**HỌC VIỆN CÔNG NGHỆ BƯU CHÍNH VIỄN THÔNG**

**KHOA CÔNG NGHỆ THÔNG TIN 2**

--🙢🕮🙠--

A picture containing graphics, logo, graphic design, symbol

Description automatically generated

***Báo cáo môn học***

**IOT VÀ ỨNG DỤNG**

***Đề tài:***

**TÌM HIỂU VỀ DẠNG TẤN CÔNG MẠNG TRONG LĨNH VỰC IOT**

***Giảng viên:* Đàm Minh Lịnh**

***Sinh viên thực hiện:*   
 1. Văn Tố Hữu - N20DCCN026**

**2. Vũ Huy Hùng - N20DCCN020**

***TP.HCM, tháng 01/2024***

# **LỜI MỞ ĐẦU**

Trong thời đại số hiện đại, sự gia tăng vọng tưởng của Internet of Things (IoT) đã mang lại những tiện ích đặc biệt cho cuộc sống hàng ngày, từ những thiết bị thông minh trong nhà cho đến các ứng dụng công nghiệp và y tế. Tuy nhiên, điều này cũng mở ra một thế giới mới của những thách thức bảo mật mạng, khi mà sự liên kết ngày càng sâu rộng của các thiết bị IoT tạo ra những cơ hội lớn cho các tấn công mạng.

Bảo vệ an ninh của hệ thống IoT trở thành một nhiệm vụ phức tạp, khiến cho việc tìm hiểu về các loại tấn công trở nên càng trọng đại. Trong ngữ cảnh này, nghiên cứu về tấn công an ninh mạng trong lĩnh vực IoT trở nên không thể phổ biến hơn, nhằm định rõ các mối đe dọa và tìm ra giải pháp bảo mật hiệu quả.

Bài viết này tập trung vào việc tìm hiểu về các tấn công an ninh mạng đối với hệ thống IoT, đồng thời phân tích cách chúng có thể ảnh hưởng đến tính bảo mật và ổn định của mạng. Chúng ta sẽ đào sâu vào các loại tấn công như DDoS, DoS, Recon, Web-based, Brute Force, Spoofing, và Mirai, đồng thời hiểu rõ về cách chúng có thể được triển khai và cách ngăn chặn chúng.

Mục tiêu của nghiên cứu này không chỉ là hiểu biết về các kỹ thuật tấn công, mà còn là xác định cách phòng ngừa và bảo vệ hệ thống IoT khỏi những mối đe dọa này. Qua đó, chúng ta hy vọng góp phần vào việc xây dựng một môi trường IoT an toàn và đáng tin cậy hơn trong thời đại ngập tràn các thiết bị kết nối.

Mục Lục

[**LỜI MỞ ĐẦU** 2](#_Toc155333952)

[**I.** **Tổng quan về các loại tấn công** 3](#_Toc155333953)

[**1.** **DdoS** 3](#_Toc155333954)

[**2.** **Brute Force** 3](#_Toc155333955)

[**3.** **Spoofing** 4](#_Toc155333956)

[**4.** **Dos** 4](#_Toc155333957)

[**5.** **Recon** 4](#_Toc155333958)

[**6.** **Web-based** 4](#_Toc155333959)

[**7.** **Mirai** 4](#_Toc155333960)

[**II.** **Dos attack với syn flood** 5](#_Toc155333961)

[**1.** **DoS là gì?** 5](#_Toc155333962)

[**2.** **Cuộc tấn công SYN Flood là gì?** 5](#_Toc155333963)

[**3.** **Làm thế nào tấn công SYN Flood ?** 5](#_Toc155333964)

[**III.** **ARP Poisoning Attack với ARP spoofing** 9](#_Toc155333965)

[**1.** **Tấn công ARP Poisoning là gì?** 9](#_Toc155333966)

[**2.** **Tấn công ARP Poisoning hoạt động như thế nào?** 10](#_Toc155333967)

[**3.** **Tấn công ARP spoofing** 10](#_Toc155333968)

[**IV.** **Mô hình học máy Random Forest** 15](#_Toc155333969)

[**1.** **Random Forest** 15](#_Toc155333970)

[2. Mô hình học máy Decision Tree 17](#_Toc155333971)

[3. Các thang đo độ chính xác của mô hình học máy 19](#_Toc155333972)

[**V.** **Trích xuất dữ liệu và xây dựng mẫu máy học** 21](#_Toc155333973)

[**1.**  **Trích xuất dữ liệu** 21](#_Toc155333974)

[**2,**  **Tạo dữ liệu cho việc train mô hình** 22](#_Toc155333975)

[**3,** **Huấn luyện mô hình** 25](#_Toc155333976)

[**4.** **Load mô hình học máy và xác định phương thức tấn công** 29](#_Toc155333977)

[**TÀI LIỆU THAM KHẢO** 31](#_Toc155333978)

1. **Tổng quan về các loại tấn công**
2. **DdoS**

DDoS là viết tắt của Distributed Denial of Service, có nghĩa là từ chối dịch vụ phân tán. DDoS là một dạng tấn công server chứa website, gây cạn kiệt tài nguyên hệ thống máy chủ, ngập lưu lượng băng thông internet và làm gián đoạn kết nối của người dùng. Trên đây là những khái niệm cơ bản giúp bạn hiểu được “DDoS và tấn công DDoS là gì?”.

Đây là kiểu tấn công phân tán, các đối tượng không chỉ sử dụng máy tính của mình mà lợi dụng cả máy tính người dùng để tấn công DDoS. Cụ thể, chúng sẽ chiếm dụng quyền kiểm soát máy tính của người dùng và gửi yêu cầu, dữ liệu đến một website hay một địa chỉ email nào đó. Tấn công DDoS ngày càng trở nên tinh vi và phức tạp, với 3 kiểu cơ bản:

Volume – based: dùng lưu lượng truy cập cao nhằm làm tràn ngập băng thông mạng.

Protocol: chủ yếu khai thác các tài nguyên trên máy chủ.

Application: là kiểu tấn công nguy hiểm nhất, tập trung vào các ứng dụng website.

1. **Brute Force**

Tấn công brute-force là một phương pháp bẻ khóa phổ biến . Một cuộc tấn công brute-force liên quan đến việc 'đoán' tên người dùng và mật khẩu để truy cập trái phép vào hệ thống, hacker sẽ sử dụng phương pháp thử và sai để cố gắng đoán thông tin đăng nhập hợp lệ. Ngoài ra ta có thể sử dụng brute-force để khai thác OTP, Timestamp , Cookie, vv... Tuy nhiên bài viết này sẽ tập trung vào brute-force mật khẩu để đăng nhập tài khoản người dùng.

Các cuộc tấn công này thường được tự động hóa bằng cách sử dụng danh sách các từ gồm tên người dùng và mật khẩu thường được sử dụng để có thể đạt được kết quả tốt nhất. Việc sử dụng các công cụ chuyên dụng có khả năng cho phép hacker thực hiện đăng nhập 1 cách tự động nhiều lần với tốc độ cao.

Brute-force là một phương pháp tấn công đơn giản và có tỷ lệ thành công cao. Bởi vì tùy thuộc vào độ dài và độ phức tạp của mật khẩu, việc bẻ khóa mật khẩu có thể mất từ vài giây đến nhiều năm. Do đó các trang web sử dụng phương thức đăng nhập dựa trên mật khẩu hoàn toàn có thể rất dễ bị tấn công nếu họ không thực hiện đầy đủ biện pháp bảo vệ bạo lực.

1. **Spoofing**

Spoofing là một hình thức giả mạo các nguồn đáng tin cậy như địa chỉ email, tên, số điện thoại, SMS hoặc URL trang web. Kẻ tấn công sẽ thay đổi một số yếu tố cơ bản như chữ cái, số hoặc biểu tượng của đối tượng mà họ muốn thực hiện Spoofing. Chẳng hạn như một Email Spoofing từ Netflix có tên miền giả mạo là “netffix.com”.

1. **Dos**

DoS viết tắt của cụm từ Denial of Service, là một kiểu tấn công từ chối dịch vụ khi đó máy tính của bạn sẽ bị tấn công bởi lưu lượng truy cập từ hệ thống của hacker. DoS là một cuộc tấn công trực tuyến thường nhắm vào một trang web hoặc máy chủ điển hình. Bằng cách làm quá tải tài nguyên hệ thống, tốc độ hệ thống của máy tính sẽ bị chậm lại đáng kể.

Cuộc tấn công này có thể khiến máy tính của bạn ngừng hoạt động hoặc tắt đột ngột. Khi hiện tượng này xảy ra sẽ ảnh hưởng nghiêm trọng đến hệ thống của máy tính và buộc máy tính phải tắt nguồn.

1. **Recon**

Tấn công do thám (Reconnaissance attack): Nếu như kẻ trộm trước khi đột nhập nhà gia chủ thì trước hết hắn ta phải đi thăm dò, quan sát ngôi nhà, đường đi lối lại, các điểm sơ hở. Tương tự như vậy đối với cuộc tấn công mạng kiểu thăm dò, kẻ tấn công sẽ thu thập thông tin về hệ thống định tấn công (nạn nhân), các dịch vụ đang chạy, các lỗ hổng. Các công cụ mà kẻ tấn công thường sử dụng trong kiểu tấn công này là công cụ chặn bắt gói tin (packet sniffer) và bộ quét cổng (port scannner).

1. **Web-based**

Tấn công web-based là một loại tấn công mà kẻ tấn công sử dụng các lỗ hổng trong các ứng dụng web để thực hiện các hành động không được ủy quyền hoặc gây ra các vấn đề bảo mật khác. Một trong những loại tấn công web-based phổ biến nhất là Cross-Site Scripting (XSS). Tấn công XSS là một trong những tấn công phổ biến và dễ bị tấn công nhất mà tất cả các Tester có kinh nghiệm đều biết đến.

1. **Mirai**

Mirai là phần mềm độc hại mà kẻ tấn công sử dụng để biến các thiết bị chạy trên bộ xử lý ARC thành Botnet hoặc Zombies. Trong đó, Botnet là mạng độc hại được sử dụng để khởi động các cuộc tấn công DDoS. Các phần mềm độc hại phổ biến khác như Computer Worm, Virus, Trojan Horse, Rootkit và Spyware.

1. **Dos attack với syn flood**
2. **DoS là gì?**

DoS viết tắt của cụm từ Denial of Service, là một kiểu tấn công từ chối dịch vụ khi đó máy tính của bạn sẽ bị tấn công bởi lưu lượng truy cập từ hệ thống của hacker. DoS là một cuộc tấn công trực tuyến thường nhắm vào một trang web hoặc máy chủ điển hình. Bằng cách làm quá tải tài nguyên hệ thống, tốc độ hệ thống của máy tính sẽ bị chậm lại đáng kể.

Cuộc tấn công này có thể khiến máy tính của bạn ngừng hoạt động hoặc tắt đột ngột. Khi hiện tượng này xảy ra sẽ ảnh hưởng nghiêm trọng đến hệ thống của máy tính và buộc máy tính phải tắt nguồn.

1. **Cuộc tấn công SYN Flood là gì?**

SYN flood (half-open attack) là một kiểu tấn công từ chối dịch vụ (Dos). Tấn công này với mục đích làm cho Server không có lưu lượng để truy cập hợp pháp. Bằng cách tiêu thụ tất cả tài nguyên server đang có sẵn. Người tấn công có thể áp đảo tất cả các cổng trên [Server](https://vnso.vn/thue-may-chu-rieng/). Làm cho thiết bị Client đáp ứng lưu lượng hợp pháp một cách chậm chạp.

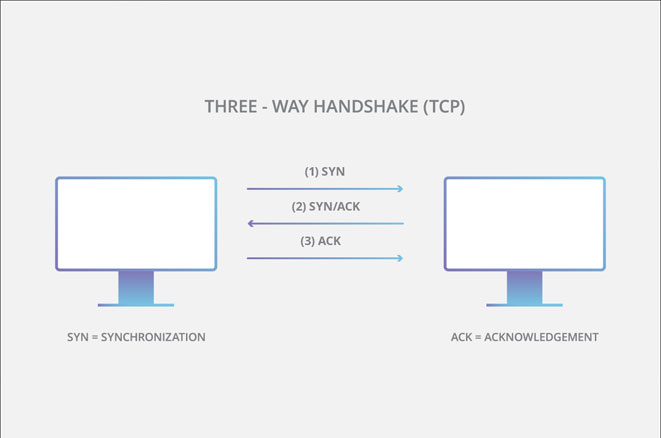
1. **Làm thế nào tấn công SYN Flood ?**

Một cuộc tấn công DDoS SYN-flood tận dụng quy trình bắt tay ba chiều TCP. Trong điều kiện bình thường, kết nối TCP được thể hiện quy trình 3 bước riêng biệt để tạo được sự kết nối như sau:

**Bước 1**: Đầu tiên, máy tấn công gửi 1 packet tin SYN đến Server để yêu cầu kết nối.

**Bước 2:** Sau khi tiếp nhận packet SYN, Server phản hồi lại máy khách bằng một packet SYN/ACK, để xác nhận thông tin từ Client.

**Bước 3:** Cuối cùng, Client nhận được packet tin SYN/ACK thì sẽ trả lời server bằng packet tin ACK báo với server biết rằng nó đã nhận được packet tin SYN/ACK, kết nối đã được thiết lập và sẵn sàng trao đổi dữ liệu.



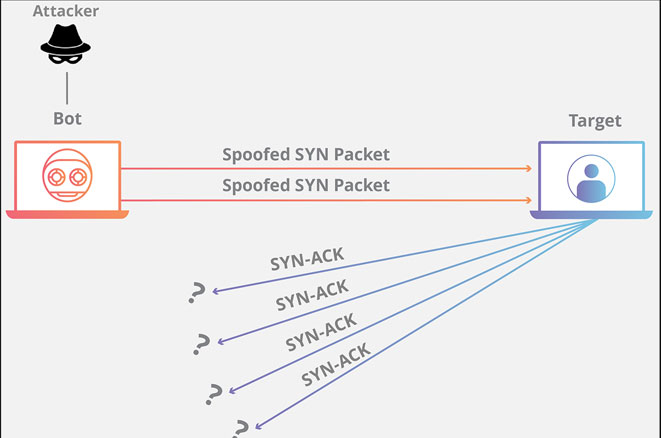
Để tạo từ chối dịch vụ (DOS), thực tế kẻ tấn công sẽ khai thác sau khi nhận được packet SYN ban đầu từ Client. Server sẽ phản hồi lại 1 hoặc nhiều packet SYN/ACK và chờ đến bước cuối cùng trong quá trình Handshake. Ở đây, cách thức thực hiện của nó như sau:

**Bước 1:** Kẻ tấn công sẽ gửi một khối lượng lớn các packet tin SYN đến Server. Được nhắm là mục tiêu và thường là các địa chỉ IP giả mạo.

**Bước 2:** Sau đó Server sẽ phản hồi lại từng yêu cầu kết nối. Để lại 1 cổng mở sẵn sàng tiếp nhận và phản hồi.

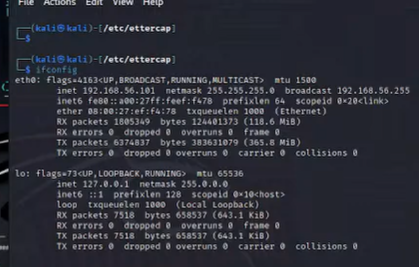
**Bước 3:** Trong khi Server chờ packet ACK ở bước cuối cùng từ Client, packet mà không bao giờ đến. Kẻ tấn công tiếp tục gửi thêm các packet SYN. Sự xuất hiện các packet SYN mới khiến [máy chủ](https://vnso.vn/thue-may-chu-rieng/) tạm thời duy trì kết nối cổng mở mới trong một thời gian nhất định. Một khi các cổng có sẵn được sử dụng thì Server không thể hoạt động như bình thường.

Trong kết nối mạng, khi Server bên này kết nối mở nhưng máy bên kia không kết nối thì được coi là half-open. Trong kiểu tấn công DDos, sau khi server gửi gói tin SYN/ACK nó sẽ phải đợi cho đến khi client trả lời. Đến khi các port trở lại bình thường. Kết quả của kiểu tấn công này được coi là cuộc tấn công half-open.



DEMO

B1: Check IP attacker and victim

* Dùng lệnh ifconfig
* IP victim Ubuntu 192.168.56.103 và ip attacker Kali-linux 192.168.56.101
* 
* Ảnh có chứa văn bản, ảnh chụp màn hình, Phông chữ

  Mô tả được tạo tự động

B2: Run apache server trên victim computer

* Dùng lệnh sudo service apache2 start để bật apache server, sudo service apache2 status để kiểm tra trạng thái của apache server.

Ảnh có chứa văn bản, ảnh chụp màn hình, phần mềm, đa phương tiện

Mô tả được tạo tự động

Ảnh có chứa văn bản, phần mềm, Phần mềm đa phương tiện, Trang web

Mô tả được tạo tự động

B3: Syn flood attack với hping 3 trên attacker computer

* Cú pháp : sudo hping3 –s –flood –V 192.5168.67.103 –p 80

Ảnh có chứa văn bản, ảnh chụp màn hình, Phông chữ

Mô tả được tạo tự động

* Bắt gói tin với wireshark thấy rằng có rất nhiều ip syn từ máy attacker đên victim và ip ask từ máy victim đến attacker

Ảnh có chứa văn bản, Phông chữ, số, ảnh chụp màn hình

Mô tả được tạo tự động

B4: Nạn nhân đã bị tấn công, lúc này truy cập vào apache server vô cùng chậm.

Ảnh có chứa văn bản, ảnh chụp màn hình, phần mềm, Website

Mô tả được tạo tự động

# **ARP Poisoning Attack với ARP spoofing**

## **Tấn công ARP Poisoning là gì?**

Address Resolution Protocol (ARP) là một quy trình kết nối liên kết địa chỉ IP với địa chỉ vật lý tĩnh của Media Access Control (MAC) qua mạng LAN. Vì địa chỉ của IP và MAC có các thành phần khác nhau nên chúng không tương thích. ARP dung hòa sự khác biệt này để đảm bảo rằng cả hai phần tử đều đồng bộ. Nếu không, chúng sẽ không nhận ra nhau.

Tấn công ARP Poisoning là một quá trình theo đó kẻ xâm nhập gửi nội dung độc hại qua mạng cục bộ (LAN) để chuyển hướng kết nối của một địa chỉ IP hợp pháp đến địa chỉ MAC của chúng. Trong quá trình này, kẻ tấn công thay thế địa chỉ MAC ban đầu sẽ kết nối với địa chỉ IP, cho phép chúng truy cập những tin nhắn mà mọi người gửi đến địa chỉ MAC xác thực.

## **Tấn công ARP Poisoning hoạt động như thế nào?**

Một số mạng có thể hoạt động trên mạng cục bộ (LAN) cùng một lúc. Mỗi mạng đang hoạt động có một địa chỉ IP cụ thể dùng làm phương tiện nhận dạng và phân biệt nó với các mạng khác. Khi dữ liệu từ các mạng khác nhau đến cổng, ARP sẽ sắp xếp chúng cho phù hợp, vì vậy mỗi mạng sẽ đi thẳng đến đích đã định.

Kẻ tấn công tạo và gửi một thông báo ARP sai đến hệ thống được định hình. Chúng thêm địa chỉ MAC của mình và địa chỉ IP của mục tiêu trong tin nhắn. Khi nhận và xử lý thông báo ARP sai, hệ thống sẽ đồng bộ địa chỉ MAC của kẻ tấn công với địa chỉ IP.

Khi mạng LAN kết nối địa chỉ IP với địa chỉ MAC của kẻ xâm nhập, kẻ xâm nhập bắt đầu nhận tất cả các thông báo dành cho địa chỉ MAC hợp pháp. Chúng có thể nghe trộm thông tin liên lạc để truy xuất dữ liệu nhạy cảm khi trao đổi, sửa đổi thông tin liên lạc bằng cách chèn nội dung độc hại hoặc thậm chí xóa dữ liệu trong khi truyền để người nhận không nhận được.

1. **Tấn công ARP spoofing**

**ARP spoofing là gì?** Ảnh có chứa ảnh chụp màn hình, văn bản, biểu đồ, bản phác thảo

Mô tả được tạo tự động

ARP spoofing là gì? ARP spoofing còn được gọi là ARP poisoning, là một cuộc tấn công Man in the Middle (MitM) cho phép những kẻ tấn công chặn giao tiếp giữa các thiết bị mạng. Cuộc tấn công sẽ diễn ra như sau:

1. Kẻ tấn công phải có quyền truy cập vào mạng. Chúng quét mạng để xác định địa chỉ IP của ít nhất hai thiết bị⁠ — giả sử đây là một máy trạm và một bộ định tuyến.

2. Kẻ tấn công sử dụng một công cụ giả mạo, chẳng hạn như Arpspoof hoặc Driftnet, để gửi phản hồi ARP giả mạo.

3. Các phản hồi giả mạo thông báo rằng địa chỉ MAC chính xác cho cả hai địa chỉ IP, thuộc bộ định tuyến và máy trạm (workstation), là địa chỉ MAC của kẻ tấn công. Điều này đánh lừa cả bộ định tuyến và máy trạm kết nối với máy của kẻ tấn công, thay vì kết nối với nhau.

4. Hai thiết bị cập nhật các mục bộ nhớ cache ARP của chúng và từ thời điểm đó trở đi, giao tiếp với kẻ tấn công thay vì trực tiếp với nhau.

5. Kẻ tấn công hiện đang bí mật đứng giữa mọi liên lạc.

DEMO

B1: Check IP attacker ,victim và router

Attacker: Kali-linux , IP: 172.20.10.3

Ảnh có chứa văn bản, ảnh chụp màn hình, phần mềm, Phần mềm đa phương tiện

Mô tả được tạo tự động

Victim: Window , IP: 172.20.10.2

Ảnh có chứa văn bản, ảnh chụp màn hình, thực đơn

Mô tả được tạo tự động

Router: IP: 172.20.10.1



B2: Tiến hành tấn công với Ettercap

* Thực hiện chọn ip cho target:

IP: 172.20.10.2 -> target 1: Victim

IP: 172.20.10.1 -> target 2: router

Ảnh có chứa văn bản, ảnh chụp màn hình, phần mềm, Phần mềm đa phương tiện

Mô tả được tạo tự động

* Tiến hành đầu độc bảng ARP của máy nạn nhân và router

Ảnh có chứa văn bản, ảnh chụp màn hình, Phần mềm đa phương tiện, phần mềm

Mô tả được tạo tự động

* Router gw ip 172.20.10.1, Mac: 08-00-27-ef-f4-78 -> Trùng với Mac của attacker -> Thành công

Ảnh có chứa văn bản, ảnh chụp màn hình, thực đơn, Phông chữ

Mô tả được tạo tự động

B3. Lấy trộm thông tin đăng nhập của victim

- Vào trang http://arduino.vn/ -> Tiến hành đăng nhậpp -> Ví dụ lấy thông password của người dùng-> Ta check thẻ html thấy form đăng nhập input password có name là "pass"

Ảnh có chứa văn bản, Trang web, phần mềm, Website

Mô tả được tạo tự động

-> Mở wireshark để bắt gói tin-> filter gói tin chứa pass với lệnh frame contains "pass" -> Như vậy thấy được pass vừa nhap : "abc" -> Thành công.

Ảnh có chứa văn bản, ảnh chụp màn hình, phần mềm, Phần mềm đa phương tiện

Mô tả được tạo tự động

1. **Mô hình học máy Random Forest**
2. **Random Forest**

Random Forest (Rừng ngẫu nhiên) là một thuật toán học có giám sát. Như tên gọi của nó, Rừng ngẫu nhiên sử dụng các cây (tree) để làm nền tảng.

Rừng ngẫu nhiên là một tập hợp của các Decision Tree, mà mỗi cây được chọn theo một thuật toán dựa vào ngẫu nhiên.

Random Forest hoạt động bằng cách đánh giá nhiều Cây quyết định ngẫu nhiên, và lấy ra kết quả được đánh giá tốt nhất trong số kết quả trả về.

**Các bước thực hiện:**

* Chọn các mẫu ngẫu nhiên từ tập dữ liệu đã cho.
* Thiết lập cây quyết định cho từng mẫu và nhận kết quả dự đoán từ mỗi quyết định cây.
* Hãy bỏ phiếu cho mỗi kết quả dự đoán.
* Chọn kết quả được dự đoán nhiều nhất là dự đoán cuối cùng.

Dự đoán:

* 1. Lấy các test features và sử dụng các Cây quyết định đã tạo ra để dự đoán kết quả, lưu nó vào một danh sách.
  2. Tính toán số lượng vote trên toàn bộ Forest cho từng kết quả
  3. Lấy kết quả có số lượng vote lớn nhất làm kết quả cuối cho mô hình

**Ảnh có chứa bản phác thảo, màu trắng, biểu đồ, hình vẽ

Mô tả được tạo tự động**

**Ưu nhược điểm của mô hình học máy Random Forest**

Ưu điểm:

Random forests được coi là một phương pháp chính xác và mạnh mẽ vì số cây quyết định tham gia vào quá trình này. Nó không bị vấn đề overfitting. Lý do chính là nó mất trung bình của tất cả các dự đoán, trong đó hủy bỏ những thành kiến. Thuật toán có thể được sử dụng trong cả hai vấn đề phân loại và hồi quy. Random forests cũng có thể xử lý các giá trị còn thiếu. Có hai cách để xử lý các giá trị này: sử dụng các giá trị trung bình để thay thế các biến liên tục và tính toán mức trung bình gần kề của các giá trị bị thiếu. Bạn có thể nhận được tầm quan trọng của tính năng tương đối, giúp chọn các tính năng đóng góp nhiều nhất cho trình phân loại.

Nhược điểm:

Random forests chậm tạo dự đoán bởi vì nó có nhiều cây quyết định. Bất cứ khi nào nó đưa ra dự đoán, tất cả các cây trong rừng phải đưa ra dự đoán cho cùng một đầu vào cho trước và sau đó thực hiện bỏ phiếu trên đó. Toàn bộ quá trình này tốn thời gian. Mô hình khó hiểu hơn so với cây quyết định, nơi bạn có thể dễ dàng đưa ra quyết định bằng cách đi theo đường dẫn trong cây.

**Các ứng dụng của Rừng ngẫu nhiên**

Chủ yếu có bốn lĩnh vực mà Rừng ngẫu nhiên chủ yếu được sử dụng:

* Ngân hàng: Lĩnh vực ngân hàng chủ yếu sử dụng thuật toán này để xác định rủi ro cho vay.
* Y học: Với sự trợ giúp của thuật toán này, các xu hướng bệnh tật và nguy cơ của bệnh có thể được xác định.
* Sử dụng đất: Chúng tôi có thể xác định các khu vực sử dụng đất tương tự bằng thuật toán này.
* Tiếp thị: Các xu hướng tiếp thị có thể được xác định bằng cách sử dụng thuật toán này.

1. Mô hình học máy Decision Tree

Cây quyết định là một cây phân cấp có cấu trúc được dùng để phân lớp các đối tượng dựa vào các dãy luật. Các thuộc tính của đối tượng có thể thuộc kiểu dữ liệu binary (nhị phân),…Đây là một trong những mô hình học máy có giám sát hoạt động hiệu quả và mạnh mẽ cho bài toán phân loại.

Ảnh có chứa văn bản, ảnh chụp màn hình, biểu đồ, Phông chữ

Mô tả được tạo tự động

Nút gốc (Root node) có được từ chọn một đặc trưng trong một dữ liệu từ tập dữ liệu dataset. Nhờ vào chỉ số đánh giá lựa chọn thuộc tính AMS để tách (Split) thành các nút quyết định (Decision node), nút quyết định có đặc trưng và điều kiện tách. Phân tách tạo các nút con (child node) và lặp lại như trên cho đến khi có nút lá (Leaf node).

Ảnh có chứa văn bản, chữ viết tay, Hình chữ nhật, Phông chữ

Mô tả được tạo tự động

Một mô hình Decision Tree trong Machine Learning giúp chúng ta quan sát một cây (tree) phát triển. Các thước đo cơ bản đánh giá mô hình Decision tree:

Entropy là thang đo độ nhiễu của một mẫu dữ liệu. Giá trị của entropy càng cao thì độ nhiễu loạn của mẫu dữ liệu càng lớn, nếu entropy càng thấp thì mẫu dữ liệu hoạt động có trật tự. Mẫu dữ liệu phân nhánh càng thuận lợi. Để đo độ giảm của entropy ta sử dụng Information Gain.

Gini Impurity là thang đo độ phân loại sai khi ta chọn ngẫu nhiên một phần tử từ tập dữ liệu. Để đo độ giảm của Gini Impurity ta sử dụng Gini Gain tương tự như Information Gain.

Mô hình Decision Tree huấn luyện lựa chọn các tham số tối ưu thường bỏ qua Entropy và Gini Impurity do không ảnh hưởng đến độ chính xác của mô hình. Một hạn chế của mô hình đó là thiếu tính khách quan vì chỉ có một cây quyết định và độ sâu của cây lớn quá thì mô hình sẽ Overfitting.

1. Các thang đo độ chính xác của mô hình học máy

Ta xây dựng các điều kiện sau đây: Condition Positive (P) là tổng số sinh viên không thuộc diện cảnh báo, Condition Negative (N) là tổng số sinh viên thuộc diện cảnh báo.

True Positive (TP) là số sinh viên dự báo không thuộc diện cảnh báo hay không thuộc diện cảnh báo thật, True Negative (TN) là số sinh viên dự báo thuộc diện cảnh báo hay diện cảnh báo thật, False Positive (FP) là số sinh viên dự báo không thuộc diện cảnh báo giả, False Negative (FN) là số sinh viên dự báo thuộc diện cảnh báo giả.

Thang đo độ chính xác

***Độ chính xác Accuracy:***là tỉ lệ số sinh viên dự báo đúng bao gồm số sinh viên thuộc diện không bị cảnh báo thật và số sinh viên thuộc diện cảnh báo thật trên tổng số sinh viên được khảo sát trong tập dữ liệu ( hay ta hiểu là cách các giá trị đo gần giá trị đích). Công thức tính là:



Ảnh có chứa ảnh chụp màn hình, biểu đồ, vòng tròn, thiết kế

Mô tả được tạo tự động

***Độ chính xác Precision:*** là tỉ lệ số sinh viên không thuộc diện cảnh báo mô hình dự đoán đúng trên tổngsố sinh viên mô hình dự báo là không thuộc diện cảnh báo (TP+FP) (hayta hiểulà khi các giá trị của các phép đo lặp lại được nhóm lại gần nhau và có độ phân tán thấp).



***Độ chính xác Recall:*** là tỉ lệ số sinh viên không thuộc diện cảnh báo mô hình dự báo đúng trên tổng số sinh viên thực sự không thuộc diện cảnh báo.



Chỉ dùng Precision khi đó mô mình chỉ đưa ra dự đoán cho sinh viên không thuộc diện cảnh báo. Khi đó Precision=1, tuy nhiên không thể nói là mô hình này tốt. Hay chỉ dùng Recall, nếu mô hình dự đoán tất cả đều là sinh viên không thuộc diện cảnh báo tức là Recall=1 tuy nhiên ta cũng không thể nói đây là mô hình tốt. Khi đó F1\_score được dử dụng, F1\_score là trung điều hoà (harmonic mean) của Precision và Recall.

***Độ chính xác F1\_score:***



Thang đo hiệu suất

Ma trận nhầm lẫn (Confusion matrix) là một kỹ thuật đo lường hiệu suất phổ biến nhất trong các mô hình phân loại. Ta có ma trận nhầm lẫn:

Confusion Matrix = 

# **V. Trích xuất dữ liệu và xây dựng mẫu máy học**

## **1. Trích xuất dữ liệu**

Ảnh có chứa văn bản, ảnh chụp màn hình, thực đơn, thiết kế

Mô tả được tạo tự động

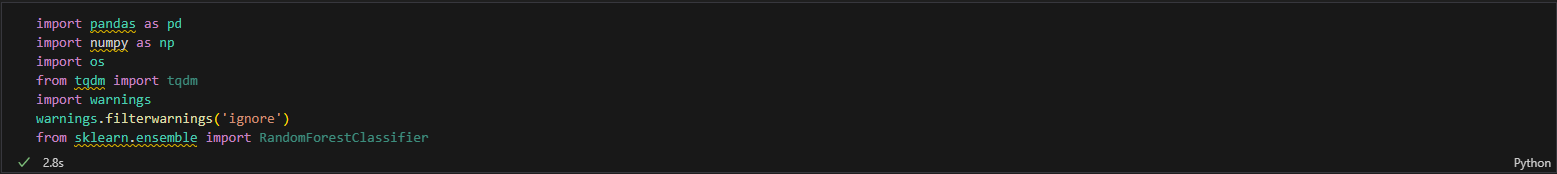
Kích thước: (378199, 47)

**Thông tin về gói tin:**

1. **flow\_duration**: Đây là thời gian tồn tại của một luồng dữ liệu, tính bằng giây hoặc một đơn vị thời gian khác. Thường được sử dụng để đo lường khoảng thời gian mà luồng gói tin được duy trì.
2. **Header\_Length**: Độ dài của phần đầu (header) trong gói tin, thường được đo lường bằng byte. Thông tin này có thể ám chỉ mức độ phức tạp của gói tin và có thể liên quan đến loại giao thức được sử dụng.
3. **Protocol Type**: Trường này chỉ ra loại giao thức mạng được sử dụng trong gói tin, ví dụ: TCP, UDP, ICMP, ARP, và các loại khác.
4. **Duration**: Thời gian tồn tại của sự kiện hoặc gói tin, thường được đo lường từ thời điểm bắt đầu đến kết thúc của sự kiện.
5. **Rate, Srate, Drate**: Các tỷ lệ liên quan đến lưu lượng mạng. Thường bao gồm tỷ lệ gửi, tỷ lệ nhận, và tỷ lệ tổng cộng, được tính bằng gói tin mỗi giây hoặc các đơn vị khác tùy thuộc vào ngữ cảnh.
6. **fin\_flag\_number, syn\_flag\_number, ...**: Số lần xuất hiện của các cờ (flags) trong gói tin. Cờ thường đại diện cho các trạng thái như kết nối, đồng bộ hóa, kết thúc, và các sự kiện khác.
7. **HTTP, HTTPS, DNS, Telnet, ...**: Số lần xuất hiện của các loại giao thức trong lưu lượng mạng. Được sử dụng để đo lường tần suất xuất hiện của các dạng giao thức khác nhau.
8. **Tot sum, Min, Max, AVG, Std**: Các thống kê mô tả về giá trị của một thuộc tính nào đó. Bao gồm tổng giá trị, giá trị nhỏ nhất, giá trị lớn nhất, giá trị trung bình, và độ lệch chuẩn.
9. **Tot size**: Tổng kích thước của dữ liệu, thường được đo lường bằng byte. Cho biết dung lượng tổng cộng của gói tin hoặc sự kiện.
10. **IAT (Inter-Arrival Time)**: Thời gian giữa các sự kiện liên tục. Được sử dụng để đo lường tần suất xuất hiện của các sự kiện.
11. **Number, Magnitude, Radius, Covariance, Variance, Weight**: Các thống kê mô tả khác về phân phối hoặc đặc điểm của dữ liệu. Các giá trị này có thể cung cấp thông tin về độ biến động, mối quan hệ giữa các thuộc tính, và trọng số của chúng.

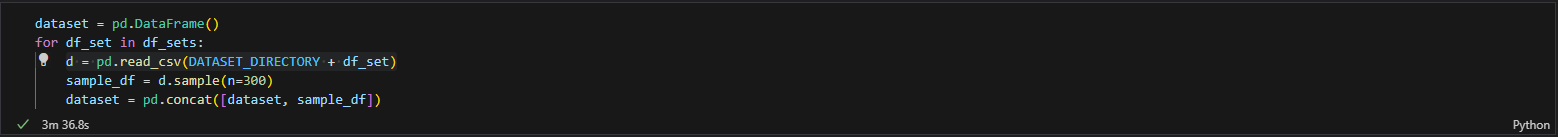
## **2, Tạo dữ liệu cho việc train mô hình**

Import các thư viện cần thiết

Ảnh có chứa văn bản, Phần mềm đa phương tiện, phần mềm, Phần mềm đồ họa

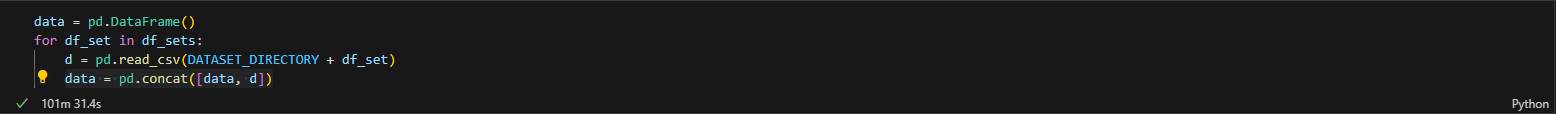
Mô tả được tạo tự động

Random từ mỗi file csv lấy 300 dòng dữ liệu

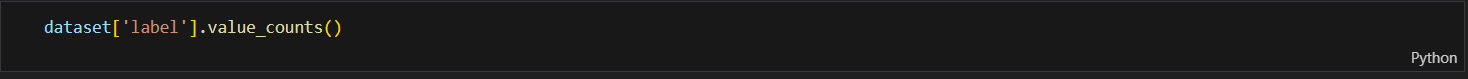
Ảnh có chứa ảnh chụp màn hình, văn bản, Phần mềm đa phương tiện, phần mềm

Mô tả được tạo tự động

Đọc tất cả dữ liệu của 169 file



Dữ liệu ban đầu có sự chênh lệch giữa các giá trị dẫn đến mất cân bằng dữ liệu

Ảnh có chứa văn bản, ảnh chụp màn hình, thực đơn

Mô tả được tạo tự động

Lưu tất cả các giá trị của trường label vào list

Ảnh có chứa văn bản, phần mềm, Phần mềm đa phương tiện, Phông chữ

Mô tả được tạo tự động

Tiến hành cân bằng dữ liệu

Ảnh có chứa văn bản, Phần mềm đa phương tiện, phần mềm, ảnh chụp màn hình

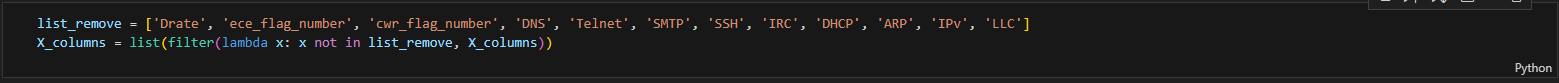
Mô tả được tạo tự động

Dữ liệu sau khi được cân bằng

Ảnh có chứa văn bản, ảnh chụp màn hình, thực đơn

Mô tả được tạo tự động

Xóa các trường không ảnh hưởng đến việc train mô hình ra khỏi dataframe



Lưu dữ liệu vào file ‘dataset.csv’



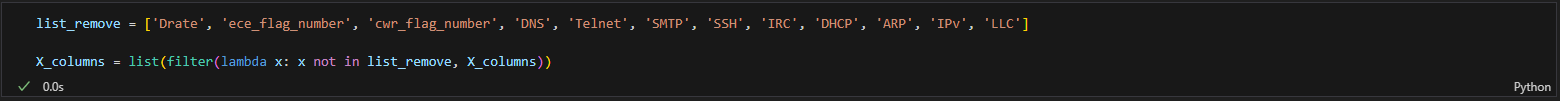
## **3,** **Huấn luyện mô hình**

Đọc dữ liệu từ fie ‘dataset.csv’



Ảnh có chứa văn bản, Phần mềm đa phương tiện, phần mềm, Phần mềm đồ họa

Mô tả được tạo tự động



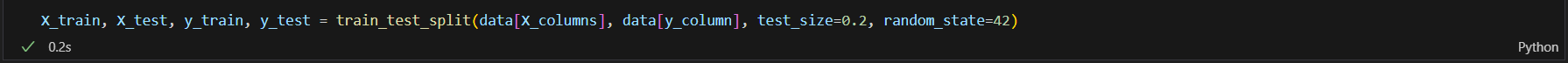
Tìm ra tham số tốt nhất cho mô hình RandomForestClassifier()

* n\_estimators: Số lượng cây trong rừng. Một giá trị lớn hơn sẽ tăng độ chính xác nhưng tốn thời gian tính toán.
* max\_depth: Độ sâu tối đa của cây. Nếu không được thiết lập, các cây sẽ được phát triển đến khi các lá chỉ chứa 1 điểm dữ liệu hoặc khi không còn cách nào để phân chia dữ liệu.

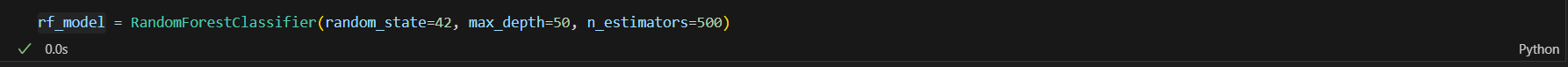
Ảnh có chứa văn bản, Phần mềm đa phương tiện, phần mềm, ảnh chụp màn hình

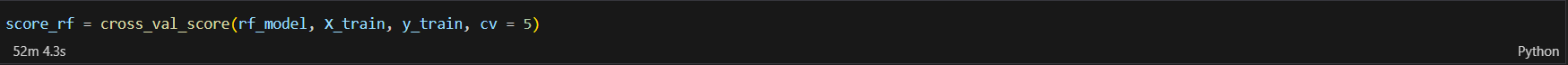
Mô tả được tạo tự động

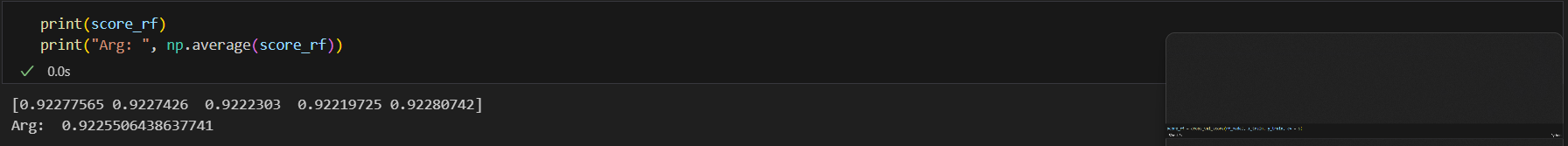
Chia dữ liệu



Xây dựng model Random Forest







Train mô hình học máy và in kết quả dự đoán

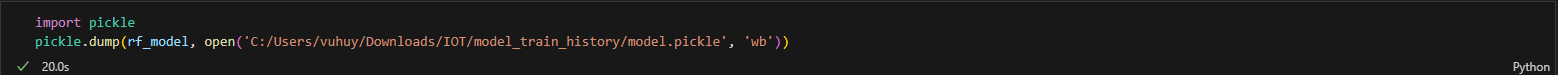
Ảnh có chứa văn bản, ảnh chụp màn hình, phần mềm, Phần mềm đa phương tiện

Mô tả được tạo tự động

Ảnh có chứa văn bản, ảnh chụp màn hình, thực đơn

Mô tả được tạo tự động

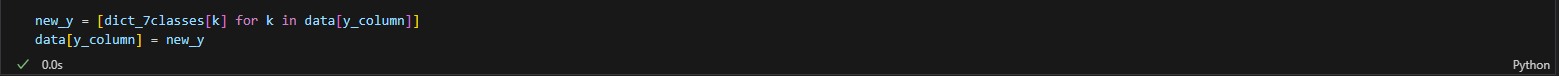
Lưu mô hình 34 classes



Phân loại tấn công

Ảnh có chứa ảnh chụp màn hình, văn bản, màn hình

Mô tả được tạo tự động



Train mô hình học máy

Ảnh có chứa văn bản, ảnh chụp màn hình, phần mềm, Phần mềm đa phương tiện

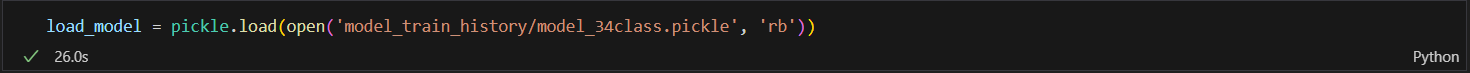
Mô tả được tạo tự động

Lưu mô hình

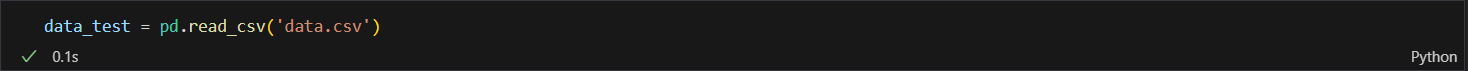


1. **Load mô hình học máy và xác định phương thức tấn công**

Load model



Đọc dữ liệu từ 1 file tấn công



Dự đoán

Ảnh có chứa văn bản, phần mềm, Phần mềm đa phương tiện, ảnh chụp màn hình

Mô tả được tạo tự động

Ảnh có chứa văn bản, ảnh chụp màn hình, Phông chữ

Mô tả được tạo tự động

# **TÀI LIỆU THAM KHẢO**

[1] <https://scikit-learn.org/stable/modules/generated/sklearn.preprocessing.StandardScaler.html>

[2] Bhuvaneswari Gopalan, What is Gini Impurity? How is it used to construct decision trees?, Dec 11, 2020, <https://www.numpyninja.com/post/what-is-gini-impurity-how-is-it-used-to-construct-decision-trees>

[3]Anshul Saini, An Introduction to Random Forest Algorithm for beginners, August 26th, 2022, <https://www.analyticsvidhya.com/blog/2021/10/an-introduction-to-random-forest-algorithm-for-beginners/>

[4] Dr. Mahesh Huddar, Build Decision Tree using Gini Index Solved Numerical Example Machine Learning, 29 tháng 1 năm 2022, <https://www.youtube.com/watch?v=zNYdkpAcP-g&t=5s>

[5] Josh Starmer, Decision and Classification Trees, Clearly Explained!!!, 26 tháng 4 năm 2021 <https://www.youtube.com/watch?v=_L39rN6gz7Y>