Phát hiện bất thường dựa trên Machine Learning cho

Mạng 5G

Jordan Lam, *Đại học Macquarie, Robert* Abbas, *Đại học Macquarie*

**Tóm tắt** — Bảo vệ mạng của tương lai được thiết lập để trở thành một lĩnh vực đầy thách thức do các mối đe dọa an ninh mạng ngày càng tăng và bề mặt tấn công mở rộng do Internet vạn vật (IoT) tạo ra, tăng tính không đồng nhất của mạng, tăng cường sử dụng các công nghệ ảo hóa và kiến trúc phân tán. Bài báo này đề xuất SDS (Bảo mật do phần mềm xác định) như một phương tiện để cung cấp một hệ thống phòng thủ mạng tự động, linh hoạt và có thể mở rộng. SDS sẽ khai thác những tiến bộ hiện tại trong học máy để thiết kế CNN (Convolutional Neural Network) bằng cách sử dụng NAS (Neural Architecture Search) để phát hiện lưu lượng mạng bất thường. SDS có thể được áp dụng cho hệ thống phát hiện xâm nhập để tạo ra khả năng phòng thủ chủ động và đầu cuối hơn cho mạng 5G. Để kiểm tra giả định này, các luồng mạng bình thường và bất thường từ một môi trường mô phỏng đã được thu thập và phân tích bằng CNN. Kết quả từ phương pháp này rất hứa hẹn vì mô hình đã xác định được lưu lượng truy cập lành tính với tỷ lệ chính xác 100% và lưu lượng truy cập bất thường với tỷ lệ phát hiện 96,4%. Điều này chứng minh hiệu quả của phân tích luồng mạng đối với nhiều cuộc tấn công độc hại phổ biến và cũng cung cấp một tùy chọn khả thi để phát hiện lưu lượng mạng độc hại được mã hóa.

**Thuật ngữ chỉ mục**—Bảo mật 5G, Bảo mật IoT, Hệ thống phát hiện xâm nhập tự động, Mạng nơ-ron tích chập, Trí tuệ nhân tạo, Bảo mật được xác định bằng phần mềm

F

# GIỚI THIỆU

O

VER Trong thập kỷ qua, sức mạnh tính toán tăng theo cấp số nhân đã cho phép các mô hình máy học như mạng nơ-ron hoạt động với hiệu quả cao hơn và mang lại kết quả ngày càng chính xác. Điều này đã dẫn đến nhiều ứng dụng mới của học máy được hình thành từ các lĩnh vực nghiên cứu truyền thống như nhận dạng giọng nói và thị giác máy tính. Trong bài báo này, một ứng dụng mới như vậy sẽ được nghiên cứu, ứng dụng CNN để phân tích lưu lượng mạng với mục tiêu cung cấp giải pháp bảo mật thích ứng cho bối cảnh mối đe dọa đa dạng của mạng 5G. Ứng dụng này sẽ được thực hiện bằng cách thu thập dữ liệu luồng mạng lành tính và bất thường từ một môi trường mô phỏng và sử dụng các luồng này làm dữ liệu đầu vào cho CNN. Luồng mạng bất thường có thể được định nghĩa là hành vi bất thường hoặc không phù hợp với các mẫu lưu lượng thông thường cho một người dùng, doanh nghiệp hoặc tổ chức cụ thể. Bài báo này sẽ giả định các luồng mạng bất thường là độc hại cho mục đích thử nghiệm, tuy nhiên trong kịch bản thực tế, lưu lượng truy cập bất thường có thể không độc hại nhưng vẫn đáng để phân tích do các tác động kinh doanh tiềm ẩn trong tương lai. Bố cục của bài báo này như sau, trước tiên bối cảnh bảo mật 5G sẽ được điều tra, điều này bao gồm việc kiểm tra môi trường hiện tại liên quan đến các kiến trúc bảo mật mà 5G có thể kế thừa từ LTE (Long Term Evolution) và sự phát triển 3GPP (Dự án Đối tác Thế hệ thứ 3) hiện tại trong bảo mật 5G. Các mối quan tâm về bảo mật trong tương lai đối với mạng 5G sau đó sẽ được xem xét, bao gồm cách số lượng IoT tăng theo cấp số nhân

arXiv:2003.03474v1 [cs. CR] 7 Tháng Ba 2020

|  |
| --- |
| * *Jordan Lam - Đại học Macquarie.*   *Thư điện tử: jordan.lam@students.mq.edu.au*   * *Robert Abbas - Đại học Macquarie. E-mail: robert.abbas@mq.edu.au Sửa đổi lần cuối ngày 6 tháng 3 năm 2020.* |

Devices đang thay đổi bối cảnh bảo mật, quản lý nhiều công nghệ, gia tăng các mối đe dọa ảo hóa, quản lý kiến trúc phân tán và các lát cắt mạng. Một giải pháp sau đó sẽ được đề xuất thông qua việc triển khai hệ thống SDS sử dụng máy học cho mạng 5G. Hệ thống được thiết kế để truy cập lưu lượng truy cập từ cả liên kết backhaul vào mạng lõi và từ liên kết kết nối ra khỏi mạng lõi để phát hiện các mối đe dọa từ đầu đến cuối và chủ động cập nhật các chính sách bảo mật phù hợp.

Thứ hai, các ứng dụng của máy học sẽ được điều tra dựa trên những tiến bộ hiện tại trong phát hiện bất thường. Những tiến bộ hiện tại trong lĩnh vực nghiên cứu này sẽ được thảo luận và các ứng dụng của kiến trúc mạng nơ-ron sẽ được so sánh để chứng minh lợi ích của CNN. Thảo luận thêm sẽ bao gồm đánh giá thiết kế của một

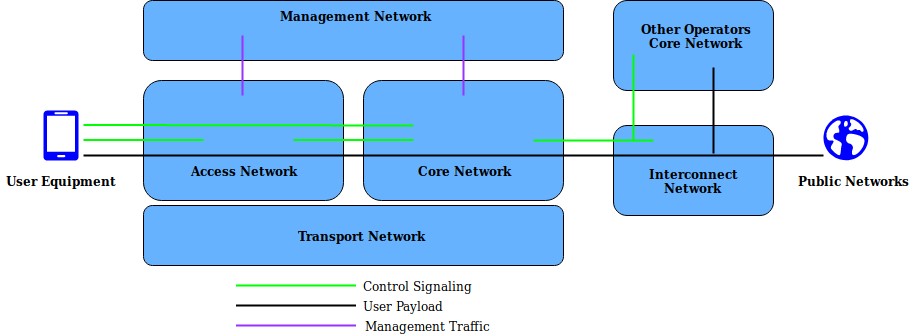
CNN với NAS và ứng dụng autoML (Automated Machine Learning) để phân tích tập dữ liệu được cung cấp để tạo ra bố cục mô hình CNN cụ thể. Cuối cùng, bố cục của tập dữ liệu thu thập được sẽ được kiểm tra và dữ liệu sẽ được xử lý trước thành hình ảnh có thể chấp nhận được đối với mô hình. Sau đó, kết quả sẽ được thu thập từ việc áp dụng mô hình (Phụ lục A) vào tập dữ liệu và những kết quả này sẽ được đánh giá về khả năng tồn tại và ứng dụng của chúng cho các trường hợp sử dụng bảo mật 5G và IoT. Mục tiêu của dự án này là cung cấp một số thông tin chi tiết về hiệu quả của máy học trong các ứng dụng phát hiện xâm nhập và cho thấy cách giải pháp này có thể được xác định hoàn toàn thông qua phần mềm cho phép tính linh hoạt, khả năng mở rộng và tính di động cao hơn trong mạng 5G.

# MÔI TRƯỜNG AN NINH MẠNG 5G

Nhu cầu môi trường và mô hình mối đe dọa đang thay đổi khi các tác nhân độc hại trở nên tiên tiến hơn và mạng trở nên phức tạp và không đồng nhất hơn. Các thiết bị IoT cũng được dự đoán sẽ tăng từ con số 27 tỷ thiết bị hiện tại lên 75 tỷ vào năm 2025, đây là một nguyên nhân gây lo ngại hơn nữa trong việc đảm bảo các thiết bị này không thể được sử dụng trong các cuộc tấn công vào mạng di động [1]. Trong lịch sử, các mạng di động đã được xây dựng với bảo mật ngay từ đầu, sử dụng nhiều hệ thống phòng thủ được triển khai trong tất cả các lớp của mạng. Đây là một dấu hiệu tốt cho việc thiết kế mạng 5G trong tương lai, tuy nhiên các mạng sẽ ngày càng trở nên không đồng nhất khi lưu lượng mạng cũ, LTE và 5G phải được hỗ trợ đồng thời và ngày càng phụ thuộc vào các công nghệ dựa trên phần mềm và ảo hóa. Sự khác biệt lớn về mạng 5G so với mạng LTE sẽ mang lại rủi ro bảo mật lớn hơn rất nhiều và là nguyên nhân gây lo ngại cho các nhà mạng trong việc duy trì dịch vụ an toàn, ổn định và đáng tin cậy.

## 2.0.1 Bối cảnh mối đe dọa hiện tại

Mạng viễn thông có thể được chia nhỏ để bao gồm bốn yếu tố logic chính là mạng truy cập vô tuyến, mạng lõi, mạng truyền tải và mạng kết nối liên quan [2]. Mỗi phần tử mạng này bao gồm ba mặt phẳng, mỗi mặt phẳng chịu trách nhiệm mang các loại lưu lượng khác nhau. Tổng quan đồ họa về cách các phần tử này tương tác được thể hiện trong Hình 1.



## Hình 1: Bức tranh lớn: Mạng viễn thông

Chúng được định nghĩa là mặt phẳng điều khiển mang lưu lượng tín hiệu, mặt phẳng người dùng mang tải trọng (lưu lượng thực tế) và mặt phẳng quản lý mang lưu lượng hành chính [2]. Từ góc độ an ninh, cả ba máy bay này đều phải đối mặt với các mối đe dọa độc đáo và cũng có các mối đe dọa thống nhất liên quan đến an ninh, cả ba máy bay đều có thể tiếp xúc với các mối đe dọa riêng và cũng có những mối đe dọa thống nhất có thể ảnh hưởng đến cả ba máy bay cùng một lúc. An ninh mạng được triển khai vào mạng viễn thông theo bốn giai đoạn sau [2]:

* Tiêu chuẩn hóa: Các nhà khai thác, nhà cung cấp và các bên liên quan đặt ra các tiêu chuẩn về cách các mạng trên toàn cầu sẽ hoạt động. Các tiêu chuẩn cũng được xác định liên quan đến việc bảo vệ mạng chống lại bất kỳ loại tác nhân độc hại nào.
* Thiết kế mạng: Các nhà cung cấp mạng thiết kế, phát triển và thực hiện các tiêu chuẩn đã thỏa thuận vào các yếu tố và hệ thống mạng chức năng, đảm bảo sản phẩm cuối cùng vừa có chức năng vừa an toàn.
* Cấu hình mạng: Trong giai đoạn triển khai mạng, các mạng được cấu hình để đạt được mức độ bảo mật đã đặt, điều này rất quan trọng trong việc thiết lập các thông số bảo mật và tăng cường hơn nữa cả bảo mật và khả năng phục hồi mạng.
* Triển khai và vận hành mạng: Đây là giai đoạn hoạt động của mạng, việc đạt được các mức độ bảo mật xác định phụ thuộc vào việc triển khai và vận hành mạng phù hợp.

Về 5G, công nghệ này có thể được định nghĩa là không chỉ cung cấp một nâng cấp gia tăng khác về tốc độ và độ trễ mà còn là một công cụ hỗ trợ cho một tập hợp các dịch vụ và trường hợp sử dụng mới, với điểm bán hàng độc đáo nhất của 5G là hiện thực hóa một IoT thực sự và môi trường liên mạng sẽ tác động đến tất cả các bộ phận của xã hội [3]. Tuy nhiên, yếu tố chính sẽ quyết định liệu 5G có thể phát huy hết tiềm năng của nó hay không là câu hỏi 5G có thể cung cấp các dịch vụ mới này an toàn và ổn định như thế nào? Cảm biến giao thông và dịch vụ Vehicleto-infrastructure là một trong những trường hợp sử dụng của thiết bị IoT [3] và điều quan trọng là ngay cả những thiết bị cơ bản này cũng phải được bảo vệ vì chúng rất dễ bị tấn công DDoS (Distributed Denial of Service). Một ví dụ rõ ràng về bảo mật IoT bị xâm phạm là cuộc tấn công Mirai đã kiểm soát được 600.000 thiết bị IoT dễ bị tấn công trong một mạng botnet, áp dụng các cuộc tấn công DDoS lớn vào các dịch vụ cao cấp như OVH và Dyn [4].

May mắn thay, các mạng viễn thông trước đây đã đảm bảo rằng bảo mật là mối quan tâm hàng đầu về kiến trúc, đây là tin tốt cho 5G. Ví dụ, liên quan đến bảo mật LTE, 3GPP Release 8 đã bổ sung một loạt các cơ chế bảo mật và xác thực tiên tiến thông qua các nút như máy chủ khả năng dịch vụ, trong khi Release 11 cung cấp các khả năng bổ sung cho mạng lõi để truy cập an toàn [3]. Những mối quan tâm về tin cậy và xác thực trong mạng cũng được chuyển sang mạng 5G vì 3GPP Release 15 bổ sung hai tùy chọn xác thực bắt buộc cho 5G và xây dựng mô hình tin cậy thông qua phân tách khóa [5]. Bằng cách này, bảo mật mạng LTE cung cấp nền tảng để kích hoạt các quy trình bảo mật 5G trong tương lai. Về bảo mật không dây lớp vật lý, ngành viễn thông được đánh giá cao so với các công nghệ không dây khác, ngay cả việc sử dụng phổ tần được cấp phép của điện thoại di động cũng bổ sung thêm các lớp bảo mật để hỗ trợ ngăn chặn việc nghe lén lưu lượng dữ liệu, thoại và video [3].

Bất chấp mức độ thiết kế bảo mật chuyên sâu này, vẫn có những lĩnh vực cần được giải quyết trong mô hình bảo mật 5G. Điều này bao gồm các bề mặt tấn công mới được đưa ra bởi việc sử dụng nhiều hơn điện toán đám mây và biên, cũng như sự hội tụ của 5G với các mạng truyền thống tạo ra các vectơ tấn công mới. Cách tiếp cận được thực hiện trong bài báo này bằng cách áp dụng phát hiện bất thường là cố gắng phát hiện tất cả lưu lượng truy cập không mong muốn trong mạng, điều này có nghĩa là lưu lượng độc hại ảnh hưởng đến cả mạng và người dùng cuối tiềm năng có thể được phát hiện sớm hơn để giảm thiểu tác động phụ. Các cuộc tấn công độc hại có thể được khái quát hóa thành hai loại tấn công zero-day và tấn công ngày đầu tiên [3]. Các cuộc tấn công zero-day là các mối đe dọa không có dấu vân tay hoặc chữ ký hiện có, các cuộc tấn công ngày là các mối đe dọa có chữ ký hoặc dấu vân tay và có thể được giảm thiểu một cách hiệu quả. Mục tiêu cuối cùng của phát hiện bất thường là cung cấp phản ứng nhanh hơn và chủ động hơn đối với các mối đe dọa chưa từng thấy trước đây (zero day) và giảm thiểu thích hợp.

## 2.0.2 Mối quan tâm về bảo mật trong tương lai

Ngoài các dịch vụ và khả năng mới mà mạng 5G sẽ cung cấp cho người dùng, 5G sẽ mang lại một loạt các mối quan tâm và cân nhắc bảo mật mới. Những thách thức bảo mật này đối với 5G có thể được chia thành bốn loại chính, quản lý IoT/V2X/M2M (Vehicle to X, Machine to Machine), kiến trúc phân tán, ảo hóa và nhiều công nghệ [6]. Bản thân các thiết bị IoT là những thiết bị rẻ tiền được thiết kế cho một mục đích sử dụng cụ thể và bảo mật thường là một suy nghĩ sau, hầu hết các thiết bị này thậm chí không có ngăn xếp IP riêng, chứ đừng nói đến hệ thống bảo mật sẵn có. Giao tiếp với người dùng cuối từ các thiết bị IoT cũng là một nguyên nhân khác gây lo ngại do giao tiếp ngang hàng không có bộ điều khiển giữa các bên, đây là một bề mặt đe dọa lớn.

Kiến trúc phân tán liên quan đến sự tách biệt giữa mặt phẳng điều khiển và người dùng. Ví dụ, theo truyền thống, mạng lõi gói bao gồm tất cả các thành phần phần cứng nằm trong trung tâm dữ liệu và các thành phần này có các thông số và giao diện đã biết. Tuy nhiên, với 5G, các thành phần cốt lõi có thể được triển khai trên biên và do bản chất của 5G là kiến trúc gốc đám mây, các thành phần này hiện cũng có trên máy chủ đám mây. Điều này tạo ra các bề mặt mối đe dọa mới do khó khăn hơn khi phải quản lý lõi gói phân tán. Việc sử dụng nhiều ảo hóa có nghĩa là giao tiếp giữa các bên dựa trên web và được thực hiện thông qua việc sử dụng API (Giao diện lập trình ứng dụng), các API này không có giao diện được thiết lập và các giao thức chung được xác định so với mạng LTE, do đó điều này tạo ra một bề mặt đe dọa bổ sung. 5G cũng trở thành một mạng khác để quản lý trong hỗn hợp mạng không đồng nhất hiện đang hoạt động. Các quy trình bảo mật cũng cần giải quyết vấn đề bảo mật các yếu tố kết nối giữa mạng 3G, LTE và 5G.

Một cái nhìn cấp cao về bối cảnh mối đe dọa 5G được hiển thị bên dưới trong Hình 2, làm nổi bật những thách thức bảo mật và các phân đoạn mạng có nguy cơ. Các mối đe dọa có thể được chia thành các loại dựa trên phần nào của mạng mà chúng đang tác động [3]:

* **Mối đe dọa thiết bị người dùng**: Botnet di động có thể khởi động các cuộc tấn công DDoS trên nhiều cấp độ mạng ảnh hưởng đến cơ sở hạ tầng 5G, máy chủ web và thiết bị người dùng. Mục tiêu là đưa các dịch vụ ngoại tuyến.
* **Mối đe dọa mạng truy cập vô tuyến đám mây**: Mối đe dọa trạm gốc giả mạo để tạo điều kiện thuận lợi cho một cuộc tấn công MITM (Man in the Middle), cuộc tấn công này có thể xâm phạm thông tin người dùng, giả mạo thông tin, theo dõi người dùng hoặc gây ra các cuộc tấn công DoS. Khai thác mạng liên kết 5G/LTE và khởi động cuộc tấn công hạ cấp.
* **Các mối đe dọa mạng cốt lõi**: Dễ bị tấn công dựa trên IP (Giao thức Internet) từ internet, botnet có thể khởi chạy các cuộc tấn công mặt phẳng người dùng và mặt phẳng điều khiển để làm suy giảm hoặc đưa cơ sở hạ tầng cốt lõi quan trọng ngoại tuyến.
* **Các mối đe dọa cắt xén mạng**: các mối đe dọa dựa trên ảo hóa do phụ thuộc vào bảo mật của hypervisor. Cần đảm bảo cách ly các chức năng và tài nguyên lát cắt khỏi các lát cắt khác, cũng như xác thực từ thiết bị người dùng hoạt động trên một lát cắt.
* **Các mối đe dọa SDN (Mạng do phần mềm xác định):** Sự tách biệt giữa kiểm soát và mặt phẳng người dùng cho phép người dùng độc hại tấn công liên kết giữa mặt phẳng điều khiển và người dùng, một cuộc tấn công DoS (Từ chối dịch vụ) có thể được thực hiện hoặc có thể giành được quyền kiểm soát qua các phần tử mạng.

## Hình 2: Tổng quan về các mối đe dọa mạng 5G từ đầu đến cuối Các yếu tố mạng cốt lõi: Chức năng mạng (NF, NFn), Chức năng tiếp xúc mạng (NEF), Chức năng kho lưu trữ mạng (NRF)

Quản lý lưu lượng được mã hóa đầu cuối là một cân nhắc khác trong bối cảnh mối đe dọa 5G đang phát triển, vì khả năng hiển thị lưu lượng trở nên hạn chế bên trong mạng 5G do mã hóa và các dịch vụ web mã hóa thêm lưu lượng truy cập của chúng. Lưu lượng truy cập được mã hóa đã tăng hơn 90% qua từng năm, với số lượng dự kiến là 80% tổng lưu lượng truy cập web sẽ được mã hóa vào năm 2019 [7]. Việc mã hóa lưu lượng mạng cho phép mức độ riêng tư và bảo mật cao hơn nhiều, tuy nhiên mã hóa tương tự này cản trở khả năng hiển thị của các nhà khai thác mạng về lưu lượng truy cập và do đó khả năng xác định xem lưu lượng truy cập này là độc hại hay lành tính. Các ứng dụng di động, đám mây và web phụ thuộc vào các cơ chế mã hóa được thực hiện tốt, sử dụng khóa và chứng chỉ để xác minh sự tin cậy. Ưu điểm của mã hóa cũng là nhược điểm của nó vì người dùng độc hại có thể sử dụng mã hóa để tránh bị phát hiện và bảo mật các hoạt động độc hại của họ.

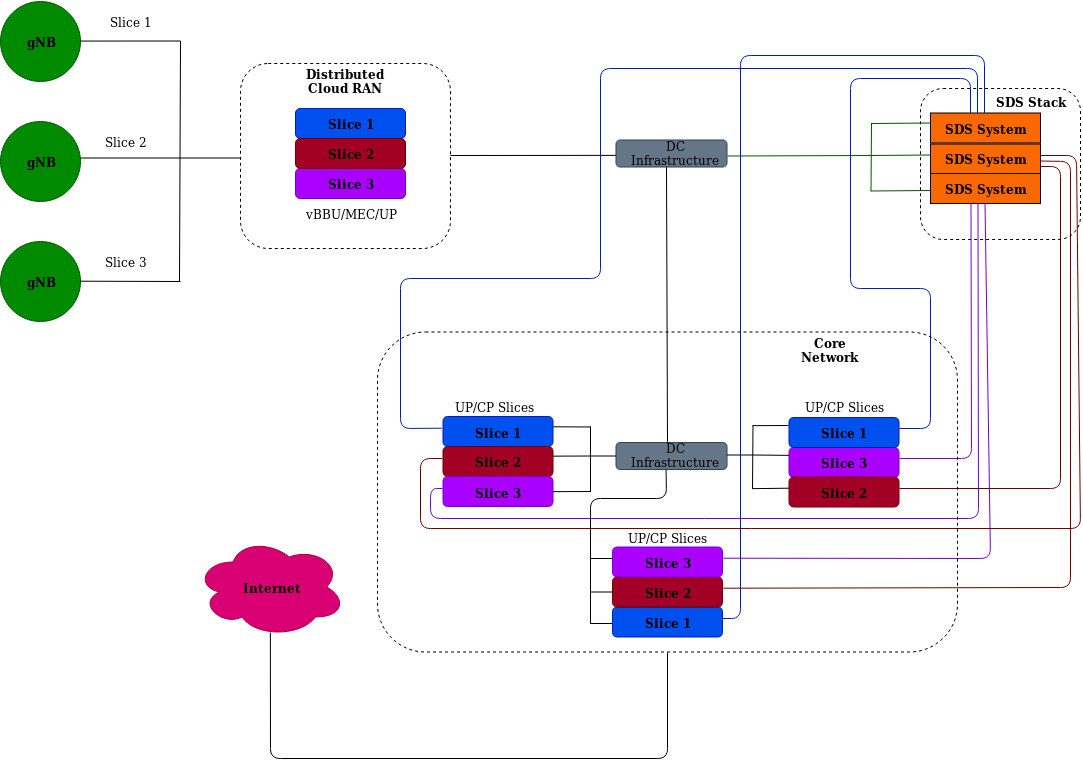
Vấn đề sau đó về mặt bảo mật là phần lớn các tổ chức không có các công cụ hoặc giải pháp để quản lý lưu lượng được mã hóa độc hại tiềm ẩn và các hệ thống không có khả năng phát hiện hiệu quả lưu lượng được mã hóa độc hại mà không ảnh hưởng đến hiệu suất mạng [7]. Các kỹ thuật truyền thống như kiểm tra gói sâu trở nên khó thực hiện hơn vì lưu lượng truy cập sẽ cần được giải mã tại một số điểm trong mạng, phân tích và sau đó mã hóa lại, đây sẽ là một quá trình tốn nhiều tài nguyên và thời gian. Thay vào đó, cả lưu lượng được mã hóa và không được mã hóa đều có thể được phân tích bằng số liệu thống kê liên quan đến luồng. Luồng mạng có thể được định nghĩa là một luồng lưu lượng truy cập với một tập hợp các mã định danh chung [8]. Phân tích số liệu thống kê luồng bằng máy học sẽ cho phép phát hiện phần mềm độc hại trong lưu lượng được mã hóa và không được mã hóa mà không cần giải mã và mã hóa lại mọi luồng.

## 2.0.3 Kiến trúc triển khai 5G SDS

Mạng 5G và các yếu tố chính của chúng như CRAN (Cloud Radio Access Network) và mạng lõi được ảo hóa, do đó được xác định hoàn toàn thông qua phần mềm. Một cách tiếp cận tương tự có thể được thực hiện để triển khai một hệ thống bảo mật tự động thông qua SDS. Hình 3. dưới đây cho thấy khả năng triển khai hệ thống SDS trong mạng 5G. Một bản sao của một lượng lưu lượng truy cập đủ từ cả liên kết backhaul và từ liên kết mạng lõi có thể được phân tích để cung cấp khả năng phát hiện bất thường mạng đầu cuối. Một bản sao dữ liệu được lấy để phân tích và xây dựng hồ sơ xác định lưu lượng truy cập lành tính và bất thường cho mô hình, cũng như bằng cách sao chép dữ liệu sẽ không có tác động đến hiệu suất mạng trong khi mô hình phân tích dữ liệu. Dữ liệu sau đó được xử lý trước để ở dạng phù hợp với mô hình máy học và phân tích các điểm bất thường, bất kỳ điểm bất thường nào được xác định sau đó được lưu trữ trong cơ sở dữ liệu của người quản lý chính sách với các tính năng lưu lượng tương ứng. Các chính sách này sau đó được gửi đến trình quản lý VNF (Chức năng mạng ảo), sau đó có thể cập nhật mô-đun IDS (Hệ thống phát hiện xâm nhập) thích hợp trong mạng lõi. Dựa trên thời gian cần thiết để mô hình xử lý dữ liệu, lịch trình đã đặt có thể được xác định để chạy mô hình để đảm bảo các chính sách trong Mô-đun IDS được cập nhật và để tăng cường hơn nữa việc học mô hình máy học. Lợi ích chính là khả năng tự động hóa việc phát hiện, cập nhật cơ sở dữ liệu và hành động thích hợp của bất kỳ luồng độc hại nào.

Hình 4. bên dưới hiển thị cách hệ thống SDS này cũng có thể được triển khai trên các lát mạng cụ thể để giám sát luồng lưu lượng và xây dựng hồ sơ lưu lượng lành tính và bất thường dựa trên các thông số kỹ thuật cần thiết cho lát cắt đó. Bố cục của sơ đồ tập trung vào sự tách biệt của CP (Mặt phẳng điều khiển) và UP (Mặt phẳng người dùng), với UP nằm trong lõi mạng hoặc trong C-RAN, UP có thể nằm trong C-RAN nếu cần ở gần biên hơn vì lý do độ trễ, CP nằm trong lõi mạng để tập trung kiểm soát mạng. Các phần tử C-RAN được phân phối bao gồm các ứng dụng của vBBU (Đơn vị băng tần cơ sở ảo hóa), MEC (Điện toán biên di động) và UP. Các đường màu cho biết các kết nối logic giữa hệ thống SDS và các thành phần mạng khác nhau, dữ liệu lát cắt được truy cập cả từ DC (Trung tâm dữ liệu) đầu tiên để giám sát lưu lượng backhaul từ C-RAN và cả từ việc phân phối các lát cắt mạng trong mạng lõi. Lợi ích chính của hệ thống SDS là nó có thể được triển khai ở các phần khác nhau của mạng một cách hiệu quả và với chi phí thấp. Bằng cách phát triển các công cụ bảo mật 5G được xác định bằng phần mềm theo cách tiếp cận dựa trên lát cắt, các mẫu bất thường có thể được xác định trên mỗi lát cắt. Một ví dụ về điều này là đào tạo mô hình để xác định các cuộc tấn công xâm nhập cho các thiết bị IoT nhỏ hoạt động trên một lát cắt mạng có khả năng được sử dụng trong botnet cho các cuộc tấn công DDoS. Tùy thuộc vào yêu cầu của người vận hành, mỗi hệ thống SDS có thể tùy chỉnh theo nhu cầu của họ.

## Hình 3: Mạng 5G với hệ thống SDS

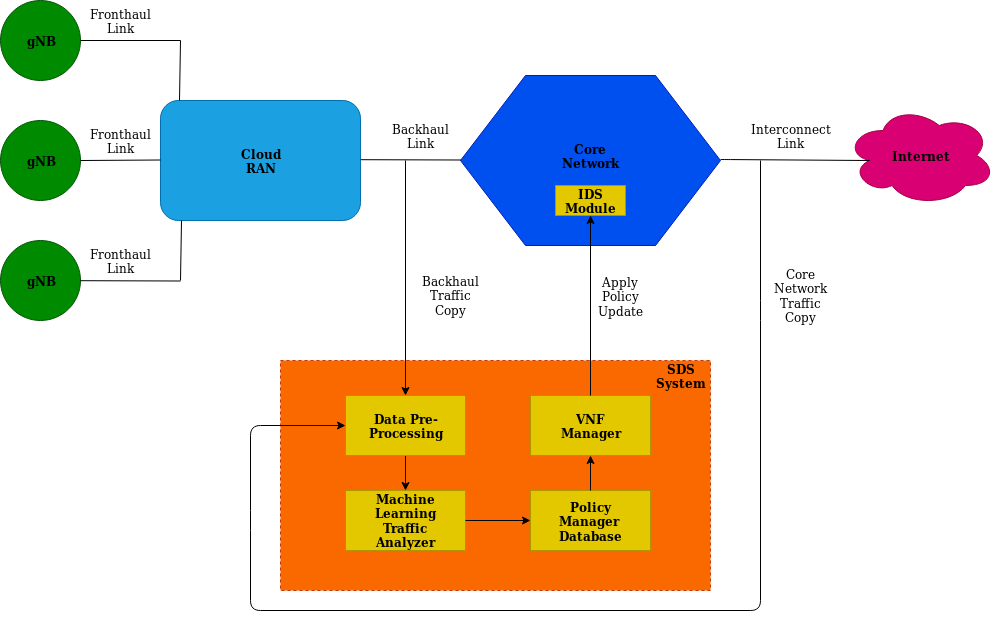


*Hình 4: Ứng dụng SDS cho các lát cắt mạng*

# PHÁT HIỆN BẤT THƯỜNG MẠNG NƠ-RON TÍCH CHẬP

Học sâu là một lĩnh vực của học máy liên quan đến việc thiết kế các mạng nơ-ron nhiều lớp, về cơ bản là các cấu trúc giống như tế bào thần kinh dựa trên toán học, sử dụng nhiều biến để giải một phương trình phức tạp. Để phát triển một mạng nơ-ron để phân loại văn bản hoặc hình ảnh đòi hỏi một lượng kỹ thuật kiến trúc đáng kể để có được một mạng phù hợp nhất với tập dữ liệu được cung cấp và có đủ mức độ chính xác [9] . Do đó, phần này sẽ khám phá những tiến bộ hiện tại trong lĩnh vực phát hiện bất thường dựa trên học máy và sau đó điều tra cách các kỹ thuật như autoML và NAS có thể tối ưu hóa thiết kế mô hình để cho phép thiết kế kiến trúc CNN vừa có thể mở rộng vừa được tối ưu hóa cao cho loại dữ liệu mà chúng đang đào tạo.

## 3.0.1 Những tiến bộ hiện tại

Phát hiện xâm nhập mạng liên quan đến vấn đề giám sát và phân biệt các luồng mạng bình thường với các luồng bất thường có thể ảnh hưởng đến tính bảo mật của hệ thống. Cả chính phủ và tổ chức đều đầu tư rất nhiều để tìm ra giải pháp đáng tin cậy để bảo vệ tài sản thông tin và tài nguyên của họ khỏi truy cập độc hại, điều này đã đưa các hệ thống phát hiện xâm nhập lên hàng đầu trong bối cảnh an ninh mạng [10]. Theo đề xuất của Denning [11], ý tưởng phát triển các hệ thống phát hiện xâm nhập sử dụng các kỹ thuật học máy là để xác định các mô hình sử dụng bất thường và lưu lượng truy cập bất thường có thể báo hiệu một nỗ lực xâm nhập mạng. Khái niệm này dẫn đến việc tạo ra một loại IDS mới dựa trên các thuật toán học thay vì cập nhật thủ công chữ ký từ các cuộc xâm nhập đã xác định trước đó. Trong ba thập kỷ qua, các kỹ thuật máy học khác nhau đã được áp dụng trong một cách tiếp cận thông thường để phát triển các mô hình phát hiện bất thường mạng. Các phương pháp này sử dụng các thuật toán học tập có giám sát, không giám sát và bán giám sát để đề xuất giải pháp phát hiện bất thường [10].

Do đó, phát hiện bất thường không phải là một lĩnh vực nghiên cứu mới trong các ứng dụng học máy và nghiên cứu hiện tại đã khám phá nhiều ứng dụng dựa trên học máy. Tuy nhiên, một số vấn đề phổ biến phát sinh như mức độ chính xác thấp do thiết kế mô hình dưới mức tối ưu, mức độ chính xác cao không thực tế do thiếu khái quát hóa mô hình và quá khớp, cũng như việc sử dụng các tập dữ liệu lỗi thời và đơn giản. Như thể hiện trong [12], độ chính xác trên 99% đạt được bằng cách sử dụng mạng nơ-ron nhiều lớp, tuy nhiên tập dữ liệu được sử dụng là bộ dữ liệu KDD99, một tập dữ liệu đã 20 năm tuổi và không đại diện cho môi trường mạng động hiện tại.

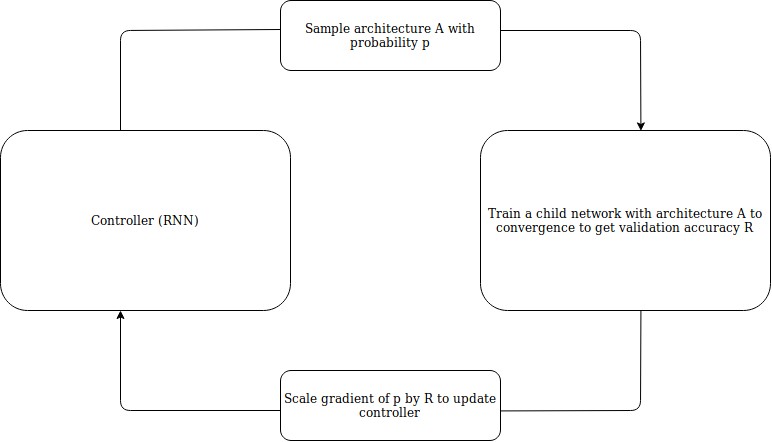
Bản thân phát hiện bất thường có thể dễ dàng được mô hình hóa như một vấn đề phân loại trong học có giám sát [10]. Học có giám sát có nghĩa là dữ liệu được gắn nhãn được sử dụng để đào tạo mô hình phát hiện bất thường. Mục tiêu của loại đào tạo này là phân loại dữ liệu thử nghiệm là dị thường hoặc bình thường trên cơ sở một tập hợp các đặc điểm cụ thể. Trong bài báo này, vấn đề phát hiện bất thường sẽ được tiếp cận từ góc độ học tập có giám sát và sử dụng kiến trúc CNN được thiết kế bằng cách sử dụng NAS để cố gắng tối ưu hóa mức độ chính xác cao nhất có thể.

Thiết kế mô hình hiệu quả đòi hỏi một mức độ đáng kể của kỹ thuật kiến trúc [9], chẳng hạn như [13] chứng minh rằng thiết kế của CNN cơ bản trong đó các lớp bổ sung chỉ được thêm vào cho mục đích thử nghiệm không cải thiện độ chính xác, cho kết quả không tối ưu ở tỷ lệ phát hiện dưới 80%. [14] chứng minh hiệu quả của việc lấy mẫu lên và xuống trên dữ liệu để cân bằng khối lượng dữ liệu bất thường và lành tính, đạt được tỷ lệ phát hiện là 99,99% bằng cách sử dụng rừng ngẫu nhiên và 99,30% bằng cách sử dụng mạng nơ-ron sâu ba lớp, những kết quả rất cao này không có khả năng đại diện cho mức độ phát hiện trong thế giới thực và tạo ấn tượng về một mô hình quá phù hợp và thiếu khái quát hóa. Phân loại hiệu quả cả lưu lượng truy cập lành tính và bất thường cũng là một vấn đề, trong hầu hết các trường hợp, các mô hình có thể xác định lưu lượng truy cập lành tính được dán nhãn với độ chính xác rất cao (99-100%), tuy nhiên việc xác định lưu lượng truy cập bất thường có thể khó khăn hơn, như được thể hiện trong [15] trong đó thuật toán rừng ngẫu nhiên được áp dụng cho bộ dữ liệu UNSW-NB15, lưu lượng truy cập lành tính được phân loại với độ chính xác 99%, Tuy nhiên, lưu lượng truy cập bất thường được phân loại là 82%, điều này có nghĩa là 18% lưu lượng truy cập dị thường về cơ bản không được phát hiện.

Cách tiếp cận của bài báo này cố gắng khắc phục và giải quyết một số vấn đề phổ biến này. Điều này được thực hiện theo hai cách chính bằng cách chọn tập dữ liệu IDS cập nhật nhất, CICIDS2018 mô phỏng môi trường trong thế giới thực và được giải thích chi tiết thêm. Và thứ hai bằng cách sử dụng mô hình CNN dựa trên NAS, đã đạt được một số mức độ chính xác cao nhất trong tập dữ liệu ImageNet và sử dụng bộ điều khiển để tự động tối ưu hóa các thông số cho mô hình. Bằng cách sử dụng cách tiếp cận này, mô hình tối ưu nhất có thể được tạo ra cho một tập dữ liệu cụ thể.

## 3.0.2 Triển khai AutoML & NAS

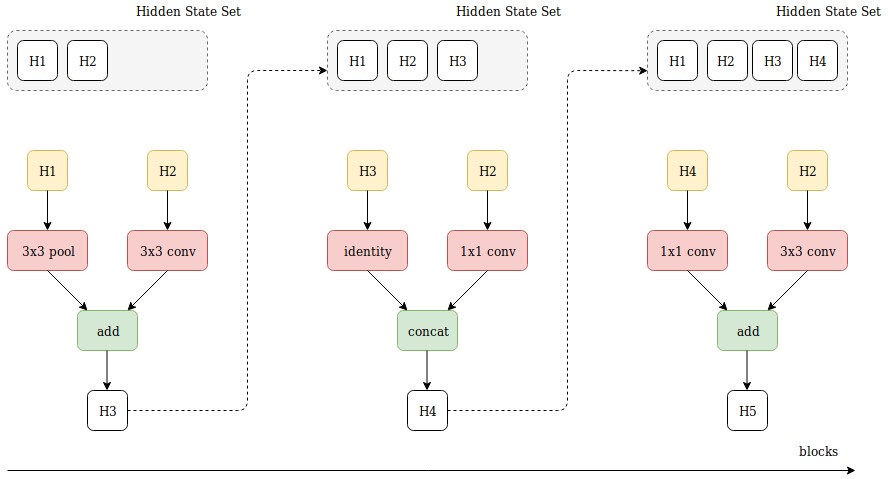
Tìm kiếm kiến trúc thần kinh mang lại sự tự động hóa cho thiết kế các mô hình mạng nơ-ron, điều này cho phép các thiết kế mô hình được tối ưu hóa nhất được tính toán mà không cần quá trình thiết kế, kiểm tra và điều chỉnh mô hình vật lý tẻ nhạt. Kỹ thuật tiên tiến này trong thiết kế mạng nơ-ron đã dẫn đến sự gia tăng của một số nền tảng máy học tự động. Trong bài báo này, các nền tảng autoML Vision và Vision Edge của Google sẽ được sử dụng để thiết kế, đào tạo, xác thực và thử nghiệm mô hình. Kiến trúc cơ bản cho phép các nền tảng này là NASNet (Mạng tìm kiếm kiến trúc thần kinh) và MNasNet (Mạng tìm kiếm kiến trúc thần kinh di động).

Tìm kiếm kiến trúc thần kinh có thể được định nghĩa là một phương pháp dựa trên gradient để tìm kiến trúc được tối ưu hóa. Cấu trúc và kết nối của mạng nơ-ron có thể được chỉ định bằng một chuỗi có độ dài thay đổi. Do đó, có thể sử dụng RNN (Mạng nơ-ron tuần hoàn) như trong Hình 5. để tạo chuỗi này [16]. Mạng được chỉ định bởi chuỗi được gọi là mạng con và việc đào tạo tập dữ liệu thực với mạng con sẽ dẫn đến sự gia tăng độ chính xác dần dần trên tập dữ liệu thử nghiệm. Độ chính xác này có thể được sử dụng làm tín hiệu phần thưởng để tính toán gradient chính sách để cập nhật bộ điều khiển. Do đó, trong lần lặp tiếp theo, bộ điều khiển sẽ cung cấp xác suất cao hơn cho các kiến trúc nhận được độ chính xác cao hơn [16]. Nói một cách đơn giản, điều này có nghĩa là bộ điều khiển có thể học cách cải thiện tìm kiếm của nó theo thời gian và tối ưu hóa vị trí của các lớp và khối của mạng nơ-ron [17].

## Hình 5: Bộ điều khiển RNN

Về mặt triển khai, tìm kiếm kiến trúc thần kinh sử dụng bộ điều khiển để tạo ra một tập hợp các siêu tham số kiến trúc của mạng. Trong trường hợp của CNN, nó có thể dự đoán chiều cao bộ lọc, chiều rộng bộ lọc, chiều cao sải chân, chiều rộng sải chân và số bộ lọc trên mỗi lớp [16]. Quá trình này sau đó được lặp lại cho đến khi số lớp vượt quá một giá trị nhất định.

Vấn đề này với NAS là áp dụng nó cho một tập dữ liệu rất lớn cực kỳ tốn nhiều tính toán. Do đó, kỹ thuật này được áp dụng cho một mẫu của tập dữ liệu [9]. Không gian tìm kiếm NAS được xác định sao cho độ phức tạp của kiến trúc không phụ thuộc vào độ sâu của mạng và kích thước của hình ảnh đầu vào. Nó đạt được điều này bằng cách chia nhỏ tất cả các CNN trong không gian tìm kiếm thành các ô có cấu trúc giống hệt nhau nhưng trọng lượng khác nhau như trong Hình 6 [9]. Do đó, việc tìm kiếm kiến trúc tối ưu nhất có thể được giảm xuống để tìm kiếm kiến trúc tế bào tốt nhất. Bằng cách tìm kiếm từng kiến trúc ô cụ thể, tốc độ được tăng lên đáng kể và ô có nhiều khả năng khái quát hóa tốt hơn. Dựa trên phương pháp đào tạo ô riêng lẻ này, mạng có thể được tối ưu hóa về tốc độ hoặc độ chính xác tùy thuộc vào kích thước không gian tìm kiếm. Điều này cho phép mạng nơ-ron đạt được mức độ chính xác rất cao trên bộ dữ liệu xác thực ImageNet ở độ chính xác 82,7% top 1 [18]. ImageNet là cơ sở dữ liệu lớn nhất cho các hình ảnh được dán nhãn chứa hơn 14 triệu hình ảnh và được sử dụng rộng rãi trong việc cung cấp điểm chuẩn để xác định hiệu suất của các mô hình CNN khác nhau [19].



## Hình 6: Tạo khối không gian tìm kiếm NAS

MnasNet mở rộng khái niệm không gian tìm kiếm NAS bằng cách triển khai không gian tìm kiếm phân cấp phân tích [20]. Không gian tìm kiếm phân cấp được phân tích hóa khuyến khích sự đa dạng lớp bổ sung trong toàn bộ mạng và cân bằng kích thước của tổng không gian tìm kiếm. Cách tiếp cận này mang lại sự linh hoạt hơn cho NAS vì các mô hình có thể được thiết kế để cân bằng tốc độ và độ chính xác. Cho đến nay, cách tiếp cận này có lợi thế lớn nhất về tốc độ. Trên tập dữ liệu ImageNet, kiến trúc MNasNet đạt được độ chính xác top 1 75,2%, so với kiến trúc mạng nơ-ron di động truyền thống, nhanh hơn 1,8 lần so với MobileNetV2 [21] và độ chính xác cao hơn 0,5%. So với kết quả NASNet có độ chính xác thấp hơn 7,5%, tuy nhiên xử lý hình ảnh trong kiến trúc nhanh hơn 2,3 lần [20].

Trong phần kết quả, NASNet và MNasNET sẽ được so sánh với các thử nghiệm được thực hiện trong 24 giờ và 3 giờ tương ứng để đánh giá sự khác biệt về kết quả. Độ trễ và sức mạnh tính toán cũng là mối quan tâm hàng đầu cho mục đích triển khai trong trường hợp này. Bằng cách tối ưu hóa một mạng nơ-ron vẫn có thể đạt được mức độ chính xác cao, độ trễ thấp khi đào tạo và cũng có thể chạy trên các thiết bị như điện thoại thông minh hiện đại, điều này sẽ cho phép triển khai linh hoạt hơn nhiều trong mạng 5G.

# BỘ DỮ LIỆU PHÁT HIỆN BẤT THƯỜNG

## 4.0.1 Tổng quan về môi trường tập dữ liệu

Phát hiện bất thường là một trong những lĩnh vực nghiên cứu hứa hẹn nhất trong việc phát hiện các cuộc tấn công mới. Tuy nhiên, việc áp dụng nó cho các ứng dụng trong thế giới thực bị cản trở do sự phức tạp của hệ thống đòi hỏi một lượng lớn thử nghiệm, điều chỉnh và đánh giá. Do đó, đối với mục đích nghiên cứu, một hệ thống mô phỏng có thể được thiết kế với một tập hợp toàn diện các xâm nhập và hành vi bất thường kết hợp với lưu lượng thông thường để phân tích phát hiện bất thường. Khi hành vi mạng và phần mềm độc hại đang thay đổi, cần phải có một môi trường mô phỏng chính xác hơn một kịch bản trong thế giới thực. Dữ liệu sau đó có thể được thu thập từ hệ thống là động và cung cấp thông tin chi tiết có ý nghĩa và thực tế hơn về hành vi lưu lượng mạng lành tính và bất thường. Thật không may, các tập dữ liệu IDS truyền thống không được thiết kế theo cách này, ví dụ như tập dữ liệu KDD CUP99 hoặc tập dữ liệu ADFA-IDS được tạo ra trong môi trường thử nghiệm chỉ bao gồm các liên kết LAN duy nhất và một hệ thống tấn công và một hệ thống phòng thủ, cách tiếp cận này đại diện cho một môi trường tĩnh và cung cấp kết quả dưới mức tối ưu và kém thực tế hơn [22] [23].

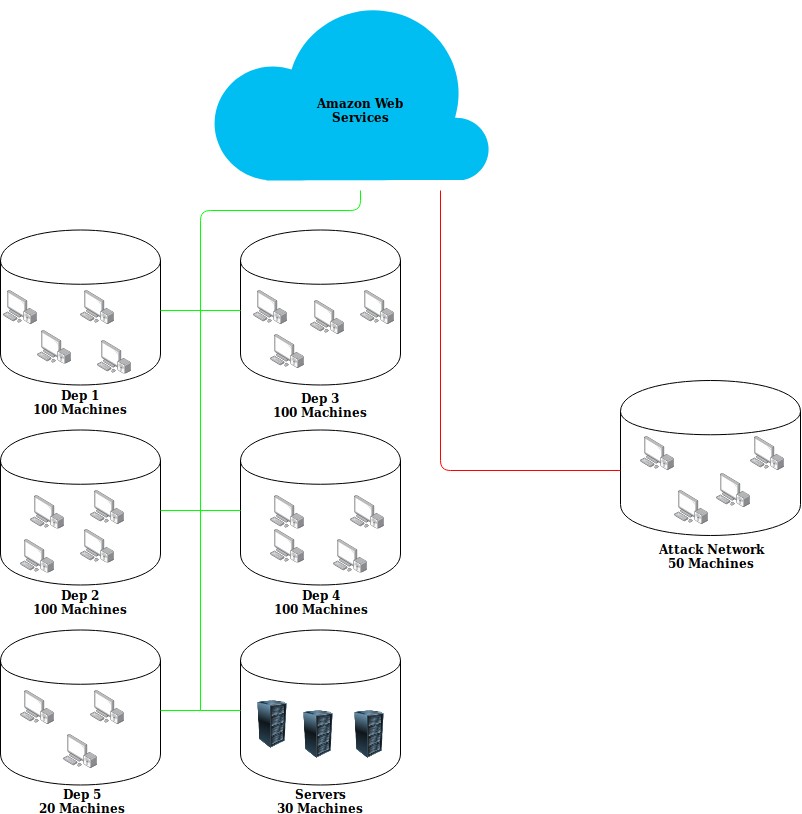
Bộ dữ liệu IDS-2018 từ Viện An ninh mạng Canada là một tập dữ liệu bắt nguồn từ một môi trường mô phỏng cố gắng giải quyết những thiếu sót này [24]. Mục tiêu chính của tập dữ liệu này là sử dụng cách tiếp cận có hệ thống để tạo ra một bộ dữ liệu điểm chuẩn đa dạng và toàn diện để phát hiện xâm nhập dựa trên việc tạo ra các hồ sơ lưu lượng truy cập lành tính và độc hại. Bản thân môi trường bao gồm 50 máy tấn công trên một tổ chức nạn nhân với 5 bộ phận, bao gồm 420 máy và 30 máy chủ. Tập dữ liệu lấy gói lưu lượng mạng và nhật ký hệ thống của mỗi máy, cũng như trích xuất 80 tính năng mạng được tổ chức dưới dạng luồng. Hình 7. dưới đây cho thấy cấu trúc liên kết mạng tổng thể là một mạng LAN phổ biến trên AWS (Amazon Web

Dịch vụ) nền tảng đám mây. 6 mạng con được cài đặt có nhãn là

Dep1 đến Dep5 và máy chủ. Máy Dep1 đến Dep4 có

Hệ điều hành Windows 8/10, Dep5 có tất cả các máy Linux đang chạy

Ubuntu, Servers có các máy chủ MS Windows khác nhau như Máy chủ ứng dụng, thư mục hoạt động và email. Mạng lưới kẻ tấn công có máy Windows 8/10 và máy Ubuntu.



*Hình 7: Cấu trúc liên kết mạng CICIDS2018*

## 4.0.2 Cấu hình mạng & Tính năng

Các giao thức được mô phỏng trong môi trường là: HTTPS (Hyper-

Giao thức truyền văn bản an toàn), HTTP (Truyền siêu văn bản

Giao thức), SMTP (Giao thức truyền thư đơn giản), POP3 (Đăng

Giao thức văn phòng 3), IMAP (Giao thức truy cập tin nhắn Internet), SSH (Secure Shell), FTP (Giao thức truyền tệp). Các loại lưu lượng được chia thành hai cấu hình, cấu hình B (lưu lượng truy cập lành tính) hoặc cấu hình M (lưu lượng truy cập độc hại). Các loại lưu lượng truy cập trong các hồ sơ này được giải thích chi tiết hơn bên dưới.

**B-Profile:** Mô tả các loại lưu lượng thông thường được mô phỏng thông qua một số thuật toán học máy với các giao thức mạng khác nhau [24]:

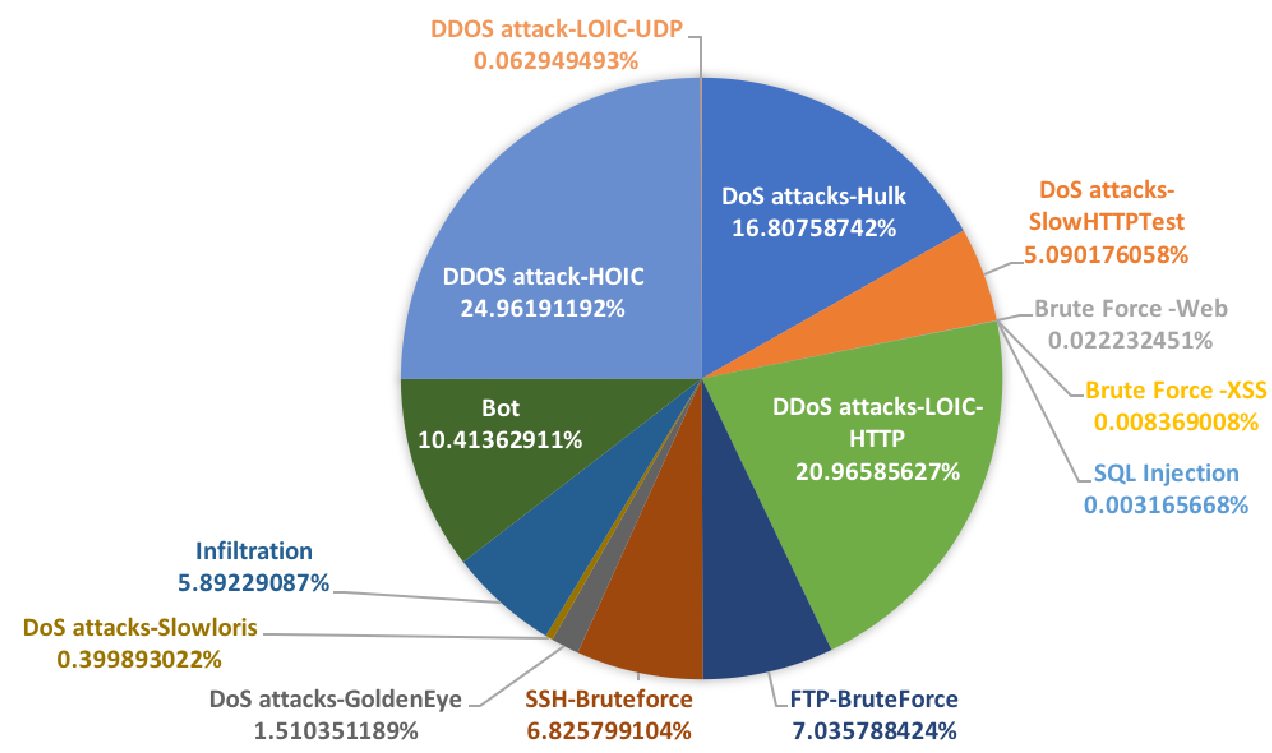
* Mô phỏng hành vi của người dùng bằng cách sử dụng các kỹ thuật phân tích thống kê học máy khác nhau như K-Means, Random Forest, SVM và J48.
* Các tính năng mạng được thu thập bao gồm kích thước gói của giao thức, số lượng gói trên mỗi luồng, các mẫu khác nhau trong tải trọng, kích thước của tải trọng và phân phối thời gian yêu cầu của một giao thức.

Các cuộc tấn công cụ thể được sử dụng trong M-Profile là các cuộc tấn công phổ biến được sử dụng bởi các tác nhân độc hại cũng như người kiểm tra thâm nhập. Chúng bao gồm nhiều tình huống khác nhau từ các cuộc tấn công dựa trên mạng, các hình thức khác nhau của HTTP DoS và DDoS, tấn công vũ phu, tấn công dựa trên web và các lỗ hổng phổ biến. Chúng cũng bao gồm các khía cạnh của OWASP top 10 2019 bao gồm các cuộc tấn công dựa trên tiêm từ SQL, xác thực bị hỏng do quản lý mật khẩu kém cho phép các cuộc tấn công vũ phu dễ dàng hơn và cấu hình sai bảo mật cho phép các lỗ hổng như heartbleed do hệ thống chưa được vá

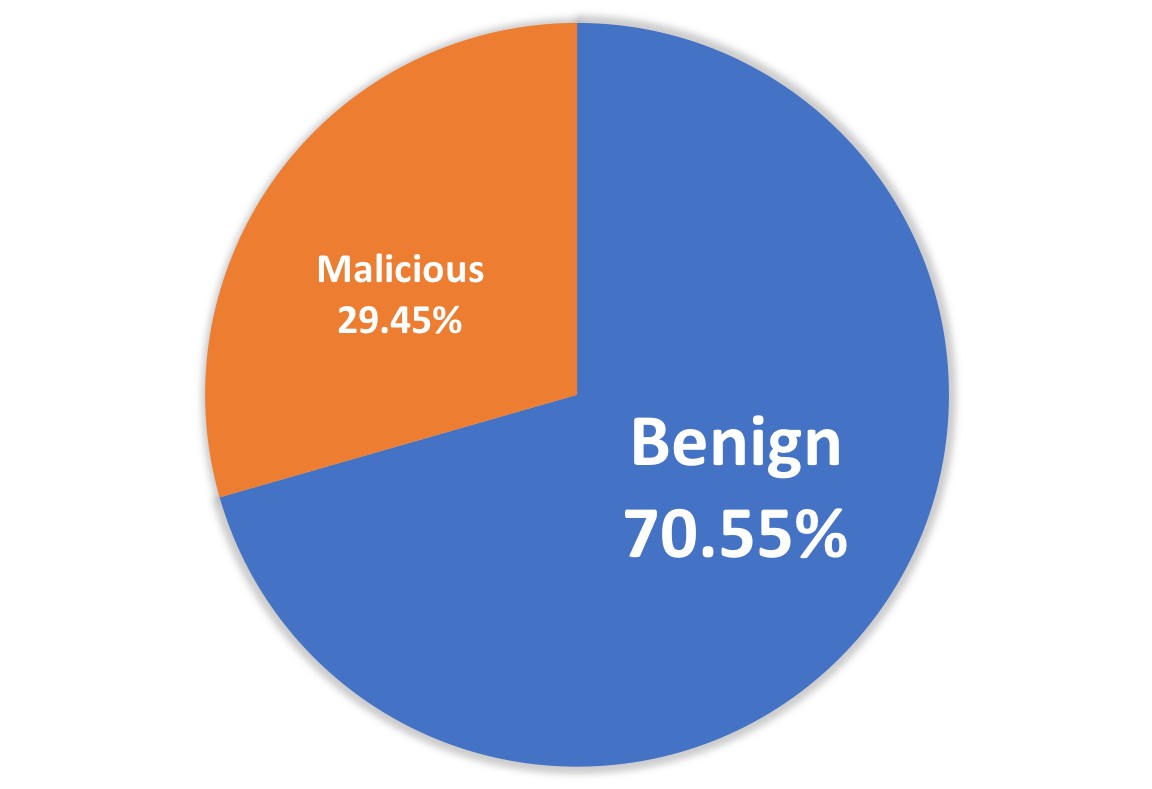
[25].

**M-Profile:** Mô tả kịch bản tấn công cho lưu lượng truy cập bất thường, sáu kịch bản tấn công khác nhau được mô phỏng [24]:

* Xâm nhập mạng nội bộ - khai thác lỗ hổng ứng dụng bằng cách gửi các tệp độc hại qua email. Khung Metasploit được sử dụng để khai thác, cho phép một cửa hậu được thực thi trên PC của nạn nhân.
* HTTP DoS - Slowloris, LOIC và HOIC gây ra từ chối dịch vụ được sử dụng, các công cụ này có thể làm cho máy chủ web không thể truy cập được. Slowloris có thể làm điều này chỉ với một máy và hiệu quả nhất đối với các máy chủ Apache [26]. Máy chủ Apache là máy chủ web phổ biến thứ hai trên internet, chiếm 26,73% máy chủ web [27].
* Tấn công ứng dụng web - Các cuộc tấn công dựa trên ứng dụng web được thử nghiệm bằng cách sử dụng Damn Vulnerable Web App (DVWA) để chèn SQL, chèn lệnh và tải lên tệp không hạn chế.
* Tấn công brute force - Sử dụng một cuộc tấn công brute force từ điển chứa 90 triệu từ chống lại các máy chủ chính để cố gắng lấy thông tin tài khoản SSH và MySQL.
* Các cuộc tấn công được cập nhật lần cuối - Các lỗ hổng được biết đến có thể ảnh hưởng đến hàng nghìn thiết bị trong một số điều kiện nhất định và nếu chúng đang chạy các phiên bản phần mềm cũ hơn, lỗi thời. Heartleech sẽ được sử dụng trong môi trường này, nó được sử dụng để quét các hệ thống dễ bị lỗi Heartbleed, một khi hệ thống được tìm thấy, chúng có thể bị khai thác và dữ liệu có thể bị lấy đi.

Để xác định các tính năng từ các cấu hình này, các gói thô ban đầu được chuyển đổi thành luồng mạng để phân tích dễ dàng hơn. Sử dụng các luồng hai chiều CICFlowMeter được tạo ra trong đó gói đầu tiên xác định hướng chuyển tiếp (nguồn đến đích) và lùi (đích đến nguồn). Do đó, từ 83 đặc điểm thống kê thu thập được từ các luồng như thời lượng, số gói, số byte, độ dài gói, chúng được tính toán riêng cho cả hướng thuận và ngược. Đối với các luồng TCP, chúng bị chấm dứt khi ngắt kết nối (sau khi nhận được gói FIN) và các luồng UDP bị chấm dứt khi hết thời gian chờ luồng.

## Hình 8. Biểu đồ hình tròn về khối lượng loại lưu lượng truy cập độc hại



## Hình 9. Biểu đồ hình tròn của tất cả các khối lượng lưu lượng truy cập

Bài báo này sẽ chia nhỏ tất cả các luồng mạng được dán nhãn thành hai luồng để phân tích, bất thường và lành tính. Benign bao gồm tất cả lưu lượng được mô tả trong B-Profile và anomalous là tất cả lưu lượng được mô tả trong M-Profile. Các cuộc tấn công khác nhau xảy ra vào các ngày khác nhau trong tổng số 10 ngày hoặc 240 giờ, các cuộc tấn công này được phân tán ngẫu nhiên trong lưu lượng truy cập lành tính. Tổng cộng có 2748235 luồng bất thường và 6584535 luồng lành tính mang lại tổng số luồng 9332770 trong tập dữ liệu. Đây là sự phân chia của 70,55% lưu lượng truy cập lành tính và 29,45% lưu lượng truy cập bất thường. Hai biểu đồ hình tròn bên dưới trong Hình 8. và Hình 9. hiển thị bảng phân tích lưu lượng truy cập trong tập dữ liệu.

# THỜI GIAN ĐẾN VÀ LỰA CHỌN TÍNH NĂNG

IAT (Inter-Arrival Time) có thể được định nghĩa là các khung hình, gói hoặc luồng trung bình đến máy chủ trong một khoảng thời gian nhất định [28]. Bằng cách kiểm tra đặc điểm này và các dạng thống kê khác của IAT như trung bình, tối thiểu, tối đa và độ lệch chuẩn của IAT của luồng mạng, lưu lượng truy cập lành tính có thể được mô hình hóa để phù hợp với phân phối Weibull. Bằng cách mô hình hóa lưu lượng truy cập lành tính đến phân phối Weibull, do đó có thể xác định lưu lượng truy cập bất thường vì nó sẽ gây ra sự bất thường và sai lệch trong phân phối [29]. Mối tương quan này có thể xác định được trên các gói, luồng và phiên cho cả giao thức truyền tải TCP (Giao thức điều khiển truyền tải) và UDP (Giao thức dữ liệu người dùng) trong lưu lượng truy cập internet [30]. Do đó, các tính năng luồng mạng IAT này có thể là dấu hiệu cho thấy sự khác biệt về các luồng lành tính và bất thường.

Các nghiên cứu hiện tại chứng minh sự phân bố Weibull được mô hình hóa cho lưu lượng truy cập internet bằng cách sử dụng các dấu vết lưu lượng truy cập được thu thập từ Nhóm nghiên cứu WAND [31]. Giám sát lưu lượng 24 giờ từ ISP đã thu thập dữ liệu từ các điểm truy cập không dây, kết nối DSL và ethernet trong môi trường đô thị [30]. Dữ liệu thu được cho thấy sự phù hợp cho các gói, luồng và phiên khi chúng giảm từ thống nhất (giá trị 1) đến phân phối Weibull.

Mở rộng khái niệm này để tập trung vào các luồng mạng, [29] đã chứng minh rằng mặc dù có sự đa dạng của các mạng về kích thước, số lượng người dùng, ứng dụng và tải, các luồng TCP lành tính của IAT cũng phù hợp với phân phối Weibull và những bất thường cụ thể trong các luồng này sẽ gây ra sai lệch trong lưu lượng truy cập. Nhiều bộ dữ liệu đã được thu thập với băng thông, kích thước và ứng dụng khác nhau để xác minh sự phù hợp này. Các tập dữ liệu được thử nghiệm trong [29] là:

* **1. MAWI3 (Đo lường và phân tích trên Internet WIDE):** Tháng 6 năm 2012, 1,4 triệu lưu lượng, được ghi lại từ một liên kết đường trục xuyên Thái Bình Dương 150Mbps giữa Nhật Bản và Hoa Kỳ.
* **2. SUT (Đại học Công nghệ Sharif):** Tháng 6 năm 2012, 2,4 triệu dòng chảy, được chụp từ cổng internet của cơ sở SUT.
* **3. MCO**: Tháng 2 năm 2011, 2,3 triệu dòng chảy, được chụp từ cổng internet của một công ty kinh doanh vừa.
* **4. NUST1 (Đại học Khoa học và Công nghệ Quốc gia):** Tháng 3 năm 2009, 2,2 triệu luồng, Được thu thập từ một bộ định tuyến điểm cuối đặt tại NUST,

Pakistan.

* **5. ISP NUST**: được chụp từ bộ định tuyến biên của một ISP quy mô trung bình và hợp nhất với các luồng tấn công được tạo ra trong NUST.

Khi phân tích lưu lượng truy cập từ các tập dữ liệu trên, [29] cho thấy rằng độ lệch trong phân phối Weibull có thể nhìn thấy khi so sánh tất cả các luồng với các luồng lành tính.

Các cuộc tấn công cụ thể vào tập dữ liệu ISP NUST cũng đã được phân tích về tỷ lệ phát hiện. Tấn công tiêm cho một cuộc tấn công lũ lụt SYN, một loại tấn công DoS bao gồm một khối lượng lớn các gói SYN với thời gian đến rất nhỏ [29]. Sự thay đổi mạnh mẽ về thời gian đến giữa các điểm đến gây ra sự bất thường trong phân phối Weibull và cho phép phát hiện các cuộc tấn công. [29] cho thấy tỷ lệ chính xác 98,8% đã đạt được với tỷ lệ báo động giả 4,8%. Điều này cho thấy mức độ khác biệt cao mà một số loại tấn công độc hại phổ biến có thể có đối với thời gian đến giữa các luồng. Khái niệm này tạo cơ sở cho quyết định lựa chọn tính năng từ tập dữ liệu CICIDS2018 và các giả định này sẽ được xác minh trong phần kết quả.

Bằng cách xem xét các nghiên cứu trước đây về hành vi luồng giao thông giữa các điểm đến, các khái niệm này có thể được mở rộng cho các mô hình máy học hiện tại để cung cấp dữ liệu được xác định rõ ràng, được dán nhãn về việc phân loại giữa luồng giao thông bất thường và lành tính. Do đó, việc lựa chọn tính năng liên quan đến quá trình lựa chọn hai phần. Phần đầu tiên là lựa chọn các tính năng tiêu chuẩn cung cấp thông tin cơ bản về luồng. Phần thứ hai liên quan đến việc chọn một số đặc điểm hạn chế thể hiện sự khác biệt rõ ràng về giá trị giữa dòng chảy lành tính và bất thường. Như đã chứng minh trước đây, dữ liệu dòng IAT có thể được đề xuất như một ứng cử viên mạnh mẽ và cụ thể hơn là các biến thể thống kê của dữ liệu dòng IAT có thể được sử dụng để phân tích thêm các mối tương quan này. Quyết định hạn chế lựa chọn tính năng này là để cung cấp cho mô hình máy học dữ liệu sạch và loại bỏ nhiễu dư thừa trong dữ liệu không có ý nghĩa trong mối tương quan giữa các luồng bất thường và lành tính. Bằng cách này, một mô hình hiệu quả hơn có thể được thiết kế, với độ chính xác cao hơn và tốc độ nhanh hơn. Do đó, 20 tính năng cùng với một cột nhãn bổ sung để phân loại từng loại dòng chảy đã được chọn và đó là:

* **Các tính năng cơ bản của Flow**: Cổng đích, Giao thức, Thời lượng luồng, Tổng gói chuyển tiếp, Tổng gói lùi, Pkts / giây
* **Siêu dữ liệu thống kê IAT**: Trung bình IAT lưu lượng, Độ lệch chuẩn IAT lưu lượng, Tối đa IAT lưu lượng, Lưu lượng

IAT tối thiểu, tổng số IAT lưu lượng, trung bình IAT chuyển tiếp,

Độ lệch chuẩn IAT chuyển tiếp, IAT tối đa chuyển tiếp,

Chuyển tiếp IAT tối thiểu, Tổng IAT lùi, Trung bình IAT lùi, Độ lệch chuẩn IAT lùi, IAT tối đa lùi, IAT tối thiểu lùi

## 5.0.1 Bộ dữ liệu tiền xử lý

Tiền xử lý tập dữ liệu liên quan đến việc chuyển đổi dữ liệu đầu vào thành dạng chính xác phù hợp với CNN, trong trường hợp này là hình ảnh 100x100x3. 20 tính năng được xác định từ tập dữ liệu được trích xuất ở định dạng tệp CSV. Đầu vào CSV được định hình lại thành hình ảnh RGB có kích thước 100 x 100 x 3, bất kỳ dữ liệu bổ sung nào còn sót lại dưới kích thước này sẽ bị loại bỏ vì tất cả các hình ảnh cho CNN được yêu cầu phải có cùng kích thước đầu vào. Kích thước hình ảnh này được chọn do cung cấp một khối lượng hình ảnh mẫu tốt cho lượng dữ liệu có sẵn (hơn 1000 hình ảnh mẫu). Nói chung, sự đánh đổi giữa việc sử dụng hình ảnh có độ phân giải cao hơn so với hình ảnh có độ phân giải thấp hơn là hình ảnh có độ phân giải cao hơn sẽ chứa các chi tiết tốt hơn khi được xử lý bởi mạng nơ-ron, tuy nhiên điều này sẽ mất nhiều thời gian hơn cho cả giai đoạn đào tạo và thử nghiệm. Hình ảnh có độ phân giải thấp hơn sẽ cung cấp ít chi tiết hơn, nhưng nhiều biểu diễn đặc điểm toàn cầu hơn và mạng nơ-ron sẽ có thể đào tạo và kiểm tra dữ liệu với tốc độ nhanh hơn. Đối với bài báo này, autoML lấy mẫu và tăng cường tất cả các hình ảnh lên kích thước hình ảnh đầu vào 224 x 224 x 3, do đó chỉ có hai cân nhắc, thứ nhất là khối lượng hình ảnh trên 1000 và đủ chi tiết tính năng được chụp. Hai ví dụ được hiển thị dưới đây trong Hình 10 và Hình 11 về hình ảnh bất thường trông như thế nào so với hình ảnh lành tính. Về mặt đồ họa, hình ảnh bất thường là ngẫu nhiên và nhiễu, trong khi hình ảnh lành tính đều đặn hơn và chứa một số mẫu có thể nhận dạng.

# KẾT QUẢ PHÁT HIỆN BẤT THƯỜNG

Phần này trình bày kết quả của mô hình autoML Vision đã triển khai trên dữ liệu hình ảnh được xử lý trước. Để tối đa hóa độ chính xác của mô hình, cả mô phỏng NASnet 24 giờ và mô phỏng MNasNet 3 giờ đều được chạy để so sánh kết quả đạt được. Bây giờ tập dữ liệu đã được xử lý trước thành hình ảnh, giờ đây bạn có thể tải những hình ảnh này lên Google AutoML Vision. Các hình ảnh được sắp xếp theo cấu trúc thư mục cho các hình ảnh lành tính và bất thường, sau đó các hình ảnh này được tải lên bộ nhớ Google Cloud Bucket cùng với tệp CSV để ánh xạ đường dẫn tệp đầu ra đến đúng nhãn. AutoML Vision định hình lại kích thước hình ảnh đầu vào thành kích thước đầu vào dự kiến của mô hình là 224 x 224 x 3. Xem phụ lục A



(a) Hình ảnh bất thường 1 (b) Hình ảnh bất thường 2

*Hình 10: Ví dụ về hình ảnh bất thường*

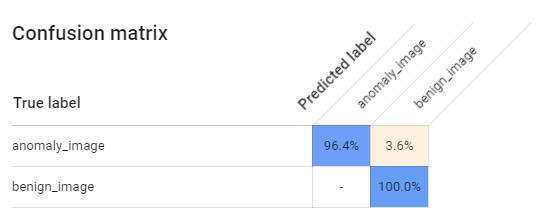
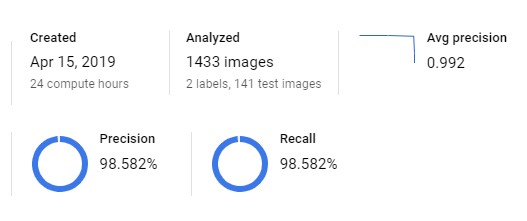


(c) Hình ảnh lành tính 1 (d) Hình ảnh lành tính 2

*Hình 11: Ví dụ về hình ảnh lành tính*

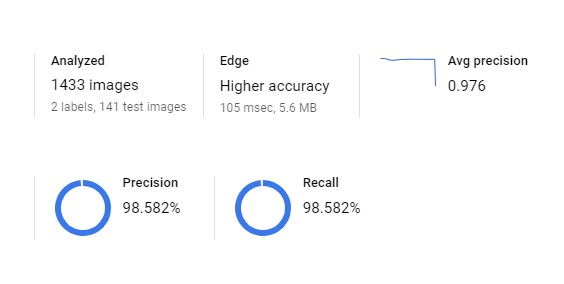
để bố trí mô hình. Với thời gian đào tạo 3 giờ và 1433 hình ảnh 100 x 100 x 3 được chia thành 925 hình ảnh lành tính và 508 hình ảnh bất thường. 141 hình ảnh thử nghiệm đạt độ chính xác trung bình là 97,6%, độ chính xác tối đa là 98,582% và khả năng thu hồi tối đa là 98,582% cho toàn bộ mô hình. Vì mô hình được phát triển trên nền tảng MNasNet Edge, nó được tối ưu hóa hơn về tốc độ so với các mô hình NAS truyền thống và không yêu cầu sức mạnh tính toán lớn và nhiều ngày để đào tạo. Việc đào tạo mô hình để có độ chính xác cao hơn sẽ mang lại thời gian xử lý là 105 mili giây cho mỗi hình ảnh cho điện thoại di động Pixel 1.

Chạy mô hình trong thử nghiệm 24 giờ cho kết quả tương tự, ngoại trừ độ chính xác trung bình cao hơn một chút ở mức 99,2%, điều này là do diện tích dưới đường cong độ chính xác thu hồi lớn hơn như trong Hình 12. so với Hình 13. Điều này có nghĩa là mô hình được tối ưu hóa với tiềm năng lớn nhất với dữ liệu được cung cấp. Đào tạo với các tập dữ liệu bổ sung và nhiều dữ liệu hơn sẽ chỉ làm cho mô hình có mức hiệu suất cao hơn. Về mặt triển khai trong thế giới thực, sẽ luôn có sự đánh đổi giữa độ chính xác và tốc độ. Tuy nhiên, trong trường hợp này, sự mất mát nhỏ về độ chính xác để tăng hiệu suất lớn hơn nhiều là mong muốn. Điều này có nghĩa là việc sử dụng tài nguyên có thể được giảm thiểu, các mối đe dọa có thể được phát hiện sớm hơn và việc đào tạo và tinh chỉnh mô hình bổ sung sau đó có thể được hoàn thành với tốc độ nhanh hơn.



*Hình 14: Ma trận nhầm lẫn*

## Hình 12: Kết quả kiểm tra trong 24 giờ



## Hình 13: Kết quả kiểm tra 3 giờ

Các chỉ số phổ biến nhất được sử dụng để xác định mức độ liên quan của kết quả bao gồm độ chính xác, khả năng nhớ lại, điểm f1 và đường cong nhớ lại độ chính xác. Độ chính xác và khả năng thu hồi được xác định từ các số liệu thống kê sau:

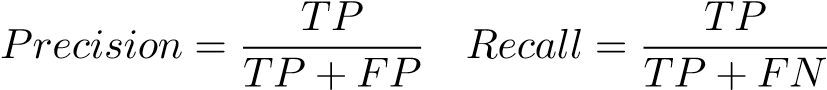
* **Dương tính đúng (TP):** Một hình ảnh bất thường được mô hình phân loại là bất thường, kết quả là Đúng

Dương tính.

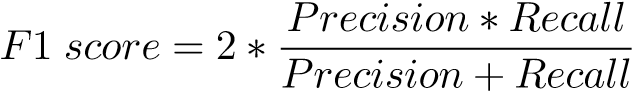
* **Dương tính giả (FP):** Một hình ảnh bất thường được mô hình phân loại là lành tính, kết quả là False Postive.
* **True Negative (TN):** Một hình ảnh lành tính được mô hình phân loại là lành tính kết quả là True Negative.
* **Âm tính giả (FN):** Một hình ảnh lành tính được mô hình phân loại là bất thường, kết quả là Sai

Âm tính.

Độ chính xác có thể được định nghĩa là tỷ lệ phần trăm các dự đoán tích cực là chính xác và khả năng nhớ lại có thể được định nghĩa là bao nhiêu phần trăm các trường hợp dương tính mà bộ phân loại phát hiện. Về mặt toán học, điều này có thể được tính như sau:



Và từ các số liệu thống kê này, điểm F1 cung cấp trung bình hài của độ chính xác và khả năng thu hồi cũng có thể được tính toán:



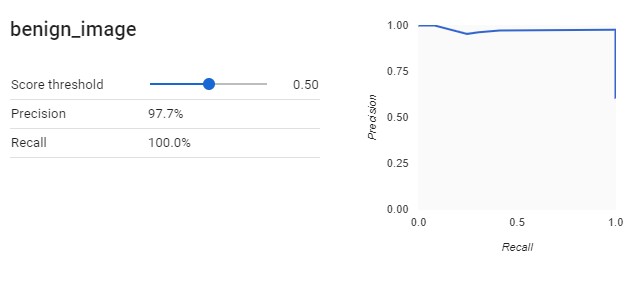
Ma trận nhầm lẫn trong Hình 14 cho thấy phần trăm dự đoán khi người phân loại chọn câu trả lời đúng, trong trường hợp này 96,4% hình ảnh bất thường được xác định là hình ảnh bất thường và 3,6% hình ảnh bất thường được xác định không chính xác là hình ảnh lành tính. Đối với hình ảnh lành tính, 0% hình ảnh lành tính đã được dự đoán sai là hình ảnh bất thường và 100% hình ảnh lành tính được xác định chính xác.

Số liệu thống kê hiệu suất chính được hiển thị trong bảng dưới đây để hiển thị và so sánh dễ dàng hơn. Lưu lượng truy cập lành tính có độ chính xác 100%, nhưng có độ chính xác là 97,7% do phân loại không chính xác một tỷ lệ nhỏ hình ảnh bất thường là lành tính. Lưu lượng truy cập bất thường có độ chính xác là 100% do tất cả các hình ảnh bất thường được phát hiện đều được phân loại chính xác, nhưng có khả năng thu hồi là 96,4% do thiếu một số hình ảnh bất thường và phân loại không chính xác chúng là lành tính.

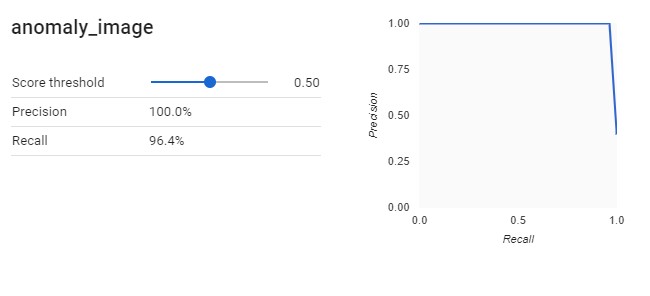
## Bảng 1: Thống kê hiệu suất

|  |  |  |  |
| --- | --- | --- | --- |
|  | Kết quả 24 giờ & 3 giờ | |  |
| **Loại giao thông** | **Chính xác** | **Nhớ** | **Điểm F1** |
| Lành | 0.977 | 1 | 0.988 |
| Bất thường | 1 | 0.964 | 0.982 |
| Trung bình | 0.9885 | 0.982 | 0.985 |

Độ chính xác so với việc thu hồi là một sự đánh đổi và điều này được thể hiện trong các đường cong thu hồi độ chính xác dưới đây trong hình 15. và Hình 16. Ngưỡng điểm được đặt ở mức 0,5 để cân bằng đồng đều các chỉ số này. Để đơn giản hóa các số liệu này thành một số, điểm F1 có thể được sử dụng, có trọng số đồng đều cả độ chính xác và khả năng thu hồi, các giá trị điểm F1 được hiển thị ở trên. Điểm F1 là một số liệu quan trọng đối với mô hình này vì cả khả năng nhớ lại và độ chính xác cần được xem xét trong phát hiện giao thông bất thường. Trong một ứng dụng trong thế giới thực, IDS cần giảm thiểu số lượng lưu lượng lành tính được xác định là bất thường càng nhiều càng tốt, trong khi vẫn cố gắng tối đa hóa tỷ lệ phát hiện lưu lượng bất thường thực sự.



## Hình 15: Dữ liệu lành tính



*Hình 16: Dữ liệu bất thường*

# THẢO LUẬN VÀ ĐỊNH HƯỚNG TƯƠNG LAI

Có nhiều lĩnh vực cần được xem xét khi cố gắng bảo mật mạng 5G, vì mạng rất đa dạng, bảo mật trở nên khó triển khai hiệu quả hơn. Cách tiếp cận của bài báo này sau đó là phát triển một hệ thống giám sát đầu cuối cho lưu lượng truy cập chạy qua mạng, bản thân đây không phải là một giải pháp bảo mật dứt khoát, chỉ là một phần của kiến trúc bảo mật tổng thể cần thiết để bảo mật mạng. Mô hình được thiết kế với bộ tính năng cơ bản và IAT được chọn trong bài báo này sử dụng autoML đã phân loại chính xác tất cả các luồng lưu lượng lành tính, đây là một kết quả rất tốt, tuy nhiên đối với các luồng lưu lượng bất thường, 96,4% lưu lượng truy cập đã được phân loại chính xác, do đó vẫn còn chỗ để cải thiện. Có sự khác biệt tối thiểu trong cả kiến trúc MNasNet (thời gian chạy 3 giờ) và kiến trúc NASNet (thời gian chạy 24 giờ), điều này có thể là do kích thước tập dữ liệu. Để xác nhận mô hình tiếp theo, thử nghiệm có thể được tiến hành với một tập dữ liệu lớn hơn, thử nghiệm cũng có thể được tiến hành với các tập dữ liệu khác nhau để đảm bảo mức độ tổng quát hợp lý trong mô hình và để kiểm tra các vấn đề quá khớp. Cuối cùng, xác định bất kỳ hình ảnh lành tính và bất thường nào tương tự nhau và thử nghiệm với các đặc điểm khác nhau để cố gắng tách biệt giữa hình ảnh lành tính và dị thường thậm chí có thể được điều tra nhiều hơn. Hình ảnh bất thường và hình ảnh lành tính càng tốt thì việc đào tạo mô hình và giảm dữ liệu và lỗi ngoại lệ càng dễ dàng hơn. NAS đã cho phép tạo ra một mô hình nâng cao cho một tập dữ liệu cụ thể được xây dựng một cách tự động và để tránh quá trình tẻ nhạt của thiết kế kiến trúc thủ công, mô hình NAS được thiết kế giờ đây có thể được xuất thành một ứng dụng tùy chỉnh để kiểm tra và tinh chỉnh thêm.

Nhìn chung, kết quả làm nổi bật hiệu quả của các kỹ thuật phát hiện hình ảnh dựa trên máy học để phân tích luồng mạng. Nghiên cứu này có thể được mở rộng theo một số hướng khác nhau như:

1. Triển khai các kỹ thuật học tập không giám sát để tạo ra một mô hình học tập bán giám sát, vì trên thực tế, phần lớn lưu lượng mạng là dữ liệu không được gắn nhãn và xử lý trước dữ liệu không được gắn nhãn thành dữ liệu được gắn nhãn sạch và có tổ chức là một quá trình tốn nhiều thời gian. Mở rộng khái niệm này, một cấu hình lưu lượng lành tính có thể được thiết kế cho một lát cắt mạng cụ thể bằng cách sử dụng các kỹ thuật học không giám sát để phân loại chung và sau đó là các kỹ thuật được giám sát để tinh chỉnh bổ sung để xác minh hồ sơ.
2. Xây dựng một cơ sở dữ liệu lưu trữ nhật ký lưu lượng, một khối lượng nhật ký cụ thể sẽ được thực hiện thường xuyên để đào tạo mạng, nghiên cứu sâu hơn có thể được tiến hành về tần suất đào tạo lại mạng, với dữ liệu mới đến, mất bao lâu để đào tạo và liệu có thể triển khai nhiều phiên bản của mạng nơ-ron không, để một thực thể có thể đào tạo trên dữ liệu mới trong khi một phiên bản khác có thể được kiểm tra trên dữ liệu hiện có.
3. Triển khai hệ thống giám sát lưu lượng theo thời gian thực với cấu hình được xây dựng bởi máy học, điều này có thể được thiết kế như một tường lửa thông minh.
4. Thiết kế một hệ thống dựa trên niềm tin nâng cao để xác thực niềm tin dựa trên phân tích luồng dự đoán.

# KẾT THÚC

Bài báo này đề xuất một giải pháp mới là áp dụng bảo mật được xác định bằng phần mềm với máy học để cung cấp khả năng bảo vệ đầu cuối cho mạng 5G. Phạm vi dự án ban đầu đã được hoàn thành và cách tiếp cận chuyển đổi các luồng mạng thành hình ảnh để phân tích bởi CNN đã chứng minh kết quả chính xác cao đối với dữ liệu có sẵn, đặc biệt là khi xem xét rằng CNN theo truyền thống được tối ưu hóa để phát hiện hình ảnh / ảnh thực. Việc áp dụng hệ thống SDS dựa trên máy học đầy hứa hẹn cho việc triển khai trong thế giới thực và một số điểm được nêu ở trên khám phá thêm điều này. Tuy nhiên, những thách thức vẫn phải được vượt qua, về mặt quản lý mạng 5G đa dạng và phức tạp, đồng thời quản lý khối lượng lớn và các biến thể của lưu lượng truy cập sẽ chảy qua chúng.

Nhìn chung, đây chỉ là khởi đầu cho các ứng dụng bảo mật dựa trên máy học. Sự tăng trưởng trong việc triển khai mạng 5G, sử dụng internet toàn cầu, kết nối thiết bị IoT và phân tích dữ liệu lớn sẽ tiếp tục mở rộng và tạo ra các bề mặt tấn công mới. Để quản lý và giảm thiểu các bề mặt tấn công này một cách hiệu quả, các hệ thống bảo mật máy học năng động và thông minh có thể phản ứng nhanh chóng với các mối đe dọa sẽ rất quan trọng.

# THAM KHẢO

1. IoT: số lượng thiết bị được kết nối trên toàn thế giới 2012-2025, Statista. [Trực tuyến]. Có sẵn: https://www.statista.com/statistics/471264/ iot-number-of-connected-devices-worldwide/. [Truy cập: 06-Apr2019].
2. Ericsson, Hướng dẫn về An ninh mạng 5G, Ericsson.com, trang 120. [3] 5G Châu Mỹ, Sự phát triển của bảo mật trong 5G, Sách trắng 5G Châu Mỹ, trang 140, tháng 10 năm 2018.
3. J. Fruhlinger, Botnet Mirai giải thích: Làm thế nào các thiết bị IoT gần như làm sập internet, CSO Online, 09-Mar-2018. [Trực tuyến]. Có sẵn: https://www.csoonline.com/article/3258748/ the-mirai-botnet-explained-how-teen-scammers-and-cctv-cameras\ n-almost-brought-down-the-internet.html. [Truy cập: 06-Apr2019].
4. 3GPP, Dự án Đối tác Thế hệ thứ 3; Nhóm thông số kỹ thuật Dịch vụ và các khía cạnh hệ thống; Kiến trúc và quy trình bảo mật cho hệ thống 5G (Bản phát hành 15), 3GPP TS 33.501 V15.4.0 (2019-03), trang 110.
5. CISCO, Áp dụng bảo mật cho thế giới 5G, CISCO, 16-Jan-2019. [Trực tuyến]. Có sẵn: https://www.cisco.com/c/dam/m/en us/ network-intelligence/service-provider/digital-transformation/ knowledge-network-webinars/pdfs/0116 SECURITY CKN PDF. Pdf. [Truy cập: 07-Apr-2019].
6. Michael Geller và Pramod Nair, Đổi mới bảo mật 5G với Cisco, CISCO, 2018. [Trực tuyến]. Có sẵn:

https://www.cisco.com/c/dam/en/us/solutions/collateral/ nhà cung cấp dịch vụ/nhà cung cấp dịch vụ-giải pháp bảo mật/ 5g-security-innovation-with-cisco-wp.pdf. [Truy cập: 07-Tháng Tư 2019].

1. Netford, Phân tích dòng chảy so với phân tích gói. Bạn nên chọn gì?, Netford Technologies, 2014. [Trực tuyến]. Có sẵn: https: //www.netfort.com/wp-content/uploads/PDF/WhitePapers/ NetFlow-Vs-Packet-Analysis-What-Should-You-Choose.pdf.

[Truy cập: 07-Apr-2019].

1. B. Zoph và V. Vasudevan, Học kiến trúc có thể chuyển đổi để nhận dạng hình ảnh có thể mở rộng, arxiv, 11-Apr-2018. [Trực tuyến]. Có sẵn:

https://arxiv.org/pdf/1707.07012.pdf. [Truy cập: 07-Apr-2019].

1. S. Naseer và Y. Saleem, Phát hiện bất thường mạng nâng cao dựa trên mạng nơ-ron sâu, PHẦN ĐẶC BIỆT VỀ CÁC MỐI ĐE DỌA MẠNG VÀ CÁC BIỆN PHÁP ĐỐI PHÓ TRONG CHĂM SÓC SỨC KHỎE

SECTOR, Tháng Sáu 2018.

1. DE Denning, Mô hình phát hiện xâm nhập, IEEE Trans. Softw. Eng., tập SE-13, số 2, trang 222232, tháng 2 năm 1987. [Trực tuyến]. Có sẵn: http://ieeexplore.ieee.org/abstract/document/ 1702202/ [Truy cập: 07-Apr-2019].
2. A. Dawoud và S. Shahristani, Học sâu để phát hiện bất thường mạng, Hội nghị quốc tế năm 2018 về Học máy và Kỹ thuật Dữ liệu (iCMLDE), 2018.
3. D. Kwon và K. Natarajan, Nghiên cứu thực nghiệm về phát hiện bất thường mạng bằng mạng nơ-ron tích chập, Hội nghị quốc tế lần thứ 38 IEEE về hệ thống máy tính phân tán năm 2018, 2018.
4. R. Abdulhammed và M. Faezipour, Phương pháp tiếp cận học sâu và máy để xâm nhập dựa trên bất thườngPhát hiện lưu lượng mạng không cân bằng, Thư cảm biến IEEE, tháng 1 năm 2019.
5. I. Alrashdi và A. Alqazzaz, AD-IoT: Phát hiện bất thường các cuộc tấn công mạng IoT Thành phố thông minh bằng cách sử dụng Machine Leaming, IEEE, 2019.
6. B. Zoph và Q. V. Le, Tìm kiếm kiến trúc thần kinh với Học tăng cường, arxiv, tháng 2 năm 2017.
7. G. Seif, Mọi thứ bạn cần biết về AutoML và Tìm kiếm kiến trúc thần kinh, Hướng tới Khoa học Dữ liệu, 21-Aug2018. [Trực tuyến]. Có sẵn: https://towardsdatascience.com/ mọi thứ bạn cần biết về-automl-and-neural-arch-\ n/itecture-search-8db1863682bf2. [Truy cập: 06-Apr-2019].
8. Bảng hiện đại để phân loại hình ảnh trên ImageNet, Papers With Code: mới nhất trong học máy. [Trực tuyến]. Có sẵn: https://paperswithcode.com/sota/ image-classification-on-imagenet. [Truy cập: 11-Apr-2019].
9. ImageNet (bằng tiếng Anh). [Trực tuyến]. Có sẵn: http://image-net.org/ về-tổng quan. [Truy cập: 15-Apr-2019].
10. M. Tan và B. Chen, MnasNet: Tìm kiếm kiến trúc thần kinh nhận biết nền tảng cho thiết bị di động, arxiv, 18-Apr-2019. [Trực tuyến]. Có sẵn:

https://arxiv.org/pdf/1807.11626.pdf. [Truy cập: 25-Apr-2019].

1. M. Sandler và A. Howard, Mobilenetv2: Phần dư đảo ngược và nút cổ chai tuyến tính, 2018. .
2. AZSecure - Dữ liệu cho Tin học Tình báo và Bảo mật, AZSecure, 2019. [Trực tuyến]. Có sẵn:https://www.azsecure-data.org/ other-data.html. [Truy cập: 27-Apr-2019].
3. Dữ liệu KDD Cup 1999, Thông tin Lưu trữ KDD UCI và Khoa học Máy tính Đại học California, Irvine. [Trực tuyến]. Có sẵn: http://kdd.ics.uci.edu/databases/kddcup99/ kddcup99.html. [Truy cập: 04-Apr-2019].
4. CSE-CIC-IDS2018 - Bộ dữ liệu - Nghiên cứu - Viện An ninh mạng Canada - UNB, Đại học New Brunswick ước tính 1785, 2019. [Trực tuyến]. Có sẵn: https://www.unb.ca/cic/ datasets/ids-2018.html. [Truy cập: 01-Apr-2019].
5. G. Ruiz, 10 rủi ro bảo mật hàng đầu của OWASP Phần I, Blog Sucuri, 28Nov-2018. [Trực tuyến]. Có sẵn: https://blog.sucuri.net/2018/10/ owasp-top-10-security-risks-part-i.html. [Truy cập: 04-Apr-2019].
6. L. Perlman, Slow LorisŁ-ŁRethinking DoS attacks, Trung bình, 09-Oct-2018. [Trực tuyến]. Có sẵn: https://medium.com/front-end-weekly/ slow-loris-rethinking-dos-attacks-bd1ca5091bfe. [Truy cập: 06Apr-2019].
7. Khảo sát máy chủ web tháng 4 năm 2019, Netcraft. [Trực tuyến]. Có sẵn: https://news.netcraft.com/archives/2019/04/22/ april-2019-web-server-survey.html. [Truy cập: 05-Apr-2019].
8. Thời gian đến liên giờ là gì, IGI Global, 2019. [Trực tuyến]. Có sẵn: https://www.igi-global.com/dictionary/inter-arrival-time/ 35848. [Truy cập: 11-Apr-2019].
9. L. Arshadi và A. Jahangir, Nghiên cứu thực nghiệm về phân phối thời gian liên đến luồng TCP cho lưu lượng thông thường và bất thường, TẠP CHÍ QUỐC TẾ VỀ HỆ THỐNG TRUYỀN THÔNG, trang 119, tháng 10 năm 2014.
10. M. Arfeen và K. Pawlikowski, Vai trò của phân phối Weibull trong mô hình lưu lượng truy cập Internet, Kỷ yếu của Đại hội Viễn thông Quốc tế lần thứ 2013 (ITC) lần thứ 25, 2013.
11. Nhóm nghiên cứu WANDNetwork, WITSArchive, 2007. [Trực tuyến]. Có sẵn: http://research.wand.net.nz/wits/. [Truy cập: 19-Apr2019].

**PHỤ LỤC**

# A: MÔ HÌNH CNN DO NAS THIẾT KẾ

