(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) **1-0053067**

(51)[2020.01] **G06F 11/30**

(13) **B**

(21) 1-2021-05375

(22) 31/08/2021

(30) 10202009754Q 01/10/2020 SG

(45) 25/11/2025 452

(43) 27/12/2021 405A

(73) Flexxon Pte. Ltd. (SG)
28 Genting Lane, #09-03, Platinum 28, Singapore 349585

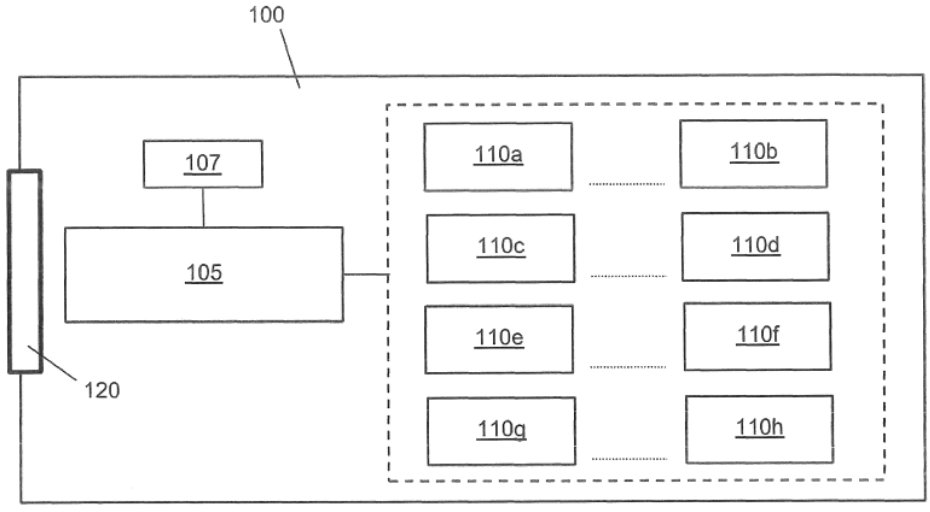
(72) CHAN MEI LING (SG); Nizar Bouguerra (TN).

(74) Công ty Luật TNHH T&G (TGVN)

(54) MÔ-ĐUN VÀ PHƯƠNG PHÁP PHÁT HIỆN CÁC HOẠT ĐỘNG ĐỘC HẠI TRONG THIẾT BỊ LƯU TRỮ

(21) 1-2021-05375

(57) Sáng chế đề xuất mô-đun và phương pháp phát hiện các hoạt động độc hại trong thiết bị lưu trữ theo đó mô-đun được cung cấp trong bộ điều khiển của thiết bị lưu trữ. Mô-đun được cấu hình để giám sát, sử dụng mạng thần kinh được huấn luyện, địa chỉ khối logic thích hợp (LBA) của hệ thống tệp của thiết bị lưu trữ có chứa dữ liệu hoặc thông tin nhạy cảm cho các hoạt động độc hại.



Hình 1

Lĩnh vực kỹ thuật được đề cập

Sáng chế liên quan đến mô-đun và phương pháp phát hiện các hoạt động độc hại trong thiết bị lưu trữ theo đó mô-đun được cung cấp trong bộ điều khiển của thiết bị lưu trữ. Mô-đun được cấu hình để giám sát, sử dụng mạng thần kinh được huấn luyện, địa chỉ khối logic thích hợp (LBA) của hệ thống tệp của thiết bị lưu trữ có chứa dữ liệu hoặc thông tin nhạy cảm cho các hoạt động độc hại.

Tình trạng kỹ thuật của sáng chế

Thiết bị lưu trữ thường bao gồm ổ đĩa thể rắn (SSD), ổ đĩa cứng (HDD), ổ đĩa quang hoặc ổ đĩa từ. Bất kể loại thiết bị lưu trữ nào đều được đánh địa chỉ tuyến tính bằng địa chỉ khối logic (LBA) của chúng. Với ổ HDD, ổ đĩa quang hoặc ổ đĩa từ, LBA chỉ định vị trí của các khối dữ liệu cụ thể được lưu trữ trong ổ đĩa. Ví dụ, LBA 0 sẽ tham chiếu đến khu vực đầu tiên trên dấu vết có thể truy cập bởi đầu đầu tiên trong ổ đĩa, như vậy, khi LBA 0 được truy cập bởi máy chủ, nội dung có ở LBA 0 sẽ được cung cấp cho máy chủ.

Tuy nhiên, không giống như các ổ đĩa được mô tả ở trên, ổ SSD bao gồm những ghi nhớ có thể xóa bằng điện và có thể lập trình lại và như vậy, sẽ không có dấu vết hoặc các đầu như được đề cập đến trong hệ thống địa chỉ khối logic. Do đó, ổ SSD phải sử dụng lớp chuyển dịch flash (FTL) như được cung cấp trong bộ điều khiển bộ nhớ flash của ổ SSD để ánh xạ địa chỉ khối logic hệ thống tệp của máy chủ tới các địa chỉ vật lý của bộ nhớ flash (ánh xạ logic đến vật lý). Nói cách khác, máy chủ sẽ vẫn sử dụng các phương pháp định địa chỉ LBA hiện có để xử lý SSD để đọc / ghi / ghi đè các hoạt động. Các lệnh này từ máy chủ sẽ bị FTL chặn lại và FTL sẽ duy trì một bản đồ về mối quan hệ giữa LBA với địa chỉ khối vật lý (PBA) của bộ nhớ flash. PBA sau đó sẽ được bộ điều khiển của SSD sử dụng để thực hiện các lệnh đã nhận.

Gần đây, ổ SSD được sử dụng rộng rãi hơn làm thiết bị lưu trữ vì ổ SSD có nhiều ưu điểm hơn so với ổ đĩa cứng cơ học truyền thống. Ví dụ, ổ SSD nhanh hơn nhiều so với ổ HDD

và có thể cung cấp hiệu suất gấp 100 lần so với ổ HDD, điều này có nghĩa là thời gian khởi động nhanh hơn và truyền tệp nhanh hơn. Ổ SSD cũng tiêu thụ ít năng lượng hơn ổ HDD giúp cải thiện hiệu suất năng lượng và nhiệt. Do đó, hiện nay ổ SSD được sử dụng rộng rãi trong các ứng dụng công nghiệp, y tế hoặc quân sự.

Thông thường, hầu hết các ổ SSD được sử dụng với máy chủ và có thể được sử dụng để lưu trữ hệ điều hành của máy chủ, tức là được sử dụng làm ổ đĩa hệ thống của máy chủ, theo đó mã được liên kết với hệ điều hành được lưu trữ trong ổ SSD và sẽ được truy cập khi máy chủ khởi động. Khi ổ SSD được sử dụng làm ổ đĩa hệ thống của máy chủ, ổ SSD sẽ có bản ghi khởi động chính (MBR) được lưu trữ tại địa chỉ khối logic (LBA) 0 và mã hệ điều hành của máy chủ được lưu trữ ở nơi khác trong thiết bị lưu trữ. Khi một máy chủ truy cập vào thiết bị lưu trữ lần đầu tiên, hướng dẫn sẽ được gửi đến LBA 0 để hướng dẫn ổ SSD gửi nội dung tại LBA 0 tới máy chủ. Điều này cho phép máy chủ đọc MBR từ LBA 0, theo đó MBR thường sẽ chứa mã chương trình có thể đọc được bằng máy tính mà khi được thực thi bởi máy chủ, cung cấp cho máy chủ khả năng đọc các phần khác của mã hệ điều hành từ thiết bị lưu trữ và khởi động máy chủ.

Ngoài ra, ổ SSD cũng có thể được sử dụng làm phương tiện lưu trữ thứ cấp như USB, thẻ nhớ hoặc thiết bị lưu trữ bên ngoài để mở rộng dung lượng lưu trữ có thể truy cập bằng máy chủ. Khi ổ SSD như vậy được máy chủ truy cập lần đầu tiên, nội dung ở LBA 0 của thiết bị lưu trữ sẽ cho máy bị chủ biết rằng nó sẽ được sử dụng như một phương tiện lưu trữ thứ cấp.

Để truy cập thông tin có trong các ứng dụng nhạy cảm, các bên thứ ba độc hại đã sử dụng nhiều phương tiện và cách khác nhau để lây nhiễm MBR của các thiết bị lưu trữ đó. Một phương pháp phổ biến liên quan đến việc bên thứ ba độc hại giành được quyền truy cập cấp hệ thống vào thiết bị lưu trữ trước khi de-root MBR hoặc các khu vực khởi động khác của thiết bị lưu trữ và cài đặt bên trong hệ điều hành bị xâm phạm.

Để bảo vệ hệ điều hành khỏi bị giả mạo và ngăn chặn quyền truy cập vào thông tin cá nhân quan trọng nếu thiết bị lưu trữ bị thất lạc, người có hiểu biết trung bình về lĩnh vực kỹ thuật tương ứng đề xuất mã hệ điều hành (bao gồm cả MBR) được mã hóa bằng phần mềm được cài đặt trong thiết bị lưu trữ và phải tuân theo các quy trình xác thực, để chỉ người dùng

được phép mới có thể truy cập MBR và mã hệ điều hành. Do bộ điều khiển sẽ không thể đọc MBR trước khi xác thực người dùng thiết bị lưu trữ, thiết bị lưu trữ có thể lưu trữ bản ghi khởi động chính "thay thế" (MBR) làm cho thông tin xác thực được thu thập và xác thực bởi một chương trình xác thực đang chạy trong thiết bị lưu trữ.

Sau khi xác thực thành công người dùng thiết bị lưu trữ, thiết bị lưu trữ ánh xạ lại LBA 0 thành MBR ban đầu, để thiết bị lưu trữ có thể nhận MBR thực và khởi động như bình thường. Nhược điểm của phương pháp này là nếu thông tin xác thực của người dùng bị xâm phạm, MBR và mã hệ điều hành cũng sẽ gặp nguy hiểm.

Ngoài ra, các giải pháp được đề xuất bởi người có hiểu biết trung bình về lĩnh vực kỹ thuật tương ứng yêu cầu hệ điều hành, hệ thống phân vùng hoặc khu vực khởi động của thiết bị lưu trữ được giám sát cần được biết và tải trước vào các giải pháp này trước khi thiết bị lưu trữ có thể được bảo vệ đầy đủ bằng các giải pháp này. Nói cách khác, các giải pháp hiện tại không thể tự động nhận dạng hệ điều hành, hệ thống phân vùng hoặc khu vực khởi động của thiết bị lưu trữ được giám sát và thông tin đó phải được người dùng cung cấp cho giải pháp giám sát hiện có. Đối với bộ điều khiển của thiết bị lưu trữ, tất cả thông tin có trong thiết bị lưu trữ bao gồm dữ liệu của người dùng và được mặc định là không thể phân biệt dữ liệu này. Điều này trở thành vấn đề nghiêm trọng khi hệ điều hành, hệ thống phân vùng hoặc khu vực khởi động của thiết bị lưu trữ được giám sát bị người dùng sửa đổi hoặc chọn sai và do đó, thiết bị lưu trữ có thể vô tình bị xâm phạm.

Vì những lý do trên, người có hiểu biết trung bình về lĩnh vực kỹ thuật tương ứng không ngừng nỗ lực để đưa ra mô-đun và phương pháp có khả năng phát hiện các hoạt động độc hại trong thiết bị lưu trữ mặc dù hệ điều hành, hệ thống phân vùng hoặc khu vực khởi động của thiết bị lưu trữ không được người dùng cung cấp tới bộ điều khiển của thiết bị.

Bản chất kỹ thuật của sáng chế

Hệ thống và phương pháp được đề xuất ở các phương án theo sáng chế giải quyết các vấn đề trên và các vấn đề khác và là một bước tiến trong lĩnh vực liên quan.

Ưu điểm đầu tiên của phương án theo sáng chế là mô-đun có thể nhận dạng loại hệ điều hành được cài đặt trong thiết bị lưu trữ.

Ưu điểm thứ hai của phương án theo sáng chế là mô-đun có thể phát hiện các hoạt động độc hại đang diễn ra ở các vị trí cụ thể trong thiết bị lưu trữ một cách tự động và hiệu quả.

Ưu điểm thứ ba của phương án theo sáng chế là địa chỉ khối logic của thiết bị lưu trữ sẽ được giám sát ở cấp phần sụn và không yêu cầu hệ điều hành khởi động trước khi phát hiện và ngăn chặn các hoạt động độc hại.

Ưu điểm thứ tư của phương án theo sáng chế là nội dung chứa trong một thiết bị lưu trữ (đã được cấu hình để hoạt động như thiết bị hệ thống của máy chủ) sẽ vẫn được bảo vệ khỏi các bên thứ ba độc hại mặc dù thiết bị lưu trữ đã bị xóa khỏi máy chủ và được cấu hình lại làm thiết bị lưu trữ thứ cấp dưới dạng mô-đun khi mô-đun được cấu hình phát hiện các hoạt động độc hại trong cả hai cấu hình.

Ưu điểm thứ năm của phương án theo sáng chế là mô-đun có thể không bị vô hiệu hóa ở cấp hệ điều hành như mô-đun được triển khai như phần sụn của của bộ điều khiển thiết bị lưu trữ.

Các ưu điểm trên được cung cấp bởi phương án theo sáng chế hoạt động theo cách sau.

Theo khía cạnh đầu tiên của sáng chế, mô-đun để phát hiện hoạt động độc hại trong thiết bị lưu trữ được tiết lộ, theo đó mô-đun được cung cấp trong bộ điều khiển của thiết bị lưu trữ, mô-đun được cấu hình để: truy xuất địa chỉ khối logic đầu tiên (LBA0) được gửi đến bộ điều khiển từ máy chủ và truy xuất nội dung ở LBA0 đầu tiên, theo đó nội dung truy xuất được sử dụng để chỉ dẫn mạng thần kinh được huấn luyện truy xuất từ mô-đun dữ liệu được cung cấp trong bộ điều khiển; nhận dạng, sử dụng nội dung ở LBA0 đầu tiên và mạng thần kinh được huấn luyện, các địa chỉ khối logic (LBA) của thiết bị lưu trữ được giám sát; nhân bản các lệnh được gửi tới các LBA do máy chủ nhận dạng tới bộ điều khiển, và nhân bản các nội dung của các LBA được nhân bản; xác định, bằng cách sử dụng mạng thần kinh được huấn luyện, nếu hoạt động độc hại đang xảy ra tại thiết bị lưu trữ dựa trên các lệnh và nội dung nhân bản, trong đó mạng thần kinh được huấn luyện cho các loại hệ điều hành khác nhau hoặc các hoạt động lưu trữ thứ cấp dựa trên quyền truy cập đọc / ghi / ghi đè trung bình các nội dung của LBA liên quan đến bản ghi khởi động chính, bảng tệp chính, khu vực khởi

động, khối thông số BIOS hoặc khối thông số BIOS mở rộng của hệ thống tệp được liên kết với hệ điều hành hoặc hoạt động lưu trữ thứ cấp.

Đối với khía cạnh đầu tiên của sáng chế, việc chỉ dẫn cho mạng thần kinh được huấn luyện liên kết bao gồm mô-đun được cấu hình để: chọn một tập hợp các số ma thuật từ nội dung ở LBA0 đầu tiên, theo đó tập hợp các số ma thuật đã chọn được sử dụng với bảng tra cứu số ma thuật để xác định một loại hệ điều hành hoặc một loại hoạt động lưu trữ thứ cấp liên kết với hệ thống tệp của bộ điều khiển lưu trữ, theo đó bảng tra cứu số ma thuật được lấy từ mô-đun dữ liệu; và chỉ dẫn mạng thần kinh được huấn luyện để phát hiện các hoạt động độc hại liên quan đến loại hệ điều hành hoặc bộ nhớ hoạt động lưu trữ thứ cấp đã xác định từ mô-đun dữ liệu.

Đối với khía cạnh đầu tiên của sáng chế, việc nhận dạng các LBA của thiết bị lưu trữ được giám sát bao gồm mô-đun được cấu hình để: nhận dạng, dựa trên loại hệ điều hành hoặc hoạt động lưu trữ thứ cấp xác định liên kết với mạng thần kinh được huấn luyện đã được chỉ dẫn, các LBA chứa dữ liệu quan trọng trong đó dữ liệu quan trọng bao gồm ít nhất một bảng tệp chính, một bản ghi khởi động chính, một khu vực khởi động, một khối thông số BIOS hoặc khối thông số BIOS mở rộng của hệ thống tệp liên kết với thiết bị lưu trữ.

Đối với khía cạnh đầu tiên của sáng chế, mô-đun được cấu hình thêm để: tối ưu hóa mạng thần kinh được huấn luyện bằng cách sử dụng hoạt động độc hại được xác định là đã xảy ra tại thiết bị lưu trữ dựa trên các lệnh và nội dung được nhân bản.

Đối với khía cạnh đầu tiên của sáng chế, mô-đun được cấu hình thêm để: khóa thiết bị lưu trữ để phản hồi xác định rằng hoạt động độc hại được xác định là đã xảy ra tại thiết bị lưu trữ dựa trên các lệnh và nội dung được nhân bản.

Đối với khía cạnh đầu tiên của sáng chế, mạng thần kinh được huấn luyện bao gồm một trong những mạng thần kinh nhân tạo, mạng thần kinh hồi quy (RNN) hoặc mạng thần kinh tích chập (CNN).

Theo khía cạnh thứ hai của sáng chế, phương pháp phát hiện hoạt động độc hại trong thiết bị lưu trữ được đề xuất, phương pháp bao gồm các bước: truy xuất, sử dụng mô-đun được cung cấp trong bộ điều khiển của thiết bị lưu trữ, một địa chỉ khối logic đầu tiên (LBA0)

được gửi tới bộ điều khiển từ máy chủ; truy xuất, sử dụng mô-đun, nội dung ở LBA0 đầu tiên, theo đó nội dung đã truy xuất được sử dụng để chỉ dẫn mạng thần kinh được huấn luyện trích xuất từ mô-đun dữ liệu được cung cấp trong bộ điều khiển; nhận dạng bằng cách sử dụng nội dung ở LBA0 đầu tiên và mạng thần kinh được huấn luyện, sử dụng mô-đun, các địa chỉ khối logic (LBA) của thiết bị lưu trữ được giám sát; nhân bản, sử dụng mô-đun, các lệnh được gửi đến các LBA do máy chủ nhận dạng tới bộ điều khiển, và nhân bản các nội dung của các LBA được nhân bản; và xác định, sử dụng mạng thần kinh được huấn luyện, nếu hoạt động độc hại đang xảy ra trên thiết bị lưu trữ dựa trên các lệnh và nội dung được nhân bản, trong đó mạng thần kinh được huấn luyện cho các loại hệ điều hành hoặc hoạt động lưu trữ thứ cấp dựa trên quyền truy cập đọc / ghi / ghi đè trung bình các nội dung của LBA liên quan đến bản ghi khởi động chính, bảng tệp chính, lĩnh vực khởi động, khối thông số BIOS hoặc khối thông số BIOS mở rộng của hệ thống tệp liên kết với hệ điều hành hoặc các hoạt động lưu trữ thứ cấp.

Đối với khía cạnh thứ hai của sáng chế, việc chỉ dẫn mạng thần kinh được huấn luyện liên quan bao gồm các bước: chọn, sử dụng mô-đun, một tập hợp các số ma thuật từ nội dung ở LBA0 đầu tiên, theo đó tập hợp các số ma thuật đã chọn được sử dụng với bảng tra cứu số ma thuật để xác định loại hệ điều hành hoặc hoạt động lưu trữ thứ cấp được liên kết với hệ thống tệp của bộ điều khiển lưu trữ, nhờ đó bảng tra cứu số ma thuật được lấy từ mô-đun dữ liệu; và chỉ dẫn, sử dụng mô-đun, mạng thần kinh được huấn luyện để phát hiện các hoạt động độc hại liên quan đến loại hệ điều hành hoặc hoạt động lưu trữ thứ cấp đã xác định từ mô-đun dữ liệu.

Đối với khía cạnh thứ hai của sáng chế, việc nhận dạng các LBA của thiết bị lưu trữ được giám sát bao gồm các bước: nhận dạng, sử dụng mô-đun, dựa trên loại hệ điều hành hoặc hoạt động lưu trữ thứ cấp được xác định liên kết với mạng thần kinh được huấn luyện được chỉ dẫn, các LBA chứa dữ liệu quan trọng trong đó dữ liệu quan trọng bao gồm ít nhất một bảng tệp chính, một bản ghi khởi động chính, một khu vực khởi động, một khối thông số BIOS hoặc khối thông số BIOS mở rộng của hệ thống tệp liên kết với thiết bị lưu trữ.

Đối với khía cạnh thứ hai của sáng chế, phương pháp này còn bao gồm các bước: tối ưu hóa, sử dụng mô-đun, mạng thần kinh được huấn luyện bằng cách sử dụng hoạt động độc hại được xác định là đã xảy ra tại thiết bị lưu trữ dựa trên các lệnh và nội dung nhân bản.

Đối với khía cạnh thứ hai của sáng chế, phương pháp này còn bao gồm các bước: khóa thiết bị lưu trữ để phản hồi xác định rằng hoạt động độc hại được xác định là đã xảy ra tại thiết bị lưu trữ dựa trên các lệnh và nội dung được nhân bản.

Đối với khía cạnh thứ hai của sáng chế, mạng thần kinh được huấn luyện bao gồm một trong những mạng thần kinh nhân tạo, mạng thần kinh hồi quy (RNN) hoặc mạng thần kinh tích chập (CNN).

Mô tả vắn tắt các hình vẽ

Các vấn đề trên và các vấn đề khác được giải quyết bằng các tính năng và ưu điểm của hệ thống và phương pháp theo sáng chế được mô tả trong phần mô tả chi tiết và thể hiện trong các bản vẽ sau đây.

Hình 1 minh họa sơ đồ khối các mô-đun tích hợp trong thiết bị lưu trữ trong theo các phương án của sáng chế;

Hình 2 minh họa sơ đồ khối các mô-đun tích hợp trong bộ điều khiển của thiết bị lưu trữ theo các phương án của sáng chế;

Hình 3 minh họa khu vực khởi động mẫu của hệ thống tệp trong thiết bị lưu trữ theo các phương án của sáng chế;

Hình 4 minh họa sơ đồ quy trình hoặc phương pháp phát hiện các hoạt động độc hại trong thiết bị lưu trữ theo các phương án của sáng chế; và

Hình 5 minh họa sơ đồ quy trình hoặc phương pháp chỉ dẫn mạng thần kinh được huấn luyện theo các phương án của sáng chế.

Mô tả chi tiết sáng chế

Sáng chế này liên quan đến mô-đun và phương pháp phát hiện các hoạt động độc hại trong thiết bị lưu trữ theo đó mô-đun được cung cấp trong bộ điều khiển của thiết bị lưu trữ. Mô-đun được cấu hình để giám sát, sử dụng mạng thần kinh được huấn luyện, địa chỉ khối logic thích hợp (LBA) của hệ thống tệp của thiết bị lưu trữ có chứa dữ liệu hoặc thông tin nhạy cảm cho các hoạt động độc hại trong đó mạng thần kinh được huấn luyện cho các loại hệ điều hành hoặc hoạt động lưu trữ thứ cấp dựa quyền truy cập đọc / ghi / ghi đè trung bình các nội dung của LBA liên quan đến bản ghi khởi động chính, bảng tệp chính, lĩnh vực khởi động, khối thông số BIOS hoặc khối thông số BIOS mở rộng của hệ thống tệp liên kết với hệ điều hành hoặc các hoạt động lưu trữ thứ cấp.

Sáng chế sẽ được mô tả chi tiết tham chiếu các phương án của chúng như được minh họa trong các hình vẽ kèm theo. Trong mô tả sau đây, nhiều tính năng cụ thể được đưa ra để cung cấp sự hiểu biết thấu đáo về các phương án của sáng chế. Tuy nhiên, đối với người có hiểu biết trung bình về lĩnh vực kỹ thuật tương ứng, các phương án có thể được thực hiện mà không có một số hoặc tất cả các tính năng cụ thể. Các phương án này cũng thuộc phạm vi của sáng chế. Hơn nữa, các bước và/hoặc cấu trúc quy trình nhất định sau đây có thể không được mô tả chi tiết và người đọc có thể tham chiếu trích dẫn tương ứng để không ảnh hưởng đến khả năng hiểu sáng chế một cách không cần thiết.

Hơn nữa, người có hiểu biết trung bình về lĩnh vực kỹ thuật tương ứng sẽ nhận ra rằng nhiều đơn vị chức năng trong bản mô tả này đã được gắn nhãn là các mô-đun trong toàn bộ đặc điểm kỹ thuật. Người có hiểu biết trung bình về lĩnh vực kỹ thuật tương ứng cũng sẽ nhận ra rằng mô-đun có thể được triển khai dưới dạng mạch, chip logic hoặc bất kỳ linh kiện rời nào. Hơn nữa, người có hiểu biết trung bình về lĩnh vực kỹ thuật tương ứng cũng sẽ nhận ra rằng mô-đun có thể được triển khai trong phần mềm mà sau đó có thể được thực thi bởi nhiều kiến trúc bộ xử lý khác nhau. Theo các phương án của sáng chế, mô-đun cũng có thể bao gồm lệnh máy tính, phần sụn hoặc mã thực thi có thể lệnh bộ xử lý máy tính thực hiện một chuỗi sự kiện dựa trên lệnh nhận được. Sự lựa chọn về việc triển khai các mô-đun được để lại như một lựa chọn thiết kế cho người có hiểu biết trung bình về lĩnh vực kỹ thuật tương ứng và không giới hạn phạm vi của sáng chế này trong bất kỳ cách nào.

Một quy trình hoặc phương pháp mẫu để phát hiện các hoạt động độc hại trong thiết bị lưu trữ theo các phương án của sáng chế được nêu trong các bước dưới đây. Các bước của quy trình hoặc phương pháp được thực hiện bởi mô-đun được cung cấp trong bộ điều khiển thiết bị lưu trữ như sau:

Bước 1: truy xuất địa chỉ khối logic đầu tiên (LBA0) được gửi đến bộ điều khiển từ máy chủ và truy xuất nội dung ở LBA0 đầu tiên, theo đó nội dung được truy xuất được sử dụng để chỉ dẫn mạng thần kinh được huấn luyện từ mô-đun dữ liệu được cung cấp trong bộ điều khiển;

Bước 2: nhận dạng, sử dụng nội dung ở LBA0 đầu tiên và mạng thần kinh được huấn luyện, các địa chỉ khối logic (LBA) của thiết bị lưu trữ được giám sát;

Bước 3: nhân bản các lệnh gửi đến các LBA do máy chủ nhận dạng tới bộ điều khiển, và nhân bản các nội dung của các LBA được nhân bản;

Bước 4: xác định, bằng cách sử dụng mạng thần kinh được huấn luyện, nếu hoạt động độc hại đang xảy ra tại thiết bị lưu trữ dựa trên các lệnh và nội dung nhân bản, trong đó mạng thần kinh được huấn luyện cho các loại hệ điều hành hoặc hoạt động lưu trữ thứ cấp khác nhau dựa trên quyền truy cập đọc / ghi / ghi đè trung bình các nội dung của LBA liên quan đến bản ghi khởi động chính, bảng tệp chính, khu vực khởi động, khối thông số BIOS hoặc khối thông số BIOS mở rộng của hệ thống tệp liên kết với hệ điều hành hoặc các hoạt động lưu trữ thứ cấp.

Theo các phương án của sáng chế, các bước nêu trên có thể được thực hiện hoặc thực thi bởi mô-đun tích hợp trong bộ điều khiển 105 của thiết bị lưu trữ 100, như minh họa trong Hình 1, theo đó thiết bị lưu trữ 100 còn bao gồm bộ nhớ đệm 107, bộ nhớ flash 110a-h và giao diện 120. Thiết bị lưu trữ 100 có thể bao gồm nhiều loại ổ SDD, bộ nhớ đệm 107 có thể bao gồm một bộ nhớ truy cập ngẫu nhiên động (DRAM) và được sử dụng để lưu vào bộ nhớ đệm cả dữ liệu người dùng và siêu dữ liệu SSD nội bộ. Bộ nhớ flash 110a-h có thể bao gồm bất kỳ loại phương tiện lưu trữ bộ nhớ máy tính bất biến điện tử nào mà có thể bị xóa và lập trình lại bằng điện tử chẳng hạn như bộ nhớ flash NAND hoặc NOR. Giao diện 120 hoạt động như giao diện vật lý giữa hệ thống máy chủ và thiết bị lưu trữ 100, theo đó các tiêu chuẩn và

giao diện lưu trữ hiện có, chẳng hạn như, nhưng không giới hạn, giao thức giao diện hệ thống máy tính nhỏ (SCSI), giao thức công nghệ truyền tải nối tiếp (SATA), giao thức nối tiếp điểm-điểm (SAS), bộ nhớ bất biến cao tốc (NVMe), giao diện thành phần ngoại vi cao tốc (PCIe) hoặc bất kỳ giao diện tương tự nào có thể được sử dụng làm liên kết cho kết nối giao tiếp thiết bị lưu trữ 100 với máy chủ như máy tính.

Bộ điều khiển 105 là một hệ thống nhúng phức tạp với quá trình xử lý và hoạt động độc lập với phần sụn và mô-đun tích hợp trong bộ điều khiển 105 để quản lý tất cả các khía cạnh của thiết bị lưu trữ 100, bao gồm bảo vệ và kiểm soát nội dung được lưu trữ trong bộ nhớ flash 110a-h. Bộ điều khiển này thường được triển khai dưới dạng thiết kế SoC (hệ thống trên chip) bao gồm nhiều khối/mô-đun chức năng với phần cứng tăng tốc được kết hợp với một hoặc nhiều lõi xử lý nhúng.

Các khối chức năng tích hợp trong bộ điều khiển 105 được minh họa trong Hình 2. Đặc biệt, Hình 2 cho thấy bộ điều khiển 105 có thể bao gồm bộ điều khiển vi mô 205, bộ đệm 210, mô-đun giao diện flash (FIM) 215a-c và mô-đun phát hiện mối đe dọa 250. Bộ điều khiển vi mô 205 bao gồm một bộ xử lý nằm bên trong bộ điều khiển 105 và có nhiệm vụ nhận và thao tác dữ liệu đến. Ở đây, thuật ngữ "bộ xử lý" được sử dụng để chỉ chung cho bất kỳ thiết bị hoặc linh kiện nào có thể xử lý các lệnh như vậy và có thể bao gồm: bộ vi xử lý, bộ vi điều khiển, thiết bị logic lập trình được hoặc thiết bị tính toán khác. Đó là, bộ điều khiển vi mô 205 có thể được cung cấp bởi bất kỳ mạch logic phù hợp nào để nhận đầu vào, xử lý chúng theo các lệnh được lưu trữ trong bộ nhớ và tạo ra kết quả đầu ra. Trong phương án này, bộ điều khiển vi mô 205 có thể là bộ xử lý lõi đơn với không gian địa chỉ bộ nhớ. Bộ đệm 210 có thể được coi là mô-đun dữ liệu vì nó có thể bao gồm SRAM (RAM tĩnh) để thực thi phần cứng của bộ điều khiển 105 hoặc lưu trữ dữ liệu/thông tin được truy cập bởi mô-đun 250. Mô-đun phát hiện mối đe dọa 250 được sử dụng để nhân bản các đầu vào/đầu ra tại bộ điều khiển 105; huấn luyện và tải mạng thần kinh được huấn luyện thích hợp để phát hiện các hoạt động độc hại có thể xảy ra trong thiết bị lưu trữ và các nhiệm vụ liên quan theo các phương án của sáng chế. FIMs 215a-c hoạt động như kết nối vật lý và logic giữa bộ điều khiển 105 và bộ nhớ flash 110a-h cho phép bộ điều khiển giao tiếp đồng thời với nhiều bộ nhớ flash. Người có hiểu biết trung bình về lĩnh vực kỹ thuật tương ứng sẽ nhận ra rằng các linh kiện bộ nhớ khác nhau được mô tả ở trên bao gồm phương tiện có thể đọc được bằng

máy tính không tạm thời và phải được sử dụng để bao gồm tất cả các phương tiện có thể đọc được bằng máy tính ngoại trừ tín hiệu lan truyền tạm thời. Thông thường, các lệnh được lưu trữ dưới dạng mã chương trình trong linh kiện bộ nhớ nhưng cũng có thể được nối cứng. Mặc dù không được hiển thị, bộ điều khiển 105 cũng bao gồm lớp chuyển dịch flash (FTL) để dịch LBA từ máy chủ sang địa chỉ khối vật lý (PBA) của bộ nhớ flash. Các hoạt động chi tiết của FTL được bỏ qua cho ngắn gọn vì nó đều được người có hiểu biết trung bình về lĩnh vực kỹ thuật tương ứng biết.

Khi máy chủ (không được hiển thị) được khởi động và giả sử rằng thiết bị lưu trữ 100 sẽ được sử dụng làm thiết bị hệ thống của máy chủ, hệ điều hành của nó sẽ không được tích hợp trong ROM hoặc RAM của máy chủ. Nó sẽ được lưu trữ trong thiết bị lưu trữ 100. Như vậy, để tạo thuận lợi cho việc tải hệ điều hành, máy chủ sẽ thực thi phần cứng được lưu trữ trong ROM của máy chủ mà gửi lệnh thích hợp đến LBA '0' (LBA0) của thiết bị lưu trữ 100. Khi nhận được các lệnh này được gửi đến LBA '0', thiết bị lưu trữ 100 sẽ gửi lại dữ liệu được lưu trữ tại địa chỉ khối vật lý tương ứng với LBA '0'. Thực chất, địa chỉ khối logic do bộ điều khiển 105 của thiết bị lưu trữ 100 nhận sẽ được FTL chuyển đổi thành địa chỉ khối vật lý phù hợp được cung cấp trong bộ điều khiển 105. Tuy nhiên, đối với máy chủ, tất cả điều này là không thể nhìn thấy và nó được hiểu rằng khi các lệnh được gửi đến LBA của thiết bị lưu trữ 100, tất cả các bản dịch cần thiết giữa LBA sang PBA sẽ tự động diễn ra trong bộ điều khiển 105.

Thông thường trong một thiết bị hệ thống, LBA đầu tiên trong lược đồ LBA, tức là LBA '0', có thể chứa, nhưng không chỉ giới hạn, bản ghi khởi động chính (MBR), bao gồm mã chương trình có thể đọc được bằng máy tính, khi được thực thi bởi máy chủ, cung cấp cho máy chủ khả năng đọc các phần khác của mã hệ điều hành từ thiết bị lưu trữ 100 và khởi động máy chủ. LBA là một lược đồ phổ biến được sử dụng để xác định vị trí của các khối dữ liệu được lưu trữ trong thiết bị lưu trữ 100 và cung cấp một phương pháp định địa chỉ tuyến tính đơn giản cho máy chủ để truy cập nội dung được lưu trữ trong thiết bị lưu trữ 100 mà máy chủ không nhận ra vị trí khu vực vật lý hoặc PBA của thiết bị lưu trữ. Như vậy, khi phân vùng khác nhau, hệ thống tệp hoặc bất kỳ khu vực đặc biệt nào khác của thiết bị lưu trữ được truy cập bởi máy chủ, LBA liên kết với các khu vực này sẽ được máy chủ gửi đến bộ điều khiển

105 của thiết bị lưu trữ 100 để bộ điều khiển 105 có thể sử dụng thông tin này để truy xuất dữ liệu/thông tin liên quan cho máy chủ.

Khi bộ điều khiển 105 nhận LBA và các lệnh liên quan từ máy chủ và trả lại nội dung của LBA cho máy chủ dựa trên các lệnh đã nhận, mô-đun phát hiện mối đe dọa 250 được cấu hình để nhân bản tất cả những điều này và điều này có thể được thực hiện bằng cách ghi lại tất cả các đầu vào và đầu ra diễn ra tại bộ điều khiển 105. Nói cách khác, mô-đun phát hiện mối đe dọa 250 có thể đạt được điều này bằng cách ghi lại các lệnh nhận được bởi bộ điều khiển 105 và LBA mà các lệnh hướng đến. Dữ liệu và/hoặc thông tin được cung cấp tại các LBA này sau đó cũng có thể được ghi lại bởi mô-đun 250 trước khi dữ liệu và/hoặc thông tin được gửi trở lại máy chủ yêu cầu.

Khu vực khởi động mẫu của hệ thống tệp được cung cấp tại địa chỉ khối logic '0' (LBA0) được thể hiển trong Hình 3. Như minh họa, khu vực khởi động 300 bao gồm nhiều trường có nhiều độ dài và hiệu số riêng của chúng. Mỗi trường sẽ có giá trị tiêu biểu của riêng nó được liên kết với một ý nghĩa hoặc lệnh cụ thể. Những giá trị này có thể bao gồm, nhưng không giới hạn, số hex hoặc số ma thuật được tạo dựa trên từng ý nghĩa / lệnh cụ thể cho từng loại hệ điều hành / tệp hệ thống / hệ thống lưu trữ và như vậy, mỗi ý nghĩa hoặc lệnh sẽ được liên kết với một giá trị độc nhất. Ví dụ: giá trị “EB” có thể được liên kết với “Bytes per sector” (số byte trên mỗi khu vực), giá trị “52” có thể được liên kết với “Sectors per Cluster” (số lượng khu vực trên mỗi cụm), giá trị “67” có thể được liên kết với “ID OEM”, giá trị “J9” có thể được liên kết với “BPB”, giá trị “34” có thể được liên kết với "BPB mở rộng" và v.v.

Theo phương án được lấy làm ví dụ của sáng chế, điểm mấu chốt là thông tin quan trọng chứa ở dữ liệu 305 của LBA0 như trong Hình 3, ví dụ: có thể bao gồm khối thông số BIOS (BPB) và BPB mở rộng và người có hiểu biết trung bình về lĩnh vực kỹ thuật tương ứng sẽ nhận ra rằng đây chỉ là một ví dụ và các nội dung khác tại LBA0 cũng có thể được sử dụng. Dựa vào thông tin có trong dữ liệu 305, thông tin sau về hệ thống tệp của thiết bị lưu trữ có thể được xác định: số byte trên mỗi khu vực, số lượng khu vực trên mỗi cụm, loại bộ mô tả phương tiện, tổng số khu vực, vị trí của bảng tệp chính (MFT) hoặc cấu trúc tương đương của nó, vị trí của bản sao của bảng tệp chính, số lượng cụm trên mỗi bản ghi MFT, số lượng cụm trên bộ đệm chỉ mục, loại hệ thống tệp, hệ điều hành và số sê-ri của tập. Thông tin

này sau đó có thể được sử dụng để xác định hệ điều hành của hệ thống tệp của thiết bị lưu trữ, hệ thống tệp của thiết bị lưu trữ và / hoặc hoạt động của hệ thống tệp của thiết bị lưu trữ. Người có hiểu biết trung bình về lĩnh vực kỹ thuật tương ứng sẽ nhận ra rằng người các thông tin khác có thể được bao gồm trong dữ liệu 305 và trong nội dung của LBA0 mà không cần sử dụng sáng chế.

Theo các phương án của sáng chế, bảng tra cứu số ma thuật có thể được tải trước vào bộ nhớ đệm 107 hoặc bộ đệm 210. Người có hiểu biết trung bình về lĩnh vực kỹ thuật tương ứng đều biết các số ma thuật liên quan đến các giá trị số không đổi được tạo ra cho thông tin hoặc dữ liệu cụ thể. Như vậy, các số ma thuật này có thể được sử dụng để nhận dạng một định dạng tệp hoặc giao thức cụ thể hoặc có thể liên quan đến các giá trị độc đáo khác biệt mà khó có thể bị nhầm lẫn với các ý nghĩa khác. Theo phương án này của sáng chế, mỗi số ma thuật trong bảng tra cứu số ma thuật được tải trước liên quan đến một loại hệ điều hành cụ thể và / hoặc một loại hệ thống tệp, chẳng hạn như hệ thống tệp lưu trữ thứ cấp. Cần lưu ý rằng bảng tra cứu này có thể được cập nhật định kỳ theo yêu cầu hoặc bất cứ khi nào một hệ điều hành mới, hệ thống tệp lưu trữ thứ cấp, hoặc các loại hệ thống tệp khác được giới thiệu. Thông tin trong bảng tra cứu số ma thuật sau đó có thể được khớp với nội dung được tìm thấy ở LBA0 và dựa trên kết quả khớp, mô-đun 250 sau đó có thể xác định loại hệ điều hành / hệ thống tệp / hệ thống lưu trữ liên kết với thiết bị lưu trữ.

Bằng cách đó, mô-đun phát hiện mối đe dọa 250 sau đó có thể sử dụng thông tin này để chỉ dẫn mạng thần kinh được huấn luyện có tích hợp trong mô-đun 250 để phát hiện các hoạt động độc hại cho một loại hệ điều hành hoặc hoạt động lưu trữ thứ cấp cụ thể vì mỗi hệ thống tệp sẽ có danh sách LBA duy nhất có chứa nội dung, thông tin hoặc dữ liệu quan trọng. Theo các phương án của sáng chế, nội dung hoặc bản ghi quan trọng bao gồm, nhưng không giới hạn, dữ liệu ảnh hưởng đến người dùng của thiết bị lưu trữ, dữ liệu ảnh hưởng đến hoạt động bình thường của thiết bị lưu trữ và / hoặc bất kỳ các dữ liệu tương tự. Nói cách khác, thông tin này có thể được mô-đun 250 sử dụng để nhận dạng các LBA trong hệ thống tệp của thiết bị lưu trữ 100 được giám sát chặt chẽ bởi hệ thần kinh được huấn luyện theo đó các LBA này có thể là duy nhất cho loại hệ thống tệp được cài đặt trong thiết bị lưu trữ. Ngoài ra, mạng thần kinh được huấn luyện tối ưu hóa cho loại được nhận dạng của hệ điều hành hoặc hệ thống tệp cũng có thể được chọn và tải. Một khi các thông số mô tả ở trên đã được

khởi tạo, mạng thần kinh được huấn luyện sau đó có thể được sử dụng bởi mô-đun 250 để giám sát thiết bị lưu trữ 100 cho các hoạt động độc hại.

Theo các phương án của sáng chế, mô hình mạng thần kinh được cung cấp trong bộ đệm 210 hoặc bộ nhớ đệm 107 và mạng thần kinh này có thể bao gồm, nhưng không giới hạn, mạng thần kinh nhân tạo chẳng hạn như mạng thần kinh hồi quy (RNN) hoặc mạng thần kinh tích chập (CNN). Mô hình mạng thần kinh này sẽ được huấn luyện trước, trước khi nó được sử dụng để phát hiện các hoạt động độc hại diễn ra trong hệ thống tệp của thiết bị lưu trữ.

Đặc biệt, mô hình mạng thần kinh sẽ được huấn luyện dựa trên dựa trên quyền truy cập đọc / ghi / ghi đè trung bình các nội dung của LBA hoặc PBA cụ thể liên quan đến bản ghi khởi động chính, bảng tệp chính, khu vực khởi động, khối thông số BIOS và / hoặc khối thông số BIOS mở rộng của hệ thống tệp được liên kết với từng loại hệ điều hành hoặc hệ thống tệp lưu trữ thứ cấp (được cài đặt trong các thiết bị lưu trữ được sử dụng làm hoạt động lưu trữ thứ cấp).

Nói cách khác, mô hình mạng thần kinh sẽ được huấn luyện dựa trên các vectơ đầu vào chẳng hạn như quyền truy cập đọc / ghi / ghi đè trung bình các nội dung của LBA thường được truy cập trong quá trình vận hành các loại hệ điều hành khác nhau và hệ thống tệp tương ứng hoặc trong quá trình hoạt động của thiết bị lưu trữ như một hệ thống lưu trữ thứ cấp. Do đó, bất kỳ hoạt động nào khác với các hành động thông thường này có thể khiến mạng thần kinh cho rằng các hoạt động kích hoạt là các hoạt động độc hại. Các hoạt động bị coi là độc hại cùng với LBA truy cập bởi các hoạt động độc hại này cũng có thể được sử dụng để huấn luyện cho mạng thần kinh theo đó sự kết hợp các dữ liệu ở trên có thể được cung cấp cho mạng thần kinh trong giai đoạn huấn luyện để tối ưu hóa việc huấn luyện của mạng thần kinh.

Theo các phương án khác của sáng chế, mạng thần kinh được huấn luyện có thể được tối ưu hơn bằng cách sử dụng các hoạt động độc hại được phát hiện trong quá trình hoạt động bình thường của thiết bị lưu trữ. Một bước tối ưu hóa nhanh chóng như vậy sẽ cải thiện đáng kể năng suất và hiệu quả của mạng thần kinh.

Theo các phương án của sáng chế, quyền truy cập đọc / ghi / ghi đè trung bình các nội dung của LBA của các hệ điều hành và hệ thống tệp khác nhau có thể thu được bằng cách ghi

các đầu vào / đầu ra tại bộ điều khiển của thiết bị lưu trữ có các hệ điều hành và hệ thống tệp khác nhau trong một khoảng thời gian. Quyền truy cập đọc / ghi / ghi đè trung bình cũng có thể thu được từ các tài nguyên của bên thứ ba và có thể được sử dụng để huấn luyện cho mạng thần kinh.

Ngoài ra, khi các LBA được truy cập cho từng hệ điều hành khác nhau, tệp hệ thống và hệ thống lưu trữ thứ cấp khác nhau giữa hệ thống này với hệ thống kia, bản ghi của các LBA chứa dữ liệu quan trọng cho các hệ thống này có thể được tạo theo đó dữ liệu quan trọng có thể bao gồm, nhưng không giới hạn, bảng tệp chính hoặc cấu trúc tệp tương đương, bản ghi khởi động chính, khu vực khởi động, các khu vực quan trọng do người dùng xác định, khu vực an toàn, khối thông số BIOS hoặc khối thông số BIOS mở rộng của hệ thống tệp. Bản ghi này sau đó có thể được liên kết với mô hình mạng thần kinh được huấn luyện và được lưu trữ trong bộ nhớ đệm 107 hoặc bộ đệm 210 hoặc ngược lại, có thể được sử dụng như một phần của dữ liệu huấn luyện được cung cấp để huấn luyện cho mạng thần kinh như mô tả ở trên. Do đó, một khi chức năng của thiết bị lưu trữ đã được nhận dạng, ví dụ để hoạt động như một thiết bị hệ thống hoặc thiết bị lưu trữ thứ cấp, các LBA của thiết bị lưu trữ chứa dữ liệu quan trọng có thể được nhận dạng từ bản ghi này.

Tóm lại, mạng thần kinh được huấn luyện để bảo vệ một số khu vực nhất định của hệ thống tệp và việc huấn luyện sẽ được thực hiện dựa trên loại hệ thống tệp được triển khai trên thiết bị lưu trữ và LBA có chứa dữ liệu quan trọng. Thông tin để nhận dạng loại hệ thống tệp có thể nhận được từ nội dung ở LBA đầu tiên, tức là LBA0. Tuy nhiên, người có hiểu biết trung bình về lĩnh vực kỹ thuật tương ứng sẽ nhận ra rằng mặc dù các nội dung có liên quan ban đầu có thể được tìm thấy tại LBA0, đối với một số loại tệp hệ thống nhất định, nó có thể quá lớn hoặc do cách thức mà thông tin được cấu trúc, nó có thể được phân phối trên nhiều LBA, ví dụ từ LBA “0” - LBA “48”. Theo các phương án của sáng chế, mỗi mạng thần kinh có thể được tối ưu hóa cho từng loại hệ thống tệp vì các LBA quan trọng khác nhau giữa hệ thống tệp này với hệ thống kia. Như vậy, loại mạng thần kinh được huấn luyện được sử dụng có thể phụ thuộc vào hệ thống tệp của thiết bị lưu trữ và hiệu suất của mạng thần kinh được huấn luyện có thể năng suất và hiệu quả hơn nếu mạng thần kinh được huấn luyện phù hợp được chọn để sử dụng với hệ thống tệp phù hợp và hành động này có thể được coi là sự chỉ dẫn cho mạng thần kinh được huấn luyện.

Hình 4 minh họa quy trình 400 để phát hiện các hoạt động độc hại trong thiết bị lưu trữ được kết nối giao tiếp với máy chủ theo các phương án của sáng chế theo đó quy trình 400 có thể được thực hiện trong mô-đun phát hiện mối đe dọa 250 như được cung cấp trong bộ điều khiển của thiết bị lưu trữ. Quy trình 400 bắt đầu ở bước 405, theo đó địa chỉ khối logic đầu tiên (LBA) được gửi đến bộ điều khiển từ máy chủ được sao chép theo quy trình 400. Quy trình 400 sau đó tiến hành truy xuất nội dung ở LBA đầu tiên, theo đó nội dung truy xuất được sử dụng để chỉ dẫn mạng thần kinh được huấn luyện truy xuất từ một mô-đun dữ liệu được cung cấp trong bộ điều khiển. Khi điều này xảy ra, một mạng thần kinh cụ thể được tối ưu hóa cho hệ thống tập tin / hệ điều hành / hệ thống lưu trữ được nhận dạng sẽ được tải và chỉ dẫn.

Dựa trên nội dung truy xuất và / hoặc mạng thần kinh được huấn luyện đã được chỉ dẫn, một bản ghi về các LBA chứa dữ liệu quan trọng cho hệ thống tệp liên kết sẽ được tải ở bước 410. Bản ghi này sau đó được sử dụng để nhận dạng các LBA của thiết bị lưu trữ được giám sát bằng quy trình 400. Tại bước 415, quy trình 400 sau đó nhân bản các lệnh được gửi đến các LBA dưới sự giám sát và nhân bản các nội dung từ các LBA này sau đó gửi đến máy chủ. Quy trình 400 sau đó ở bước 420, xác định dựa trên các lệnh và nội dung nhân bản nếu các hoạt động độc hại đang diễn ra tại thiết bị lưu trữ.

Nếu quy trình 400 ở bước 420 xác định rằng các hoạt động độc hại đang diễn ra trong thiết bị lưu trữ, quy trình 400 sau đó sẽ chuyển sang bước 425, theo đó một báo động hoặc cảnh báo phù hợp sẽ được đưa ra hoặc cách khác, thiết bị lưu trữ có thể bị khóa. Quy trình 400 sau đó sẽ kết thúc. Ngược lại, nếu không có hoạt động độc hại nào được phát hiện bởi quy trình 400 ở bước 420, quy trình 400 sau đó sẽ kết thúc. Quy trình 400 sau đó sẽ tự lặp lại mỗi khi thiết bị lưu trữ khởi động hoặc khởi tạo để có thể phát hiện bất kỳ hoạt động độc hại nào có thể xảy ra.

Hình 5 minh họa quy trình 500 có thể được thực hiện trong mô-đun 250 để chỉ dẫn mạng thần kinh được huấn luyện truy xuất từ mô-đun dữ liệu trong quá trình khởi động hoặc khởi tạo máy chủ liên kết. Quy trình 500 bắt đầu ở bước 505 bằng cách chọn một tập hợp các giá trị hoặc các số ma thuật từ nội dung được tìm thấy ở LBA đầu tiên (như được sao chép bởi quy trình 400 ở bước 405) hoặc tại các LBA khác nếu nội dung vượt quá LBA đầu

tiên. Những tập hợp các giá trị hoặc các số ma thuật này sau đó được so sánh với bảng tra cứu số ma thuật đã được tải trước vào bộ nhớ đệm hoặc bộ đệm của thiết bị lưu trữ. Bằng cách khớp tập hợp các giá trị / các số ma thuật với tập hợp các giá trị / các số ma thuật có trong bảng tra cứu số ma thuật, quy trình 500 sau đó có thể xác định loại hệ điều hành và hệ thống tệp của nó hoặc có thể xác định loại cấu hình hệ thống (ví dụ: hệ thống tệp lưu trữ thứ cấp) được liên kết với hệ thống tệp của thiết bị lưu trữ. Các LBA quan trọng đối với hệ thống tệp được nhận dạng cũng được nhận dạng ở bước này để mạng thần kinh được huấn luyện biết rằng nó phải giám sát các LBA này. Quy trình 500 sau đó tiến hành chỉ dẫn mạng thần kinh được huấn luyện dựa trên thông tin này ở bước 515, do đó tăng tốc tốc độ phát hiện của mạng thần kinh được huấn luyện vì nó đã được chỉ dẫn để sử dụng với hệ thống tệp thích hợp.

Người có hiểu biết trung bình về lĩnh vực kỹ thuật tương ứng có thể thay đổi, thay thế, biến thể và sửa đổi, tất cả đều thuộc phạm vi của các yêu cầu bảo hộ của sáng chế.

YÊU CẦU BẢO HỘ

1. Mô-đun phát hiện hoạt động độc hại trong thiết bị lưu trữ, theo đó mô-đun được cung cấp trong bộ điều khiển của thiết bị lưu trữ, mô-đun được cấu hình để:

truy xuất địa chỉ khối logic đầu tiên (LBA0) được gửi đến bộ điều khiển từ máy chủ và truy xuất nội dung ở LBA0 đầu tiên, theo đó nội dung được truy xuất được sử dụng để chỉ dẫn mạng thần kinh được huấn luyện được truy xuất từ mô-đun dữ liệu được cung cấp trong bộ điều khiển, mạng thần kinh đã nói được sử dụng bởi mô-đun đã nói để giám sát thiết bị lưu trữ đã nói để phát hiện hoạt động độc hại;

nhận dạng, sử dụng nội dung ở LBA0 đầu tiên và mạng thần kinh được huấn luyện, các địa chỉ khối logic (LBA) của thiết bị lưu trữ mà để được giám sát;

nhân bản các lệnh được gửi đến các LBA được nhận dạng bởi máy chủ tới bộ điều khiển, và nhân bản các nội dung của các LBA được nhân bản;

xác định, sử dụng mạng thần kinh được huấn luyện, nếu hoạt động độc hại đang xảy ra tại thiết bị lưu trữ dựa trên các lệnh và các nội dung được nhân bản, trong đó mạng thần kinh được huấn luyện cho các loại khác nhau của các hệ điều hành hoặc các hoạt động lưu trữ thứ cấp dựa trên quyền truy cập đọc/ghi/ghi đè trung bình của các nội dung ở các LBA liên quan đến các bản ghi khởi động chính, các bản ghi quan trọng, các bảng tệp chính, các khu vực khởi động, các khối thông số BIOS hoặc các khối thông số BIOS mở rộng của các hệ thống tệp được liên kết với các hệ điều hành hoặc các hoạt động lưu trữ thứ cấp.

2. Mô-đun theo điểm 1, trong đó việc chỉ dẫn của mạng thần kinh đã nói được sử dụng bởi mô-đun đã nói mà giám sát thiết bị lưu trữ đã nói để phát hiện hoạt động độc hại bao gồm mô-đun được cấu hình để:

chọn tập hợp các số ma thuật từ nội dung ở LBA0 đầu tiên, theo đó tập hợp các số ma thuật đã chọn được sử dụng với bảng tra cứu số ma thuật để xác định loại của hệ điều hành hoặc loại của hoạt động lưu trữ thứ cấp được liên kết với hệ thống tệp của bộ điều khiển, theo đó bảng tra cứu số ma thuật được lấy từ mô-đun dữ liệu; và

chỉ dẫn mạng thần kinh được huấn luyện đã nói để phát hiện các hoạt động độc hại liên quan đến loại đã xác định của hệ điều hành hoặc hoạt động lưu trữ thứ cấp từ mô-đun dữ liệu, mạng thần kinh đã nói được sử dụng bởi mô-đun đã nói mà giám sát thiết bị lưu trữ

đã nói để phát hiện hoạt động độc hại.

3. Mô-đun theo điểm 2, trong đó việc chỉ dẫn mạng thần kinh được huấn luyện bao gồm mô-đun được cấu hình để chọn mạng thần kinh được huấn luyện đã nói được sử dụng bởi mô-đun đã nói mà giám sát thiết bị lưu trữ đã nói để phát hiện hoạt động độc hại, mà đã được tối ưu hóa cho loại đã xác định của hệ điều hành hoặc loại đã xác định của hoạt động lưu trữ thứ cấp được liên kết với hệ thống tệp của bộ điều khiển.

4. Mô-đun theo điểm 1, trong đó việc nhận dạng các LBA của thiết bị lưu trữ mà để được giám sát bao gồm mô-đun được cấu hình để:

nhận dạng, dựa trên loại đã xác định của hệ điều hành hoặc hoạt động lưu trữ thứ cấp được liên kết với mạng thần kinh được huấn luyện được chỉ dẫn được sử dụng bởi mô-đun đã nói mà giám sát thiết bị lưu trữ đã nói để phát hiện hoạt động độc hại, các LBA mà chứa dữ liệu quan trọng theo đó dữ liệu quan trọng bao gồm ít nhất bảng tệp chính, bản ghi khởi động chính, khu vực khởi động, khối thông số BIOS hoặc khối thông số BIOS mở rộng của hệ thống tệp được liên kết với thiết bị lưu trữ.

5. Mô-đun theo điểm 1, trong đó mô-đun được cấu hình thêm để:

tối ưu hóa mạng thần kinh được huấn luyện sử dụng hoạt động độc hại được xác định là đã xảy ra tại thiết bị lưu trữ dựa trên các lệnh và các nội dung được nhân bản.

6. Mô-đun theo điểm 1 hoặc 5, trong đó mô-đun được cấu hình thêm để:

khóa thiết bị lưu trữ để phản hồi sự xác định rằng hoạt động độc hại được xác định là đã xảy ra tại thiết bị lưu trữ dựa trên các lệnh và các nội dung được nhân bản.

7. Mô-đun theo điểm bất kỳ trong số các điểm từ 1 đến 6, trong đó mạng thần kinh được huấn luyện bao gồm mạng thần kinh nhân tạo.

8. Mô-đun theo điểm 7, trong đó mạng thần kinh nhân tạo bao gồm mạng thần kinh hồi quy (Recurrent Neural Network, RNN) hoặc mạng thần kinh tích chập (Convolutional Neural Network, CNN).

9. Phương pháp phát hiện hoạt động độc hại trong thiết bị lưu trữ bao gồm các bước để: truy xuất, sử dụng mô-đun được cung cấp trong bộ điều khiển của thiết bị lưu trữ, địa chỉ khối logic đầu tiên (LBA0) được gửi đến bộ điều khiển từ máy chủ;

truy xuất, sử dụng mô-đun, nội dung ở LBA0 đầu tiên, theo đó nội dung được truy xuất được sử dụng để chỉ dẫn mạng thần kinh được huấn luyện được truy xuất từ mô-đun dữ liệu được cung cấp trong bộ điều khiển, mạng thần kinh đã nói được sử dụng bởi mô-đun đã nói để giám sát thiết bị lưu trữ đã nói để phát hiện hoạt động độc hại;

nhận dạng sử dụng nội dung ở LBA0 đầu tiên và mạng thần kinh được huấn luyện, sử dụng mô-đun, các địa chỉ khối logic (LBA) của thiết bị lưu trữ mà để được giám sát;

nhân bản, sử dụng mô-đun, các lệnh được gửi đến các LBA được nhận dạng bởi máy chủ tới bộ điều khiển, và nhân bản các nội dung của các LBA được nhân bản; và

xác định, sử dụng mạng thần kinh được huấn luyện, nếu hoạt động độc hại đang xảy ra tại thiết bị lưu trữ dựa trên các lệnh và các nội dung được nhân bản, trong đó mạng thần kinh được huấn luyện cho các loại khác nhau của các hệ điều hành hoặc các hoạt động lưu trữ thứ cấp dựa trên quyền truy cập đọc/ghi/ghi đè trung bình của các nội dung ở các LBA liên quan đến các bản ghi khởi động chính, các bản ghi quan trọng, các bảng tệp chính, các khu vực khởi động, các khối thông số BIOS hoặc các khối thông số BIOS mở rộng của các hệ thống tệp được liên kết với các hệ điều hành hoặc các hoạt động lưu trữ thứ cấp.

10. Phương pháp theo điểm 9, trong đó việc chỉ dẫn của mạng thần kinh được huấn luyện được liên kết được sử dụng bởi mô-đun đã nói mà giám sát thiết bị lưu trữ đã nói để phát hiện hoạt động độc hại, bao gồm các bước để:

chọn, sử dụng mô-đun, tập hợp các số ma thuật từ nội dung ở LBA0 đầu tiên, theo đó tập hợp các số ma thuật đã chọn được sử dụng với bảng tra cứu số ma thuật để xác định loại của hệ điều hành hoặc loại của hoạt động lưu trữ thứ cấp được liên kết với hệ thống tệp của bộ điều khiển, theo đó bảng tra cứu số ma thuật được lấy từ mô-đun dữ liệu; và

chỉ dẫn, sử dụng mô-đun, mạng thần kinh được huấn luyện để phát hiện các hoạt động độc hại liên quan đến loại đã xác định của hệ điều hành hoặc hoạt động lưu trữ thứ cấp từ mô-đun dữ liệu, mạng thần kinh đã nói được sử dụng bởi mô-đun đã nói để giám sát thiết bị lưu trữ đã nói để phát hiện hoạt động độc hại.

11. Phương pháp theo điểm 10, trong đó việc chỉ dẫn mạng thần kinh được huấn luyện được sử dụng bởi mô-đun đã nói mà giám sát thiết bị lưu trữ đã nói để phát hiện hoạt động độc hại, bao gồm bước để chọn mạng thần kinh được huấn luyện mà đã được tối ưu hóa cho

loại đã xác định của hệ điều hành hoặc loại đã xác định của hoạt động lưu trữ thứ cấp được liên kết với hệ thống tệp của bộ điều khiển.

12. Phương pháp theo điểm 9, trong đó việc nhận dạng các LBA của thiết bị lưu trữ mà để được giám sát bao gồm các bước để:

nhận dạng, sử dụng mô-đun, dựa trên loại đã xác định của hệ điều hành hoặc hoạt động lưu trữ thứ cấp được liên kết với mạng thần kinh được huấn luyện được chỉ dẫn được sử dụng bởi mô-đun đã nói mà giám sát thiết bị lưu trữ đã nói để phát hiện hoạt động độc hại, các LBA mà chứa dữ liệu quan trọng theo đó dữ liệu quan trọng bao gồm ít nhất bảng tệp chính, bản ghi khởi động chính, khu vực khởi động, khối thông số BIOS hoặc khối thông số BIOS mở rộng của hệ thống tệp được liên kết với thiết bị lưu trữ.

13. Phương pháp theo điểm 9, trong đó phương pháp này còn bao gồm bước để: tối ưu hóa, sử dụng mô-đun, mạng thần kinh được huấn luyện sử dụng hoạt động độc hại

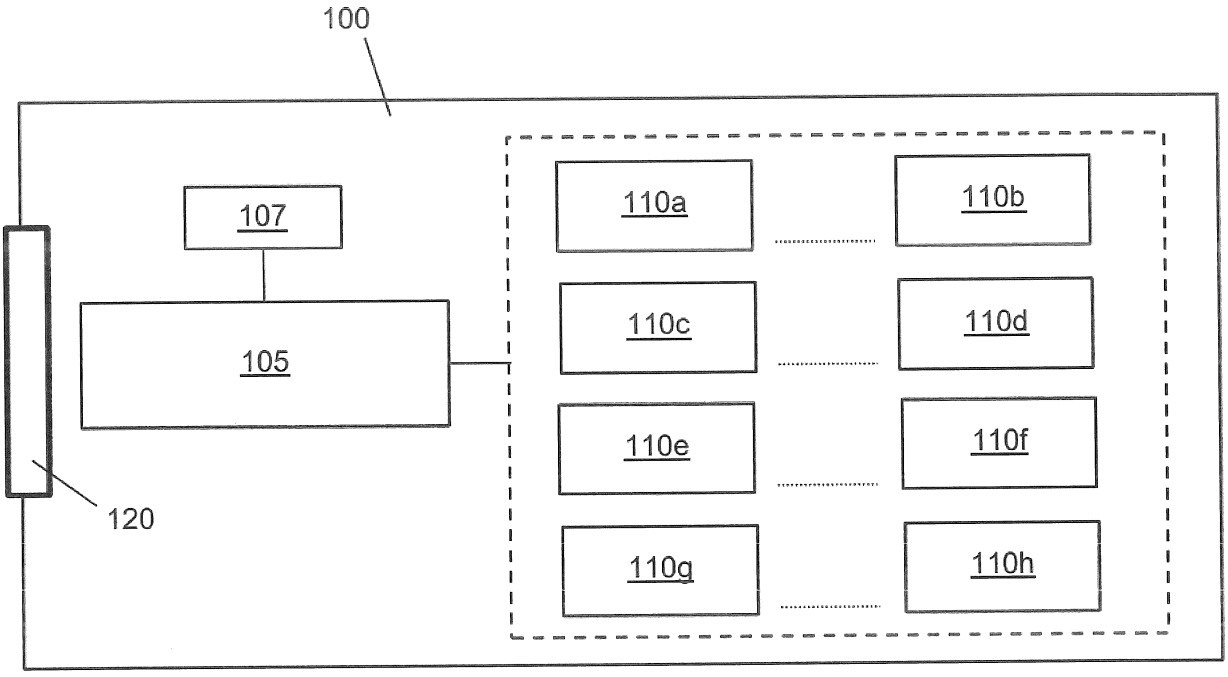
được xác định là đã xảy ra tại thiết bị lưu trữ dựa trên các lệnh và các nội dung được nhân bản.

14. Phương pháp theo điểm 9 hoặc 13, trong đó phương pháp này còn bao gồm bước để:

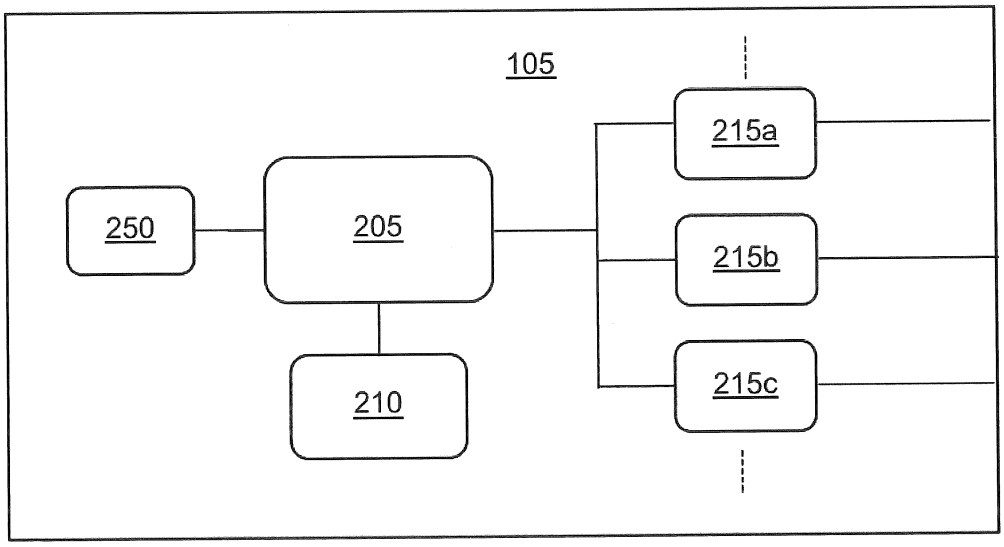
khóa, sử dụng mô-đun, thiết bị lưu trữ để phản hồi sự xác định rằng hoạt động độc hại được xác định là đã xảy ra tại thiết bị lưu trữ dựa trên các lệnh và các nội dung được nhân bản.

15. Phương pháp theo điểm bất kỳ trong số các điểm từ 9 đến 14, trong đó mạng thần kinh được huấn luyện bao gồm mạng thần kinh nhân tạo.

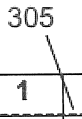
16. Phương pháp theo điểm 15, trong đó mạng thần kinh nhân tạo bao gồm mạng thần kinh hồi quy (Recurrent Neural Network, RNN) hoặc mạng thần kinh tích chập (Convolutional Neural Network, CNN).


100
107
105
120
110a
110b
110c
110d
110e
110f
110g
110h

Hình 1

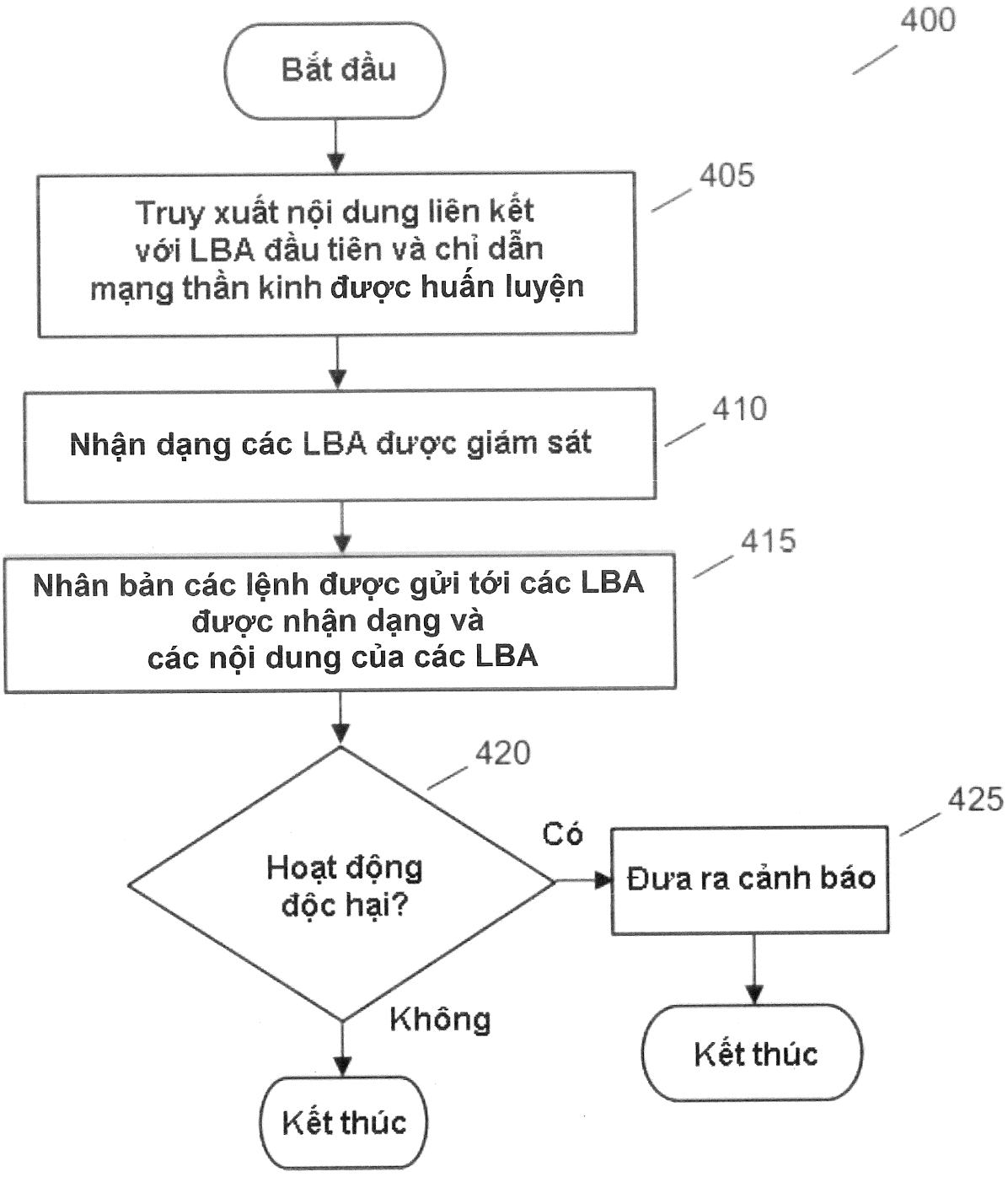

105
250
205
210
215a
215b
215c

Hình 2

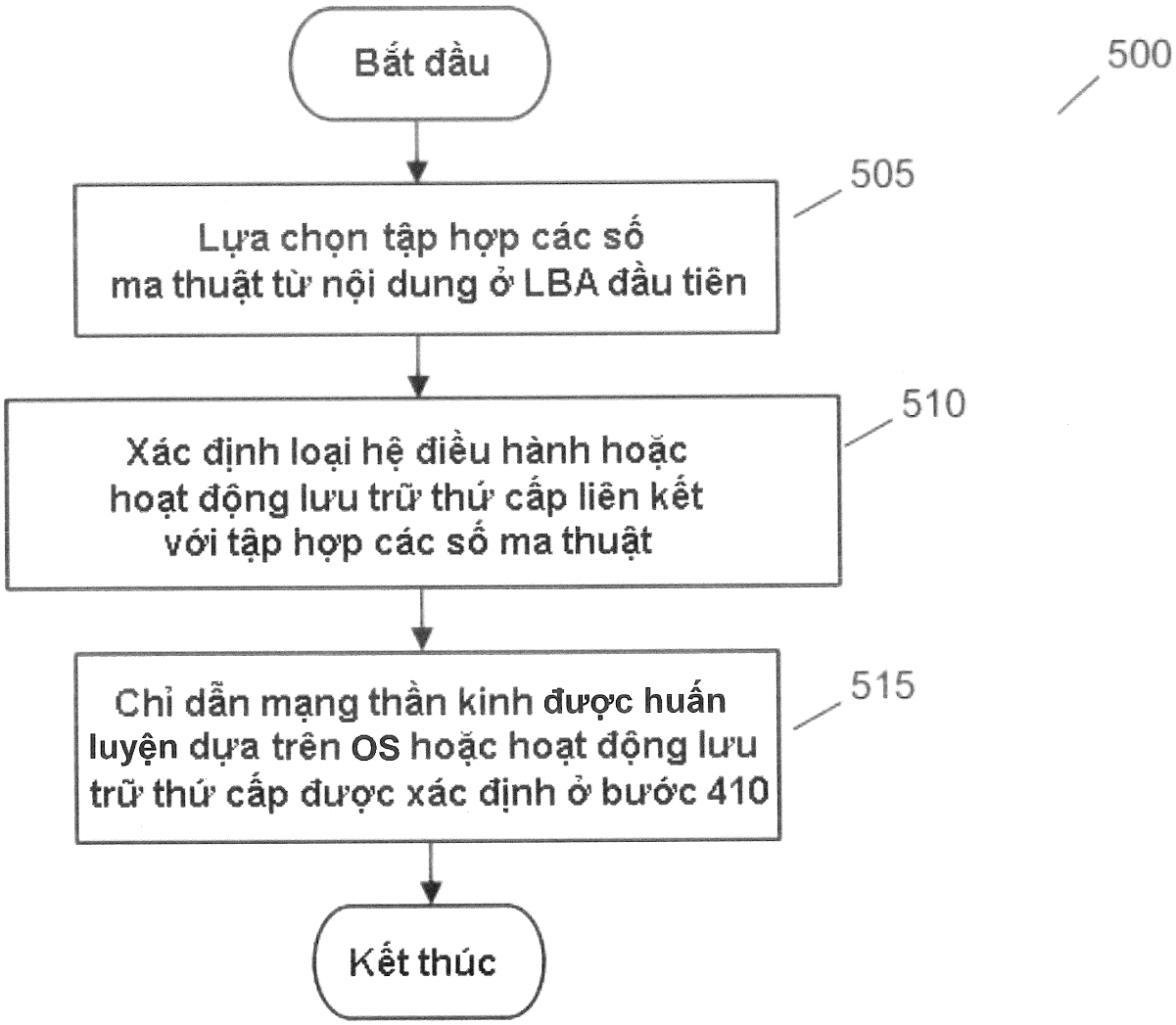


Hiệu số	0	1	2	3	4	5	6	7	8	9	A	B	C	D
00027389F0	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF
0002738A00	EB	52	90	4E	55	67	89	20	20	20	20	00	02	00
0002738A10	74	62	4F	FF	B4	MN	DE	C1	D3	GG	45	69	00	00
0002738A20	90	4E	55	67	89	FF	KL	20	20	20	00	56	34	00
0002738A30	4F	FF	B4	MN	DE	89	PG	34	00	56	J6	23	23	00
0002738A40	01	J7	K8	D4	34	00	98	23	00	23	N3	F4	45	01
0002738A50	23	34	00	8G	23	00	56	45	01	F4	8K	32	6H	85
0002738A60	9O	23	00	J7	45	01	78	6H	85	32	5G	2S	BV	54
0002738A70	01	45	01	4D	6H	85	54	BV	54	2S	F5	J9	MN	56
0002738A80	6Y	6H	85	6G	BV	54	75	D4	34	00	98	C3	7J	23
0002738A90	L0	BV	54	20	20	20	D4	34	00	98	56	78	N3	F4
0002738AA0	G5	7J	9L	C1	D3	GG	FF	FF	FF	8K	23	05	8K	32
0002738AB0	FF	FF	FF	FF	90	20	20	20	00	5G	F4	00	5G	2S
0002738AC0	20	20	20	00	5F	D3	GG	45	69	F5	32	H6	F5	7J
0002738AD0	D3	GG	45	69	D4	34	00	98	G5	L8	2S	09	L8	2G
⋮	⋮	⋮	⋮	⋮	⋮	⋮	⋮	⋮	⋮	⋮	⋮	⋮	⋮	⋮

Hình 3


400
Bắt đầu
405
Truy xuất nội dung liên kết với LBA đầu tiên và chỉ dẫn mạng thần kinh được huấn luyện
410
Nhận dạng các LBA được giám sát
415
Nhân bản các lệnh được gửi tới các LBA được nhận dạng và các nội dung của các LBA
420
Hoạt động độc hại?
Có
425
Đưa ra cảnh báo
Kết thúc
Không
Kết thúc

Hình 4


Bắt đầu
500
505
Lựa chọn tập hợp các số ma thuật từ nội dung ở LBA đầu tiên
510
Xác định loại hệ điều hành hoặc hoạt động lưu trữ thứ cấp liên kết với tập hợp các số ma thuật
515
Chỉ dẫn mạng thần kinh được huấn luyện dựa trên OS hoặc hoạt động lưu trữ thứ cấp được xác định ở bước 410
Kết thúc

Hình 5