|  |  |  |
| --- | --- | --- |
|  | BAN CƠ YẾU CHÍNH PHỦ  “HỌC VIỆN KỸ THUẬT MẬT MÃ” | Mẫu 2 |

BÁO CÁO CHUYÊN ĐỀ SỐ 5.1

“Phân tích, thiết kế kiến trúc hệ thống”

NHIỆM VỤ: “Nghiên cứu và ứng dụng nền tảng học sâu để xây dựng hệ thống phát hiện mã độc trực tuyến”.

Mã số: 06/2022/CB.

Cơ quan chủ trì: Học viện Kỹ thuật Mật mã

Chủ nhiệm: ThS. Lê Đức Thuận

Hà Nội - 2023

|  |  |  |
| --- | --- | --- |
|  | BAN CƠ YẾU CHÍNH PHỦ  “HỌC VIỆN KỸ THUẬT MẬT MÃ” |  |

BÁO CÁO CHUYÊN ĐỀ SỐ 5.1

“Phân tích, thiết kế kiến trúc hệ thống”

NHIỆM VỤ: “Nghiên cứu và ứng dụng nền tảng học sâu để xây dựng hệ thống phát hiện mã độc trực tuyến”.

Mã số: 06/2022/CB.

Cơ quan chủ trì: Học viện Kỹ thuật Mật mã

Chủ nhiệm: ThS. Lê Đức Thuận

|  |  |
| --- | --- |
| **Người thực hiện chuyên đề** | **Cơ quan chủ trì** |
| *(Họ tên và chữ ký)* | *(Họ tên và chữ ký)* |

Hà Nội - 2023

MỤC LỤC

[MỤC LỤC 1](#_Toc129761723)

[DANH MỤC HÌNH ẢNH 2](#_Toc129761724)

[DANH MỤC BẢNG 3](#_Toc129761725)

[1. GIẢI PHÁP TỔNG THỂ 4](#_Toc129761726)

[1.1. Thông tin chung về giải pháp 4](#_Toc129761727)

[1.2. Mô hình triển khai 5](#_Toc129761728)

[1.3. Quy chế đồng bộ thống nhất cho đối tượng người dùng 6](#_Toc129761729)

[1.4. Các tính năng chung của BCYSecAI 7](#_Toc129761730)

[2. PHÂN TÍCH, THIẾT KẾ KIẾN TRÚC HỆ THỐNG PHẦN MỀM BCYSecAI 10](#_Toc129761731)

[2.1. Kiến trúc hệ thống tổng thể 10](#_Toc129761732)

[2.2. Thiết kế các hệ thống thành phần 11](#_Toc129761733)

[2.2.1. Hệ thống BCYSecAI server 11](#_Toc129761734)

[2.2.2. Hệ thống BCYSecAI máy trạm Windows 17](#_Toc129761735)

[2.2.3. Hệ thống BCYSecAI máy trạm Android/iOS 21](#_Toc129761736)

# DANH MỤC HÌNH ẢNH

[Hình 1. Mô hình giải pháp BCYSecAI 4](#_Toc129761603)

[Hình 2: Kiến trúc tổng thể của BCYSecAI 9](#_Toc129761604)

[Hình 3: Biểu đồ ca sử dụng gói BCYSecAI server 10](#_Toc129761605)

[Hình 4: Biểu đồ ca sử dụng gói BCYSecAI Windows 16](#_Toc129761606)

[Hình 5: Biểu đồ ca sử dụng gói BCYSecAI Android 21](#_Toc129761607)

# DANH MỤC BẢNG

[Bảng 1. Tổng hợp các yêu cầu chức năng hệ thống 7](#_Toc129761694)

[Bảng 2. Ca sử dụng Đăng nhập/đăng xuất 12](#_Toc129761695)

[Bảng 3. Ca sử dụng Cập nhật CSDL mã độc 12](#_Toc129761696)

[Bảng 4. Ca sử dụng Cấu hình hệ thống 13](#_Toc129761697)

[Bảng 5. Ca sử dụng Huấn luyện mô hình 14](#_Toc129761698)

[Bảng 6. Ca sử dụng Quét virus/mã độc 14](#_Toc129761699)

[Bảng 7. Ca sử dụng Xử lý kết quả rà quét 15](#_Toc129761700)

[Bảng 8. Ca sử dụng Giám sát hệ thống 16](#_Toc129761701)

[Bảng 9. Ca sử dụng Báo cáo thống kê 16](#_Toc129761702)

[Bảng 10. Ca sử dụng Đăng nhập/đăng xuất 17](#_Toc129761703)

[Bảng 11. Ca sử dụng Cấu hình hệ thống 18](#_Toc129761704)

[Bảng 12. Ca sử dụng Quét virus/mã độc 19](#_Toc129761705)

[Bảng 13. Ca sử dụng Xử lý kết quả rà quét 19](#_Toc129761706)

[Bảng 14. Ca sử dụng Giám sát hệ thống Windows 20](#_Toc129761707)

[Bảng 15. Ca sử dụng Báo cáo thống kê 21](#_Toc129761708)

# 1. GIẢI PHÁP TỔNG THỂ

## 1.1. Thông tin chung về giải pháp

**Mục tiêu:** Xây dựng giải pháp Giám sát và phòng chống mã độc quản lý tập trung.

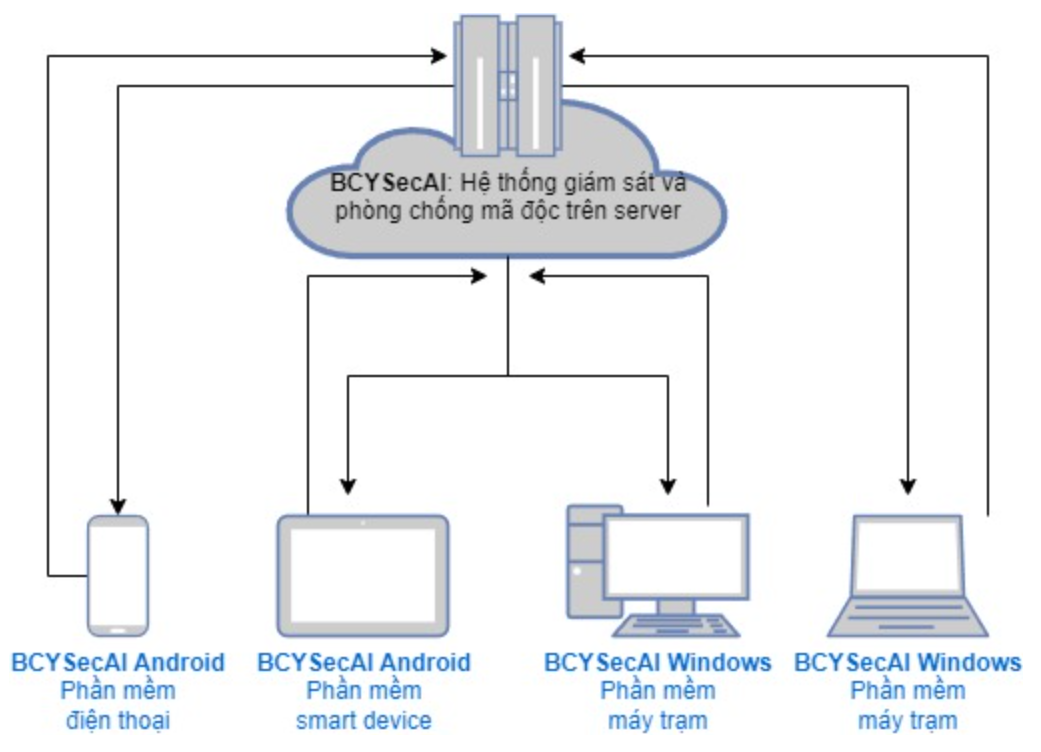
**Tên hệ thống:** BCYSecAI

**Các thành phần hệ thống:** Gồm 3 phần: server, máy trạm Windows, máy trạm điện thoại (Android)

**Mô tả hệ thống:**

* Hệ thống có thể được triển khai trong mạng nội bộ hoặc triển khai trong hệ thống mạng có kết nối Internet và đám mây. Hệ thống được thiết kế đặc biệt hoạt động theo mô hình quản lý tập trung trên máy chủ nội bộ hoặc máy chủ trên đám mây, bảo vệ an toàn tối đa cho từng máy tính cũng như trên toàn hệ thống mạng trước những nguy cơ về virus, trojan, rootkit, spyware, adware, v.v.
* Hệ thống cho phép phòng chống mã độc theo thời gian thực, đặc biệt tích hợp các công nghệ phát hiện mã độc dựa trên phân tích hành vi, giúp ngăn chặn virus mà không cần cập nhật mẫu. Do đó có thể bảo vệ máy tính chống lại các nguy cơ về virus như phần mềm gián điệp, keylogger hay các loại mã độc mã hóa tống tiền Ransomeware, v.v.
* Hệ thống được tích hợp chức năng thống kê, báo cáo giúp người quản trị mạng sẽ luôn nắm được thông tin tổng quan cũng như chi tiết mới nhất về tình hình mã độc trong toàn hệ thống, biết được loại virus nào đang lây lan trong mạng, những máy nào bị nhiễm virus, xử lý triệt để virus hay chưa, những máy nào chưa cập nhật chương trình diệt virus mới nhất, v.v. Với những thông tin này, người quản trị sẽ chủ động đưa ra các phương án xử lý chính xác và kịp thời, nhằm ngăn chặn tối đa các nguy cơ có thể ảnh hưởng tới hệ thống.
* Dữ liệu và quyền riêng tư sẽ được bảo vệ an toàn dù người sử dụng đang làm gì, ở bất cứ đâu như lướt web, tham gia mạng xã hội hay thực hiện các giao dịch trực tuyến.
* Các công cụ quản lý cho phép người quản trị cài đặt chương trình diệt virus, đặt lịch quét, ra lệnh quét cho các máy tính trong mạng từ xa, giảm thiểu thời gian, công sức và chi phí để quản trị hệ thống diệt virus trong mạng.

## 1.2. Mô hình triển khai



Hình 1. Mô hình giải pháp BCYSecAI

Đây là giải pháp diệt virus tổng thể, áp dụng những công nghệ tiên tiến nhất của BCYSecAI, hoạt động theo mô hình client/server, quản lý tập trung thống nhất. Sử dụng một Server đặt tại trụ sở chính. Các máy trạm sẽ cài BCYSecAI Client và kết nối với Server thông qua IP hoặc qua domain. Hoạt động của mô hình này như sau:

* BCYSecAI Server cập nhật các mẫu virus mới từ máy chủ của BCYSecAI về Server. Từ đây sẽ tiến hành cập nhật thống nhất xuống tất cả các máy trạm.
* BCYSecAI Client trên máy trạm sẽ tự động phát hiện và xử lý (Auto Protect) các virus, trojan, spyware, adware ngay khi chúng xâm nhập vào máy tính. Xử lý toàn bộ các virus lây lan qua USB, qua web, qua chia sẻ thư mục, virus lây qua lỗ hổng của phần mềm cũng như các trojan. Gửi báo cáo tình hình diệt virus về cho Server.
* BCYSecAI Server giúp cho người quản trị hệ thống có thể nắm  được tình hình virus trong toàn mạng, biết được máy nào trong mạng bị nhiễm virus gì. Người quản trị có thể đặt lịch, ra lệnh cho các máy tính trong mạng đồng thời xử lý virus vào 1 thời điểm.
* Nếu có virus mới xuất hiện trong mạng, người quản trị chỉ cần cập nhật mẫu virus mới nhất trên Server. Sau đó Server sẽ tự động cập nhật xuống các máy trạm, để xử lý đồng thời trên tất cả các máy.
* Trong trường hợp hệ thống được phân cấp quản lý với nhiều máy chủ, máy chủ đặt ở trung tâm và các máy chủ đặt ở các chi nhánh, thì Quản trị có thể tùy biến thiết lập hệ thống để máy chủ đặt tại các chi nhánh, thì Quản trị có thế tùy biến thiết lập hệ thống để máy chủ đặt tại trung tâm đóng vai trò quản lý toàn bộ thông tin của máy chủ đặt các chi nhánh, điều này giúp cho người quản trị ở máy chủ trung tâm kiểm soát một cách tốt nhất tình hình phòng chống virus trên toàn hệ thống.

## 1.3. Quy chế đồng bộ thống nhất cho đối tượng người dùng

Bên cạnh giải pháp về kỹ thuật, cần có một quy chế thống nhất trên toàn bộ hệ thống. Quy chế áp dụng đồng bộ sẽ giúp cho các giải pháp về kỹ thuật phát huy được hiệu quả cao nhất và giúp cho việc vận hành hệ thống được thông suốt. Sau đây là một số quy định với những người tham gia hệ thống:

**Đối với ngời sử dụng:**

* Người sử dụng chỉ dùng giải pháp diệt virus BCYSecAI do cơ quan quy định, không tự ý cài đặt các giải pháp diệt virus khác. Không tự ý tắt hoặc gỡ bỏ giải pháp BCYSecAI. Nếu không kết nối online với hệ thống mạng nội bộ của cơ quan thì phải định kỳ nối vào mạng để cập nhật phiên bản của giải pháp diệt virus BCYSecAI mới nhất theo quy định của quản trị.
* Khi xảy ra sự cố , đặc biệt những trường hợp nghi là do virus máy tính gây ra, người sử dụng cần phải có những ứng xử kịp thời theo những quy định chung, để đảm bảo virus không tiếp tục phá hoại máy tính của mình cũng như không lây lan ra toàn bộ hệ thống.

Để làm được điều đó, người sử dụng phải tuân thủ các quy tắc sau đây:

* Khi gặp bất kỳ sự cố nào, người sử dụng cần phải báo cáo cho quản trị mạng để xử lý, trong trường hợp không có sự trợ giúp của người quản trị mạng kịp thời, cần phải ngắt máy tính ra khỏi mạng để giảm nguy cơ virus lây lan ra toàn hệ thống.
* Nếu không liên lạc được với quản trị mạng vì một lý do nào đó, người sử dụng cần liên lạc trực tiếp với Trung tâm An ning mạng (qua số điện thoại trợ giúp khách hàng) để có được giải pháp khắc phục kịp thời.
* Khi diệt xong virus trên máy tính mới đưa trở lại hệ thống mạng theo sự chỉ dẫn của quản trị mạng.
* Trong trường hợp bất khả kháng (đang phục vụ cho khách hàng hoặc đang cung cấp những dịch vụ nghiệp vụ quan trọng không thể ngắt máy tính ra khỏi mạng) người sử dụng phải thông báo chi tiết cho người quản trị để có biện pháp phòng ngừa sự lây lan.

**Đối với quản trị:**

* Người quản trị thường xuyên kiểm tra các version của các chương trình diệt virus trên máy người dùng. Kiểm tra thường xuyên xem người dùng có cài đúng phiên bản diệt virus cơ quan quy định không. Phiên bản diệt virus có được update thường xuyên không.
* Sử dụng các tool tiện ích tích hợp sẵn trên giao diện của BCYSecAI để xử lý những vấn đề của máy tính khi cần.
* Nếu có nghi ngờ có biến thể virus mới xuất hiện trong mạng cần liên hệ ngay với Trung tâm hỗ trợ kỹ thuật của BCYSecAI để cùng phối hợp giải quyết.

## 1.4. Các tính năng chung của BCYSecAI

Bảng 1. Tổng hợp các yêu cầu chức năng hệ thống

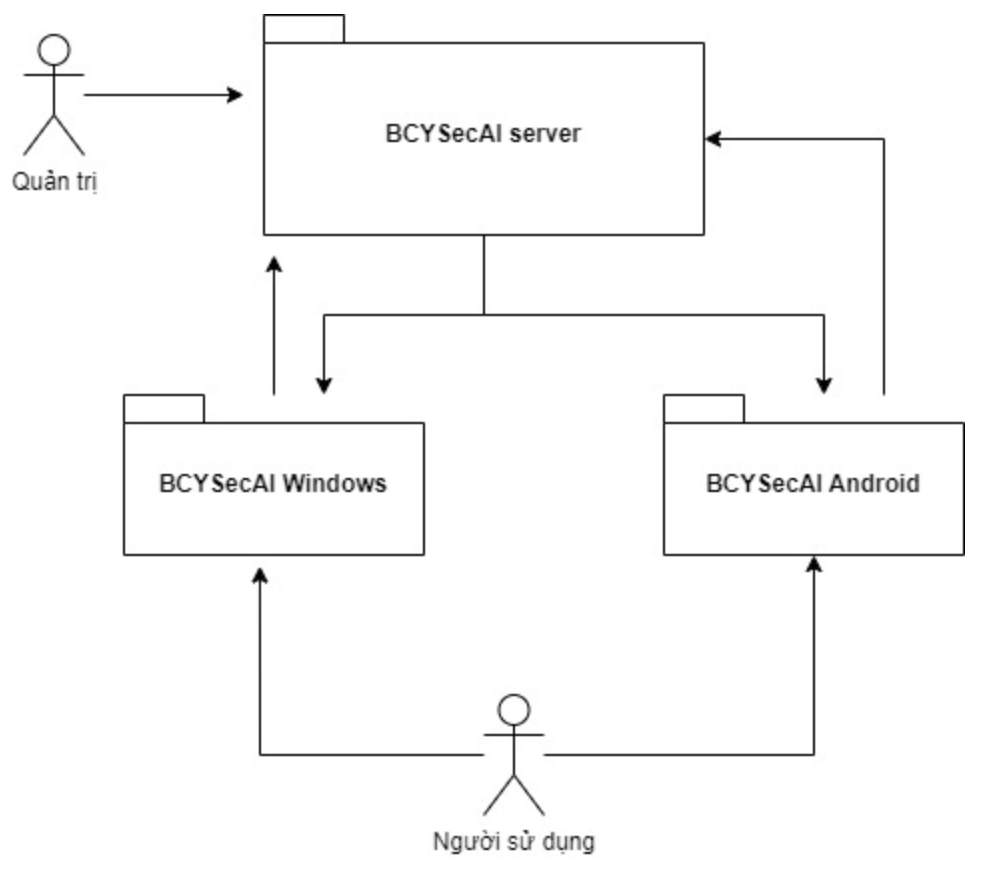
|  |  |  |
| --- | --- | --- |
| **STT** | **Chức năng** | **Ghi chú** |
|  | Tích hợp công nghệ trí tuệ nhân tạo AI |  |
|  | Giao dịch online an toàn |  |
|  | Chống phần mềm gián điệp |  |
|  | Real-time Protection – Bảo vệ thời gian thực |  |
|  | Safe Run – Thực thi an toàn |  |
|  | Quét và diệt virus theo thời gian thực: phần mềm hoạt động ở chế độ nền có khả năng kiểm soát và bảo vệ theo thời gian thực tất cả các dữ liệu trong ổ cứng, bộ nhớ, các thiết bị cắm ngoài (USB, CD/DVD, thẻ nhớ...) và mạng Internet |  |
|  | Tải phần mềm an toàn |  |
|  | Chống phần mềm Quảng cáo |  |
|  | Chống giả mạo các phần mềm virus |  |
|  | Diệt virus siêu đa hình |  |
|  | Khả năng quét kết nối mã hóa dựa trên giao thức HTTPS/SSL |  |
|  | Quét virus theo hành vi |  |
|  | Công nghệ điện toán đám mây |  |
|  | Bảo vệ truy nhập web và diệt virus mạng |  |
|  | Tự phòng vệ trước sự tấn công của malware |  |
|  | Kiểm soát truy cập web đen |  |
|  | Hỗ trợ các chế độ quét: Quét thông thường, Quick Scan - Quét nhanh, Smart Scan Quét thông minh, Deep Scan - Quét sâu toàn bộ máy, Quét các file nén |  |
|  | Cập nhật mẫu nhận diện từng phần |  |
|  | Quản lý tình hình virus trên các máy trạm tại Server |  |
|  | Quản lý tập trung theo mô hình phân cấp nhiều máy chủ, cho phép cảnh báo tới người quản trị khi có mối hiểm họa lây lan. |  |
|  | Quản lý, theo dõi trạng thái, phiên bản của BCYSecAI Client trên các máy trạm |  |
|  | Hỗ trợ cài đặt, triển khai máy tram từ xa thông qua máy chủ |  |
|  | Thống kê và báo cáo tình hình virus trên toàn hệ thống |  |
|  | Đặt lịch quét định kì thống nhất cho tất cả các máy trạm trong hệ thống. Trong trường hợp người quản trị đặt lịch quét định kỳ cho máy trạm, mọi thay đổi về lịch quét định kỳ từ phía người sử dụng máy trạm sẽ bị loại bỏ mỗi khi máy trạm kết nối tới máy chủ |  |
|  | Ra lệnh từ xa cho từng nhóm hay tất cả các máy trạm trong hệ thống quét virus vào một thời điểm bất kì |  |
|  | Report tình hình lây nhiễm mã độc, chia sẻ thông tin, dữ liệu thống kê tình hình lây nhiễm mã độc với hệ thống kỹ thuật của Bộ Thông tin và Truyền thông |  |

# 2. PHÂN TÍCH, THIẾT KẾ KIẾN TRÚC HỆ THỐNG PHẦN MỀM BCYSecAI

## 2.1. Kiến trúc hệ thống tổng thể

Hệ thống BCYSecAI gồm 3 hệ thống thống con. Ba hệ thống con này tương ứng với ba gói phần mềm trên máy chủ, trên máy trạm Windows và trên máy trạm Android, như mô tả trong Biểu đồ Gói – Hình 2, bao gồm:

* BCYSecAI server
* BCYSecAI Windows
* BCYSecAI Android

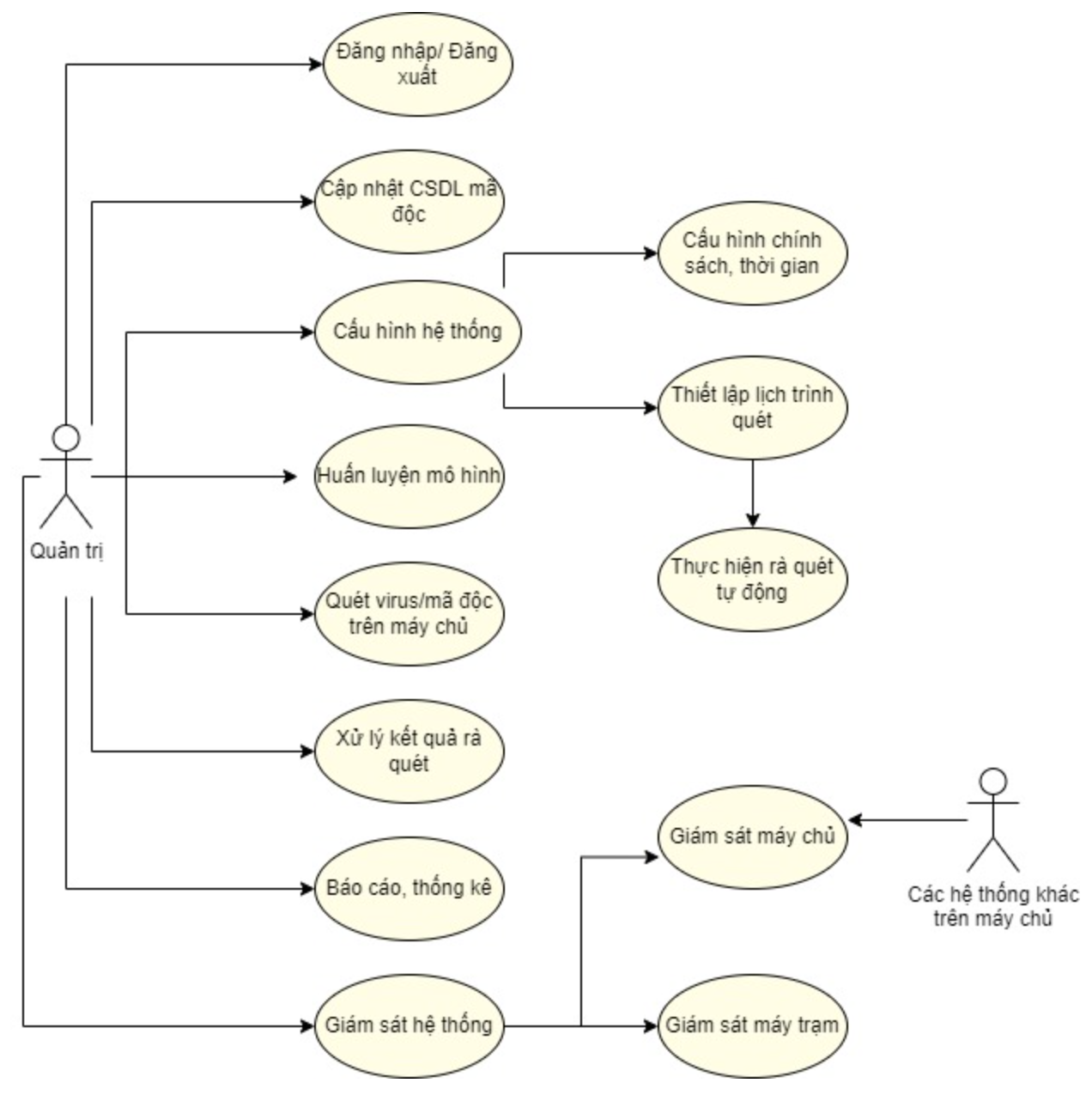


Hình 2: Kiến trúc tổng thể của BCYSecAI

## 2.2. Thiết kế các hệ thống thành phần

### 2.2.1. Hệ thống BCYSecAI server

**Biểu đồ ca sử dụng trong gói**



Hình 3: Biểu đồ ca sử dụng gói BCYSecAI server

**Mô tả các ca sử dụng**

Bảng 2. Ca sử dụng Đăng nhập/đăng xuất

|  |  |
| --- | --- |
| Ca sử dụng | Đăng nhập/đăng xuất |
| Tác nhân | Quản trị |
| Mô tả | Người dùng đăng nhập vào hệ thống từ trình duyệt/Hoặc đăng xuất khỏi hệ thống |
| Tiền điều kiện | Đăng nhập/Đăng xuất hệ thống thành công |
| Luồng sự kiện | Bắt đầu từ giao diện đăng nhập (Hoặc người dùng chọn Đăng xuất)   1. Màn hình ứng dụng hiển thị form đăng nhập 2. Nhập tên đăng nhập và mật khẩu 3. Kiểm tra tên đăng nhập và mật khẩu ở máy trạm 4. Xác thực trên server 5. Chuyển vào trang chủ quản trị nếu đăng nhập thành công. Ngược lại, thông báo lỗi |
| Hậu điều kiện | Nếu ca sử dụng này thực hiện thành công, người dùng sẽ được hiều hướng đến trang quản trị; nếu không thành công sẽ hiển thị trạng thái lỗi. |

Bảng 3. Ca sử dụng Cập nhật CSDL mã độc

|  |  |
| --- | --- |
| Ca sử dụng | Cập nhật CSDL mã độc |
| Tác nhân | Người quản trị |
| Mô tả | Cập nhật thêm các mẫu mã độc mới và huấn luyện bổ sung cho hệ thống |
| Tiền điều kiện | Đăng nhập hệ thống thành công |
| Luồng sự kiện | Ca sử dụng này bắt đầu khi người dùng muốn vào nhóm hội thảo để đọc tin   1. Màn hình ứng dụng hiển thị Form cập nhật 2. Chọn nguồn cập nhật 3. Huấn luyện tăng cường cho hệ thống 4. Cập nhật mô hình |
| Hậu điều kiện | Nếu ca sử dụng này thực hiện thành công, tham số và trọng số mô hình được cập nhật; nếu không thành công sẽ hiển thị trạng thái lỗi. |

Bảng 4. Ca sử dụng Cấu hình hệ thống

|  |  |
| --- | --- |
| Ca sử dụng | Cấu hình hệ thống |
| Tác nhân | Người quản trị |
| Mô tả | Cấu hình hệ thống: cấu hình máy chủ, các chính sách máy trạm, lập lịch rà quét, v.v. |
| Tiền điều kiện | Đăng nhập hệ thống thành công |
| Luồng sự kiện | Ca sử dụng này bắt đầu khi người dùng chọn chức năng Cấu hình trên menu   1. Màn hình ứng dụng hiển thị form lựa chọn cấu hình 2. Cấu hình chính sách 3. Lập lịch rà quét 4. Cấu hình chung cho các máy trạm |
| Luồng phụ | Lập lịch rà quét:  3.1. Lựa chọn thời gian  3.2. Lựa chọn các nội dung quét  3.3. Lập lịch và giám sát thực hiện |
| Hậu điều kiện | Nếu ca sử dụng này thực hiện thành công, cấu hình, lịch trình sẽ được cập nhật; nếu không thành công sẽ hiển thị trạng thái lỗi. |

Bảng 5. Ca sử dụng Huấn luyện mô hình

|  |  |
| --- | --- |
| Ca sử dụng | Huấn luyện mô hình |
| Tác nhân | Người quản trị |
| Mô tả | Mô tả cách hoạt động khi người dùng muốn huấn luyện lại mạng |
| Tiền điều kiện | Đăng nhập hệ thống thành công |
| Luồng sự kiện | Ca sử dụng này bắt đầu khi người dùng nhấn vào chức năng huấn luyện.   1. Màn hình ứng dụng hiển thị form cấu hình huấn luyện: số vòng lặp, hệ số lỗi, độ sâu 2. Huấn luyện và hiệu chỉnh 3. Cập nhật kết quả huấn luyện |
| Hậu điều kiện | Nếu ca sử dụng này thực hiện thành công, người dùng sẽ xem được bản rõ của tin nhắn; nếu không thành công sẽ hiển thị trạng thái lỗi. |

Bảng 6. Ca sử dụng Quét virus/mã độc

|  |  |
| --- | --- |
| Ca sử dụng | Quét virus/mã độc |
| Tác nhân | Người quản trị/Lập lịch tự động |
| Mô tả | Mô tả cách hoạt động khi người dùng chọn rà quét hoặc kích hoạt tự động |
| Tiền điều kiện | Đăng nhập hệ thống thành công |
| Luồng sự kiện | Ca sử dụng này bắt đầu khi người dùng chọn chức năng Rà quét mã độc; hoặc khi rà quét tự động; hoặc khi có tác động lên hệ thống từ người dùng   1. Màn hình ứng dụng hiển thị form các lựa chọn rà quét 2. Rà quét hệ thống theo mô hình đã huấn luyện 3. Tổng hợp, báo cáo kết quả rà quét 4. Cập nhật kết quả học tăng cường cho mã độc mới |
| Hậu điều kiện | Nếu ca sử dụng này thực hiện thành công, hệ thống được rà quét virus/mã độc; nếu không thành công sẽ hiển thị trạng thái lỗi. |

Bảng 7. Ca sử dụng Xử lý kết quả rà quét

|  |  |
| --- | --- |
| Ca sử dụng | Xử lý kết quả rà quét |
| Tác nhân | Người quản trị |
| Mô tả | Mô tả cách hoạt động khi mô-đun Rà quét mã độc đã thực hiện xong |
| Tiền điều kiện | Thực hiện rà quét thành công |
| Luồng sự kiện | Ca sử dụng này bắt đầu khi muốn xử lý kết quả rà quét từ báo cáo của hệ thống   1. Lựa chọn các hình thức xử lý 2. Xử lý tương ứng 3. Hiển thị kết quả |
| Hậu điều kiện | Nếu ca sử dụng này thực hiện thành công, kết quả rà quét mã độc được xử lý; nếu không thành công sẽ hiển thị trạng thái lỗi. |

Bảng 8. Ca sử dụng Giám sát hệ thống

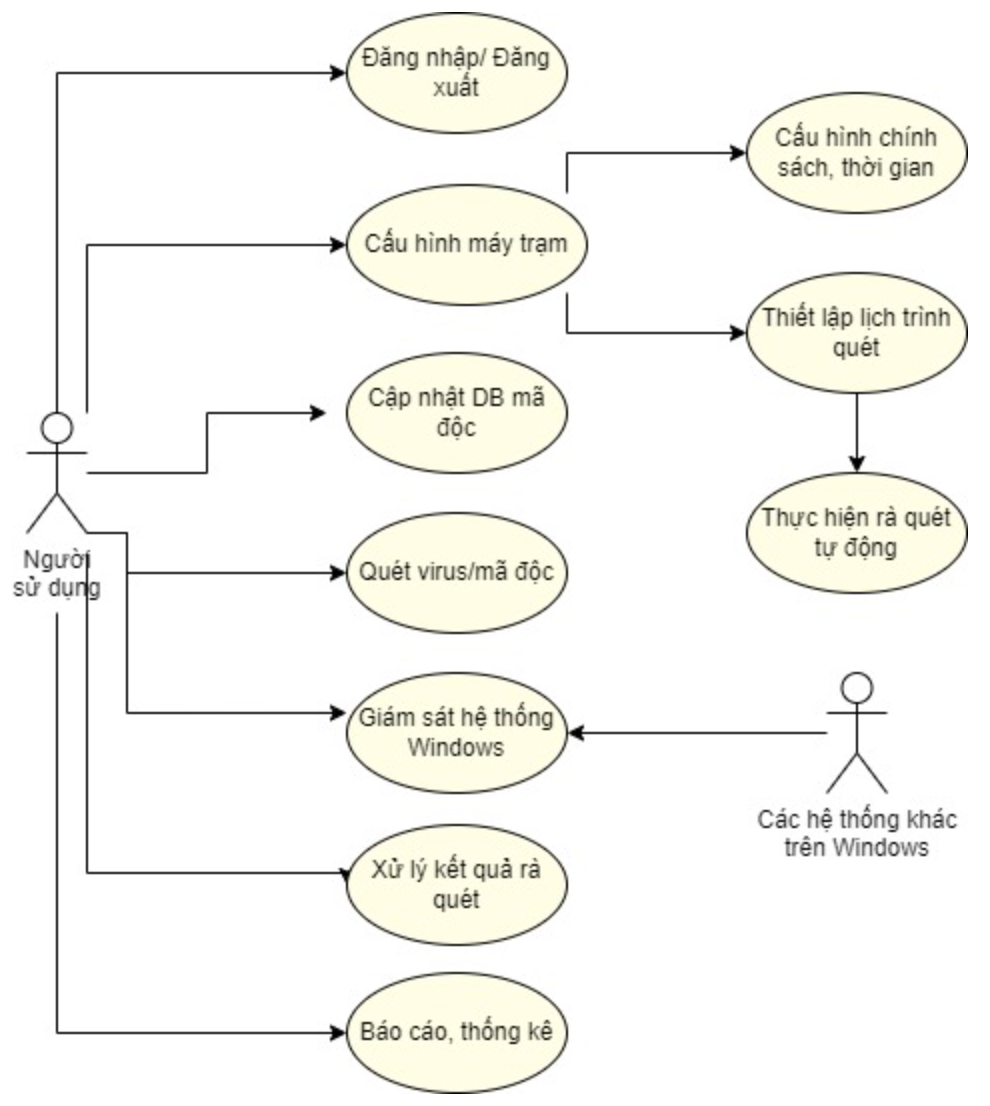
|  |  |
| --- | --- |
| Ca sử dụng | Giám sát hệ thống |
| Tác nhân | Người quản trị thực hiện, hệ thống chạy ngầm |
| Mô tả | Khi người quản trị lập lịch và thực hiện hệ thống |
| Tiền điều kiện |  |
| Luồng sự kiện | Hệ thống chạy ngầm   1. Giám sát hoạt động trên file: thêm, sửa, xóa 2. Giám sát hoạt động Download, Upload 3. Gọi mô-đun rà quét khi có dấu hiệu bất thường |
| Hậu điều kiện | Nếu ca sử dụng này thực hiện thành công, người dùng sẽ xem được bản rõ của tin nhắn; nếu không thành công sẽ hiển thị trạng thái lỗi. |

Bảng 9. Ca sử dụng Báo cáo thống kê

|  |  |
| --- | --- |
| Ca sử dụng | Báo cáo thống kê |
| Tác nhân | Người quản trị |
| Mô tả | Mô tả cách hoạt động khi người dùng sử dụng chức năng Báo cáo, thống kê |
| Tiền điều kiện | Đăng nhập hệ thống thành công |
| Luồng sự kiện | Ca sử dụng này bắt đầu khi người dùng muốn vào nhóm hội thảo để đọc tin   1. Màn hình ứng dụng hiển thị các chức năng Báo cáo, Thống kê 2. Thống kê theo tuần, tháng 3. Xuất dữ liệu báo cáo ra excel, pdf |
| Hậu điều kiện | Nếu ca sử dụng này thực hiện thành công, người dùng sẽ xem được bản rõ của tin nhắn; nếu không thành công sẽ hiển thị trạng thái lỗi. |

### 2.2.2. Hệ thống BCYSecAI máy trạm Windows

**Biểu đồ ca sử dụng trong gói**



Hình 4: Biểu đồ ca sử dụng gói BCYSecAI Windows

**Mô tả các ca sử dụng**

Bảng 10. Ca sử dụng Đăng nhập/đăng xuất

|  |  |
| --- | --- |
| Ca sử dụng | Đăng nhập/đăng xuất |
| Tác nhân | Quản sử dụng |
| Mô tả | Người dùng đăng nhập vào hệ thống từ trình duyệt/Hoặc đăng xuất khỏi hệ thống |
| Tiền điều kiện | Đăng nhập/Đăng xuất hệ thống thành công |
| Luồng sự kiện | Bắt đầu từ giao diện đăng nhập (Hoặc người dùng chọn Đăng xuất)   1. Màn hình ứng dụng hiển thị form đăng nhập 2. Nhập tên đăng nhập và mật khẩu 3. Kiểm tra tên đăng nhập và mật khẩu ở máy trạm 4. Xác thực trên server 5. Chuyển vào trang chủ quản trị nếu đăng nhập thành công. Ngược lại, thông báo lỗi |
| Hậu điều kiện | Nếu ca sử dụng này thực hiện thành công, người dùng sẽ được hiều hướng đến trang quản trị; nếu không thành công sẽ hiển thị trạng thái lỗi. |

Bảng 11. Ca sử dụng Cấu hình hệ thống

|  |  |
| --- | --- |
| Ca sử dụng | Cấu hình hệ thống |
| Tác nhân | Quản sử dụng |
| Mô tả | Cấu hình hệ thống: cấu hình máy chủ, các chính sách máy trạm, lập lịch rà quét, v.v. |
| Tiền điều kiện | Đăng nhập hệ thống thành công |
| Luồng sự kiện | Ca sử dụng này bắt đầu khi người dùng chọn chức năng Cấu hình trên menu   1. Màn hình ứng dụng hiển thị form lựa chọn cấu hình 2. Cấu hình chính sách 3. Lập lịch rà quét 4. Cấu hình chung cho các máy trạm |
| Luồng phụ | Lập lịch rà quét:  3.1. Lựa chọn thời gian  3.2. Lựa chọn các nội dung quét  3.3. Lập lịch và giám sát thực hiện |
| Hậu điều kiện | Nếu ca sử dụng này thực hiện thành công, cấu hình, lịch trình sẽ được cập nhật; nếu không thành công sẽ hiển thị trạng thái lỗi. |

Bảng 12. Ca sử dụng Quét virus/mã độc

|  |  |
| --- | --- |
| Ca sử dụng | Quét virus/mã độc |
| Tác nhân | Quản sử dụng |
| Mô tả | Mô tả cách hoạt động khi người dùng chọn rà quét hoặc kích hoạt tự động |
| Tiền điều kiện | Đăng nhập hệ thống thành công |
| Luồng sự kiện | Ca sử dụng này bắt đầu khi người dùng chọn chức năng Rà quét mã độc; hoặc khi rà quét tự động; hoặc khi có tác động lên hệ thống từ người dùng   1. Màn hình ứng dụng hiển thị form các lựa chọn rà quét 2. Rà quét hệ thống theo mô hình đã huấn luyện 3. Tổng hợp, báo cáo kết quả rà quét 4. Cập nhật kết quả học tăng cường cho mã độc mới |
| Hậu điều kiện | Nếu ca sử dụng này thực hiện thành công, hệ thống được rà quét virus/mã độc; nếu không thành công sẽ hiển thị trạng thái lỗi. |

Bảng 13. Ca sử dụng Xử lý kết quả rà quét

|  |  |
| --- | --- |
| Ca sử dụng | Xử lý kết quả rà quét |
| Tác nhân | Quản sử dụng |
| Mô tả | Mô tả cách hoạt động khi mô-đun Rà quét mã độc đã thực hiện xong |
| Tiền điều kiện | Thực hiện rà quét thành công |
| Luồng sự kiện | Ca sử dụng này bắt đầu khi muốn xử lý kết quả rà quét từ báo cáo của hệ thống   1. Lựa chọn các hình thức xử lý 2. Xử lý tương ứng 3. Hiển thị kết quả |
| Hậu điều kiện | Nếu ca sử dụng này thực hiện thành công, kết quả rà quét mã độc được xử lý; nếu không thành công sẽ hiển thị trạng thái lỗi. |

Bảng 14. Ca sử dụng Giám sát hệ thống Windows

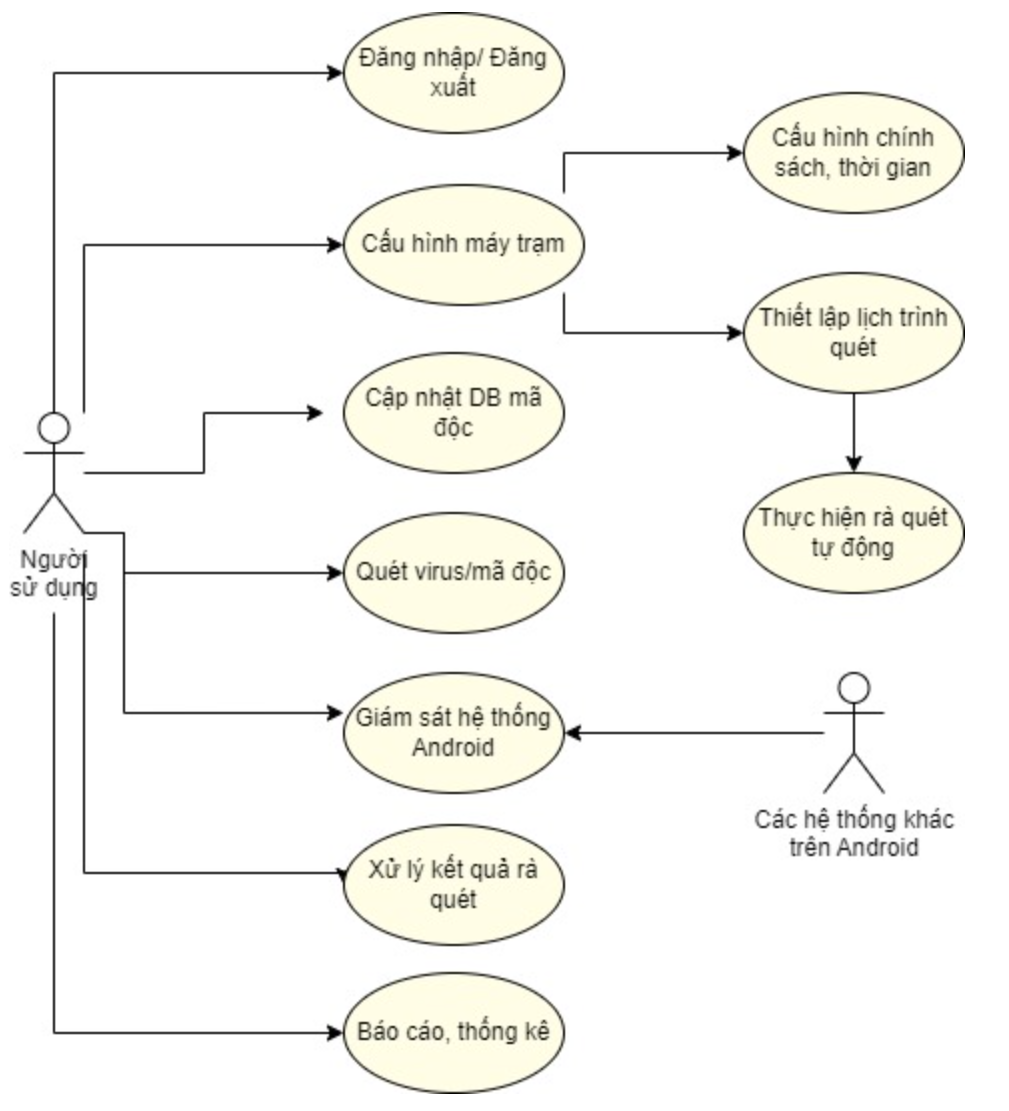
|  |  |
| --- | --- |
| Ca sử dụng | Giám sát hệ thống Windows |
| Tác nhân | Quản sử dụng, hệ thống chạy ngầm |
| Mô tả | Khi người quản trị lập lịch và thực hiện hệ thống |
| Tiền điều kiện |  |
| Luồng sự kiện | Hệ thống chạy ngầm   1. Giám sát hoạt động trên file: thêm, sửa, xóa 2. Giám sát hoạt động Download, Upload 3. Gọi mô-đun rà quét khi có dấu hiệu bất thường |
| Hậu điều kiện | Nếu ca sử dụng này thực hiện thành công, người dùng sẽ xem được bản rõ của tin nhắn; nếu không thành công sẽ hiển thị trạng thái lỗi. |

Bảng 15. Ca sử dụng Báo cáo thống kê

|  |  |
| --- | --- |
| Ca sử dụng | Báo cáo thống kê |
| Tác nhân | Quản sử dụng |
| Mô tả | Mô tả cách hoạt động khi người dùng sử dụng chức năng Báo cáo, thống kê |
| Tiền điều kiện | Đăng nhập hệ thống thành công |
| Luồng sự kiện | Ca sử dụng này bắt đầu khi người dùng muốn vào nhóm hội thảo để đọc tin   1. Màn hình ứng dụng hiển thị các chức năng Báo cáo, Thống kê 2. Thống kê theo tuần, tháng 3. Xuất dữ liệu báo cáo ra excel, pdf |
| Hậu điều kiện | Nếu ca sử dụng này thực hiện thành công, người dùng sẽ xem được bản rõ của tin nhắn; nếu không thành công sẽ hiển thị trạng thái lỗi. |

### 2.2.3. Hệ thống BCYSecAI máy trạm Android/iOS

**Biểu đồ ca sử dụng trong gói**



Hình 5: Biểu đồ ca sử dụng gói BCYSecAI Android

**Mô tả các ca sử dụng**

Các ca sử dụng cho phần mềm máy trạm Android tương tự như các ca sử dụng trong phần mềm máy trạm Windows nhưng thực hiện trên môi trường Android.