực bao gồm các nội dung xử lý được yêu cầu bởi người dùng, bộ xác định thứ hai phát hiện xem ID người dùng được bao gồm trong yêu cầu xác thực có được mô tả trong danh sách ID người dùng hay không và, khi ID người dùng được mô tả, thông báo bộ xử lý xác thực, bộ xử lý xác thực xác định kết quả xác thực là thất bại dựa vào thông báo từ bộ xác định thứ hai, và khi một số lượng định trước các yêu cầu xác thực hoặc nhiều hơn với các nội dung xử lý định trước và cùng một ID người dùng được lưu giữ trong bảng lịch sử xác thực trong một khoảng thời gian định trước, bộ cập nhật bổ sung ID người dùng vào danh sách ID người dùng.

Hệ thống xác thực theo phương án thứ hai bao gồm: thiết bị xác thực thứ nhất để nhận thông tin truy cập thứ nhất của người dùng và truy vấn về loại xác thực từ thiết bị thương mại thứ nhất, xác định mức rủi ro thứ nhất của việc truy cập từ người dùng đến thiết bị thương mại thứ nhất, nhận dạng loại xác thực đối với người dùng dựa vào mức rủi ro thứ nhất và phản hồi lại thiết bị thương mại thứ nhất, nhận mật khẩu người dùng nhập vào theo loại xác thực và yêu cầu xác thực từ thiết bị thương mại thứ nhất, thực hiện quy trình xác thực người dùng dựa vào mật khẩu người dùng nhập vào, và phản hồi lại thiết bị thương mại thứ nhất về kết quả xác thực; thiết bị xác thực thứ hai để nhận thông tin truy cập thứ hai của người dùng và truy vấn về loại xác thực từ thiết bị thương mại thứ hai, xác định mức rủi ro thứ hai của việc truy cập từ người dùng đến thiết bị thương mại thứ hai, nhận dạng loại xác thực đối với người dùng dựa vào mức rủi ro thứ hai và phản hồi lại thiết bị thương mại thứ hai, nhận mật khẩu người dùng nhập vào theo loại xác thực và yêu cầu xác thực từ thiết bị thương mại thứ hai, thực hiện quy trình xác thực người dùng dựa vào mật khẩu người dùng nhập vào, và phản hồi lại thiết bị thương mại thứ hai về kết quả xác thực; và bảng xác định rủi ro thông thường mà lưu giữ điều kiện xác định rủi ro thông thường để tính toán mức rủi ro của việc truy cập từ người dùng đến thiết bị thương mại thứ nhất hoặc thiết bị thương mại thứ hai, trong đó thiết bị xác thực thứ nhất bao gồm bảng điều kiện cập nhật thứ nhất lưu giữ điều kiện cập nhật thứ nhất để cập nhật

điều kiện xác định rủi ro thông thường, xác định mức rủi ro thứ nhất dựa vào thông tin truy cập thứ nhất và điều kiện xác định rủi ro thông thường, và cập nhật điều kiện xác định rủi ro thông thường khi yêu cầu xác thực từ thiết bị thương mại thứ nhất thỏa mãn điều kiện cập nhật thứ nhất, và thiết bị xác thực thứ hai bao gồm bảng điều kiện cập nhật thứ hai lưu giữ điều kiện cập nhật thứ hai để cập nhật điều kiện xác định rủi ro thông thường, xác định mức rủi ro thứ hai dựa vào thông tin truy cập thứ hai và điều kiện xác định rủi ro thông thường, và cập nhật điều kiện xác định rủi ro thông thường khi yêu cầu xác thực từ thiết bị thương mại thứ hai thỏa mãn điều kiện cập nhật thứ hai.

Tốt hơn là, trong hệ thống xác thực theo phương án thứ hai, thiết bị xác thực thứ nhất bao gồm bảng xác định rủi ro riêng lẻ lưu giữ điều kiện xác định rủi ro riêng lẻ để tính toán mức rủi ro của việc truy cập từ người dùng đến thiết bị thương mại thứ nhất, bảng điều kiện cập nhật thứ nhất lưu giữ điều kiện cập nhật thứ ba để cập nhật điều kiện xác định rủi ro riêng lẻ, và thiết bị xác thực thứ nhất cập nhật điều kiện xác định rủi ro riêng lẻ khi yêu cầu xác thực từ thiết bị thương mại thứ nhất thỏa mãn điều kiện cập nhật thứ ba.

Phương pháp xác thực theo phương án thứ ba là phương pháp xác thực bằng thiết bị xác thực bao gồm bảng xác định rủi ro để lưu giữ điều kiện xác định rủi ro để tính toán mức rủi ro của việc truy cập từ người dùng đến thiết bị thương mại, bộ xác định, bộ phản hồi thứ nhất, bộ xử lý xác thực, bộ phản hồi thứ hai, bảng điều kiện cập nhật mà lưu giữ điều kiện cập nhật để cập nhật điều kiện xác định rủi ro, và bộ cập nhật, phương pháp xác thực bao gồm các bước sau: khiến bộ xác định nhận thông tin truy cập của người dùng và truy vấn về loại xác thực từ thiết bị thương mại, xác định mức rủi ro của việc truy cập dựa vào thông tin truy cập và điều kiện xác định rủi ro, và nhận dạng loại xác thực đối với người dùng dựa vào mức rủi ro; khiến bộ phản hồi thứ nhất phản hồi lại thiết bị thương mại về loại xác thực được nhận dạng bởi bộ xác định; khiến bộ xử lý xác thực nhận mật khẩu người dùng nhập vào theo loại xác thực và yêu cầu xác thực từ thiết bị thương mại để thực hiện quy trình xác thực người dùng dựa vào mật khẩu người dùng nhập vào; khiến bộ phản hồi thứ hai phản hồi lại

thiết bị thương mại về kết quả xác thực bằng bộ xử lý xác thực; và khiến bộ cập nhật cập nhật điều kiện xác định rủi ro khi yêu cầu xác thực từ thiết bị thương mại thỏa mãn điều kiện cập nhật.

Phương pháp xác thực theo phương án thứ tư là phương pháp xác thực bằng bảng xác định rủi ro thông thường mà lưu giữ điều kiện xác định rủi ro thông thường để tính toán mức rủi ro của việc truy cập từ người dùng đến thiết bị thương mại thứ nhất hoặc thiết bị thương mại thứ hai, thiết bị xác thực thứ nhất bao gồm bảng điều kiện cập nhật thứ nhất mà lưu giữ điều kiện cập nhật thứ nhất để cập nhật điều kiện xác định rủi ro thông thường, và thiết bị xác thực thứ hai bao gồm bảng điều kiện cập nhật thứ hai mà lưu giữ điều kiện cập nhật thứ hai để cập nhật điều kiện xác định rủi ro thông thường, phương pháp xác thực bao gồm các bước: khiến thiết bị xác thực thứ nhất thực hiện các bước sau: nhận thông tin truy cập thứ nhất của người dùng và truy vấn về loại xác thực từ thiết bị thương mại thứ nhất, xác định mức rủi ro thứ nhất của việc truy cập từ người dùng đến thiết bị thương mại thứ nhất dựa vào thông tin truy cập thứ nhất và điều kiện xác định rủi ro thông thường, và nhận dạng loại xác thực đối với người dùng dựa vào mức rủi ro thứ nhất; phản hồi lại thiết bị thương mại thứ nhất về loại xác thực được nhận dạng; thu mật khẩu người dùng nhập vào theo loại xác thực và yêu cầu xác thực từ thiết bị thương mại thứ nhất và thực hiện quy trình xác thực người dùng dựa vào mật khẩu người dùng nhập vào; phản hồi lại thiết bị thương mại thứ nhất về kết quả xác thực; và cập nhật điều kiện xác định rủi ro thông thường khi yêu cầu xác thực từ thiết bị thương mại thứ nhất thỏa mãn điều kiện cập nhật thứ nhất, và khiến thiết bị xác thực thứ hai thực hiện các bước sau: nhận thông tin truy cập thứ hai của người dùng và truy vấn về loại xác thực từ thiết bị thương mại thứ hai, xác định mức rủi ro thứ hai của việc truy cập từ người dùng đến thiết bị thương mại thứ hai dựa vào thông tin truy cập thứ hai và điều kiện xác định rủi ro thông thường, và nhận dạng loại xác thực đối với người dùng dựa vào mức rủi ro thứ hai; phản hồi lại thiết bị thương mại thứ hai về loại xác thực được nhận dạng; nhận mật khẩu người dùng nhập vào theo loại xác thực và yêu cầu xác thực từ thiết bị thương mại thứ hai và thực

hiện quy trình xác thực người dùng dựa vào mật khẩu người dùng nhập vào; phản hồi lại thiết bị thương mại thứ hai về kết quả xác thực; và cập nhật điều kiện xác định rủi ro thông thường khi yêu cầu xác thực từ thiết bị thương mại thứ hai thỏa mãn điều kiện cập nhật thứ hai.

Hiệu quả của sáng chế

Theo sáng chế, do bộ cập nhật so sánh yêu cầu xác thực từ thiết bị thương mại với điều kiện cập nhật được lưu giữ trong bảng điều kiện cập nhật và cập nhật điều kiện xác định rủi ro khi điều kiện cập nhật được thỏa mãn, điều kiện xác định rủi ro có thể được cập nhật ngay lập tức dựa vào yêu cầu xác thực từ máy chủ thương mại theo yêu cầu xử lý từ người dùng. Ngoài ra, do yêu cầu xác thực từ thiết bị thương mại được sử dụng để xác định xem có cập nhật điều kiện xác định rủi ro hay không, điều kiện xác định rủi ro có thể được cập nhật ngay mà không phải thu thập thông tin mới về rủi ro từ máy chủ bên ngoài và mức an toàn của việc xác thực người dùng có thể được tăng.

Mô tả vắn tắt các hình vẽ

Fig.1 là biểu đồ cấu hình của hệ thống xác thực theo một phương án của sáng chế.

Fig.2 là bảng thể hiện ví dụ về bảng lịch sử truy cập.

Fig.3 là bảng thể hiện ví dụ về bảng điều kiện cập nhật xác định rủi ro.

Fig.4 là biểu đồ thể hiện ví dụ về cấu hình phần cứng của máy chủ.

Fig.5 là biểu đồ trình tự của quy trình xác thực theo phương án của sáng chế.

Fig.6 là biểu đồ cấu hình của hệ thống xác thực theo cải biến thứ nhất.

Fig.7 là biểu đồ cấu hình của hệ thống xác thực theo cải biến thứ hai.

Fig.8 là biểu đồ thể hiện các dòng quy trình tính toán mức rủi ro và quy trình cập nhật bảng xác định rủi ro.

Fig.9 là bảng thể hiện ví dụ về bảng điều kiện cập nhật xác định rủi ro.

Mô tả chi tiết sáng chế

Sau đây, phương án của sáng chế sẽ được mô tả chi tiết.

Fig.1 là biểu đồ cấu hình của hệ thống xác thực theo một phương án của sáng chế. Như được thể hiện trên Fig.1, hệ thống xác thực bao gồm máy chủ thương mại 1 và máy chủ xác thực 2. Người dùng sử dụng thiết bị đầu cuối người dùng 3 để truy cập máy chủ thương mại 1 và sử dụng dịch vụ được cung cấp bởi máy chủ thương mại 1. Phản hồi lại yêu cầu từ máy chủ thương mại 1, máy chủ xác thực 2 thực hiện xác thực cá nhân dựa vào việc xác thực trên cơ sở rủi ro đối với người dùng thiết bị đầu cuối người dùng 3 đang truy cập máy chủ thương mại 1 và thông báo kết quả xác thực đến máy chủ thương mại 1 là nguồn yêu cầu.

Thiết bị đầu cuối người dùng 3 được nối với máy chủ thương mại 1 thông qua mạng 4 ví dụ như Internet. Ví dụ, thiết bị đầu cuối người dùng 3 là máy tính cá nhân, thiết bị đầu cuối máy tính bảng, điện thoại thông minh, điện thoại di động, hoặc đồ gia dụng thông minh, bao gồm bộ đầu vào để nhận các đăng nhập khác nhau (ID đăng nhập, mật khẩu, và tương tự) từ người dùng, bộ hiển thị để hiển thị các loại thông tin khác nhau, và bộ truyền thông để nối mạng 4, và có chức năng tương tự như trình duyệt.

Máy chủ thương mại 1 bao gồm bộ xử lý thương mại 11, bộ vấn tin loại xác thực 12, và bộ yêu cầu xác thực 13.

Khi có truy cập từ thiết bị đầu cuối người dùng 3, bộ xử lý thương mại 11 thu thập địa chỉ IP nguồn truy cập và thông tin thiết bị đầu cuối của thiết bị đầu cuối người dùng 3. Thông tin thiết bị đầu cuối sẽ được mô tả sau. Khi quy trình vấn tin việc xác thực được yêu cầu từ thiết bị đầu cuối người dùng 3, bộ xử lý thương mại 11 truyền màn hình xác thực theo loại xác thực được nhận dạng bởi máy chủ xác thực 2 đến thiết bị đầu cuối người dùng 3. Trong trường hợp này, loại xác thực liên quan đến loại của phương pháp xác thực đối với người dùng mà các ví dụ của nó bao gồm việc xác thực bằng mật khẩu có sử dụng mật khẩu cố định và việc xác thực bằng hai nhân tố mà kết hợp việc xác thực bằng mật khẩu với việc xác thực bằng mã thông báo phần cứng. Khi loại xác thực là

việc xác thực bằng hai nhân tố, màn hình xác thực bao gồm trường nhập để nhập mật khẩu cố định và trường nhập để nhập mật khẩu được hiển thị trên mã thông báo phần cứng. Khi quy trình vấn tin việc xác thực là quy trình đăng nhập, màn hình xác thực cũng bao gồm trường nhập cho ID người dùng. Phương pháp nhận dạng loại xác thực bằng máy chủ xác thực 2 sẽ được mô tả sau đây.

Khi việc xác thực bởi máy chủ xác thực 2 thành công và người dùng sử dụng thiết bị đầu cuối người dùng 3 được xác định là người dùng hợp lệ, bộ xử lý thương mại 11 thực hiện quy trình chuyển tiền bằng cách thực hiện quy trình thương mại định trước và phản hồi lại thiết bị đầu cuối người dùng 3 về kết quả xử lý. Mặt khác, khi việc xác thực bởi máy chủ xác thực 2 thất bại, bộ xử lý thương mại 11 thông báo thiết bị đầu cuối người dùng 3 về thất bại khi xác thực và một lần nữa truyền màn hình xác thực đến thiết bị đầu cuối người dùng 3.

Khi có truy cập từ thiết bị đầu cuối người dùng 3, để chuẩn bị cho quy trình đăng nhập từ người dùng, bộ vấn tin loại xác thực 12 truyền địa chỉ IP nguồn truy cập và thông tin thiết bị đầu cuối của thiết bị đầu cuối người dùng 3 được thu thập bởi bộ xử lý thương mại 11 đến máy chủ xác thực 2 và truy vấn về loại xác thực tương ứng với quy trình đăng nhập của người dùng. Khi quy trình vấn tin việc xác thực được yêu cầu từ thiết bị đầu cuối người dùng 3 sau khi đăng nhập, bộ vấn tin loại xác thực 12 truyền địa chỉ IP nguồn truy cập và quy trình được yêu cầu đến máy chủ xác thực 2 và truy vấn về loại xác thực tương ứng với quy trình được yêu cầu bởi người dùng. Bộ vấn tin loại xác thực 12 thu thập loại xác thực được nhận dạng bởi máy chủ xác thực 2 phản hồi lại truy vấn.

Khi mật khẩu được nhập bởi người dùng đến màn hình xác thực của thiết bị đầu cuối người dùng 3 được thông báo từ thiết bị đầu cuối người dùng 3, bộ yêu cầu xác thực 13 truyền mật khẩu người dùng nhập vào, ID người dùng, và địa chỉ IP đến máy chủ xác thực 2 và yêu cầu quy trình xác thực. Bộ yêu cầu xác thực 13 thu thập kết quả xác thực từ máy chủ xác thực 2.

Máy chủ xác thực 2 bao gồm bộ xác định rủi ro 21, bộ phản hồi loại xác

thực 22, bảng xác định rủi ro 23, bộ xử lý xác thực 24, bộ cập nhật xác định rủi ro 25, bộ phản hồi kết quả xác thực 26, bảng xác thực 27, bảng lịch sử xác thực 28, và bảng điều kiện cập nhật xác định rủi ro 29.

Bộ xác định rủi ro 21 nhận dạng loại xác thực tương ứng với quy trình đăng nhập bởi người dùng hoặc quy trình được yêu cầu bởi người dùng đến máy chủ thương mại 1 phản hồi lại truy vấn từ bộ vấn tin loại xác thực 12 của máy chủ thương mại 1. Bộ xác định rủi ro 21 tính toán mức rủi ro dựa vào thông tin truy cập ví dụ như địa chỉ IP và thông tin thiết bị đầu cuối được nhận từ máy chủ thương mại 1 cùng với truy vấn loại xác thực và trên điều kiện xác định rủi ro được ghi trong bảng xác định rủi ro 23, và nhận dạng loại xác thực.

Điều kiện xác định rủi ro được ghi trong bảng xác định rủi ro 23 là điều kiện được sử dụng khi tính toán mức rủi ro của việc truy cập từ thiết bị đầu cuối người dùng 3. Ví dụ, lịch sử truy cập và thông tin thiết bị đầu cuối tại thời điểm truy cập ví dụ như được thể hiện trên Fig.2 được ghi trong bảng lịch sử truy cập (không được thể hiện), và bộ xác định rủi ro 21 phân tích mẫu hành vi trong quá khứ của người dùng từ lịch sử truy cập và thông tin thiết bị đầu cuối, so sánh mẫu hành vi trong quá khứ với thông tin truy cập được nhận từ máy chủ thương mại 1 dựa vào điều kiện xác định rủi ro, và tính toán mức rủi ro. Trong trường hợp này, lịch sử truy cập bao gồm ngày và giờ truy cập, địa chỉ IP của nguồn truy cập, và tương tự. Thông tin thiết bị đầu cuối bao gồm thông tin OS chỉ báo OS hoặc trình duyệt chạy trên thiết bị đầu cuối người dùng 3, thông tin trình duyệt ví dụ như phiên bản trình duyệt hoặc thiết đặt ngôn ngữ, và thông tin CPU chỉ báo CPU được nối với thiết bị đầu cuối người dùng 3.

Khi độ khớp giữa thông tin truy cập được nhận từ máy chủ thương mại 1 và mẫu hành vi trong quá khứ là cao, mức rủi ro là thấp, và khi độ khớp là thấp, mức rủi ro là cao.

Trong bảng xác định rủi ro 23, danh sách địa chỉ IP mô tả các địa chỉ IP mà có nhiều khả năng là những người phá hoại và biểu thức điều kiện mà xác định mức rủi ro cao khi địa chỉ IP của người dùng được nhận từ máy chủ thương

mại 1 khớp với địa chỉ IP trong danh sách địa chỉ IP được ghi làm điều kiện xác định rủi ro.

Bộ xác định rủi ro 21 nhận dạng loại xác thực đối với người dùng dựa vào mức rủi ro được tính toán. Ví dụ, bộ xác định rủi ro 21 tính toán ba mức rủi ro từ mức 1 đến mức 3, nhận dạng việc xác thực bằng mật khẩu là loại xác thực trong trường hợp mức 1 (độ rủi ro thấp), nhận dạng loại xác thực hai nhân tố là loại xác thực trong trường hợp mức 2, và xác định khóa quy trình xác thực (vô hiệu hóa việc xác thực) trong trường hợp mức 3 (độ rủi ro cao).

Bộ phản hồi loại xác thực 22 thông báo máy chủ thương mại 1 về loại xác thực được nhận dạng bởi bộ xác định rủi ro 21.

Bộ xử lý xác thực 24 nhận mật khẩu người dùng nhập vào, ID người dùng, địa chỉ IP, và thông tin tương tự cùng với yêu cầu xác thực từ bộ yêu cầu xác thực 13 của máy chủ thương mại 1. Mật khẩu cố định của người dùng, phương trình tính toán cho mật khẩu dùng một lần, và thông tin tương tự được ghi trong bảng xác thực 27, và bộ xử lý xác thực 24 sử dụng thông tin để xác định xem mật khẩu được nhận từ máy chủ thương mại 1 có hợp lệ hay không. Việc xác thực thành công khi mật khẩu được nhận từ máy chủ thương mại 1 là hợp lệ và thất bại khi mật khẩu là không hợp lệ.

Khi bộ xử lý xác thực 24 nhận yêu cầu xác thực từ bộ yêu cầu xác thực 13, bộ xử lý xác thực 24 ghi ID người dùng và địa chỉ IP, các nội dung của quy trình xử lý được yêu cầu từ người dùng, và kết quả xác thực trong bảng lịch sử xác thực 28. Các yêu cầu xác thực được nhận từ bộ yêu cầu xác thực 13 trong một thời gian định trước và các kết quả xác thực đối với các yêu cầu xác thực được ghi trong bảng lịch sử xác thực 28.

Bộ phản hồi kết quả xác thực 26 phản hồi lại máy chủ thương mại 1 về kết quả xác thực bằng bộ xử lý xác thực 24.

Bộ cập nhật xác định rủi ro 25 tham khảo bảng điều kiện cập nhật xác định rủi ro 29 dựa vào yêu cầu xác thực và kết quả xác thực được ghi trong bảng lịch sử xác thực 28 và xác định xem có cập nhật điều kiện xác định rủi ro trong

bảng xác định rủi ro 23 hay không. Điều kiện cập nhật để cập nhật điều kiện xác định rủi ro và quy trình cập nhật được tiến hành khi điều kiện cập nhật được thỏa mãn được ghi trong bảng điều kiện cập nhật xác định rủi ro 29. Mỗi lần quy trình xác thực được thực hiện bởi bộ xử lý xác thực 24, bộ cập nhật xác định rủi ro 25 kiểm tra xem yêu cầu xác thực thỏa mãn điều kiện cập nhật được ghi trong bảng điều kiện cập nhật xác định rủi ro 29 có được thực hiện hay không, khi được thực hiện, ngay lập tức thực hiện quy trình cập nhật tương ứng.

Fig.3 thể hiện ví dụ về các nội dung được ghi của bảng điều kiện cập nhật xác định rủi ro 29. Ví dụ, khi các yêu cầu xác thực đối với X1 (trong đó X1 là số nguyên bằng hoặc lớn hơn 2) ID người dùng hoặc nhiều hơn được tạo ra từ cùng một địa chỉ IP trong một khoảng thời gian định trước và tất cả các yêu cầu xác thực đều có kết quả là thất bại, bộ cập nhật xác định rủi ro 25 xác định rằng có nhiều khả năng là địa chỉ IP thuộc về người phá hoại, ngay lập tức bổ sung địa chỉ IP vào danh sách địa chỉ IP trong bảng xác định rủi ro 23, và cập nhật điều kiện xác định rủi ro.

Khi các yêu cầu xác thực đối với X2 (trong đó X2 là số nguyên lớn hơn X1) ID người dùng hoặc nhiều hơn được tạo ra từ cùng một địa chỉ IP trong một thời gian định trước, ngay cả nếu chỉ có quy trình xác thực mà các kết quả là xác thực thành công, bộ cập nhật xác định rủi ro 25 ngay lập tức bổ sung địa chỉ IP vào danh sách địa chỉ IP trong bảng xác định rủi ro 23 và cập nhật điều kiện xác định rủi ro. Đó là do, có thể hình dung được rằng, người phá hoại đã tạo ra các yêu cầu xác thực với số lượng lớn các ID người dùng và có quy trình xác thực trong đó mật khẩu khớp một cách trùng hợp.

Đối với máy chủ thương mại 1 và máy chủ xác thực 2 được mô tả ở trên, máy tính bao gồm CPU (bộ xử lý trung tâm) 401, bộ nhớ chính 402, giao diện mạng 403, và thiết bị lưu giữ bất biến 404 như được thể hiện trên Fig.4 có thể được sử dụng tương ứng. Ví dụ, thiết bị lưu giữ bất biến 404 là HDD (ổ đĩa cứng) hoặc SDD (ổ thể rắn) và lưu giữ chương trình được thực hiện bởi CPU 401. Các chức năng tương ứng của máy chủ thương mại 1 và máy chủ xác thực

2 được thực hiện khi CPU 401 tải chương trình được lưu giữ trong thiết bị lưu giữ bất biến 404 đến bộ nhớ chính 402 và thực hiện chương trình.

Tiếp theo, quy trình xác thực bằng hệ thống xác thực theo phương án sẽ được mô tả dựa vào biểu đồ trình tự được thể hiện trên Fig.5. Trong Fig.5, quy trình xác thực bao gồm việc đăng nhập bởi người dùng và quy trình xác thực khi quy trình vấn tin việc xác thực được yêu cầu sau khi đăng nhập sẽ được mô tả.

Bước S101: Người dùng sử dụng thiết bị đầu cuối người dùng 3 và truy cập máy chủ thương mại 1. Tại thời điểm này, bộ xử lý thương mại 11 thu thập địa chỉ IP nguồn truy cập và thông tin thiết bị đầu cuối của thiết bị đầu cuối người dùng 3.

Bước S102: Bộ vấn tin loại xác thực 12 của máy chủ thương mại 1 truy vấn máy chủ xác thực 2 về loại quy trình xác thực được thực hiện đối với quy trình đăng nhập của người dùng. Tại thời điểm này, bộ vấn tin loại xác thực 12 truyền thông tin truy cập bao gồm địa chỉ IP nguồn truy cập và thông tin thiết bị đầu cuối được thu thập trong bước S101 đến máy chủ xác thực 2.

Bước S103: Phản hồi lại truy vấn từ bộ vấn tin loại xác thực 12, bộ xác định rủi ro 21 của máy chủ xác thực 2 tính toán mức rủi ro của việc truy cập từ người dùng và nhận dạng loại quy trình xác thực theo mức rủi ro.

Ví dụ, bộ xác định rủi ro 21 so sánh lần truy cập hiện thời từ người dùng với mẫu hành vi trong quá khứ của người dùng dựa vào lịch sử truy cập và thông tin thiết bị đầu cuối được ghi trong bảng lịch sử truy cập, và tính toán mức rủi ro dựa vào kết quả so sánh. Ngoài ra, ví dụ, bộ xác định rủi ro 21 phát hiện xem địa chỉ IP nguồn truy cập của lần truy cập hiện thời từ người dùng có được bao gồm trong danh sách địa chỉ IP được ghi trong bảng xác định rủi ro 23 hay không và, khi được bao gồm, nâng cao mức rủi ro.

Hơn nữa, bộ xác định rủi ro 21 nhận dạng loại quy trình xác thực dựa vào mức rủi ro được tính toán. Ví dụ, bộ xác định rủi ro 21 nhận dạng việc xác thực bằng mật khẩu bằng cách sử dụng mật khẩu cố định làm loại xác thực.

Bước S104: Bộ phản hồi loại xác thực 22 thông báo máy chủ thương mại 1 về loại xác thực được nhận dạng bởi bộ xác định rủi ro 21.

Bước S105: Bộ xử lý thương mại 11 của máy chủ thương mại 1 truyền màn hình xác thực theo loại xác thực được nhận dạng bởi máy chủ xác thực 2 tới thiết bị đầu cuối người dùng 3.

Bước S106: Người dùng nhập ID người dùng và nhập khẩu vào màn hình xác thực của thiết bị đầu cuối người dùng 3. ID người dùng và mật khẩu được nhập được thông báo đến máy chủ thương mại 1 từ thiết bị đầu cuối người dùng 3. Ví dụ, người dùng nhập mật khẩu cố định được ghi nhớ.

Bước S107: Khi mật khẩu được thông báo từ thiết bị đầu cuối người dùng 3, bộ yêu cầu xác thực 13 của máy chủ thương mại 1 truyền mật khẩu cùng với ID người dùng và địa chỉ IP đến máy chủ xác thực 2 và tạo ra yêu cầu xác thực.

Bước S108: Bộ xử lý xác thực 24 của máy chủ xác thực 2 thực hiện quy trình xác thực theo yêu cầu xác thực từ máy chủ thương mại 1. Cụ thể là, bộ xử lý xác thực 24 đối chiếu mật khẩu được ghi trong bảng xác thực 27 với mật khẩu được nhận từ máy chủ thương mại 1 cùng với yêu cầu xác thực và xác định việc khớp/không khớp của kết quả đối chiếu. Khi kết quả đối chiếu khớp, việc xác định rằng việc truy cập từ người dùng hợp lệ được tạo ra và việc xác thực thành công. Khi việc xác thực thành công, bộ xử lý xác thực 24 ghi ngày và thời gian truy cập, địa chỉ IP, thông tin thiết bị đầu cuối, và thông tin tương tự về lần truy cập hiện thời vào bảng lịch sử truy cập. Mặt khác, khi kết quả đối chiếu không khớp, việc xác thực thất bại. Trong ví dụ được thể hiện trên Fig.5 quy trình đăng nhập được coi là đã thành công.

Khi bộ xử lý xác thực 24 nhận yêu cầu xác thực, bộ xử lý xác thực 24 ghi ID người dùng và địa chỉ IP, các nội dung của quy trình xử lý được yêu cầu từ người dùng (trong trường hợp này, quy trình đăng nhập), và kết quả xác thực vào bảng lịch sử xác thực 28.

Bước S109: Bộ phản hồi kết quả xác thực 26 phản hồi lại máy chủ

thương mại 1 về kết quả của quy trình xác thực bằng bộ xử lý xác thực 24.

Khi việc xác thực thành công, bộ xử lý thương mại 11 của máy chủ thương mại 1 thực hiện quy trình đăng nhập của người dùng. Mặt khác, khi việc xác thực thất bại, bộ xử lý thương mại 11 thông báo thiết bị đầu cuối người dùng 3 về việc xác thực thất bại này và một lần nữa truyền màn hình xác thực đến thiết bị đầu cuối người dùng 3.

Bước S110: Bộ cập nhật xác định rủi ro 25 tham khảo bảng điều kiện cập nhật xác định rủi ro 29 dựa vào yêu cầu xác thực và kết quả xác thực được ghi trong bảng lịch sử xác thực 28 và xác định xem có cập nhật điều kiện xác định rủi ro trong bảng xác định rủi ro 23 hay không. Khi điều kiện cập nhật được thỏa mãn, bộ cập nhật xác định rủi ro 25 ngay lập tức thực hiện quy trình cập nhật bảng xác định rủi ro 23.

Ví dụ, khi các yêu cầu xác thực đối với X2 ID người dùng hoặc nhiều hơn từ cùng một địa chỉ IP được ghi trong bảng lịch sử xác thực 28 trong một khoảng thời gian định trước, bộ cập nhật xác định rủi ro 25 ngay lập tức bổ sung địa chỉ IP vào danh sách địa chỉ IP trong điều kiện xác định rủi ro và cập nhật điều kiện xác định rủi ro. Điều kiện xác định rủi ro được cập nhật được sử dụng để tính toán lần lượt các mức rủi ro bằng bộ xác định rủi ro 21.

Bước S111: Sau khi đăng nhập, người dùng sử dụng thiết bị đầu cuối người dùng 3 và yêu cầu quy trình mà vấn tin việc xác thực.

Bước S112: Khi quy trình vấn tin việc xác thực được yêu cầu từ thiết bị đầu cuối người dùng 3, bộ vấn tin loại xác thực 12 của máy chủ thương mại 1 truy vấn máy chủ xác thực 2 về loại quy trình xác thực được thực hiện. Tại thời điểm này, bộ vấn tin loại xác thực 12 thông báo máy chủ xác thực 2 về thông tin truy cập bao gồm địa chỉ IP nguồn truy cập và thông tin thiết bị đầu cuối. Bộ vấn tin loại xác thực 12 có thể ngoài ra còn thông báo máy chủ xác thực 2 về ID người dùng và quy trình xử lý được yêu cầu.

Bước S113: Phản hồi lại việc vấn tin từ bộ vấn tin loại xác thực 12, bộ xác định rủi ro 21 của máy chủ xác thực 2 tính toán mức rủi ro của việc truy cập

từ người dùng và nhận dạng loại quy trình xác thực theo mức rủi ro. Bộ xác định rủi ro 21 tính toán mức rủi ro sử dụng điều kiện xác định rủi ro được cập nhật trong bước S110.

Mức rủi ro khác có thể được tính toán theo quy trình xử lý được yêu cầu từ người dùng. Ví dụ, khi máy chủ thương mại 1 cung cấp dịch vụ ngân hàng Internet, mức rủi ro cao hơn có thể được tính toán cho quy trình chuyển tiền khi so sánh với quy trình xác nhận số dư.

Bộ xác định rủi ro 21 có thể phát hiện xem địa chỉ IP nguồn truy cập của lần truy cập hiện thời từ người dùng có được bao gồm trong danh sách địa chỉ IP được ghi trong bảng xác định rủi ro 23 hay không và, khi được bao gồm, nâng mức rủi ro.

Bộ xác định rủi ro 21 nhận dạng loại quy trình xác thực dựa vào mức rủi ro được tính toán. Ví dụ, bộ xác định rủi ro 21 nhận dạng việc xác thực bằng hai nhân tố mà kết hợp việc xác thực bằng mật khẩu với việc xác thực bằng mã thông báo phần cứng làm loại xác thực.

Bước S114: Bộ phản hồi loại xác thực 22 thông báo máy chủ thương mại 1 về loại xác thực được nhận dạng bởi bộ xác định rủi ro 21.

Bước S115: Bộ xử lý thương mại 11 của máy chủ thương mại 1 truyền màn hình xác thực theo loại xác thực được nhận dạng bởi máy chủ xác thực 2 đến thiết bị đầu cuối người dùng 3.

Bước S116: Người dùng nhập mật khẩu vào màn hình xác thực của thiết bị đầu cuối người dùng 3. Mật khẩu được nhập được thông báo đến máy chủ thương mại 1 từ thiết bị đầu cuối người dùng 3. Ví dụ, người dùng nhập mật khẩu cố định đã được ghi nhớ và mật khẩu được hiển thị trên mã thông báo phần cứng.

Bước S117: Khi mật khẩu được thông báo từ thiết bị đầu cuối người dùng 3, bộ yêu cầu xác thực 13 của máy chủ thương mại 1 truyền mật khẩu cùng với ID người dùng và địa chỉ IP đến máy chủ xác thực 2 và thực hiện yêu cầu

xác thực.

Bước S118: Bộ xử lý xác thực 24 của máy chủ xác thực 2 thực hiện quy trình xác thực theo yêu cầu xác thực từ máy chủ thương mại 1. Cụ thể là, bộ xử lý xác thực 24 đối chiếu mật khẩu được ghi trong bảng xác thực 27 với mật khẩu được nhận từ máy chủ thương mại 1 cùng với yêu cầu xác thực và xác định việc khớp/không khớp của kết quả đối chiếu. Khi kết quả đối chiếu khớp, việc xác định rằng việc truy cập từ người dùng hợp lệ được thực hiện và việc xác thực thành công. Mặt khác, khi kết quả đối chiếu không khớp, việc xác thực thất bại.

Khi bộ xử lý xác thực 24 nhận yêu cầu xác thực, bộ xử lý xác thực 24 ghi ID người dùng và địa chỉ IP, các nội dung của quy trình xử lý được yêu cầu từ người dùng, và kết quả xác thực trong bảng lịch sử xác thực 28.

Bước S119: Bộ phản hồi kết quả xác thực 26 phản hồi lại máy chủ thương mại 1 về kết quả của quy trình xác thực bằng bộ xử lý xác thực 24.

Khi việc xác thực thành công, bộ xử lý thương mại 11 của máy chủ thương mại 1 thực hiện quy trình chuyển tiền bằng cách thực hiện quy trình thương mại định trước và phản hồi lại thiết bị đầu cuối người dùng 3 về kết quả xử lý. Mặt khác, khi việc xác thực thất bại, bộ xử lý thương mại 11 thông báo thiết bị đầu cuối người dùng 3 về sự thất bại khi xác thực và một lần nữa truyền màn hình xác thực đến thiết bị đầu cuối người dùng 3.

Bước S120: Bộ cập nhật xác định rủi ro 25 tham khảo bảng điều kiện cập nhật xác định rủi ro 29 dựa vào yêu cầu xác thực và kết quả xác thực được ghi trong bảng lịch sử xác thực 28 và xác định xem có cập nhật điều kiện xác định rủi ro trong bảng xác định rủi ro 23 hay không. Khi điều kiện cập nhật được thỏa mãn, bộ cập nhật xác định rủi ro 25 ngay lập tức thực hiện quy trình cập nhật bảng xác định rủi ro 23. Điều kiện xác định rủi ro được cập nhật được sử dụng để tính toán lần lượt các mức rủi ro bằng bộ xác định rủi ro 21.

Khi quy trình vấn tin việc xác thực được yêu cầu một lần nữa từ người dùng, quy trình quay trở về bước S111.

Như được mô tả ở trên, theo phương án, điều kiện xác định rủi ro được ghi trong bảng xác định rủi ro 23 có thể được cập nhật ngay dựa vào yêu cầu xác thực từ máy chủ thương mại 1 theo yêu cầu xử lý từ người dùng. Ví dụ, khi yêu cầu xác thực khả nghi mà bị nghi ngờ là cực kỳ có khả năng là gian lận hoặc tương tự được tạo ra, yêu cầu xác thực có thể ngay lập tức được phản chiếu trong điều kiện xác định rủi ro. Theo đó, ngay cả khi quy trình đăng nhập được hoàn tất dựa vào yêu cầu xác thực khả nghi, do điều kiện xác định rủi ro được cập nhật trong thời gian thực, mức rủi ro có thể được nâng lên và độ xác thực có thể được tăng khi quy trình vấn tin việc xác thực được yêu cầu sau đó. Ngoài ra, điều kiện xác định rủi ro có thể được cập nhật trong máy chủ xác thực 2 mà không cần thu thập thông tin mới về rủi ro từ máy chủ bên ngoài và mức an toàn của việc xác thực người dùng có thể được tăng.

Hệ thống xác thực theo phương án được mô tả ở trên có thể được áp dụng cho, ví dụ, ngân hàng Internet. Máy chủ thương mại 1 tương ứng với máy chủ thương mại của ngân hàng. Người dùng truy cập và đăng nhập vào máy chủ thương mại 1 bằng cách sử dụng thiết bị đầu cuối người dùng 3 và thực hiện các quy trình ví dụ như xác nhận số dư, chuyển tiền, gửi tiền. Ví dụ, khi yêu cầu xác thực cùng với đăng nhập là khả nghi, yêu cầu xác thực khớp điều kiện cập nhật xác định rủi ro, và điều kiện xác định rủi ro được cập nhật trong thời gian thực, do loại xác thực với độ xác thực cao được định danh theo điều kiện xác định rủi ro được cập nhật đối với quy trình chuyển tiền tiếp theo, mức an toàn có thể được tăng.

Cải biến thứ nhất

Fig.6 là biểu đồ cấu hình của hệ thống xác thực theo cải biến thứ nhất. Cải biến thứ nhất khác với phương án được thể hiện trên Fig.1 ở chỗ bộ xác định rủi ro thứ hai 200 được bố trí trong máy chủ xác thực 2. Danh sách ID người dùng có độ rủi ro cao mô tả các ID người dùng bị nghi ngờ là có khả năng cao là đã bị tấn công bởi những người phá hoại được ghi trong bảng xác định rủi ro 23. Ngoài ra, điều kiện cập nhật và quy trình cập nhật để bổ sung, khi quy trình định

trước được thực hiện trong một số lần định trước trong một khoảng thời gian nhất định bởi cùng một ID người dùng, ID người dùng vào danh sách ID người dùng có độ rủi ro cao được ghi trong bảng điều kiện cập nhật xác định rủi ro 29.

Bộ xác định rủi ro thứ hai 200 phát hiện xem ID người dùng được nhận cùng với yêu cầu xác thực từ bộ yêu cầu xác thực 13 của máy chủ thương mại 1 có được bao gồm trong danh sách ID người dùng có độ rủi ro cao hay không và đưa kết quả phát hiện đến bộ xử lý xác thực 24.

Khi ID người dùng được nhận cùng với yêu cầu xác thực được bao gồm trong danh sách ID người dùng có độ rủi ro cao, bộ xử lý xác thực 24 xác định rằng việc xác thực thất bại ngay cả nếu mật khẩu người dùng nhập vào là hợp lệ. Mặt khác, khi ID người dùng được nhận cùng với yêu cầu xác thực không được bao gồm trong danh sách ID người dùng có độ rủi ro cao, bộ xử lý xác thực 24 thực hiện quy trình xác thực và ghi yêu cầu xác thực và kết quả xác thực trong bảng lịch sử xác thực 28.

Bộ cập nhật xác định rủi ro 25 tham khảo bảng điều kiện cập nhật xác định rủi ro 29 dựa vào yêu cầu xác thực và kết quả xác thực được ghi trong bảng lịch sử xác thực 28 và xác định xem có cập nhật bảng xác định rủi ro 23 (điều kiện xác định rủi ro) hay không. Khi quy trình định trước được thực hiện một số lần định trước trong một khoảng thời gian nhất định bởi cùng một ID người dùng, bộ cập nhật xác định rủi ro 25 ngay lập tức bổ sung ID người dùng vào danh sách ID người dùng có độ rủi ro cao trong bảng xác định rủi ro 23 và cập nhật điều kiện xác định rủi ro.

Trong trường hợp này, quy trình định trước là, ví dụ, quy trình chuyển tiền với lượng bằng với lượng giới hạn tối đa. Khi quy trình chuyển tiền với lượng bằng với lượng giới hạn tối đa được lặp lại trong một khoảng thời gian ngắn, quy trình bị nghi ngờ là có nhiều khả năng được thực hiện bởi người phá hoại. Do đó, bằng cách bổ sung ID người dùng vào danh sách ID người dùng có độ rủi ro cao trong bảng xác định rủi ro 23, có bộ xác định rủi ro thứ hai 200 phát hiện xem ID người dùng được nhận cùng với yêu cầu xác thực có được bao

gồm trong danh sách ID người dùng có độ rủi ro cao trước quy trình xác thực đối với các quy trình chuyển tiền tiếp theo hay không, và thông báo bộ xử lý xác thực 24 về kết quả phát hiện, các quy trình chuyển tiền bất hợp pháp có thể được ngăn ngừa.

Cải biến thứ hai

Các hình vẽ từ Fig.7 đến Fig.9 thể hiện cải biến thứ hai. Fig.7 là biểu đồ cấu hình của hệ thống xác thực theo cải biến thứ hai. Như được thể hiện trên Fig.7, hệ thống xác thực theo cải biến thứ hai bao gồm hai máy chủ thương mại 1A và 1B, máy chủ xác thực 2A được sử dụng bởi máy chủ thương mại 1A, máy chủ xác thực 2B được sử dụng bởi máy chủ thương mại 1B, và máy chủ xác thực thông thường 5 mà có thể truy cập được từ các máy chủ xác thực 2A và 2B. Các máy chủ thương mại 1A và 1B có cấu hình tương tự như máy chủ thương mại 1 theo phương án được mô tả ở trên. Ngoài ra, các máy chủ xác thực 2A và 2B có cấu hình tương tự như máy chủ xác thực 2 theo phương án được mô tả ở trên.

Máy chủ xác thực thông thường 5 bao gồm bảng xác định rủi ro thông thường 51 mà có thể tham chiếu đến và được cập nhật bởi các máy chủ xác thực 2A và 2B. Điều kiện xác định rủi ro thông thường được sử dụng khi tính toán mức rủi ro của việc truy cập từ thiết bị đầu cuối người dùng 3 được ghi trong bảng xác định rủi ro thông thường 51. Ví dụ, trong bảng xác định rủi ro thông thường 51, danh sách địa chỉ IP có độ rủi ro cao mô tả các địa chỉ IP mà cực kỳ có khả năng là những người phá hoại và biểu thức điều kiện mà xác định rằng mức rủi ro là cực kỳ cao khi địa chỉ IP của người dùng được nhận từ máy chủ thương mại 1A hoặc 1B khớp với địa chỉ IP trong danh sách địa chỉ IP có độ rủi ro cao được ghi làm điều kiện xác định rủi ro thông thường.

Fig.8 thể hiện các cấu hình của các máy chủ xác thực 2A và 2B và máy chủ xác thực thông thường 5 trong hệ thống xác thực được thể hiện trên Fig.7. Ngoài ra, Fig.8 thể hiện các dòng (các dòng dữ liệu) của quy trình tính toán mức rủi ro và quy trình cập nhật bảng xác định rủi ro bằng các máy chủ xác thực 2A

và 2B.

Các bộ xác định rủi ro 21A và 21B, các bộ phản hồi loại xác thực 22A và 22B, các bảng xác định rủi ro (các bảng xác định rủi ro riêng lẻ) 23A và 23B, các bộ xử lý xác thực 24A và 24B, các bộ cập nhật xác định rủi ro 25A và 25B, các bộ phản hồi kết quả xác thực 26A và 26B, các bảng xác thực 27A và 27B, các bảng lịch sử xác thực 28A và 28B, và các bảng điều kiện cập nhật xác định rủi ro 29A và 29B của các máy chủ xác thực 2A và 2B lần lượt tương ứng với bộ xác định rủi ro 21, bộ phản hồi loại xác thực 22, bảng xác định rủi ro 23, bộ xử lý xác thực 24, bộ cập nhật xác định rủi ro 25, bộ phản hồi kết quả xác thực 26, bảng xác thực 27, bảng lịch sử xác thực 28, và bảng điều kiện cập nhật xác định rủi ro 29 của máy chủ xác thực 2 được thể hiện trên Fig.1.

Fig.9 thể hiện ví dụ về các nội dung được ghi của các bảng điều kiện cập nhật xác định rủi ro 29A và 29B. Ví dụ, khi các yêu cầu xác thực đối với X1 (trong đó X1 là số nguyên bằng hoặc lớn hơn 2) ID người dùng hoặc nhiều hơn được tạo ra từ cùng một địa chỉ IP trong một khoảng thời gian định trước và tất cả các yêu cầu xác thực đều có kết quả là xác thực thất bại, các bộ cập nhật xác định rủi ro 25A và 25B xác định rằng có nhiều khả năng là địa chỉ IP thuộc về người phá hoại, ngay lập tức bổ sung địa chỉ IP vào danh sách địa chỉ IP trong các bảng xác định rủi ro 23A và 23B, và cập nhật điều kiện xác định rủi ro.

Ví dụ, khi các yêu cầu xác thực đối với X2 (trong đó X2 là số nguyên lớn hơn X1) ID người dùng hoặc nhiều hơn được tạo ra từ cùng một địa chỉ IP trong một khoảng thời gian định trước và tất cả các yêu cầu xác thực có kết quả là xác thực thất bại, các bộ cập nhật xác định rủi ro 25A và 25B ngay lập tức bổ sung địa chỉ IP vào danh sách địa chỉ IP có độ rủi ro cao trong bảng xác định rủi ro thông thường 51 và cập nhật điều kiện xác định rủi ro thông thường.

Giá trị ngưỡng X1 của điều kiện cập nhật để cập nhật điều kiện xác định rủi ro (điều kiện xác định rủi ro riêng lẻ) của máy chủ của chính nó có thể là khác nhau giữa bảng điều kiện cập nhật xác định rủi ro 29A và bảng điều kiện cập nhật xác định rủi ro 29B. Đó là do mức an toàn được yêu cầu khác nhau phụ

thuộc vào máy chủ thương mại. Khi mức an toàn cao được yêu cầu, giá trị ngưỡng X1 được thiết đặt với giá trị nhỏ.

Tốt hơn là, điều kiện cập nhật để cập nhật điều kiện xác định rủi ro thông thường của bảng xác định rủi ro thông thường 51 là giống như với bảng điều kiện cập nhật xác định rủi ro 29A và bảng điều kiện cập nhật xác định rủi ro 29B. Đó là do bảng xác định rủi ro thông thường 51 được chia sẻ bởi các máy chủ xác thực và việc có các máy chủ xác thực tương ứng cập nhật điều kiện xác định rủi ro thông thường theo cùng một tiêu chí (điều kiện cập nhật) là được ưu tiên hơn việc mỗi máy chủ xác thực cập nhật điều kiện xác định rủi ro thông thường theo tiêu chí của riêng nó (điều kiện cập nhật).

Như được thể hiện trên Fig.8, khi có truy vấn về loại xác thực từ máy chủ thương mại 1A, bộ xác định rủi ro 21A của máy chủ xác thực 2A tính toán mức rủi ro của việc truy cập từ người dùng bằng cách liên hệ đến bảng xác định rủi ro 23A và bảng xác định rủi ro thông thường 51 và nhận dạng loại quy trình xác thực theo mức rủi ro. Ví dụ, bộ xác định rủi ro 21A phát hiện xem địa chỉ IP nguồn truy cập của lần truy cập hiện thời từ người dùng có được bao gồm trong danh sách địa chỉ IP có độ rủi ro cao được ghi trong bảng xác định rủi ro thông thường 51 hay không và, khi được bao gồm, nâng mức rủi ro lên mức cao nhất.

Bộ cập nhật xác định rủi ro 25A tham khảo bảng điều kiện cập nhật xác định rủi ro 28A dựa vào yêu cầu xác thực và kết quả xác thực được ghi trong bảng lịch sử xác thực 28A và xác định xem có cập nhật bảng xác định rủi ro 23A hoặc bảng xác định rủi ro thông thường 51 hay không. Khi điều kiện cập nhật để cập nhật bảng xác định rủi ro 23A được thỏa mãn, bộ cập nhật xác định rủi ro 25A ngay lập tức thực hiện quy trình cập nhật bảng xác định rủi ro 23A. Ngoài ra, khi điều kiện để cập nhật bảng xác định rủi ro thông thường 51 được thỏa mãn, bộ cập nhật xác định rủi ro 25A ngay lập tức thực hiện quy trình cập nhật bảng xác định rủi ro thông thường 51.

Bảng xác định rủi ro thông thường được cập nhật 23A và bảng xác định rủi ro thông thường được cập nhật 51 được sử dụng để tính toán lần lượt các

mức rủi ro bằng bộ xác định rủi ro 21A.

Các quy trình xử lý tương tự như máy chủ xác thực 2A được thực hiện bởi máy chủ xác thực 2B.

Các điều kiện xác định rủi ro của các bảng xác định rủi ro 23A và 23B được cập nhật tương ứng bằng các bộ cập nhật xác định rủi ro 25A và 25B của chính các máy chủ của chúng. Mặt khác, điều kiện xác định rủi ro thông thường của bảng xác định rủi ro thông thường 51 được cập nhật bởi các bộ cập nhật xác định rủi ro 25A và 25B. Khi tính toán mức rủi ro, bộ xác định rủi ro 21A của máy chủ xác thực 2A có thể tham chiếu điều kiện xác định rủi ro thông thường được cập nhật bởi bộ cập nhật xác định rủi ro 25B của máy chủ xác thực 2B. Ngoài ra, khi tính toán mức rủi ro, bộ xác định rủi ro 21B của máy chủ xác thực 2B có thể tham chiếu điều kiện xác định rủi ro thông thường được cập nhật bởi bộ cập nhật xác định rủi ro 25A của máy chủ xác thực 2A.

Như được mô tả ở trên, bằng cách đề xuất bảng xác định rủi ro thông thường 51 mà có thể tham chiếu đến và được cập nhật từ các máy chủ xác thực 2A và 2B, khi có yêu cầu xử lý từ người phá hoại đến một trong các máy chủ thương mại 1A và 1B, thông tin ví dụ như địa chỉ IP của người phá hoại có thể được bổ sung vào bảng xác định rủi ro thông thường 51 và được chia sẻ bởi các máy chủ xác thực 2A và 2B. Do điều kiện xác định rủi ro thông thường của bảng xác định rủi ro thông thường 51 được cập nhật bởi các máy chủ xác thực, thông tin mới nhất về những người phá hoại được phản chiếu và mức an toàn của việc xác thực người dùng có thể được tăng hơn nữa.

Do các máy chủ xác thực 2A và 2B lần lượt bao gồm các bảng xác định rủi ro 23A và 23B, việc xác thực trên cơ sở rủi ro theo các điều kiện riêng lẻ có thể được thực hiện bằng cách liên hệ đến các bảng xác định rủi ro 23A và 23B.

Khi hệ thống xác thực được thể hiện trên các Fig.7 và Fig.8 được ứng dụng cho giao dịch ngân hàng Internet, các máy chủ thương mại 1A và 2B có thể được coi lần lượt là máy chủ thương mại của ngân hàng A và máy chủ thương mại của ngân hàng B. Khi yêu cầu xác thực khả nghi được tạo ra từ máy

chủ thương mại ngân hàng A 1A đến máy chủ xác thực 2A, máy chủ xác thực 2A bổ sung địa chỉ IP của người dùng đã truy cập máy chủ thương mại ngân hàng A 1A vào bảng xác định rủi ro thông thường 51 và cập nhật điều kiện xác định rủi ro thông thường trong thời gian thực. Khi người dùng với cùng một địa chỉ IP truy cập máy chủ thương mại ngân hàng B 1B, do máy chủ xác thực 2B có thể liên hệ đến điều kiện xác định rủi ro thông thường được cập nhật bởi máy chủ xác thực 1A và nhận dạng loại xác thực với khả năng xác thực cao theo quy trình đăng nhập bởi người dùng, mức an toàn có thể được tăng. Như được mô tả ở trên, khi yêu cầu xác thực khả nghi được tạo ở một ngân hàng đã biết, thông tin (địa chỉ IP của người dùng) có thể được sử dụng ngay lập tức để tính toán mức rủi ro của việc xác thực ở các ngân hàng khác. Hơn nữa, thông thường, không có ý nghĩa khi ngân hàng B ghi ID người dùng có mức rủi ro cao của ngân hàng A vào bảng xác định rủi ro thông thường 51 do các ID người dùng ở ngân hàng này khác với ở ngân hàng khác ngay cả đối với cùng một người, khi người dùng truy cập các máy chủ thương mại ngân hàng từ thiết bị đầu cuối cụ thể, địa chỉ IP thông thường được sử dụng không liên quan đến việc ngân hàng nào được truy cập. Do đó, hiệu quả được tạo ra nhờ việc ghi địa chỉ IP có mức rủi ro cao trong bảng xác định rủi ro thông thường 51 là đáng kể.

Ngoài ra, do các máy chủ xác thực 2A và 2B lần lượt bao gồm các bảng xác định rủi ro 23A và 23B, các ngân hàng A và B có thể tạo cấu hình độc lập các điều kiện xác định rủi ro. Theo cách này, điều kiện xác định rủi ro được tạo cấu hình độc lập bởi mỗi ngân hàng và điều kiện xác định rủi ro thông thường được chia sẻ và được cập nhật bởi các ngân hàng có thể được áp dụng song song.

Trong cải biến thứ hai được mô tả ở trên, ít nhất một trong số các máy chủ xác thực 2A và 2B có thể được tạo cấu hình bằng cách bổ sung bộ xác định rủi ro thứ hai 200 được mô tả ở trên. Ngoài ra, trong ít nhất một trong số các máy chủ xác thực 2A và 2B, bộ cập nhật xác định rủi ro 25A hoặc 25B có thể được tạo cấu hình để chỉ cập nhật điều kiện xác định rủi ro thông thường của bảng xác định rủi ro thông thường 51 mà không cập nhật điều kiện xác định rủi

ro của bảng xác định rủi ro 23A hoặc 23B.

Trong khi các Fig.7 và Fig.8 thể hiện ví dụ trong đó hai máy chủ thương mại và hai máy chủ xác thực được đề xuất, ba máy chủ thương mại hoặc nhiều hơn và ba máy chủ xác thực hoặc nhiều hơn có thể được đề xuất và ba máy chủ xác thực hoặc nhiều hơn có thể được tạo cấu hình để chia sẻ bảng xác định rủi ro thông thường 51.

Mỗi trong số các máy chủ thương mại có thể được coi là máy chủ thương mại tương ứng với mỗi kênh chuyển tiền ví dụ như máy tính cá nhân, điện thoại di động, và điện thoại thông minh. Khi yêu cầu xác thực khả nghi được tạo ra trên kênh chuyển tiền đã biết, thông tin (địa chỉ IP của người dùng hoặc tương tự) có thể được sử dụng ngay lập tức để tính toán mức rủi ro của việc xác thực trên các kênh chuyển tiền khác và mức an toàn có thể được tăng.

Ít nhất một phần máy chủ xác thực 2 theo phương án được mô tả ở trên có thể được tạo cấu hình bằng phần cứng hoặc bằng phần mềm. Khi được tạo cấu hình bằng phần mềm, chương trình thực hiện ít nhất một phần các chức năng của máy chủ xác thực 2 có thể được chứa trong phương tiện ghi ví dụ như đĩa mềm và CD-ROM để đọc và được thực hiện bởi máy tính. Phương tiện ghi không bị giới hạn ở phương tiện ghi lắp tháo rời được và không lắp tháo rời được ví dụ như đĩa từ và đĩa quang và có thể là phương tiện ghi cố định ví dụ như thiết bị đĩa cứng và bộ nhớ.

Chương trình thực hiện ít nhất một phần các chức năng của máy chủ xác thực 2 có thể được phân phối thông qua đường truyền thông (bao gồm truyền thông vô tuyến) ví dụ như Internet. Ngoài ra, chương trình có thể được phân phối thông qua đường hữu tuyến hoặc đường vô tuyến ví dụ như Internet hoặc được phân phối bằng cách được lưu giữ trong phương tiện ghi trong trạng thái được mã hóa, trạng thái được điều biến, hoặc trạng thái nén.

Sáng chế không bị giới hạn bởi phương án được mô tả ở trên và các bộ phận có thể được cải biến khi thực hiện sáng chế mà không xa rời phạm vi của sáng chế. Ngoài ra, các bộ phận được bộc lộ trong phương án được mô tả ở trên

có thể được kết hợp với nhau nếu phù hợp hoặc một số bộ phận có thể được loại bỏ. Hơn nữa, các bộ phận của các phương án khác nhau có thể được kết hợp với nhau nếu phù hợp.

Trong khi sáng chế đã được mô tả chi tiết theo phương án cụ thể của nó, người có trình độ trung bình trong lĩnh vực hiển nhiên hiểu rằng các cải biến khác nhau có thể được tạo ra mà không xa rời khỏi nguyên lý và phạm vi của sáng chế.

Sáng chế này dựa trên, và các yêu cầu bảo hộ hưởng quyền ưu tiên từ, đơn sáng chế Nhật Bản số 2014-050476, nộp ngày 13 tháng 3 năm 2014, toàn bộ nội dung được thể hiện ở đây để tham chiếu.

Danh mục các số chỉ dẫn

1	Máy chủ thương mại
2	Máy chủ xác thực
3	Thiết bị đầu cuối người dùng
4	Mạng
11	Bộ xử lý thương mại
12	Bộ vấn tin loại xác thực
13	Bộ yêu cầu xác thực
21	Bộ xác định rủi ro
22	Bộ phản hồi loại xác thực
23	Bảng xác định rủi ro
24	Bộ xử lý xác thực
25	Bộ cập nhật xác định rủi ro
26	Bộ phản hồi kết quả xác thực
27	Bảng xác thực
28	Bảng lịch sử xác thực
29	Bảng điều kiện cập nhật xác định rủi ro

YÊU CẦU BẢO HỘ

1. Hệ thống xác thực, bao gồm:

thiết bị xác thực thứ nhất được tạo cấu hình để nhận thông tin truy cập thứ nhất của người dùng và truy vấn về loại xác thực từ thiết bị thương mại thứ nhất, xác định mức rủi ro thứ nhất của việc truy cập từ người dùng đến thiết bị thương mại thứ nhất, nhận dạng loại xác thực đối với người dùng dựa vào mức rủi ro thứ nhất và phản hồi lại thiết bị thương mại thứ nhất, nhận mật khẩu người dùng nhập vào theo loại xác thực và yêu cầu xác thực từ thiết bị thương mại thứ nhất, thực hiện quy trình xác thực người dùng dựa vào mật khẩu người dùng nhập vào, và phản hồi lại thiết bị thương mại thứ nhất về kết quả xác thực;

thiết bị xác thực thứ hai được tạo cấu hình để nhận thông tin truy cập thứ hai của người dùng và truy vấn về loại xác thực từ thiết bị thương mại thứ hai, xác định mức rủi ro thứ hai của việc truy cập từ người dùng đến thiết bị thương mại thứ hai, nhận dạng loại xác thực đối với người dùng dựa vào mức rủi ro thứ hai và phản hồi lại thiết bị thương mại thứ hai, nhận mật khẩu người dùng nhập vào theo loại xác thực và yêu cầu xác thực từ thiết bị thương mại thứ hai, thực hiện quy trình xác thực người dùng dựa vào mật khẩu người dùng nhập vào, và phản hồi lại thiết bị thương mại thứ hai về kết quả xác thực; và

bảng xác định rủi ro thông thường được tạo cấu hình để lưu giữ điều kiện xác định rủi ro thông thường để tính toán mức rủi ro của việc truy cập từ người dùng đến thiết bị thương mại thứ nhất hoặc thiết bị thương mại thứ hai, trong đó:

thiết bị xác thực thứ nhất bao gồm bảng điều kiện cập nhật thứ nhất được tạo cấu hình để lưu giữ điều kiện cập nhật thứ nhất để cập nhật điều kiện xác định rủi ro thông thường, và được tạo cấu hình để xác định mức rủi ro thứ nhất dựa vào thông tin truy cập thứ nhất và điều kiện xác định rủi ro thông thường, và cập nhật điều kiện xác định rủi ro thông thường khi yêu cầu xác thực từ thiết bị thương mại thứ nhất thỏa mãn điều kiện cập nhật thứ nhất,

thiết bị xác thực thứ hai bao gồm bảng điều kiện cập nhật thứ hai được

tạo cấu hình để lưu giữ điều kiện cập nhật thứ hai để cập nhật điều kiện xác định rủi ro thông thường, và được tạo cấu hình để xác định mức rủi ro thứ hai dựa vào thông tin truy cập thứ hai và điều kiện xác định rủi ro thông thường, và cập nhật điều kiện xác định rủi ro thông thường khi yêu cầu xác thực từ thiết bị thương mại thứ hai thỏa mãn điều kiện cập nhật thứ hai,

thiết bị xác thực thứ nhất còn bao gồm bảng xác định rủi ro riêng lẻ được tạo cấu hình để lưu giữ điều kiện xác định rủi ro riêng lẻ để tính toán mức rủi ro của việc truy cập từ người dùng đến thiết bị thương mại thứ nhất,

bảng điều kiện cập nhật thứ nhất được tạo cấu hình để lưu giữ điều kiện cập nhật thứ ba để cập nhật điều kiện xác định rủi ro riêng lẻ, và

thiết bị xác thực thứ nhất được tạo cấu hình để cập nhật điều kiện xác định rủi ro riêng lẻ khi yêu cầu xác thực từ thiết bị thương mại thứ nhất thỏa mãn điều kiện cập nhật thứ ba.

Fig.1

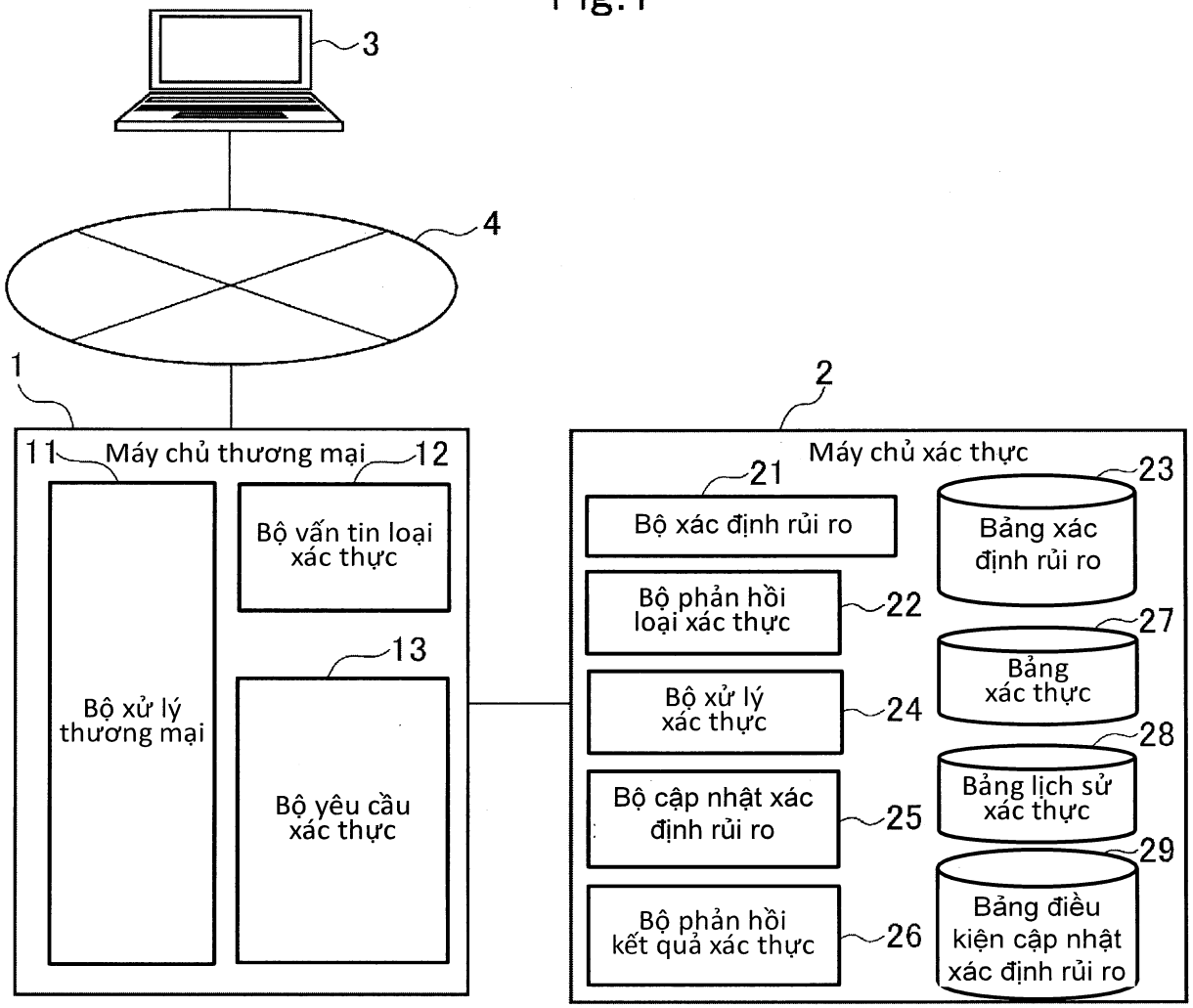


Fig.2

Lịch sử truy cập		Thông tin thiết bị đầu cuối		
Ngày và giờ truy cập	Địa chỉ IP	Thông tin OS	Thông tin trình duyệt	Thông tin CPU
• • •	• • •	• • •	• • •	• • •
⋮	⋮	⋮	⋮	⋮

Fig.3

Điều kiện cập nhật	Quy trình cập nhật
Khi các yêu cầu xác thực đối với X1 ID người dùng hoặc nhiều hơn được tạo ra từ cùng một địa chỉ ID trong một khoảng thời gian định trước và tất cả các yêu cầu xác thực đều có kết quả là xác thực thất bại	Bổ sung địa chỉ ID vào danh sách địa chỉ ID trong bảng xác định rủi ro
Khi các yêu cầu xác thực đối với X2 ID người dùng hoặc nhiều hơn được tạo ra từ cùng một địa chỉ ID trong một khoảng thời gian định trước	Bổ sung địa chỉ ID vào danh sách địa chỉ ID trong bảng xác định rủi ro
⋮	⋮

Fig.4

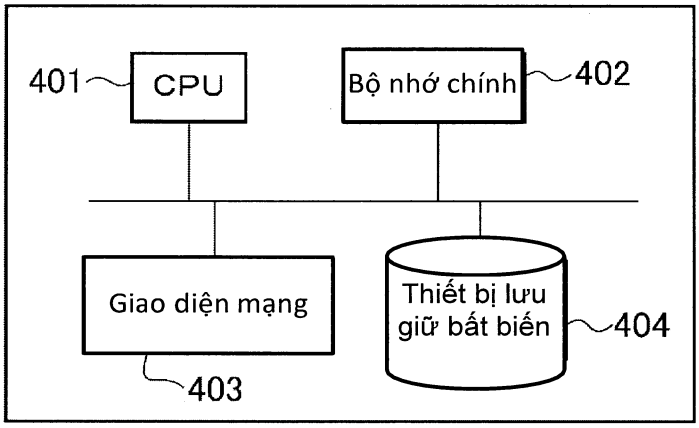


Fig.5

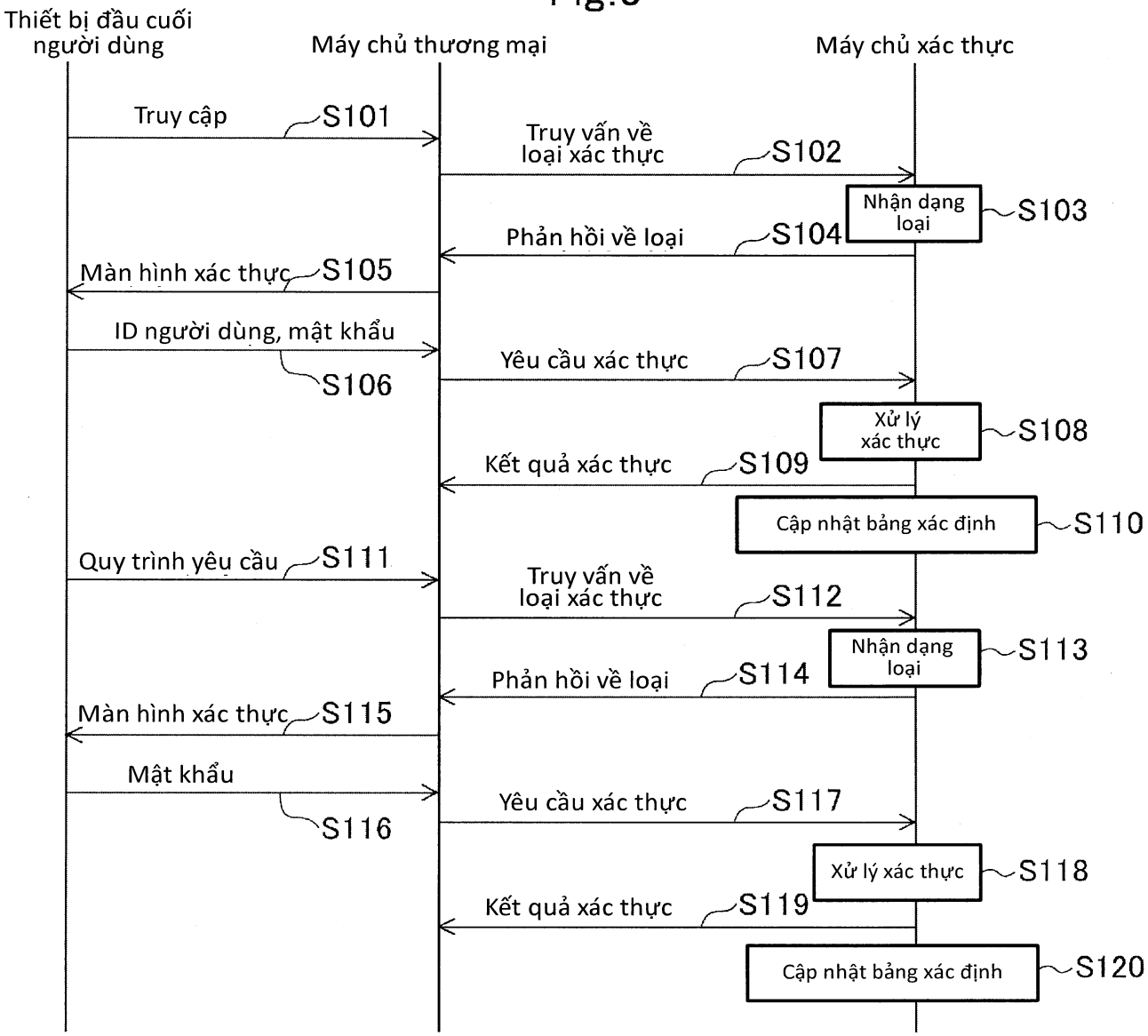

Thiết bị đầu cuối người dùng
Máy chủ thương mại
Máy chủ xác thực
Truy cập
S101
Truy vấn về loại xác thực
S102
Nhận dạng loại
S103
Phản hồi về loại
S104
Màn hình xác thực
S105
ID người dùng, mật khẩu
S106
Yêu cầu xác thực
S107
Xử lý xác thực
S108
Kết quả xác thực
S109
Cập nhật bảng xác định
S110
Quy trình yêu cầu
S111
Truy vấn về loại xác thực
S112
Nhận dạng loại
S113
Phản hồi về loại
S114
Màn hình xác thực
S115
Mật khẩu
S116
Yêu cầu xác thực
S117
Xử lý xác thực
S118
Kết quả xác thực
S119
Cập nhật bảng xác định
S120

Fig.6

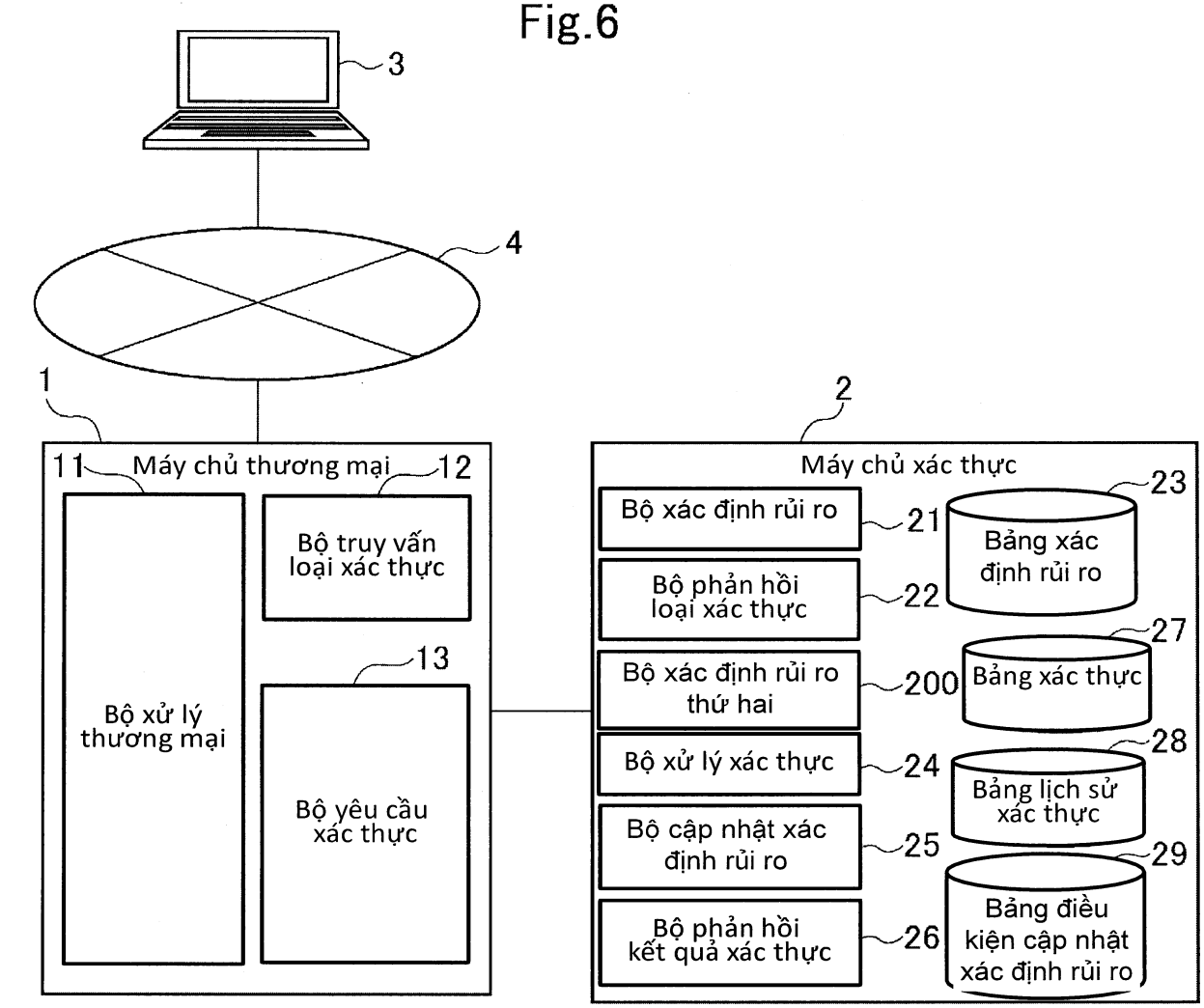

3
4
1
2
11
Máy chủ thương mại
12
Bộ truy vấn loại xác thực
13
Bộ xử lý thương mại
Bộ yêu cầu xác thực
Máy chủ xác thực
Bộ xác định rủi ro
21
Bộ phản hồi loại xác thực
22
Bộ xác định rủi ro thứ hai
200
Bộ xử lý xác thực
24
Bộ cập nhật xác định rủi ro
25
Bộ phản hồi kết quả xác thực
26
23
Bảng xác định rủi ro
27
Bảng xác thực
28
Bảng lịch sử xác thực
29
Bảng điều kiện cập nhật xác định rủi ro

Fig.7

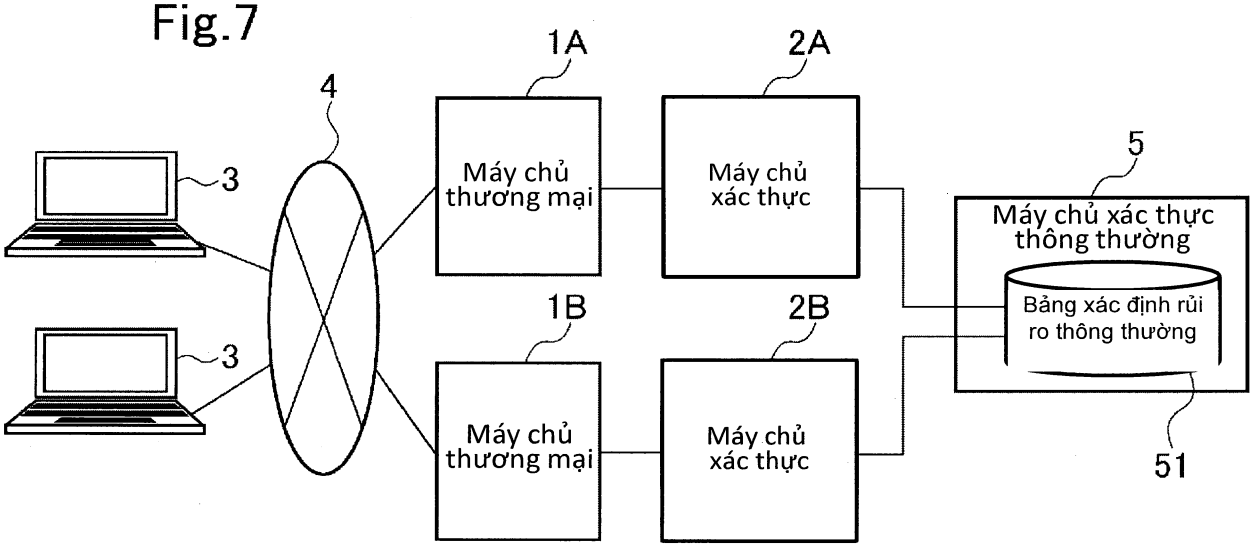

1A
2A
4
3
3
Máy chủ thương mại
Máy chủ xác thực
5
Máy chủ xác thực thông thường
Bảng xác định rủi ro thông thường
1B
2B
Máy chủ thương mại
Máy chủ xác thực
51

Fig.8

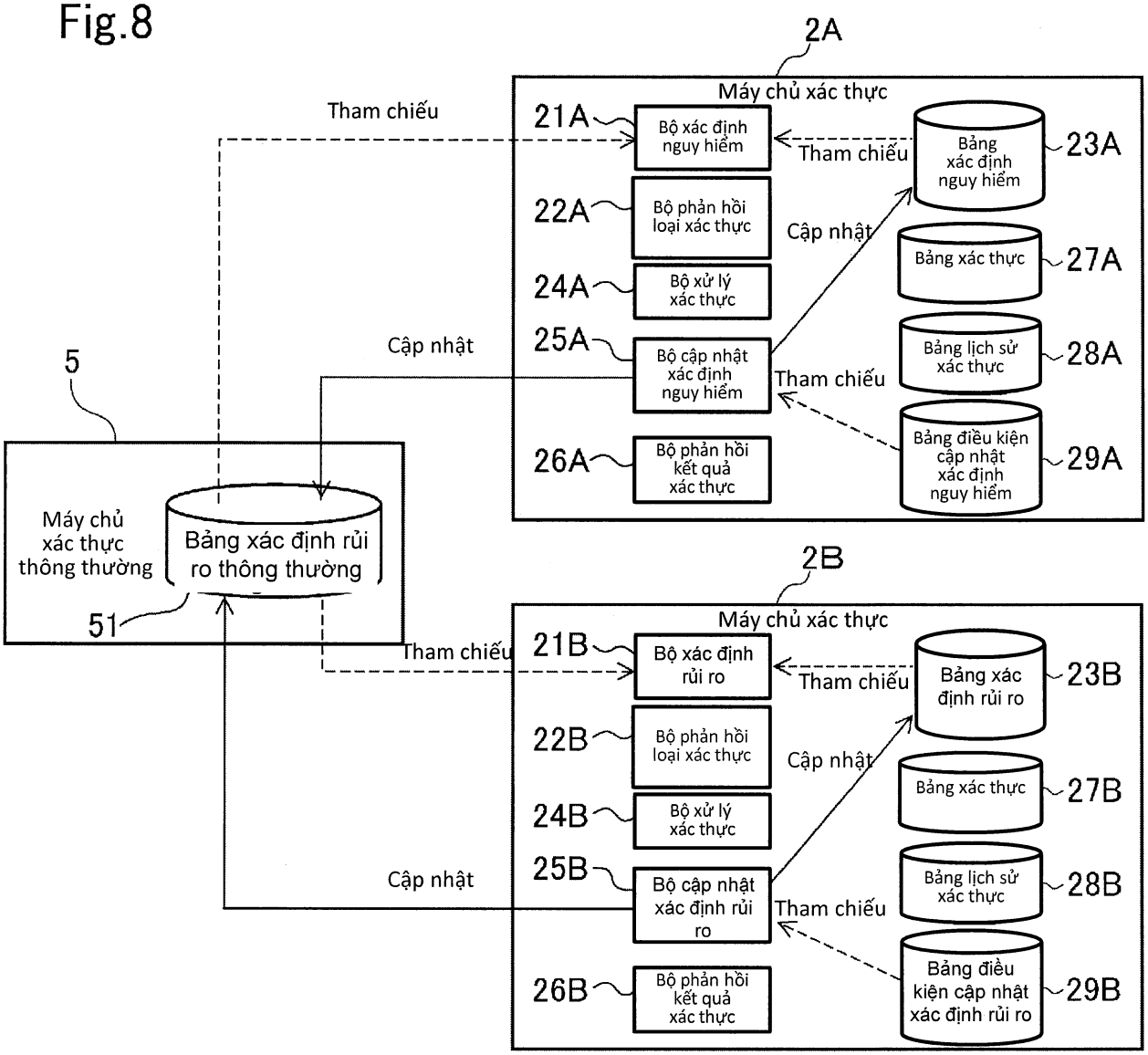


Fig.9

Điều kiện cập nhật	Quy trình cập nhật
Khi các yêu cầu xác thực liên quan đến X1 ID người dùng hoặc nhiều hơn được tạo ra từ cùng một địa chỉ ID trong một khoảng thời gian định trước và tất cả các yêu cầu xác thực đều có kết quả là xác thực thất bại	Bổ sung địa chỉ IP vào danh sách địa chỉ IP trong bảng xác định rủi ro của chính máy chủ đó
• • •	• • •
Khi các yêu cầu xác thực liên quan đến X2 ID người dùng hoặc nhiều hơn được tạo ra từ cùng một địa chỉ ID trong một khoảng thời gian định trước và tất cả các yêu cầu xác thực đều có kết quả là xác thực thất bại	Bổ sung địa chỉ IP vào danh sách địa chỉ IP có mức rủi ro cao trong bảng xác định rủi ro thông thường
• • •	• • •