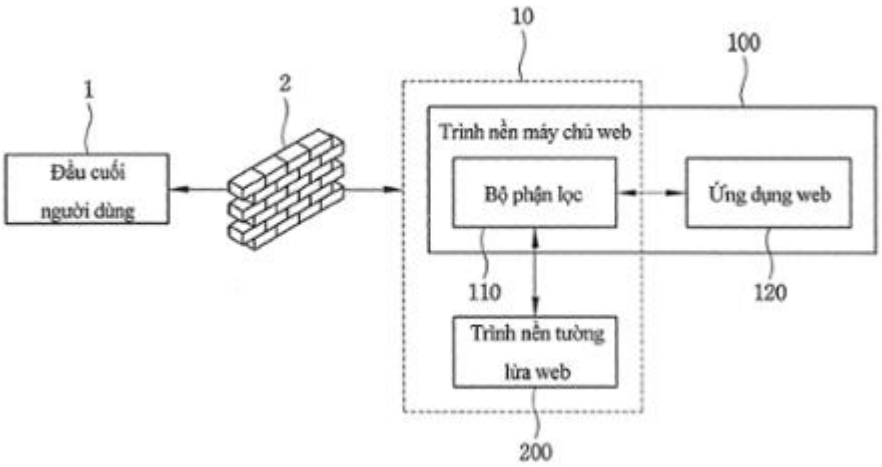
(12) BẢN MÔ TẢ SÁNG CHẾ THUỘC BẰNG ĐỘC QUYỀN SÁNG CHẾ
(19) **Cộng hòa xã hội chủ nghĩa Việt Nam (VN)**
CỤC SỞ HỮU TRÍ TUỆ
(11) **1-0042102**
(51)[7] **H04L 29/06**
(13) **B**

(21) 1-2019-05104
(22) 11/10/2018
(86) PCT/KR2018/011981 11/10/2018
(87) WO2019/231057 A1 05/12/2019
(30) 10-2018-0063747 01/06/2018 KR
(45) 25/12/2024 441
(43) 25/02/2020 383A
(73) F1 SECURITY INC. (KR)
H-1 952AB, KIST, 5, Hwarang-ro 14-gil, Seongbuk-gu, Seoul 08393, Republic of Korea
(72) LEE In Young (KR); LEE Dae Ho (KR); CHOI Sung Su (KR); HWANG Young Suk (KR); LEE Dong Geun (KR); KIM Ki Hwan (KR).
(74) Công ty TNHH Lê & Lê (LE & LE)

(54) HỆ THỐNG VÀ PHƯƠNG PHÁP PHÁT HIỆN VÀ NGĂN CHẶN TẤN CÔNG WEB

(57) Sáng chế đề cập đến hệ thống phát hiện và ngăn chặn tấn công web và phương pháp của nó để phát hiện và ngăn chặn các cuộc tấn công ứng dụng web qua máy chủ web cung cấp dịch vụ web. Sáng chế có thể cung cấp dịch vụ an ninh web tùy chỉnh bởi khách hàng mà không ảnh hưởng tới độ ổn định và tính sẵn sàng của ứng dụng web.



**Lĩnh vực kỹ thuật được đề cập**

Sáng chế đề cập đến việc phát hiện và ngăn chặn tấn công web để phát hiện và ngăn chặn các cuộc tấn công ứng dụng web thông qua máy chủ web cung cấp các dịch vụ web. Cụ thể hơn, sáng chế đề cập đến hệ thống phát hiện và ngăn chặn tấn công web, và phương pháp của nó, hệ thống và phương pháp này có thể xác định có ngăn chặn dữ liệu yêu cầu web hay không bằng cách phân tích dữ liệu yêu cầu web nhận được trong máy chủ web.

**Tình trạng kỹ thuật của sáng chế**

Khi các cuộc tấn công qua Internet đang tiến hoá và phát triển từng ngày, các cuộc tấn công qua web thông thường (các cổng 80 và 443) cũng đã được đa dạng hoá. Ngoài ra, các phương pháp tấn công thông minh thực hiện phát hiện liên tục và tấn công các lỗ hổng chức năng cụ thể của các ứng dụng tiếp tục xuất hiện.

Khó xử lý được các phương pháp tấn công thông minh như vậy bằng cách sử dụng các tường lửa mạng thông thường, các hệ thống phát hiện xâm nhập (IDS), và hệ thống ngăn chặn xâm nhập (IPS) đã biết, v.v..

Các dịch vụ web thông qua các dịch vụ đám mây như là AWS (đám mây dịch vụ web Amazon), Microsoft Azure, v.v., đang ngày càng trở nên tích cực. Ngoài ra, có nhu cầu đề xuất hệ thống phát hiện và ngăn chặn hiệu quả các cuộc tấn công web trong khi loại bỏ được sự phụ thuộc vào cơ sở hạ tầng cơ bản mà vẫn dễ dàng sử dụng hệ thống với chi phí thấp ngay cả trong môi trường đám mây.

Để đáp ứng các nhu cầu này, công bố đơn yêu cầu cấp patent Hàn Quốc số 10-2010-0058695 (công bố ngày 04 tháng 06 năm 2010) bộc lộ một mô hình trên cơ sở lược sử phát hiện tấn công ứng dụng web và phương pháp áp dụng chọn lọc mô hình đó, nhưng các nhu cầu nêu trên không được đáp ứng.

Nói cách khác, kỹ thuật đã biết như mô tả ở trên không thể cung cấp cho khách hàng dịch vụ an ninh web tuỳ chỉnh mà không ảnh hưởng tới độ ổn định và tính sẵn sàng của ứng dụng web. Ngoài ra, có khả năng cao về độ trễ truyền thông phụ thuộc vào trạng thái của mạng Internet, và thông tin DNS phải được thay đổi tới thông tin IP của nhà cung cấp dịch vụ. Do đó, để cung cấp các dịch vụ qua HTTPS, xác thực SSL và khoá cá nhân phải được tải lên nhà cung cấp dịch vụ tường lửa web.

Tư liệu patent 1: Công bố đơn yêu cầu cấp patent Hàn Quốc số 10-2010-0058695 (công bố ngày 04 tháng 06 năm 2010)

**Bản chất kỹ thuật của sáng chế**

Vấn đề kỹ thuật cần giải quyết

Do đo, sáng chế đã được thực hiện với lưu ý là các vấn đề nêu trên xảy ra trong tình trạng kỹ thuật, và mục đích thứ nhất của sáng chế là đề xuất hệ thống phát hiện và ngăn chặn tấn công web, hệ thống này có khả năng: cung cấp dịch vụ an ninh web tuỳ chỉnh bởi khách hàng mà không ảnh hưởng tới độ ổn định và tính sẵn sàng của ứng dụng web; cung cấp dịch vụ an ninh web bất kể tình trạng của mạng Internet; cung cấp cài đặt, cập nhật, và nâng cấp phiên bản dễ dàng của phần mềm; cung cấp các dịch vụ an ninh trong khi duy trì cấu hình mạng hiện có; cung cấp các dịch vụ an ninh mà không thay đổi IP và thông

tin DNS; cung cấp ngăn chặn xác thực SSL và khoá cá nhân bị lộ và giảm chi phí ban đầu của việc giới thiệu; có thể áp dụng với môi trường máy chủ đám mây một cách trơn chu; và có thể áp dụng với hệ thống an ninh ứng dụng web, máy chủ web được cài đặt trong hệ thống đám mây, một điểm cuối của đầu máy chủ ứng dụng di động, một điểm cuối của giao diện người dùng IOT, và một điểm cuối của đầu máy chủ.

Ngoài ra, mục đích thứ hai của sáng chế là đề xuất phương pháp phát hiện và ngăn chặn tấn công web, phương pháp này có khả năng: cung cấp dịch vụ an ninh web tuỳ chỉnh bởi khách hàng mà không ảnh hưởng tới độ ổn định và tính sẵn sàng của ứng dụng web; cung cấp dịch vụ an ninh web bất kể tình trạng của mạng Internet; cung cấp cài đặt, cập nhật, và nâng cấp phiên bản dễ dàng trên phần mềm; cung cấp các dịch vụ an ninh trong khi duy trì cấu hình mạng hiện có; cung cấp các dịch vụ an ninh mà không thay đổi IP và thông tin DNS; cung cấp ngăn chặn xác thực SSL và khoá cá nhân bị lộ và giảm chi phí ban đầu của việc giới thiệu; có thể áp dụng với môi trường máy chủ đám mây một cách trơn chu; và có thể áp dụng với hệ thống an ninh ứng dụng web, máy chủ web được cài đặt trong hệ thống đám mây, một điểm cuối của đầu máy chủ ứng dụng di động, một điểm cuối của giao diện người dùng IOT, và một điểm cuối của đầu máy chủ.

Giải pháp kỹ thuật

Để thực hiện mục đích thứ nhất nêu trên, sáng chế đề xuất hệ thống phát hiện và ngăn chặn tấn công web, hệ thống này bao gồm: bộ phận lọc nhận dữ liệu yêu cầu web từ đầu cuối người dùng, và điều khiển ứng dụng web để duy trì trạng thái chờ; và trình nền tường lửa web nhận dữ liệu yêu cầu web từ bộ phận

lọc, và xác định nguy cơ bằng cách phân tích dữ liệu yêu cầu web và truyền nguy cơ xác định được của dữ liệu yêu cầu web tới bộ phận lọc.

Bộ phận lọc có thể bao gồm: mô-đun truyền thông thứ nhất thực hiện truyền thông với trình nền tường lửa web bằng cách sử dụng cùng giao thức, và nhận nguy cơ xác định được của dữ liệu yêu cầu web từ trình nền tường lửa web; và mô-đun điều khiển thứ nhất điều khiển mô-đun truyền thông thứ nhất để chuẩn bị cho nguy cơ xác định được của dữ liệu yêu cầu web.

Trình nền tường lửa web có thể bao gồm: mô-đun truyền thông thứ hai nhận dữ liệu yêu cầu web từ bộ phận lọc; mô-đun xác định nguy cơ xác định nguy cơ bằng cách phân tích dữ liệu yêu cầu web nhận được trong mô-đun truyền thông thứ hai; và mô-đun thay đổi dữ liệu sửa đổi dữ liệu yêu cầu web khi xác định được rằng nguy cơ xác định được của dữ liệu yêu cầu web thể hiện những thay đổi trong dữ liệu yêu cầu web là cần thiết để phát ra dữ liệu yêu cầu web đã sửa đổi, trong đó mô-đun truyền thông thứ hai có thể truyền dữ liệu yêu cầu web đã sửa đổi tới bộ phận lọc.

Bộ phận lọc có thể còn bao gồm: mô-đun lưu trữ để lưu trữ dữ liệu yêu cầu web và nguy cơ xác định được của dữ liệu yêu cầu web, trong đó mô-đun điều khiển thứ nhất có thể điều khiển mô-đun truyền thông thứ nhất để chuẩn bị cho nguy cơ xác định được của dữ liệu yêu cầu web bằng cách sử dụng nguy cơ xác định được của dữ liệu yêu cầu web được lưu trữ trong mô-đun lưu trữ.

Bộ phận lọc có thể còn bao gồm: mô-đun thu nhận thông tin thu nhận địa chỉ IP (giao thức Internet) và thông tin URL (uniform resource locator - định vị tài nguyên đồng nhất) của đầu cuối người dùng đã truyền dữ liệu yêu cầu web từ dữ liệu yêu cầu web, trong đó mô-đun truyền thông thứ nhất có thể truyền tới mô-

đun truyền thông thứ hai địa chỉ IP và thông tin URL của đầu cuối người dùng, địa chỉ IP và thông tin URL được thu nhận trong mô-đun thu nhận thông tin, mô-đun xác định nguy cơ có thể xác định nguy cơ của dữ liệu yêu cầu web bằng cách phân tích địa chỉ IP và thông tin URL của đầu cuối người dùng, địa chỉ IP và thông tin URL nhận được trong mô-đun truyền thông thứ hai, và khi xác định được rằng địa chỉ IP và thông tin URL của đầu cuối người dùng là không đủ để xác định nguy cơ của dữ liệu yêu cầu web, mô-đun xác định nguy cơ có thể phát ra yêu cầu thông tin bổ sung, và mô-đun truyền thông thứ hai có thể truyền yêu cầu thông tin bổ sung tới mô-đun truyền thông thứ nhất.

Mô-đun thu nhận thông tin có thể thu nhận thông tin bổ sung kết hợp với yêu cầu thông tin bổ sung từ dữ liệu yêu cầu web, mô-đun truyền thông thứ nhất có thể truyền thông tin bổ sung thu nhận được trong mô-đun thu nhận thông tin từ dữ liệu yêu cầu web tới mô-đun truyền thông thứ hai, mô-đun xác định nguy cơ có thể xác định nguy cơ của dữ liệu yêu cầu web bằng cách phân tích thông tin bổ sung nhận được trong mô-đun truyền thông thứ hai, và mô-đun truyền thông thứ hai có thể truyền nguy cơ xác định được của dữ liệu yêu cầu web tới mô-đun truyền thông thứ nhất mà nguy cơ này được thu nhận bằng cách phân tích thông tin bổ sung trong mô-đun xác định nguy cơ.

Để thực hiện mục đích thứ hai nêu trên, sáng chế đề xuất phương pháp phát hiện và ngăn chặn tấn công web, phương pháp này bao gồm: nhận, bởi bộ phận lọc, dữ liệu yêu cầu web từ đầu cuối người dùng; điều khiển, bởi bộ phận lọc, ứng dụng web để duy trì trạng thái chờ; truyền, bởi bộ phận lọc, dữ liệu yêu cầu web tới trình nền tường lửa web; xác định, bởi trình nền tường lửa web, nguy cơ bằng cách phân tích dữ liệu yêu cầu web; và truyền, bởi trình nền tường lửa web, nguy cơ của dữ liệu yêu cầu web tới bộ phận lọc.

Bước truyền, bởi trình nền tường lửa web, nguy cơ của dữ liệu yêu cầu web tới bộ phận lọc có thể bao gồm: điều khiển, bởi mô-đun điều khiển thứ nhất, mô-đun truyền thông thứ nhất để chuẩn bị cho nguy cơ của dữ liệu yêu cầu web nhận được trong mô-đun điều khiển thứ nhất từ trình nền tường lửa web.

Bước xác định, bởi trình nền tường lửa web, nguy cơ bằng cách phân tích dữ liệu yêu cầu web có thể bao gồm: sửa đổi, bởi trình nền tường lửa web, dữ liệu yêu cầu web khi xác định được rằng nguy cơ xác định được của dữ liệu yêu cầu web thể hiện việc sửa đổi dữ liệu yêu cầu web là cần thiết; và phát, bởi trình nền tường lửa web, dữ liệu yêu cầu web đã sửa đổi mà trong đó dữ liệu yêu cầu web đã được sửa đổi, và bước truyền, bởi trình nền tường lửa web, nguy cơ của dữ liệu yêu cầu web tới bộ phận lọc có thể bao gồm: truyền, bởi trình nền tường lửa web, dữ liệu yêu cầu web đã sửa đổi tới bộ phận lọc.

Bước truyền, bởi trình nền tường lửa web, nguy cơ của dữ liệu yêu cầu web tới bộ phận lọc có thể bao gồm: lưu trữ, bởi bộ phận lọc, dữ liệu yêu cầu web và nguy cơ xác định được của dữ liệu yêu cầu web; và điều khiển, bởi mô-đun điều khiển thứ nhất, mô-đun truyền thông thứ nhất để chuẩn bị cho nguy cơ của dữ liệu yêu cầu web bằng cách sử dụng nguy cơ xác định được đã lưu trữ của dữ liệu yêu cầu web.

Bước truyền, bởi bộ phận lọc, dữ liệu yêu cầu web tới trình nền tường lửa web có thể bao gồm: thu nhận, bởi bộ phận lọc, địa chỉ IP và thông tin URL của đầu cuối người dùng đã truyền dữ liệu yêu cầu web; truyền, bởi bộ phận lọc, địa chỉ IP thu nhận được và thông tin URL của đầu cuối người dùng tới trình nền tường lửa web; xác định, bởi trình nền tường lửa web, nguy cơ của dữ liệu yêu cầu web bằng cách phân tích địa chỉ IP và thông tin URL của đầu cuối người

dùng; phát, bởi trình nền tường lửa web, yêu cầu thông tin bổ sung khi địa chỉ IP và thông tin URL của đầu cuối người dùng là không đủ để xác định nguy cơ của dữ liệu yêu cầu web; và truyền, bởi trình nền tường lửa web, yêu cầu thông tin bổ sung tới bộ phận lọc.

Bước truyền, bởi trình nền tường lửa web, yêu cầu thông tin bổ sung tới bộ phận lọc có thể bao gồm: thu nhận, bởi bộ phận lọc, thông tin bổ sung kết hợp với yêu cầu thông tin bổ sung từ dữ liệu yêu cầu web; truyền, bởi bộ phận lọc, thông tin bổ sung thu nhận được từ dữ liệu yêu cầu web tới trình nền tường lửa web; xác định, bởi trình nền tường lửa web, nguy cơ của dữ liệu yêu cầu web bằng cách phân tích thông tin bổ sung; và truyền, bởi trình nền tường lửa web, nguy cơ xác định được của dữ liệu yêu cầu web mà nguy cơ này được xác định bằng cách phân tích thông tin bổ sung tới bộ phận lọc.

Hiệu quả có lợi

Theo hệ thống phát hiện và ngăn chặn tấn công web và phương pháp của nó theo sáng chế được mô tả ở trên, trước tiên, dịch vụ an ninh web tuỳ chỉnh bởi khách hàng mà không ảnh hưởng tới độ ổn định và tính sẵn sàng của ứng dụng web có thể được cung cấp.

Tiếp theo, thứ hai, sáng chế cung cấp dịch vụ an ninh web bất kể tình trạng của mạng Internet.

Ngoài ra, thứ ba, sáng chế có thể đề xuất việc cài đặt, cập nhật, và nâng cấp phiên bản dễ dàng của phần mềm.

Tiếp theo, thứ tư, sáng chế có thể cung cấp các dịch vụ an ninh trong khi duy trì cấu hình mạng hiện có.

Ngoài ra, thứ năm, sáng chế có thể cung cấp các dịch vụ an ninh mà không thay đổi IP và thông tin DNS.

Tiếp theo, thứ sáu, sáng chế có thể ngăn xác thực SSL và khoá cá nhân bị lộ, và giảm chi phí ban đầu của việc giới thiệu.

Ngoài ra, thứ bảy, sáng chế, có thể áp dụng cho môi trường máy chủ đám mây một cách trơn chu.

Tiếp theo, thứ tám, sáng chế có thể áp dụng cho hệ thống an ninh ứng dụng web, máy chủ web được cài đặt trong hệ thống đám mây, điểm cuối của đầu máy chủ ứng dụng di động, điểm cuối của giao diện người dùng IOT, và điểm cuối của đầu máy chủ.

**Mô tả vắn tắt các hình vẽ**

Fig.1 là hình vẽ thể hiện sơ đồ cấu hình của hệ thống phát hiện và ngăn chặn tấn công web theo một phương án thực hiện sáng chế.

Fig.2 là hình vẽ thể hiện sơ đồ cấu hình của bộ phận lọc, bộ phận lọc này là một cấu hình bộ phận theo sáng chế.

Fig.3 là hình vẽ thể hiện sơ đồ cấu hình của trình nền tường lửa web, trình nền này là một cấu hình bộ phận theo sáng chế.

Fig.4 là hình vẽ thể hiện lưu đồ của phương pháp phát hiện và ngăn chặn tấn công web theo một phương án thực hiện sáng chế.

**Mô tả chi tiết sáng chế**

Mọi thuật ngữ hoặc từ ngữ được sử dụng ở đây không nên hiểu là chỉ bị giới hạn ở nghĩa thông dụng và nghĩa theo từ điển mà cần hiểu là có nghĩa và khái niệm được xác định trong phạm vi của sáng chế.

Trong bản mô tả, phần mô tả của một bộ phận nhất định "bao gồm" phương tiện cấu thành nhất định có khả năng còn bao gồm các thành phần khác, và không được loại trừ các thành phần khác trừ khi có tuyên bố cụ thể khác. Hơn nữa, các thuật ngữ "bộ phận ...", "mô-đun ...", và "phương tiện ..." được mô tả trong bản mô tả đề cập đến bộ phận để xử lý ít nhất một chức năng hoặc hoạt động, và có thể được thực hiện bằng phần cứng, phần mềm, hoặc sự kết hợp của chúng.

Các thuật ngữ được sử dụng trong các phương án thực hiện sáng chế sẽ được mô tả vắn tắt, và các phương án thực hiện sẽ được mô tả chi tiết.

Các thuật ngữ kỹ thuật và khoa học được sử dụng ở đây có cùng nghĩa như hiểu biết thông thường bởi người có hiểu biết trung bình về lĩnh vực kỹ thuật trong các phương án lấy làm ví dụ thực hiện sáng chế. Cũng sẽ hiểu được là các thuật ngữ, như là các thuật ngữ được định nghĩa trong các từ điển thông dụng, phải được hiểu là có ý nghĩa phù hợp với ý nghĩa của chúng trong khung cảnh của kỹ thuật liên quan và sẽ không được hiểu theo nghĩa lý tưởng hoá hoặc quá chính thức trừ khi được định nghĩa rõ ràng ở đây. Ngoài ra, các thuật ngữ được sử dụng ở đây được định nghĩa để mô tả thích hợp các phương án lấy làm ví dụ thực hiện sáng chế và vì vậy có thể thay đổi tuỳ thuộc vào ý định của người dùng hoặc người vận hành, hoặc khách hàng. Do đó, các thuật ngữ phải được định nghĩa dựa trên toàn bộ phần mô tả của bản mô tả.

Theo một ví dụ của sáng chế, mặc dù các thuật ngữ bao gồm số thứ tự như thứ nhất hoặc thứ hai có thể được sử dụng để mô tả các chi tiết khác nhau, nhưng các chi tiết không bị giới hạn ở các thuật ngữ này. Các thuật ngữ này được sử dụng để phân biệt một chi tiết với một chi tiết tiết khác. Ví dụ, chi tiết thứ nhất có thể được gọi là chi tiết thứ hai, và chi tiết thứ hai có thể tương tự được gọi là chi tiết thứ nhất mà không nằm ngoài phạm vi của sáng chế. Như được sử dụng ở đây, thuật ngữ "và/hoặc" bao gồm bất kỳ và mọi sự kết hợp của một hoặc nhiều mục được liệt kê.

Ngoài ra, theo phương án lấy làm ví dụ, biểu diễn dạng số ít được sử dụng ở đây bao gồm cả biểu diễn dạng số nhiều trừ khi chúng có ý nghĩa hoàn toàn trái ngược trong ngữ cảnh.

Hơn nữa, trong bản mô tả này, thuật ngữ "bao gồm" hoặc "có" chỉ sự có mặt của một đặc tính, số, bước, hoạt động, chi tiết, bộ phận, hoặc sự kết hợp của chúng đã được mô tả và không loại trừ sự có mặt hoặc bổ sung của ít nhất một đặc tính, số, bước, hoạt động, chi tiết, bộ phận khác, hoặc sự kết hợp của chúng.

Theo một phương án lấy làm ví dụ, "mô-đun" hoặc "bộ phận" thực hiện ít nhất một chức năng hoặc hoạt động, và có thể được thực hiện bằng phần cứng, phần mềm, hoặc sự kết hợp của chúng. Hơn nữa, trừ khi "các mô-đun" hoặc "các bộ phận" phải được thực hiện bằng phần cứng nhất định, nhiều "mô-đun" hoặc nhiều "bộ phận" có thể được tích hợp trong ít nhất một mô-đun và được thực hiện là ít nhất một bộ xử lý (không được thể hiện trên hình vẽ).

Theo các phương án lấy làm ví dụ, trong trường hợp mà một bộ phận nhất định được "nối" với bộ phận khác, nó có thể bao gồm không chỉ trường hợp bộ phận đó được "nối trực tiếp" với bộ phận khác, mà còn bao gồm cả

trường hợp bộ phận đó được "nối điện" với bộ phận khác với một chi tiết khác bố trí giữa chúng.

Sau đây, các phương án thực hiện sáng chế sẽ được mô tả chi tiết có tham khảo các hình vẽ kèm theo.

Fig.1 là hình vẽ thể hiện sơ đồ cấu hình của hệ thống phát hiện và ngăn chặn tấn công web theo một phương án thực hiện sáng chế, Fig.2 là hình vẽ thể hiện sơ đồ cấu hình của bộ phận lọc, bộ phận lọc này là một cấu hình bộ phận theo sáng chế, và Fig.3 là hình vẽ thể hiện sơ đồ cấu hình của trình nền tường lửa web, trình nền này là một cấu hình bộ phận theo sáng chế.

Tham khảo các hình vẽ từ Fig.1 đến Fig.3, hệ thống 10 để phát hiện và ngăn chặn tấn công web có thể bao gồm bộ phận lọc 110 và trình nền tường lửa web 200.

Ngoài ra, bộ phận lọc 110 có thể bao gồm mô-đun điều khiển thứ nhất 111, mô-đun truyền thông thứ nhất 112, mô-đun thu nhận thông tin 113, và mô-đun lưu trữ 114.

Ngoài ra, trình nền tường lửa web 200 có thể bao gồm mô-đun truyền thông thứ hai 210, mô-đun xác định nguy cơ 220, và mô-đun thay đổi dữ liệu 230.

Bộ phận lọc 110 có thể nhận dữ liệu yêu cầu web từ đầu cuối người dùng 1, và điều khiển ứng dụng web 120 để duy trì trạng thái chờ.

Ngoài ra, bộ phận lọc 110 có thể được sử dụng bằng cách nhúng trong trình nền máy chủ web 100.

Ở đây, đầu cuối người dùng 1 có thể được sử dụng trong các thiết bị điện khác nhau như là điện thoại thông minh, đồng hồ thông minh, kính thông minh, máy tính bảng, máy tính xách tay, v.v..

Ngoài ra, trình nền tường lửa web 200 có thể nhận dữ liệu yêu cầu web từ bộ phận lọc 110, và xác định nguy cơ bằng cách phân tích dữ liệu yêu cầu web.

Trình nền tường lửa web 200 có thể truyền nguy cơ xác định được của dữ liệu yêu cầu web tới bộ phận lọc 110.

Ở đây, trình nền tường lửa web 200 có thể được sử dụng bằng cách phân tách hoàn toàn về mặt vật lý với bộ phận lọc 110 mà bộ phận lọc này được sử dụng bằng cách nhúng trong trình nền máy chủ web 100.

Do đó, ứng dụng web 120 không bị ảnh hưởng ngay cả khi hư hỏng hoặc lỗi xảy ra trong tường lửa web.

Do đó, khi thực hiện cập nhật hoặc nâng cấp phiên bản trên tường lửa web, chức năng yêu cầu dữ liệu web, bởi trình nền máy chủ web 100, có thể sẵn sàng mà không cần hoạt động lại trình nền máy chủ web 100 và không cần dừng hoạt động của nó.

Mô-đun truyền thông thứ nhất 112 và mô-đun truyền thông thứ hai 210 có thể thực hiện truyền thông với nhau bằng cách sử dụng cùng giao thức.

Ngoài ra, mô-đun truyền thông thứ nhất 112 có thể nhận nguy cơ xác định được của yêu cầu dữ liệu web từ trình nền tường lửa web 200.

Ngoài ra, mô-đun điều khiển thứ nhất 111 có thể điều khiển mô-đun truyền thông thứ nhất 112 để chuẩn bị cho nguy cơ xác định được của dữ liệu yêu cầu web, là dữ liệu nhận được trong mô-đun truyền thông thứ nhất 112 từ trình nền tường lửa web 200.

Cụ thể, mô-đun điều khiển thứ nhất 111 có thể điều khiển mô-đun truyền thông thứ nhất 112 ngăn chặn dữ liệu yêu cầu web tương ứng khi xác định được rằng nguy cơ xác định được của yêu cầu dữ liệu web thể hiện là việc ngăn chặn dữ liệu yêu cầu web là hợp lý.

Ngoài ra, mô-đun điều khiển thứ nhất 111 có thể điều khiển mô-đun truyền thông thứ nhất 112 truyền dữ liệu yêu cầu web tương ứng tới ứng dụng web 120 khi xác định được rằng nguy cơ xác định được của dữ liệu yêu cầu web thể hiện là việc truyền qua dữ liệu yêu cầu web là hợp lý.

Ngoài ra, mô-đun truyền thông thứ nhất 112 có thể nhận dữ liệu phản hồi liên quan tới dữ liệu yêu cầu web từ ứng dụng web 120.

Ngoài ra, mô-đun truyền thông thứ nhất 112 có thể truyền dữ liệu phản hồi liên quan tới dữ liệu yêu cầu web tới mô-đun truyền thông thứ hai 210.

Ngoài ra, mô-đun truyền thông thứ nhất 112 có thể nhận nguy cơ xác định được của dữ liệu phản hồi được xác định trong mô-đun xác định nguy cơ 220 từ mô-đun truyền thông thứ hai 210.

Thêm vào đó, mô-đun điều khiển thứ nhất 111 có thể điều khiển mô-đun truyền thông thứ nhất 112 chuẩn bị cho nguy cơ xác định được của dữ liệu phản hồi nhận được trong mô-đun truyền thông thứ nhất 112 từ mô-đun truyền thông thứ hai 210.

Cụ thể, mô-đun điều khiển thứ nhất 111 có thể điều khiển mô-đun truyền thông thứ nhất 112 ngăn chặn dữ liệu phản hồi tương ứng khi xác định được rằng nguy cơ xác định được của dữ liệu phản hồi thể hiện việc ngăn chặn dữ liệu phản hồi là hợp lý.

Ngoài ra, mô-đun điều khiển thứ nhất 111 có thể điều khiển mô-đun truyền thông thứ nhất 112 truyền dữ liệu phản hồi tương ứng tới đầu cuối người dùng 1, là đầu cuối đã truyền dữ liệu yêu cầu web khi xác định được rằng nguy cơ xác định được của dữ liệu phản hồi thể hiện việc truyền qua dữ liệu phản hồi là hợp lý.

Mô-đun truyền thông thứ hai 210 có thể nhận dữ liệu yêu cầu web từ bộ phận lọc 110.

Ngoài ra, mô-đun xác định nguy cơ 220 có thể xác định nguy cơ bằng cách phân tích dữ liệu yêu cầu web nhận được trong mô-đun truyền thông thứ hai 210 từ mô-đun truyền thông thứ nhất 112.

Ngoài ra, mô-đun xác định nguy cơ 220 có thể xác định được nguy cơ bằng cách phân tích dữ liệu phản hồi nhận được trong mô-đun truyền thông thứ hai 210 từ mô-đun truyền thông thứ nhất 112.

Ở đây, nguy cơ được xác định trong mô-đun xác định nguy cơ 220 là để xác định những nguy cơ tấn công khác nhau có thể chứa trong dữ liệu yêu cầu web, dữ liệu phản hồi cho dữ liệu yêu cầu web, v.v..

Cụ thể, mô-đun xác định nguy cơ 220 có thể xác định được rằng những thay đổi trong dữ liệu yêu cầu web, dữ liệu phản hồi, v.v. là cần thiết khi dữ liệu yêu cầu web, dữ liệu phản hồi, v.v. bao gồm những nguy cơ tấn công web trên

cơ sở HTTPS/HTTP v1.0, v1.1, v2, và xác định được rằng việc ngăn chặn dữ liệu yêu cầu web, dữ liệu phản hồi, v.v. là hợp lý.

Ngoài ra, mô-đun xác định nguy cơ 220 có thể xác định được rằng dữ liệu yêu cầu web, dữ liệu phản hồi, v.v. là bất thường, khi yêu cầu dữ liệu web, dữ liệu phản hồi, v.v. bao gồm một tham chiếu thứ nhất định trước là ít nhất một trong số nhúng mã, xác thực và quản lý phiên bị hỏng, lộ dữ liệu nhạy cảm, đối tượng bên ngoài XML (XXE), điều khiển truy cập bị hỏng, cấu hình bảo mật sai, kịch bản chéo trang (XSS), chuyển đổi ngược tuần tự không an toàn, sử dụng các thành phần có lỗ hổng đã biết, và đăng nhập và giám sát không đủ. Do đó, mô-đun xác định nguy cơ 220 có thể lấy được kết quả mà việc ngăn chặn dữ liệu yêu cầu web, dữ liệu phản hồi, v.v. là hợp lý, và xác định được rằng các thay đổi trong dữ liệu yêu cầu web, dữ liệu phản hồi, v.v. là cần thiết.

Ở đây, nhúng mã có thể bao gồm nhúng mã SQL/XQuery/XPath/LDAP.

Ngoài ra, mô-đun xác định nguy cơ 220 có thể lấy được kết quả mà việc ngăn chặn dữ liệu yêu cầu web, dữ liệu phản hồi, v.v. là hợp lý bằng cách sử dụng quy tắc thứ nhất định trước trong ít nhất một trong các quy tắc để bảo vệ chống lại những người gửi thư rác hoặc hoạt động độc hại đã biết (REQUEST-910-IP-REPUTATION), các quy tắc khoá phương pháp (PUT, PATCH, v.v.) (REQUEST-911-METHOD-ENFORCEMENT), các quy tắc bảo vệ chống lại các cuộc tấn công từ chối dịch vụ (DoS) (REQUEST-912-DOS-PROTECTION), các quy tắc bảo vệ chống lại bộ quét cổng và môi trường (REQUEST-913-SCANNER-DETECTION), các quy tắc bảo vệ chống lại vấn đề giao thức và mã hoá (REQUEST-920-PROTOCOL-ENFORCEMENT), các quy tắc bảo vệ chống lại nhúng tiêu đề, giấu yêu cầu, và chia tách phản hồi

(REQUEST-921-PROTOCOL-ATTACK), các quy tắc bảo vệ chống lại các cuộc tấn công tệp và đường dẫn (REQUEST-930-APPLICATION-ATTACK-LFI), các quy tắc bảo vệ chống lại chèn tệp từ xa (RFI) (REQUEST-931-APPLICATION-ATTACK-RFI), các quy tắc bảo vệ chống lại thực thi mã từ xa (REQUEST-932-APPLICATION-ATTACK-RCE), các quy tắc bảo vệ chống lại các cuộc tấn công nhúng mã PHP (REQUEST-933-APPLICATION-ATTACK-PHP), các quy tắc bảo vệ chống lại kịch bản chéo trang (REQUEST-941-APPLICATION-ATTACK-XSS), các quy tắc bảo vệ chống lại các cuộc tấn công nhúng mã SQL (REQUEST-942-APPLICATION-ATTACK-SQLI), và các quy tắc bảo vệ chống lại các cuộc tấn công ấn định phiên làm việc (REQUEST-943-APPLICATION-ATTACK-SESSION-FIXATION). Ngoài ra, mô-đun xác định nguy cơ 220 có thể xác định rằng những thay đổi trong dữ liệu yêu cầu web, dữ liệu phản hồi, v.v. là cần thiết.

Ngoài ra, khi dữ liệu yêu cầu web, dữ liệu phản hồi, v.v. bao gồm ít nhất một tham chiếu thứ nhất định trước, mô-đun xác định nguy cơ 220 có thể xác định rằng những thay đổi trong dữ liệu yêu cầu web, dữ liệu phản hồi, v.v. là cần thiết.

Ngoài ra, mô-đun xác định nguy cơ 220 có thể xác định nguy cơ của dữ liệu yêu cầu web, dữ liệu phản hồi, v.v. bằng cách xác định rằng dữ liệu yêu cầu web, dữ liệu phản hồi, v.v. có đáp ứng tiêu chuẩn an toàn dữ liệu (PCI DSS) hay không.

Nói cách khác, mô-đun xác định nguy cơ 220 có thể lấy được kết quả mà dữ liệu yêu cầu web, dữ liệu phản hồi, v.v. là bình thường khi dữ liệu yêu cầu web, dữ liệu phản hồi, v.v. đáp ứng tiêu chuẩn an toàn dữ liệu PCI (PCI

DSS). Ngoài ra, mô-đun xác định nguy cơ 220 có thể lấy được kết quả mà việc chặn dữ liệu yêu cầu web, dữ liệu phản hồi, v.v. là hợp lý khi dữ liệu yêu cầu web, dữ liệu phản hồi, v.v. không đáp ứng tiêu chuẩn an toàn dữ liệu PCI (PCI DSS), và xác định được rằng những thay đổi trong dữ liệu yêu cầu web, dữ liệu phản hồi, v.v. là cần thiết.

Ngoài ra, mô-đun xác định nguy cơ 220 có thể lấy được kết quả mà việc chặn dữ liệu yêu cầu web, dữ liệu phản hồi, v.v. là hợp lý khi dữ liệu yêu cầu web, dữ liệu phản hồi, v.v. bao gồm tham chiếu thứ hai định trước của ít nhất một lỗ hổng liệt kê thư mục, lỗ hổng tải xuống tệp, lỗ hổng kịch bản chéo trang, lỗ hổng tải lên tệp, lỗ hổng WebDAV, lỗ hổng chú thích kỹ thuật (technote), lỗ hổng zeroboard, và lỗ hổng nhúng mã SQL, và xác định được rằng những thay đổi trong dữ liệu yêu cầu web, dữ liệu phản hồi, v.v. là cần thiết.

Ngoài ra, mô-đun xác định nguy cơ 220 có thể lấy được kết quả mà việc chặn dữ liệu yêu cầu web, dữ liệu phản hồi, v.v. là hợp lý khi dữ liệu yêu cầu web, dữ liệu phản hồi, v.v. tương ứng với giả mạo tệp URI, và xác định được rằng những thay đổi trong dữ liệu yêu cầu web, dữ liệu phản hồi, v.v. là cần thiết.

Ngoài ra, khi mô-đun xác định nguy cơ 220 xác định được rằng những thay đổi trong dữ liệu yêu cầu web, bởi mô-đun thay đổi dữ liệu 230, là cần thiết theo nguy cơ xác định được của dữ liệu yêu cầu web, mô-đun thay đổi dữ liệu 230 có thể sửa đổi dữ liệu yêu cầu web, và phát ra dữ liệu yêu cầu web đã sửa đổi.

Ngoài ra, việc sửa đổi, bởi mô-đun thay đổi dữ liệu 230, dữ liệu yêu cầu web có thể bao gồm những thay đổi trong dữ liệu vận chuyển (payload) của dữ liệu yêu cầu web.

Ngoài ra, mô-đun thay đổi dữ liệu 230 có thể sửa đổi dữ liệu yêu cầu web bằng cách sử dụng quy tắc thứ nhất định trước trong ít nhất một trong các quy tắc để bảo vệ chống lại những người gửi thư rác hoặc hoạt động độc hại đã biết (REQUEST-910-IP-REPUTATION), các quy tắc khoá phương pháp (PUT, PATCH, v.v.) (REQUEST-911-METHOD-ENFORCEMENT), các quy tắc bảo vệ chống lại các cuộc tấn công từ chối dịch vụ (DoS) (REQUEST-912-DOS-PROTECTION), các quy tắc bảo vệ chống lại bộ quét cổng và môi trường (REQUEST-913-SCANNER-DETECTION), các quy tắc bảo vệ chống lại vấn đề giao thức và mã hoá (REQUEST-920-PROTOCOL-ENFORCEMENT), các quy tắc bảo vệ chống lại nhúng tiêu đề, giấu yêu cầu, và chia tách phản hồi (REQUEST-921-PROTOCOL-ATTACK), các quy tắc bảo vệ chống lại các cuộc tấn công tệp và đường dẫn (REQUEST-930-APPLICATION-ATTACK-LFI), các quy tắc bảo vệ chống lại chèn tệp từ xa (RFI) (REQUEST-931-APPLICATION-ATTACK-RFI), các quy tắc bảo vệ chống lại thực thi mã từ xa (REQUEST-932-APPLICATION-ATTACK-RCE), các quy tắc bảo vệ chống lại các cuộc tấn công nhúng mã PHP (REQUEST-933-APPLICATION-ATTACK-PHP), các quy tắc bảo vệ chống lại kịch bản chéo trang (REQUEST-941-APPLICATION-ATTACK-XSS), các quy tắc bảo vệ chống lại các cuộc tấn công nhúng mã SQL (REQUEST-942-APPLICATION-ATTACK-SQLI), và các quy tắc bảo vệ chống lại các cuộc tấn công ấn định phiên làm việc (REQUEST-943-APPLICATION-ATTACK-

SESSION-FIXATION). Ngoài ra, mô-đun thay đổi dữ liệu 230 có thể phát ra dữ liệu yêu cầu web đã sửa đổi.

Ngoài ra, mô-đun xác định nguy cơ 220 và mô-đun thay đổi dữ liệu 230 đã mô tả ở trên có thể áp dụng, ngoài dữ liệu yêu cầu web, sửa đổi dữ liệu yêu cầu web, hoặc dữ liệu phản hồi kết hợp với dữ liệu yêu cầu web đã sửa đổi.

Ngoài ra, mô-đun truyền thông thứ hai 210 có thể truyền dữ liệu yêu cầu web đã sửa đổi tới bộ phận lọc 110.

Ngoài ra, dữ liệu yêu cầu web, và nguy cơ xác định được của dữ liệu yêu cầu web có thể được lưu trữ trong mô-đun lưu trữ 114.

Cụ thể, ít nhất một trong số dữ liệu yêu cầu web nhận được trong mô-đun truyền thông thứ nhất 112 từ mô-đun truyền thông thứ hai 210, và nguy cơ xác định được của dữ liệu yêu cầu web xác định được trong mô-đun xác định nguy cơ 220 có thể được lưu trữ trong mô-đun lưu trữ 114.

Ngoài ra, ít nhất một trong số dữ liệu phản hồi nhận được trong mô-đun truyền thông thứ nhất 112 từ mô-đun truyền thông thứ hai 210, và nguy cơ xác định được của dữ liệu phản hồi được xác định trong mô-đun xác định nguy cơ 220 có thể được lưu trữ trong mô-đun lưu trữ 114 .

Ngoài ra, bằng cách sử dụng nguy cơ xác định được của dữ liệu yêu cầu web được lưu trữ trong mô-đun lưu trữ 114 đã mô tả ở trên, mô-đun điều khiển thứ nhất 111 có thể điều khiển mô-đun truyền thông thứ nhất 112 để chuẩn bị nguy cơ xác định được của dữ liệu yêu cầu web.

Cụ thể, mô-đun điều khiển thứ nhất 111 có thể xác định được rằng nguy cơ xác định được tương ứng của dữ liệu yêu cầu web có được lưu trữ trong mô-

đun lưu trữ 114 khi mô-đun truyền thông thứ nhất 112 nhận dữ liệu yêu cầu web từ đầu cuối người dùng 1.

Ngoài ra, khi nguy cơ xác định được tương ứng của dữ liệu yêu cầu web được lưu trữ trong mô-đun lưu trữ 114, mô-đun điều khiển thứ nhất 111 có thể điều khiển mô-đun truyền thông thứ nhất 112 chuẩn bị cho nguy cơ xác định được của dữ liệu yêu cầu web bằng cách sử dụng nguy cơ xác định được tương ứng của dữ liệu yêu cầu web.

Nói cách khác, khi được thể hiện là việc chặn dữ liệu yêu cầu web là hợp lý trong nguy cơ xác định được tương ứng của dữ liệu yêu cầu web được lưu trữ trong mô-đun lưu trữ 114, mô-đun điều khiển thứ nhất 111 có thể điều khiển mô-đun truyền thông thứ nhất 112 ngăn chặn dữ liệu yêu cầu web tương ứng.

Ngoài ra, khi được thể hiện là việc truyền qua dữ liệu yêu cầu web là hợp lý trong nguy cơ xác định được tương ứng của dữ liệu yêu cầu web được lưu trữ trong mô-đun lưu trữ 114, mô-đun điều khiển thứ nhất 111 có thể điều khiển mô-đun truyền thông thứ nhất 112 truyền dữ liệu yêu cầu web tương ứng tới ứng dụng web 120.

Ngoài ra, bằng cách sử dụng nguy cơ xác định được của dữ liệu phản hồi lưu trữ trong mô-đun lưu trữ 114 đã mô tả ở trên, mô-đun điều khiển thứ nhất 111 có thể điều khiển mô-đun truyền thông thứ nhất 112 chuẩn bị cho nguy cơ xác định được của dữ liệu phản hồi.

Cụ thể, mô-đun điều khiển thứ nhất 111 có thể xác định được là nguy cơ xác định được của dữ liệu phản hồi tương ứng có được lưu trữ trong mô-đun

lưu trữ 114 hay không khi mô-đun truyền thông thứ nhất 112 nhận dữ liệu phản hồi từ ứng dụng web 120.

Ngoài ra, khi nguy cơ xác định được của dữ liệu phản hồi tương ứng được lưu trữ trong mô-đun lưu trữ 114, mô-đun điều khiển thứ nhất 111 có thể điều khiển mô-đun truyền thông thứ nhất 112 chuẩn bị cho nguy cơ xác định được của dữ liệu phản hồi bằng cách sử dụng nguy cơ xác định được của dữ liệu phản hồi tương ứng.

Nói cách khác, khi được thể hiện là việc chặn dữ liệu phản hồi là hợp lý trong nguy cơ xác định được của dữ liệu phản hồi lưu trữ trong mô-đun lưu trữ 114, mô-đun điều khiển thứ nhất 111 có thể điều khiển mô-đun truyền thông thứ nhất 112 ngăn chặn dữ liệu phản hồi tương ứng.

Ngoài ra, khi được thể hiện là việc truyền qua dữ liệu phản hồi là hợp lý trong nguy cơ xác định được của dữ liệu phản hồi lưu trữ trong mô-đun lưu trữ 114, mô-đun điều khiển thứ nhất 111 có thể điều khiển mô-đun truyền thông thứ nhất 112 truyền dữ liệu phản hồi tương ứng tới đầu cuối người dùng 1.

Như được mô tả ở trên, nguy cơ xác định được của dữ liệu yêu cầu web hoặc nguy cơ xác định được của dữ liệu phản hồi được lưu trữ trong mô-đun lưu trữ 114, và vì vậy bộ phận lọc 110 có thể thực hiện lọc nhanh chóng và chính xác dữ liệu yêu cầu web. Do đó, có hiệu quả là có thể chuẩn bị cho trường hợp mà truyền và nhận giữa trình nền tường lửa web 200 và bộ phận lọc 110 không trơn chu.

Ngoài ra, mô-đun thu nhận thông tin 113 có thể nhận địa chỉ IP (Internet protocol - giao thức Internet) và thông tin URL (uniform resource locator - định

vị tài nguyên đồng nhất) của đầu cuối người dùng 1 đã truyền dữ liệu yêu cầu web từ dữ liệu yêu cầu web.

Ngoài ra, mô-đun truyền thông thứ nhất 112 có thể truyền địa chỉ IP và thông tin URL của đầu cuối người dùng 1 được thu nhận trong mô-đun thu nhận thông tin 113 tới mô-đun truyền thông thứ hai 210.

Ngoài ra, mô-đun xác định nguy cơ 220 có thể xác định được nguy cơ của dữ liệu yêu cầu web bằng cách phân tích địa chỉ IP và thông tin URL của đầu cuối người dùng 1 nhận được trong mô-đun truyền thông thứ hai 210.

Ngoài ra, mô-đun xác định nguy cơ 220 có thể phát yêu cầu thông tin bổ sung khi địa chỉ IP và thông tin URL của đầu cuối người dùng 1 là không đủ để xác định nguy cơ của dữ liệu yêu cầu web.

Ngoài ra, mô-đun truyền thông thứ hai 210 có thể truyền yêu cầu thông tin bổ sung tới mô-đun truyền thông thứ nhất 112.

Ngoài ra, mô-đun thu nhận thông tin 113 có thể nhận thông tin bổ sung kết hợp với yêu cầu thông tin bổ sung từ dữ liệu yêu cầu web.

Ngoài ra, mô-đun truyền thông thứ nhất 112 có thể truyền thông tin bổ sung thu nhận được từ dữ liệu yêu cầu web bởi mô-đun thu nhận thông tin 113 tới mô-đun truyền thông thứ hai 210.

Ngoài ra, mô-đun xác định nguy cơ 220 có thể phân tích thông tin bổ sung nhận được trong mô-đun truyền thông thứ hai 210 từ mô-đun truyền thông thứ nhất 112, và xác định nguy cơ của dữ liệu yêu cầu web.

Ngoài ra, mô-đun truyền thông thứ hai 210 có thể truyền tới mô-đun truyền thông thứ nhất 112 nguy cơ xác định được của dữ liệu yêu cầu web được xác định bằng cách phân tích thông tin bổ sung bởi mô-đun xác định nguy cơ 220.

Fig.4 là hình vẽ thể hiện lưu đồ của phương pháp phát hiện và ngăn chặn tấn công web theo một phương án thực hiện sáng chế.

Tham khảo Fig.4, trong bước S430, bộ phận lọc 110 có thể nhận dữ liệu yêu cầu web từ đầu cuối người dùng 1.

Sau đó, trong bước S431, bộ phận lọc 110 có thể điều khiển ứng dụng web 120 để duy trì trạng thái chờ.

Sau đó, trong đó S432, bộ phận lọc 110 có thể truyền dữ liệu yêu cầu web tới trình nền tường lửa web 200.

Bộ phận lọc 110 có thể thu nhận địa chỉ IP và thông tin URL của đầu cuối người dùng 1 đã truyền dữ liệu yêu cầu web.

Sau đó, bộ phận lọc 110 có thể truyền địa chỉ IP thu nhận được và thông tin URL của đầu cuối người dùng 1 tới trình nền tường lửa web 200.

Ngoài ra, trình nền tường lửa web 200 có thể xác định nguy cơ của dữ liệu yêu cầu web bằng cách phân tích địa chỉ IP và thông tin URL của đầu cuối người dùng 1.

Sau đó, trình nền tường lửa web 200 có thể phát yêu cầu thông tin bổ sung khi địa chỉ IP và thông tin URL của đầu cuối người dùng 1 là không đủ để xác định nguy cơ của dữ liệu yêu cầu web.

Ngoài ra, trình nền tường lửa web 200 có thể truyền yêu cầu thông tin bổ sung tới bộ phận lọc 110.

Sau đó, bộ phận lọc 110 có thể thu nhận thông tin bổ sung kết hợp với yêu cầu thông tin bổ sung từ yêu cầu của dữ liệu web.

Ngoài ra, bộ phận lọc 110 có thể truyền thông tin bổ sung thu nhận được từ dữ liệu yêu cầu web tới trình nền tường lửa web 200.

Sau đó, trình nền tường lửa web 200 có thể xác định nguy cơ của dữ liệu yêu cầu web bằng cách phân tích thông tin bổ sung.

Ngoài ra, trình nền tường lửa web 200 có thể truyền nguy cơ xác định được của dữ liệu yêu cầu web được xác định bằng cách phân tích thông tin bổ sung tới bộ phận lọc 110.

Sau đó, trong bước S433, trình nền tường lửa web 200 có thể xác định nguy cơ bằng cách phân tích dữ liệu yêu cầu web.

Ngoài ra, trình nền tường lửa web 200 có thể sửa đổi dữ liệu yêu cầu web khi trình nền tường lửa web 200 xác định được rằng những thay đổi trong dữ liệu yêu cầu web là cần thiết theo sự xác định đã thực hiện.

Sau đó, trình nền tường lửa web 200 có thể phát dữ liệu yêu cầu web đã sửa đổi mà trong đó dữ liệu yêu cầu web được sửa đổi.

Tiếp theo, trong bước S434, trình nền tường lửa web 200 có thể truyền nguy cơ xác định được của dữ liệu yêu cầu web tới bộ phận lọc 110.

Tiếp theo, mô-đun điều khiển thứ nhất 111 của bộ phận lọc 110 có thể điều khiển mô-đun truyền thông thứ nhất 112 của bộ phận lọc 110 để chuẩn bị

cho nguy cơ xác định được của dữ liệu yêu cầu web nhận được từ trình nền tường lửa web 200.

Ngoài ra, trình nền tường lửa web 200 có thể truyền dữ liệu yêu cầu web đã sửa đổi tới bộ phận lọc 110.

Sau đó, bộ phận lọc 110 có thể lưu trữ dữ liệu yêu cầu web và nguy cơ xác định được của dữ liệu yêu cầu web.

Tiếp theo, bằng cách sử dụng dữ liệu yêu cầu web đã lưu trữ và nguy cơ xác định được của dữ liệu yêu cầu web, mô-đun điều khiển thứ nhất 111 của bộ phận lọc 110 có thể điều khiển mô-đun truyền thông thứ nhất 112 của bộ phận lọc 110 chuẩn bị cho nguy cơ xác định được đã lưu trữ của dữ liệu yêu cầu web.

Các cấu hình và hoạt động của hệ thống phát hiện và ngăn chặn tấn công web và phương pháp của nó theo sáng chế có thể được sử dụng như được mô tả ở trên. Trong khi, trong phần mô tả sáng chế ở trên, các phương án cụ thể đã được mô tả, nhưng các biến thể khác nhau có thể được thực hiện mà không nằm ngoài phạm vi của sáng chế.

Mặc dù sáng chế đã được mô tả có tham khảo các phương án giới hạn và các hình vẽ, sáng chế không bị giới hạn ở đó, và các biến thể và các thay đổi khác nhau có thể được thực hiện bởi người có hiểu biết trung bình về lĩnh vực kỹ thuật liên quan của sáng chế.

Người có hiểu biết trung bình về lĩnh vực kỹ thuật sẽ hiểu rằng sáng chế có thể nằm ở một dạng sửa đổi mà không nằm ngoài các đặc điểm thiết yếu của nền tảng đã mô tả ở trên. Vì vậy, các phương án đã mô tả ở trên sẽ được coi là cách thức mô tả, mà không phải cách thức giới hạn sáng chế. Phạm vi của sáng

chế được thể hiện trong các điểm yêu cầu bảo hộ thay vì phần mô tả ở trên, và mọi khác biệt trong phạm vi sẽ được hiểu là nằm trong sáng chế.

Mô tả các số chỉ dẫn

1: đầu cuối người dùng

2: tường lửa mạng

10: hệ thống phát hiện và ngăn chặn tấn công web

100: trình nền máy chủ web

110: bộ phận lọc

111: mô-đun điều khiển thứ nhất

112: mô-đun truyền thông thứ nhất

113: mô-đun thu nhận thông tin

114: mô-đun lưu trữ

120: ứng dụng web

200: trình nền tường lửa web

210: mô-đun truyền thông thứ hai

220: mô-đun xác định nguy cơ

230: mô-đun thay đổi dữ liệu

Áp dụng công nghiệp

Theo hệ thống phát hiện và ngăn chặn tấn công web, và phương pháp của nó theo sáng chế, trước tiên, dịch vụ an ninh web được tuỳ chỉnh bởi khách hàng mà không ảnh hưởng tới độ ổn định và tính sẵn sàng của ứng dụng web có

thể được cung cấp, dịch vụ an ninh web bất kể tình trạng của mạng Internet có thể được cung cấp, việc cài đặt, cập nhật, và nâng cấp phiên bản dễ dàng trên phần mềm có thể được cung cấp, các dịch vụ an ninh trong khi duy trì cấu hình mạng hiện có có thể được cung cấp, các dịch vụ an ninh mà không thay đổi IP và thông tin DNS có thể được cung cấp, xác thực SSL và khoá cá nhân có thể được ngăn chặn bị lộ và chi phí ban đầu của việc giới thiệu có thể giảm đi, ứng dụng với môi trường máy chủ đám mây một cách trơn chu luôn sẵn sàng, và ứng dụng với hệ thống an ninh ứng dụng web, máy chủ web được cài đặt trong hệ thống đám mây, và điểm cuối của đầu máy chủ ứng dụng di động, đầu cuối của giao diện người dùng IOT, và đấu cuối của đầu máy chủ có thể luôn sẵn sàng.

Hệ thống phát hiện và ngăn chặn tấn công web, và phương pháp của nó có những hiệu quả khác nhau có thể tác động tích cực lên các ngành công nghiệp phần mềm và giải pháp an ninh và có thể được sử dụng theo nhiều cách.

## YÊU CẦU BẢO HỘ

1. Hệ thống phát hiện và ngăn chặn tấn công web, hệ thống này bao gồm:

bộ xử lý phần cứng được tạo cấu hình để thực hiện hoạt động của bộ phận lọc và trình nền tường lửa web;

bộ phận lọc nhận dữ liệu yêu cầu web từ đầu cuối người dùng, và điều khiển ứng dụng web để duy trì trạng thái chờ; và

trình nền tường lửa web nhận dữ liệu yêu cầu web từ bộ phận lọc, và xác định nguy cơ bằng cách phân tích dữ liệu yêu cầu web và truyền nguy cơ xác định được của dữ liệu yêu cầu web tới bộ phận lọc,

trong đó bộ phận lọc bao gồm:

mô-đun truyền thông thứ nhất thực hiện truyền thông với trình nền tường lửa web bằng cách sử dụng cùng giao thức, và nhận nguy cơ xác định được của dữ liệu yêu cầu web từ trình nền tường lửa web; và

mô-đun điều khiển thứ nhất điều khiển mô-đun truyền thông thứ nhất để chuẩn bị cho nguy cơ xác định được của dữ liệu yêu cầu web;

trong đó trình nền tường lửa web bao gồm:

mô-đun truyền thông thứ hai nhận dữ liệu yêu cầu web từ bộ phận lọc;

mô-đun xác định nguy cơ xác định nguy cơ bằng cách phân tích dữ liệu yêu cầu web nhận được trong mô-đun truyền thông thứ hai; và

mô-đun thay đổi dữ liệu sửa đổi dữ liệu yêu cầu web khi xác định

được rằng nguy cơ xác định được của dữ liệu yêu cầu web thể hiện các thay đổi trong dữ liệu yêu cầu web là cần thiết để phát dữ liệu yêu cầu web đã sửa đổi,

trong đó mô-đun truyền thông thứ hai truyền dữ liệu yêu cầu web đã sửa đổi tới bộ phận lọc;

trong đó bộ phận lọc còn bao gồm: mô-đun thu nhận thông tin thu nhận địa chỉ IP (giao thức Internet) và thông tin URL (định vị tài nguyên đồng nhất) của đầu cuối người dùng đã truyền dữ liệu yêu cầu web từ dữ liệu yêu cầu web,

trong đó mô-đun truyền thông thứ nhất truyền tới mô-đun truyền thông thứ hai địa chỉ IP và thông tin URL của đầu cuối người dùng, địa chỉ IP và thông tin URL thu nhận được trong mô-đun thu nhận thông tin;

mô-đun xác định nguy cơ xác định nguy cơ của dữ liệu yêu cầu web bằng cách phân tích địa chỉ IP và thông tin URL của đầu cuối người dùng, địa chỉ IP và thông tin URL nhận được trong mô-đun truyền thông thứ hai, và khi xác định được là địa chỉ IP và thông tin URL của đầu cuối người dùng là không đủ để xác định nguy cơ của dữ liệu yêu cầu web, mô-đun xác định nguy cơ phát yêu cầu thông tin bổ sung; và

mô-đun truyền thông thứ hai truyền yêu cầu thông tin bổ sung tới mô-đun truyền thông thứ nhất; và

trong đó mô-đun thu nhận thông tin thu nhận thông tin bổ sung kết hợp với yêu cầu thông tin bổ sung từ dữ liệu yêu cầu web;

mô-đun truyền thông thứ nhất truyền thông tin bổ sung thu nhận được trong mô-đun thu nhận thông tin từ dữ liệu yêu cầu web tới mô-đun truyền thông

thứ hai;

mô-đun xác định nguy cơ xác định nguy cơ của dữ liệu yêu cầu web bằng cách phân tích thông tin bổ sung nhận được trong mô-đun truyền thông thứ hai; và

mô-đun truyền thông thứ hai truyền nguy cơ xác định được của dữ liệu yêu cầu web tới mô-đun truyền thông thứ nhất mà nguy cơ xác định được này được thu nhận bằng cách phân tích thông tin bổ sung trong mô-đun xác định nguy cơ.

2. Hệ thống theo điểm 1, trong đó bộ phận lọc còn bao gồm: mô-đun lưu trữ để lưu trữ dữ liệu yêu cầu web và nguy cơ xác định được của dữ liệu yêu cầu web,

trong đó mô-đun điều khiển thứ nhất điều khiển mô-đun truyền thông thứ nhất để chuẩn bị cho nguy cơ xác định được của dữ liệu yêu cầu web bằng cách sử dụng nguy cơ xác định được của dữ liệu yêu cầu web được lưu trữ trong mô-đun lưu trữ.

3. Phương pháp phát hiện và ngăn chặn tấn công web, phương pháp này bao gồm các bước:

nhận, bởi bộ phận lọc, dữ liệu yêu cầu web từ đầu cuối người dùng;

điều khiển, bởi bộ phận lọc, ứng dụng web để duy trì trạng thái chờ;

truyền, bởi bộ phận lọc, dữ liệu yêu cầu web tới trình nền tường lửa web;

xác định, bởi trình nền tường lửa web, nguy cơ bằng cách phân tích dữ liệu yêu cầu web; và

truyền, bởi trình nền tường lửa web, nguy cơ của dữ liệu yêu cầu web tới

bộ phận lọc,

trong đó bước truyền, bởi trình nền tường lửa web, nguy cơ dữ liệu yêu cầu web tới bộ phận lọc bao gồm: điều khiển, bởi mô-đun điều khiển thứ nhất, mô-đun truyền thông thứ nhất để chuẩn bị cho nguy cơ dữ liệu yêu cầu web nhận được trong mô-đun điều khiển thứ nhất từ trình nền tường lửa web;

trong đó bước truyền, bởi bộ phận lọc, dữ liệu yêu cầu web tới trình nền tường lửa web bao gồm:

thu nhận, bởi bộ phận lọc, địa chỉ IP (giao thức Internet) và thông tin URL (định vị tài nguyên đồng nhất) của đầu cuối người dùng đã truyền dữ liệu yêu cầu web;

truyền, bởi bộ phận lọc, địa chỉ IP và thông tin URL thu nhận được của đầu cuối người dùng tới trình nền tường lửa web;

xác định, bởi trình nền tường lửa web, nguy cơ dữ liệu yêu cầu web bằng cách phân tích địa chỉ IP và thông tin URL của đầu cuối người dùng;

phát, bởi trình nền tường lửa web, yêu cầu thông tin bổ sung khi địa chỉ IP và thông tin URL của đầu cuối người dùng là không đủ để xác định nguy cơ của dữ liệu yêu cầu web; và

truyền, bởi trình nền tường lửa web, yêu cầu thông tin bổ sung tới bộ phận lọc; và

trong đó bước truyền, bởi trình nền tường lửa web, yêu cầu thông tin bổ sung tới bộ phận lọc bao gồm:

thu nhận, bởi bộ phận lọc, thông tin bổ sung kết hợp với yêu cầu

thông tin bổ sung từ dữ liệu yêu cầu web;

truyền, bởi bộ phận lọc, thông tin bổ sung thu nhận được từ dữ liệu yêu cầu web tới trình nền tường lửa web;

xác định, bởi trình nền tường lửa web, nguy cơ của dữ liệu yêu cầu web bằng cách phân tích thông tin bổ sung; và

truyền, bởi trình nền tường lửa web, nguy cơ xác định được của dữ liệu yêu cầu web, mà nguy cơ này được xác định bằng cách phân tích thông tin bổ sung, tới bộ phận lọc.

4. Phương pháp theo điểm 3, trong đó bước xác định, bởi trình nền tường lửa web, nguy cơ bằng cách phân tích dữ liệu yêu cầu web bao gồm:

sửa đổi, bởi trình nền tường lửa web, dữ liệu yêu cầu web khi xác định được rằng nguy cơ xác định được của dữ liệu yêu cầu web thể hiện việc sửa đổi dữ liệu yêu cầu web là cần thiết; và

phát, bởi trình nền tường lửa web, dữ liệu yêu cầu web đã sửa đổi trong đó dữ liệu yêu cầu web đã được sửa đổi, và

truyền, bởi trình nền tường lửa web, nguy cơ của dữ liệu yêu cầu web tới bộ phận lọc bao gồm:

truyền, bởi trình nền tường lửa web, dữ liệu yêu cầu web đã sửa đổi tới bộ phận lọc.

5. Phương pháp theo điểm 3, trong đó bước truyền, bởi trình nền tường lửa web, nguy cơ của dữ liệu yêu cầu web tới bộ phận lọc bao gồm:

lưu trữ, bởi bộ phận lọc, dữ liệu yêu cầu web và nguy cơ xác định được của dữ liệu yêu cầu web; và

điều khiển, bởi mô-đun điều khiển thứ nhất, mô-đun truyền thông thứ nhất để chuẩn bị cho nguy cơ của dữ liệu yêu cầu web bằng cách sử dụng nguy cơ xác định được đã lưu trữ của dữ liệu yêu cầu web.

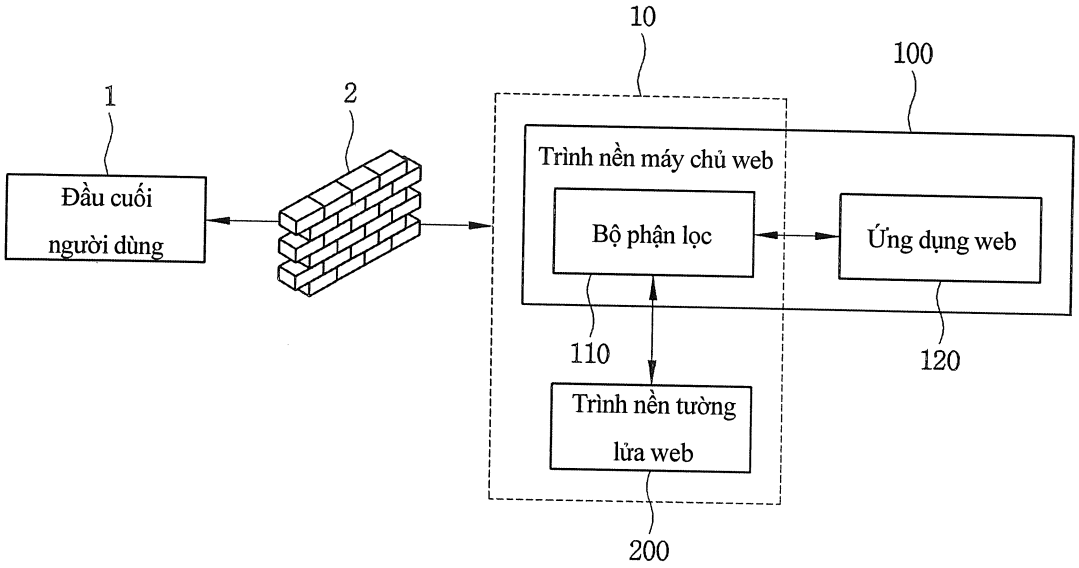

10
100
1
2
Đầu cuối người dùng
Trình nền máy chủ web
Bộ phận lọc
Ứng dụng web
110
120
Trình nền tường lửa web
200

**Fig. 1**

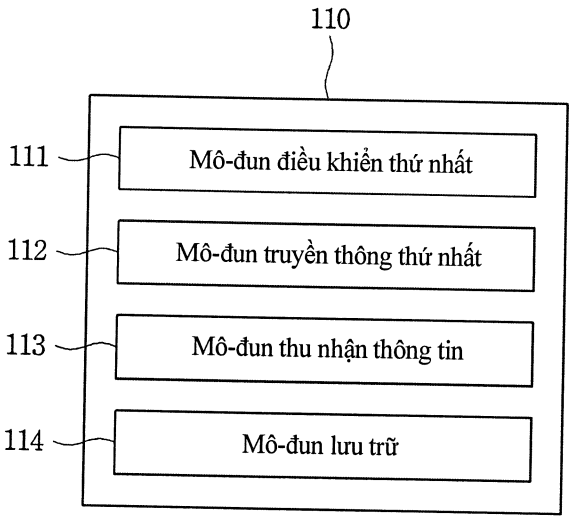

110
111
Mô-đun điều khiển thứ nhất
112
Mô-đun truyền thông thứ nhất
113
Mô-đun thu nhận thông tin
114
Mô-đun lưu trữ

**Fig. 2**

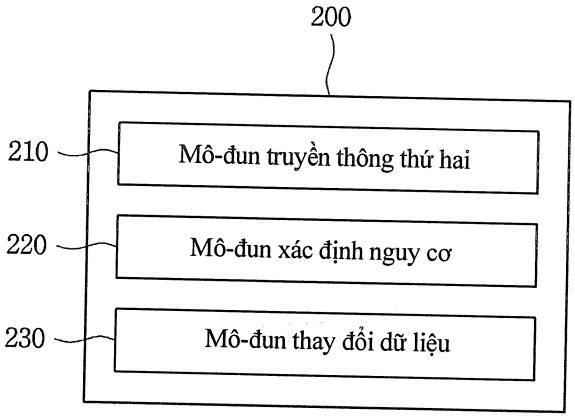

200
210
Mô-đun truyền thông thứ hai
220
Mô-đun xác định nguy cơ
230
Mô-đun thay đổi dữ liệu

**Fig. 3**

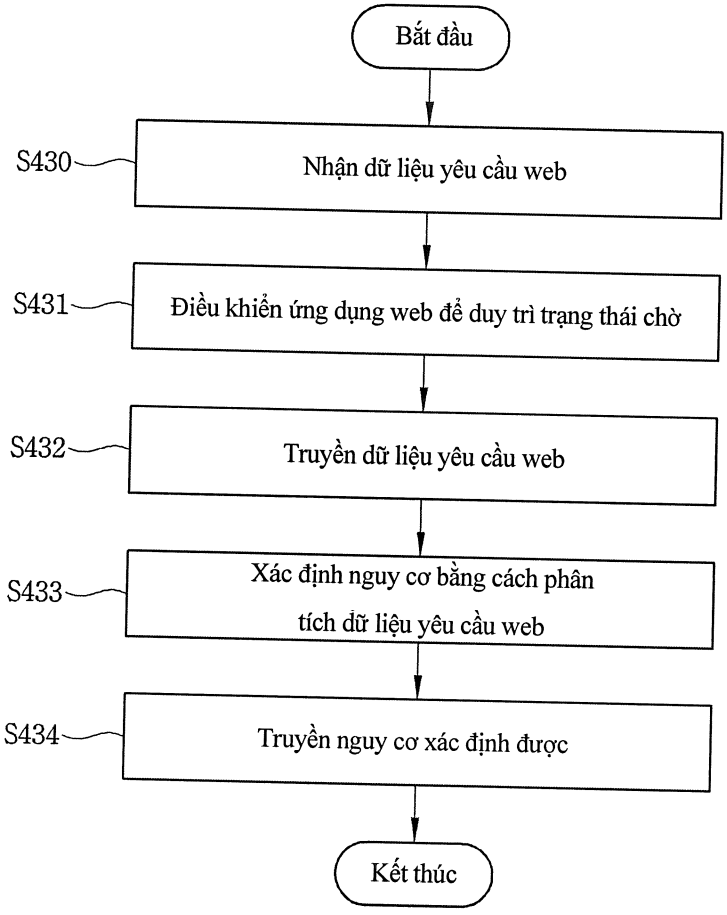

Bắt đầu
S430
Nhận dữ liệu yêu cầu web
S431
Điều khiển ứng dụng web để duy trì trạng thái chờ
S432
Truyền dữ liệu yêu cầu web
S433
Xác định nguy cơ bằng cách phân tích dữ liệu yêu cầu web
S434
Truyền nguy cơ xác định được
Kết thúc

**Fig. 4**