**GIẢI PHÁP CẢNH BÁO SỚM TẤN CÔNG**

**DỰA VÀO PHÂN TÍCH LOG**

Thạc sĩ : Lê Ngọc Hiếu\*, Nguyễn Đức Huy\*\*, Ts Nguyễn Hồng Sơn\*\*\*,

Nguyễn Thị Thanh Hằng\*\*\*\*, Nguyễn Thị Yến Khương\*\*\*\*\*

1. **TÓM TẮT**

Với xu hướng công nghệ phát triển mạnh mẽ ở hầu hết các lĩnh vực như hiện nay, bảo mật và an toàn thông tin vẫn luôn là một trong những chủ đề được nhiều người quan tâm và tập trung nghiên cứu nhằm tìm ra giải pháp để đảm bảo sự an toàn cho các hệ thống thông tin, hạn chế tối đa những thiệt hại đến sự phát triển và tồn tại của doanh nghiệp. Đứng trước thách thức lớn nhất hiện nay là tội phạm an ninh mạng có thể xâm nhập vào hệ thống thông tin của doanh nghiệp vào bất kì lúc nào , bài toán đặt ra là làm sao để các doanh nghiệp có thể chủ động bảo vệ thông tin, thúc đẩy tính riêng tư của dữ liệu và người dùng, giúp doanh nghiệp có chiến lược đúng đắn về bảo mật và an toàn thông tin trong hoạt động kinh doanh . Nếu một hệ thông quản lý thông tin không vững chắc thì sẽ tạo cơ hội cho tội phạm công nghệ cao hoạt động, gây ra những tổn hại rất lớn đến sự phát triển và tồn tại cho các tổ chức , doanh nghiệp. Chính vì vậy, đề tài “ ***Giải pháp cảnh báo sớm tấn công dựa vào phân tích LOG*** “ được đưa ra để cảnh báo và phát hiện sớm khi có bất kì dấu hiệu bất thường nào đối với hệ thống thông tin của các tổ chức, doanh nghiệp .Giải pháp này được thực hiện dựa trên phương pháp phân tích các cuộc tấn công có chủ đích APT và xử lý tách các dữ liệu Logs và kết hợp thuật toán AI, cụ thể là Machine Learning – Deep Leanring.

**Từ khóa** : Bảo mật và an ninh mạng, Tấn công có chủ đích APT ,” Giải pháp cảnh báo sớm tấn công dựa vào phân tích LOG” , Trí tuệ nhân tạo (AI), Machine Learning – Deep Learning.

1. **MỞ ĐẦU:**

Cùng với xu hướng phát triển mạnh mẽ của cuộc cách mạng Công nghiệp 4.0 như hiện nay, mạng Internet ngày càng được chứng minh là một “huyết mạch” quan trọng không thể thiếu đối với cuộc sống con người nói chung và trong Công nghệ nói riêng. Bên cạnh những ưu điểm và lợi thế, Internet cũng đem đến không ít những rủi ro cho các doanh nghiệp và các tổ chức thông qua hệ thống mạng.

Thực tế cho thấy, tình hình tấn công mạng hiện nay ngày càng phát triển với mức độ nguy hiểm cũng theo đó mà tăng lên từng ngày. Mỗi ngày trên Thế giới phải đối mặt với hàng nghìn cuộc tấn công liên quan đến vấn đề bảo mật và an ninh mạng, gây thiệt hại hàng nghìn tỷ USD do các vụ đánh cắp dữ liệu hoặc tấn công vào các hệ thống thông tin trọng yếu của các doanh nghiệp và tổ chức. Theo thống kê từ VNCERT, tính đến ngày 25/6/2018, hệ thống đã ghi nhận 1.122 sự cố tấn công lừa đảo, 3.200 sự cố tấn công thay đổi giao diện và 857 sự cố phát tán mã độc Malware trên Website. Các mối đe dọa này tập trung vào hai nhóm chính là đánh cắp thông tin nhạy cảm từ các tổ chức, cá nhân, ngân hàng và cài mã độc tống tiền, đảo tiền ,v.v… bằng tấn công có chủ đích APT(Advanced Persistent Threat) ­– một trong số các phương thức tấn công được thực hiện bởi tội phạm an ninh mạng công nghệ cao là các tấn công có chủ đích APT. Với các kỹ thật tinh vi , mục tiêu chính của tấn công APT là đột nhập vào hệ thống để đạt được quyền truy cập liên tục , đánh cắp dữ liệu nhiều hơn là gây thiệt hại cho hệ thống mạng hoặc các tổ chức, theo đó APT thường nhắm đến các tổ chức trong các ngành có thông tin giá trị cao như quốc phòng , sản xuất và công nghiệp tài chính . Việc ngăn ngừa toàn diện các cuộc tấn công có chủ đích APT hiện nay còn gặp nhiều khó khăn dù các tổ chức, doanh nghiệp vẫn chi hàng tỷ USD mỗi năm cho công tác phòng chống.

Từ thực tế trên và nhận thấy tầm quan trọng của việc đảm bảo an ninh mạng trước các đợt tấn công APT ngày càng bùng phát, “Giải pháp cảnh báo sớm tấn công dựa vào phân tích LOG” được nghiên cứu nhằm cảnh báo sớm đến người quản trị về loại tấn công APT dựa vào hệ thống LOGS. Giải pháp này được thực hiện dựa trên phương pháp phân tích các cuộc tấn công có chủ đích APT và xử lý tách các dữ liệu Logs và kết hợp thuật toán AI, cụ thể là Machine Learning – Deep Leanring để phân tích dữ liệu ,mang lại hiệu quả cao trong việc cảnh báo sớm tấn công được nhanh và chính xác hơn.

1. **CÁC CÔNG TRÌNH NGHIÊN CỨU LIÊN QUAN**
2. *Các công trình nghiên cứu quốc tế*.

Đã có rất nhiều các công trình nghiên cứu về các cuộc tấn công có chủ đích APT được thực hiện nghiên cứu bởi các nhà khoa học nổi tiếng trên Thế Giới , trong đó có thể kể đến các công trình nghiên cứu đạt kết quả tiêu biểu như sau.

Đầu tiên, , các ví dụ về APT được cung cấp trong đề tài “Assessing Outbound Traffic to Uncover Advanced Persistent Threat” [1] năm 2011 bởi tác giả Beth E. Binde, Russ McRee, dựa trên các tiền đề là : xác định và mô tả mối đe dọa dai dẳng (APT), ddề xuất phương pháp kỹ thuật để giảm thiểu mối đe dọa ,bao gồm các công cụ hữu ích trong việc phát hiện APT có thể.

Nart Villeneuve and James Bennett đã thảo luận về cách các kỹ thuật phát hiện tiên tiến có thể được sử dụng để xác định các liên lạc ra lệnh và điều khiển phần mềm độc hại liên quan đến các cuộc tấn trong bài nghiên cứu “Detecting APT Activity with Network Traffic Analysis” [2] được đưa ra vào năm 2012 . Bài viết này tập trung vào việc sử dụng trí thông minh mối đe dọa này để phát hiện hoạt động APT với phân tích lưu lượng mạng.

Năm 2014, trong nghiên cứu “Advanced persistent threat detection” [3] , một loạt các kỹ thuật được tiết lộ để phát hiện các mối đe dọa dai dẳng và phần mềm độc hại đã được đưa ra Tác giả đã xem xét ở nhiều khía cạnh khác nhau đề đưa ra những kết luận về cách thức để phát hiện sự xuất hiện của các phần mềm độc hại.

Tiếp theo là nghiên cứu “Advanced Persistent Threat Detection Based On Network Traffic Noise Pattern and Analysis” [4] của tác giả S. C. Y. Ng \*,a and M. Bakhtiarib được đưa ra năm 2016. Ở đề tài nghiên cứu này , tác giả nhằm vào các góc độ khác nhau để phát hiện tấn công APT bằng cách tập trung vào các khu vực khác nhau bên cạnh các lỗ hổng Zero-Day, với thành tựu đạt được là bằng chứng về kết nối và mô hình lưu lượng của từng chức năng tấn công được ghi lại trong các công cụ giám sát lưu lượng. Công việc trong tương lai của nghiên cứu này là triển khai khung đề xuất với mạng máy tính thực tế với các thiết bị ngoại vi mạng thực và hệ thống máy tính thực thay vì môi trường ảo. Bên cạnh đó, nghiên cứu này nhằm phân tích kỹ thuật của Knock Onock được hacker sử dụng để liên lạc với C&C Server theo yêu cầu.

Năm 2018, trong đề tài nghiên cứu “Advanced Persistent Threat Analysis using Splunk” [5] của tác giả Harikrishnan V N và Gireesh Kumar T , tác giả đã phân tích các APT bằng cách sử dụng Splunk-Security Information and Event Management (SIEM), và dựa trên kết quả phân tích được , tác giả đã phát triển một tập hợp các tính năng mà mọi APT đều có chúng. Bên cạnh đó, tác giả cũng đang đề xuất một cách tiếp cận hiệu quả để xác định sự hoàn thiện của APT này bằng cách sử dụng công nghệ hiện đại được gọi là bộ công cụ học máy.

Theo nghiên cứu của Kaspersky Lab , hai tác giải Artur Rot và Boguslaw Olszewski trong bài bài báo về “Advanced Persistent Threats Attacks in Cyberspace. Threats, Vulnerabilities, Methods of Protection” [6] đã trình bày hiện tượng APT và lấp đầy những khoảng trống trong tài liệu chủ đề về mối nguy hiểm của APT đối với thực tế đối với bất kỳ tổ chức và công ty nào, và phương pháp và phương tiện phòng thủ chống lại các cuộc tấn công. Các tác giả cũng đã trình bày một mô hình phòng thủ nhiều lớp hiệu quả.

Một cách tiếp cận sáng tạo có khả năng phân tích khối lượng mạng lớn nhất định để phát hiện các tín hiệu yếu liên quan đến các dữ liệu và các hoạt động APT đáng ngờ khác đã được đưa ra trong bài báo “Analysis of high volumes of network traﬃc for Advanced Persistent Threat detection” [7]. Kết quả nghiên cứu này c cho phép các chuyên gia bảo mật tập trung phân tích của họ vào một nhóm máy chủ nhỏ trong số hàng ngàn máy móc đặc trưng cho các tổ chức lớn.

Trong bài hướng dẫn “Cyber Security Monitoring and Logging Guide”[8] đã trình bày chi tiết về cách giám sát và ghi nhật ký các sự kiện an ninh mạng . Nó cung cấp cho bạn lời khuyên thiết thực về cách quản lý nhật ký hiệu quả, xử lý các sự kiện đáng ngờ, sử dụng trí thông minh an ninh mạng và giải quyết các thách thức. Nó được thiết kế để cho phép bạn ưu tiên và quản lý vô số nhật ký sự kiện; xây dựng một quy trình giám sát an ninh mạng hiệu quả và tìm hiểu về nơi và cách bạn có thể nhận trợ giúp.

1. *Các công trình nghiên cứu và các bài báo ở Việt Nam.*

Ở Việt Nam , chủ yếu các công trình nghiên cứu trong nước được áp dụng kế thừa từ các công trình nghiên cứu quốc tế , sử dụng các công nghệ Pattern recognition kết hợp Machine learning để phát hiện các cuộc tấn công hệ thống mạng với sự hỗ trợ cảnh báo đắc lực của Syslogs. Nhiều giải pháp xây dựng một hệ thống cảnh báo xâm nhập trên thực tế đã được triển khai rất hiệu quả và được đánh giá cao. Tuy nhiên các giải pháp này chỉ triển khai hệ thống trên một phân đoạn mạng nhỏ, nên chưa đánh giá được hết hiệu suất của hệ thống và các vấn đề hệ thống cảnh sẽ gặp phải khi triển khai thực tế, các mẫu nhận dạng chưa đầy đủ, các loại tấn công đa dạng và xuất hiện mới các phương thức tấn công ngày càng nhiều.

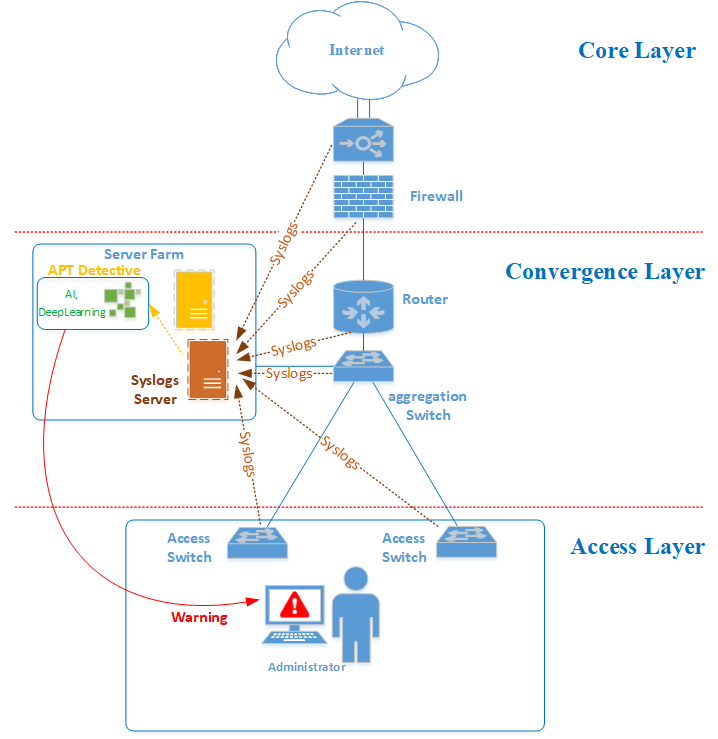
Hiệu quả của các hệ thống này đóng góp rất nhiều vào việc đảm bảo an toàn an ninh mạng tại các doanh nghiệp , nhưng cần rất nhiều chi phí lẫn nhân công ban đầu để xây dựng và triển khai hệ thống . Bên cạnh đó , yêu cầu đặt ra là cần kế thừa các nghiên cứu cần có, nghiên cứu thêm những công nghệ mới để có thể xây dựng ra 1 ứng dụng có khả năng thông báo đến các nhà quản trị, cảnh báo trước các tất công có thể xảy ra dựa vào các dấu hiệu bất thường, các hành động trinh sát của kẻ tấn công trong mạng cục bộ - điều mà các nhà quản trị, doanh nghiệp thực sự cần vì tính cấp thiết mà ứng dụng mang lại.

1. **ĐỀ XUẤT:**

Mục tiêu của đề tài này không chỉ nhằm mô tả về ứng dụng đề xuất, mà còn tiến hành xây dựng mô hình thu thập dữ liệu Logs đầu vào và đầu ra để cảnh báo sớm tấn công APT dựa vào hệ thống Logs (Logs ở thiết bị mạng). Nhờ áp dụng AI, cụ thể là Machine Learning – Deep Leanring để có thể mang lại hiệu quả cao trong việc cảnh báo sớm tấn công được nhanh và chính xác hơn.

1. *Mô hình và phạm vi thu thập dữ liệu*
   1. *Mô tả mô hình*

* Lớp Core Layer: Lớp này bao gồm các thiết bị mạng core như Router Loadbalancing và Firewall.
* *Lớp Access Layer*: Tại đây người dùng kết nối vào hệ thống mạng qua các thiết bị Switch Access.
* *Lớp Convergence Layer*: Lớp này bao gồm các thành phần mạng như vùng DMZ, Router Lớp 3 để định tuyến, thiết bị Switch trung tâm có khả năng chịu tải lưu lượng lớn, và vùng Server Farm.
* *Server thu thập Logs:* Được đặt tại vùng Server Farm, các thành phần Logs từ các Host, các Device, các node mạng,… sẽ được tập trung về Server này.
* *Ứng dụng đề xuất:* Đặt tại vùng máy chủ, tại đây là nơi tập trung các dữ liệu Logs được thu về, từ đó ta có thể dễ dàng kết nối và phân tích Logs.



Hình 1 : Mô hình nghiên cứu hệ thống mạng

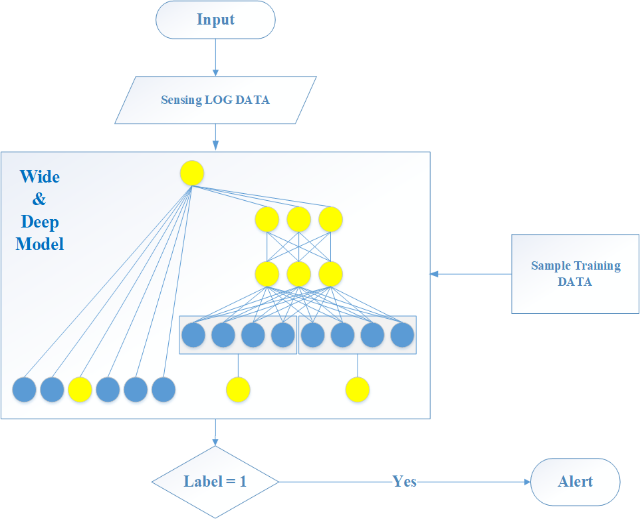
* 1. *Phạm vi thu thập dữ liệu*
* Đầu vào: dữ liệu Logs được lấy từ nguồn là các thiết bị mạng. Server Syslogs có nhiệm vụ thu thập dữ liệu đầu vào ở dạng thô và phân loại, định nghĩa lại và đồng nhất nội dung để hệ thống xử lý.
* Kỹ thuật xử lý: Sử dụng bộ dữ liệu Logs lấy được dựa trên tính chất tiền tấn công APT để huấn luyện, từ đó ứng dụng Deep Learning để nhận biết các dòng Logs có dấu hiệu tiền tấn công APT, từ đó đưa ra cảnh báo sớm tấn công.
* Đầu ra: Sau khi ứng dụng đã xử lý, hệ thống sẽ trả về kết quả là có dấu hiệu tấn công sớm của APT, từ đó có thể gửi các cảnh báo đến người dùng qua các công cụ thông báo như E-mail, SMS,…

1. *Đề xuất xây dựng các mức cảnh báo tấn công*:

Từ các dấu hiệu nhận biết trên, hệ thống sẽ đưa ra các mức cảnh báo phù hợp đến người quản trị.

* Cảnh báo dựa vào lưu lượng mạng: Trong 1 thời gian ngắn có lưu lượng lớn được ghi Logs lại, hoặc tồn tại một gói tin được nhận có dung lượng lớn (BigSize)
* Cảnh báo dựa vào truy cập bất thường: Telnet, SSH, Remote Destop
* Các công cụ dò quét hệ thống: Ping, Tracer, Nmap Trace

Để có thể đưa ra được các mức cảnh báo trên, hệ thống cần có các module hỗ trợ xử lý để có thể phân tích và đưa ra kết quả chuẩn xác nhất. Các module chính mà hệ thống sử dụng bao gồm: Module đọc Logs và xử lý dữ liệu; Module xử lý dữ liệu; Module cảnh báo. Trong đó, module Đọc Logs và xử lý dữ liệu có chức năng đọc Logs và đưa vào cơ sở dữ liệu của ứng dụng. Sau đó, Logs này sẽ được hiệu chỉnh và chỉ lưu lại những luồng dữ liệu đã được lọc theo cấu hình trước, tức là phải có dấu hiệu cần lưu lại mới lưu vào LOG. Tiếp theo, dựa trên 3 mức cảnh báo được nêu trên của APT, module xử lý dữ liệu bằng cách sử dụng thuật toán Deep Learning kết hợp với mạng Neuron học sâu để phân lớp ra các lớp có các nguy cơ tấn công, nhiễm virus hay bị Trojan. Cuối cùng là module Cảnh báo sẽ sử dụng thuật toán dựa vào kết quả từ học sâu (Deep Learning) ở Module 2, ta có kết quả mức cảnh báo gồm 4 cấp độ, bắt đầu từ thông báo, nhắc nhở, cảnh báo và cuối cùng là báo động.



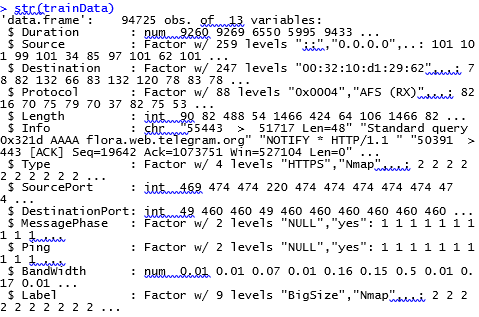
Hình 2 : Sơ đồ mô tả giải thuật đề xuất

Với việc đề xuất ứng dụng cảnh báo tấn công dựa vào phân tích Logs, đề tài này hướng tới xây dựng một hệ thống có khả năng nhận biết mối nguy hiểm trước khi cuộc tấn công xảy ra để cảnh báo đến người quản trị một cách sớm nhất. Bên cạnh đó với việc áp dụng thuật toán thông minh đề xuất là AI, Machine Learning – Deep Learning trong xử lý các file Logs dữ liệu thô để phân tích thống kê sẽ giúp cho người quản trị có công cụ hỗ trợ đắc lực, cũng như mở ra hướng phát triển sâu hơn về Trí tuệ nhân tạo và Máy học trong an toàn thông tin, hướng đến độ chính xác cao và hoàn thiện bộ dữ liệu mẫu.

1. **KẾT QUẢ:**

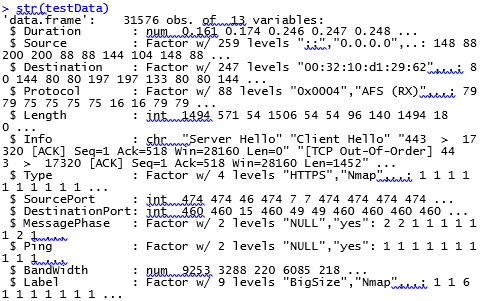
# *Thực nghiệm và kết quả mô phỏng.*

1. Mô tả thực nghiệm như sau:
   * Ta lấy 75% số lượng LOG có trong tập log đã thu thập được tạo thành tập dữ liệu ***huấn luyện*** (trainData).



Hình 3: Tập dữ liệu ***huấn luyện*** (trainData) từ 75% số lượng LOG đã thu thập được.

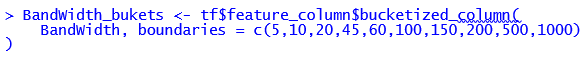
* + Ta lấy 25% số lượng LOG còn lại, làm tập ***test***.



Hình 4: Tập ***test*** từ 25% số lượng LOG còn lại

1. *Kết quả chạy thực nghiệm trên R-Studio như sau:*

* Phân chia BandWidth:



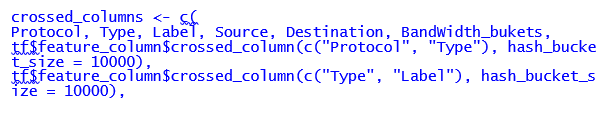
Hình 5

* Tạo các cột cơ bản:



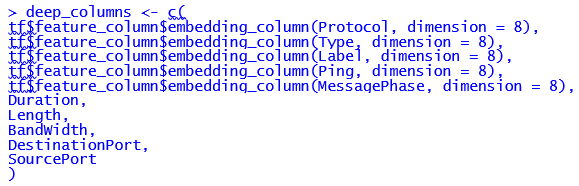
Hình 6

* Tạo các cột và chiều dữ liệu có ảnh hưởng:



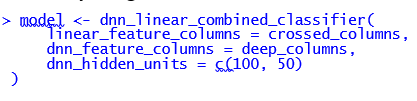
Hình 7.

* Tạo các cột có deep Features:



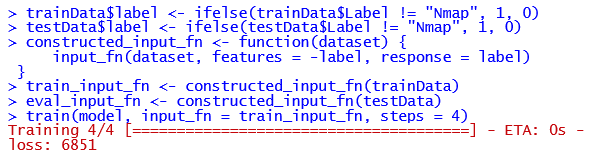
Hình 8

* Xây dựng mô hình



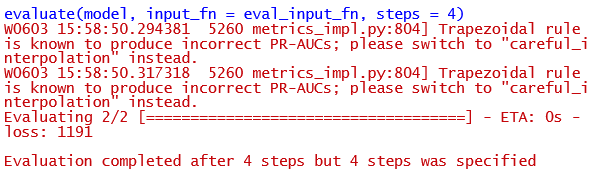
Hình 9

* Cho máy học, huấn luyện



Hình 10.

* Kết quả đạt được :



Hình 11.

* Nhận xét kết quả đạt được:
* Như vậy trong tập test, ta có khoảng 1191 dòng log mà không phù hợp và loại ra, tỷ lệ không hợp lệ là 1191 / 31.576
* Như vậy trong tập train, ta có khoảng 6851 bị sai trên tổng số 94.725 dòng dữ liệu log, đạt tỉ lệ sai là 6851 / 94.725
* Khi thay đổi tỷ lệ giữa dữ liệu test và huấn luyện là 80% - 20% :
  + Ta lấy 80% số lượng LOG có trong tập log đã thu thập được tạo thành tập dữ liệu ***huấn luyện*** (trainData)
  + Ta lấy 20% số lượng LOG còn lại, làm tập ***test***.
* Kết quả đạt được:
* Như vậy trong tập test, ta có khoảng 1501 dòng log mà không phù hợp và loại ra, tỷ lệ không hợp lệ là 1501 / 25.260
* Như vậy trong tập train, ta có khoảng 6134 bị sai trên tổng số 101.041 dòng dữ liệu log, đạt tỉ lệ sai là 6134 / 101.041
* Khi thay đổi tỷ lệ giữa dữ liệu test và huấn luyện là 70% - 30% :
  + Ta lấy 70% số lượng LOG có trong tập log đã thu thập được tạo thành tập dữ liệu ***huấn luyện*** (trainData)
  + Ta lấy 30% số lượng LOG còn lại, làm tập ***test***.

**Kết quả đạt được:**

* Như vậy trong tập test, ta có khoảng 2410 dòng log mà không phù hợp và loại ra, tỷ lệ không hợp lệ là 2430 / 37.890
* Như vậy trong tập train, ta có khoảng 5652 bị sai trên tổng số 88.411 dòng dữ liệu log, đạt tỉ lệ sai là 5652 / 88.411

# *Mô tả ứng dụng đề xuất.*

Ứng dụng đề xuất là ứng dụng được cài đặt trên web có tích hợp các module được mô tả ở trên, trong đó phần xử lý dữ liệu và học máy, ở đây là *Wide and Deep Learning* sẽ được tích hợp bằng Python library vào phần Backend. Ứng dụng đề xuất chạy trên môi trường Internet hoặc Intranet để xứ lý, cấu hình các tính năng của ứng dụng. Ứng dụng đề xuất gồm các chức năng chính: Chức năng quản trị hệ thống; Chức năng điều chỉnh vị trí đọc File Log (Cấu hình đọc File Log); Chức năng xem các Traffic thông qua Log đã đọc; Chức năng điều chỉnh các thông báo,… và còn một số chức năng cơ bản khác.

Việc ứng dụng khai phá dữ liệu và khoa học dữ liệu vào trong bảo vệ LAN và phòng ngừa tấn công LAN hiện đang là một trong những xu thế hiện nay. Việc kết hợp các thuật toán thông minh với các công cụ giám sát mạng hiện có cũng là một trong những hướng phát triển phổ biến được đánh giá cao nhằm giúp bảo vệ, cảnh báo và giám sát an ninh trên mạng nói chung và mạng LAN nói riêng được tốt hơn.

1. **KẾT LUẬN:**

Đề tài giúp người đọc có được những cái nhìn tổng quan về chủ đề An toàn và bảo mật an ninh mạng, trong đó bao gồm các kỹ thuật tấn công cơ bản và đặc biệt là tấn công APT, ngoài ra còn có ứng dụng Trí tuệ nhân tạo (AI), Machine Learning – Deep Learning vào việc phân tích dữ liệu.

Tuy nhiên, đề tài vẫn tồn tại một số hạn chế như kết quả đạt được chưa khái quát được cho mọi trường hợp, trong tương lai sẽ sớm cập nhật và bổ sung để đề tài được hoàn thiện hơn. Thế nhưng khi xét về mặt thực tiễn, đề tài đã đưa ra được giải pháp và xây dựng thành công phần mềm cảnh báo tấn công dựa vào phân tích Logs, đặc biệt là tấn công APT, từ đó có thể giúp cho người quản trị nhận biết được mối nguy hiểm trước khi nó được xảy ra.

Dựa trên những kết quả đã đặt được và những hạn chế còn tồn tại, trong tương lai chúng tôi đang cố gắng nghiên cứu các mô hình tấn công mạng, các phương pháp trinh sát mới nhằm phát hiện và cảnh báo tốt hơn, đồng thời tiến hành nghiên cứu và phát triển các thuật toán để cải thiện hiệu quả thu thập và phân tích dữ liệu Logs.

**TÀI LIỆU THAM KHẢO**

[1]. Beth E. Binde, Russ McRee, “SANS Technology Institute, Assessing Outbound Traffic to Uncover Advanced Persistent Threat”, Joint Written Project, Terrence J. O’Connor 5/22/2011 .

[2]. Nart Villeneuve and James Bennett, “Detecting APT Activity with Network Traffic Analysis”, Trend Micro Incorporated Research Paper 2012.

[3]. “Advanced Persistent Threat Detection” ,Cross-Reference To Related Applications ,This application is a continuation of U.S. patent applica tion Ser. No. 14/263,955 filed on Apr. 28, 2014, the entire content of which is hereby incorporated by reference.

[4]. S. C. Y. Ng \*,a and M. Bakhtiarib, “Advanced Persistent Threat Detection Based On Network Traffic Noise Pattern and Analysis”, ISSN (online): 2462-1927 | Vol. 2, No. 1. Pages 1-18, 2016

[5]. Harikrishnan V N,Gireesh Kumar T, “Advanced Persistent Threat Analysis using Splunk”, Volume 118 No. 20 2018, 3761-3768 ,ISSN: 1314-3395

[6]. Artur Rot, “Advanced Persistent Threats Attacks in Cyberspace”. Threats, Vulnerabilities, Methods of Protection , Computer Science and Information Systems, pp. 113–117,DOI: 10.15439/2017F488 ISSN 2300-5963 ACSIS, Vol. 12

[7]. Department Of Engineering Enzo Ferrari, “Analysis of high volumes of network traﬃc for Advanced Persistent Threat detection”, University of Modena and Reggio Emilia, Italy.

[8]. Principal Author Jason Creasey, “Cyber Security Monitoring and Logging Guide”,Version 1, Managing Director, Jerakano Limited.