PHƯƠNG PHÁP PHÁT HIỆN BẤT THƯỜNG ĐỂ CẢNH BÁO TẤN CÔNG MẠNG

Vũ Đức Thịnh*, Trần Thị Bích Vân
Trường Đại học Công nghiệp Thực phẩm TP.HCM
*Email: *thinhvd@hufi.edu.vn*
Ngày nhận bài: 20/5/2022; Ngày chấp nhận đăng: 15/7/2022

TÓM TẮT

Trong nghiên cứu này, nhóm tác giả đề xuất một phương pháp phát hiện bất thường để cảnh báo tấn công mạng bằng cách sử dụng bộ công cụ Elastic Stack thu thập và phân tích dữ liệu log của các ứng dụng; sau đó ứng dụng học máy và thuật toán PCA để phát hiện các hành vi, dấu hiệu, các điểm bất thường trong dữ liệu log, từ đó dự đoán các hành động của người dùng trên các ứng dụng là hành động tấn công, xâm nhập trái phép hay là hành động truy cập bình thường; đồng thời cũng so sánh kết quả cảnh báo của phương pháp đề xuất với kỹ thuật học máy Elastic đang được sử dụng trong bộ công cụ Elastic Stack.

Từ khóa: PCA, phát hiện bất thường, tấn công.

1. MỞ ĐẦU

Phát hiện sự bất thường là để giải quyết vấn đề của việc tìm kiếm các mẫu trong dữ liệu không phù hợp với hành vi mong đợi. Những mẫu không phù hợp này thường được gọi là bất thường, ngoại lệ, bất ngờ, đặc thù, v.v. Phát hiện bất thường được sử dụng rộng rãi trong nhiều lĩnh vực như: y tế, chứng khoán, tài chính, an ninh mạng, quân sự, v.v.; ví dụ: một mẫu lưu lượng bất thường trong một hệ thống mạng máy tính có nghĩa rằng một tin tặc đang tấn công và gửi dữ liệu nhạy cảm đến một điểm mà không được phép, các bất thường trong dữ liệu giao dịch thẻ tín dụng có thể cho phép nhận dạng hành vi trộm cắp [2].

Trong bài báo này, nhóm tác giả đã sử dụng bộ công cụ ELK Stack (Beat, Logstash, Elastic Search, Kibana) [1] để thu thập và phân tích data log của các services; phát hiện dấu hiệu bất thường bằng cách sử dụng kỹ thuật Dimensionality Reduction (DR); theo dõi, dự đoán, phát hiện và cảnh báo các hành vi, điểm, dấu hiệu bất thường trong các file log, traffic vào ra hệ thống, các hành động xâm nhập trái phép hay các hành động truy cập hợp pháp trong quá trình hoạt động của hệ thống bằng thuật toán Principal Component Analysis (PCA).

2. CƠ SỞ LÝ THUYẾT

2.1. Khái niệm về phát hiện bất thường

Phát hiện sự bất thường (Anomaly Detection) là xác định các sự kiện, mẫu khác biệt đáng kể so với các hành vi hoặc khuôn mẫu tiêu chuẩn. Các dị thường trong dữ liệu còn được gọi là độ lệch chuẩn, giá trị ngoại lệ, nhiễu, vật lạ, v.v. Trong bối cảnh phát hiện bất thường mạng hoặc xâm nhập mạng và phát hiện lạm dụng thì 2 thuật ngữ được sử dụng phổ biến là bất thường và ngoại lệ. Ví dụ: các hoạt động làm tăng lưu lượng mạng đột biến thường đáng chú ý, mặc dù một hoạt động tăng đột biến như vậy có thể nằm ngoài nhiều kỹ thuật phát hiện bất thường truyền thống; một mẫu lưu lượng bất thường trong một hệ thống mạng máy tính có

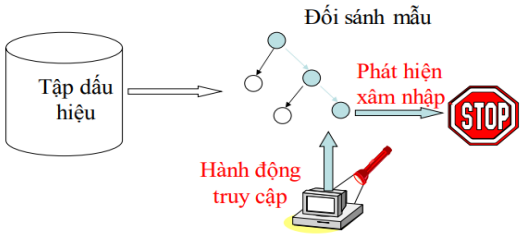
nghĩa rằng một tin tặc đang tấn công và gửi dữ liệu nhạy cảm đến một điểm mà không được phép [2].

2.2. Các phương pháp phát hiện bất thường

2.2.1. Phương pháp dựa trên dấu hiệu

Dấu hiệu là những đặc trưng khi hệ thống bị virus, tấn công, xâm nhập trái phép, v.v. đã được thống kê được trong quá trình hệ thống vận hành và được lưu lại. Hệ thống sẽ triển khai so sánh giữa các dữ liệu đã thu thập với các dấu hiệu khi phát hiện xâm nhập được lưu trữ trong cơ sở dữ liệu của hệ thống xét xem hành động đang được diễn ra đó là an toàn hay không an toàn.

Kỹ thuật này đơn giản hiệu quả trong các trường hợp đã từng gặp các mối đe dọa và đã được lưu trữ trong cơ sở dữ liệu của hệ thống nhưng không hiệu quả trong những trường hợp chưa gặp phải bao giờ. Đây cũng là mặt hạn chế của phương pháp này, nên rất ít dùng trong mô hình mạng lớn hay giao thức ứng dụng vì không thể theo dõi bao quát hết các thành phần có trong hệ thống và có độ tin cậy thấp.



Hình 1. Mô tả dấu hiệu xâm nhập

2.2.2. Phát hiện dựa vào hành động

Kỹ thuật phát hiện dựa vào bất thường là quá trình tổng hợp các hành động thông thường trong một khoảng thời gian từ nhiều đối tượng như những người dùng, máy chủ, kết nối mạng hay các dịch vụ tạo thành hồ sơ thông tin để miêu tả hành động bình thường sau đó so sánh với các sự kiện diễn ra trên hệ thốn để phát hiện bình thường hay bất thường. Phương pháp này có độ chính xác cao khi một hệ thống phát hiện bất thường được thiết lập trong hệ thống và đã có thời gian vận hành dài để triển khai phân tích hoặc học tất cả các hành động bình thường của hệ thống.

2.2.3. Phương pháp phát hiện dựa trên mô hình

Phương pháp phát hiện dựa trên mô hình áp dụng các kĩ thuật, phương pháp học máy; trí tuệ nhận tạo; mô hình sử dụng các thuật toán để phát hiện ra các thời điểm bình thường hay bất bình thường, triển khai các qui luật phát hiện tấn công một cách tự động từ các cơ sở dữ liệu mô phỏng. Phương pháp này được sử dụng rộng rãi trong các hệ thống dự đoán, phát hiện các cuộc tấn công hay xâm nhập trái phép kể cả cũ hay mới tuy nhiên nhiều lúc nó có thể đưa ra các cảnh báo nhầm so với hai phương pháp trên.

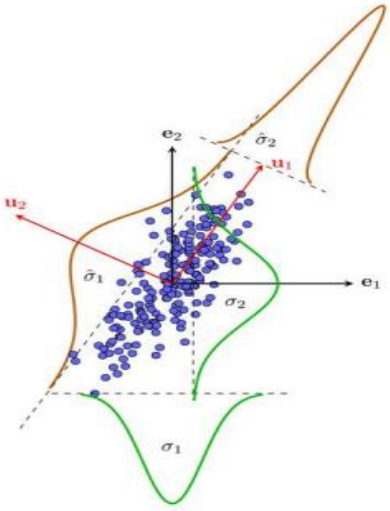
2.2.4. Kỹ thuật phát hiện dựa vào phân tích trạng thái giao thức

Hiện nay, các kẻ tấn công thường thông qua các giao thức mạng để tấn công hay xâm nhập bất hợp pháp vào hệ thống. Mỗi giao thức điều có cấu trúc và cách hoạt động riêng biệt, kỹ thuật phát hiện dựa vào phân tích trạng thái giao thức sử dụng các dữ liệu hoạt động hợp lệ của giao thức có sẵn trong hệ thống để xem xét có hành vi tấn công đang xảy ra hay không.

Hạn chế của phương pháp này tập trung dữ liệu, bởi vì phải phân tích và thực hiện giám sát trạng thái hoạt động cho nhiều phiên làm việc cùng lúc; còn một vấn đề nữa là phương pháp này không thể phát hiện các cuộc tấn công có dấu hiệu đặt trưng như các phương pháp trên bởi vì giao thức thừa nhận đây là các hành vi thông thường, ví dụ: thực hiện lập đi lập lại hành động bình thường nhiều lần trong một khoảng thời gian ngắn như tấn công từ chối dịch vụ. Mặc khác có thể xảy ra xung đột giữa giao thức hệ thống và giao thức hiện có trong mạng [2].

2.3. Thuật toán Principal Component Analysis (PCA)

PCA là thuật toán phân tích đa biến dựa trên các véc tơ đặc trưng. Đây là phương pháp thống kê dùng chuyển đổi trực giao để di chuyển tọa độ n gốc của tập dữ liệu đến tọa độ m mới (m <n) [3]. PCA luôn luôn tìm thấy véc tơ trực giao n ngoài tập dữ liệu theo chiều n. Những véc tơ đó là véc tơ riêng của ma trận hiệp phương sai và tập con của véc tơ m mà có thể bao phủ hầu hết các biến trong tập dữ liệu, kết quả là giảm kích thước từ n sang m. Mặc khác, PCA hướng đến tạo tập dữ liệu thành không gian con mới kích thước nhỏ hơn với phương sai tối đa. PCA được sử dụng rộng rãi trong nhiều ứng dụng, từ phát hiện bất thường đến dự đoán tấn công. Mục đích chính của PCA có khả năng chiếu các quan sát được mô tả bởi các biến thể P với ít hơn các thành phần trực giao N [4]. Để có cái nhìn trực quan hơn, chúng ta cùng theo dõi Hình dưới đây



Hình 2. PCA dưới góc nhìn thống kê [5]

Trong không gian ban đầu tại hình 2 với các vector cơ sở màu đen e1,e2, phương sai theo mỗi chiều dữ liệu đều lớn. Trong không gian mới với các vector cơ sở màu đỏ u1,u2, phương sai theo chiều thứ hai $\hat{\sigma}2$ rất nhỏ so với $\sigma 2$. Điều này nghĩa là khi chiếu dữ liệu lên u2 ta được các điểm rất gần nhau và gần với kỳ vọng theo chiều đó. Trong trường hợp này, kỳ vọng theo mọi chiều bằng 0 nên ta có thể thay thế toạ độ theo chiều u2 bằng 0. Rõ ràng là nếu dữ liệu có phương sai càng nhỏ theo một chiều nào đó thì khi xấp xỉ chiều đó bằng một hằng số, sai số xảy ra càng nhỏ. PCA thực chất là đi tìm một phép xoay tương ứng với một ma trận trực giao sao cho trong hệ toạ độ mới, tồn tại các chiều có phương sai nhỏ mà ta có thể bỏ qua; ta chỉ cần giữ lại các chiều/thành phần khác quan trọng hơn.

Nghiên cứu này này tập trung vào phát hiện bất thường từ các dữ liệu log. sử dụng PCA để tách biệt các mẫu lập lại trong các véc tơ đặc trưng, bằng cách đó các mẫu có thông điệp bất thường dễ dàng phát hiện hơn. Với PCA để nắm bắt phương sai đúng và tránh kết quả lệch, dữ liệu ban đầu phải được điều chỉnh sao cho trung bình cộng của tất cả các điểm dữ liệu bằng 0. Sau khi dữ liệu đã được chuẩn hóa, ma trận hiệp phương sai có thể được tính toán. Ma trận hiệp

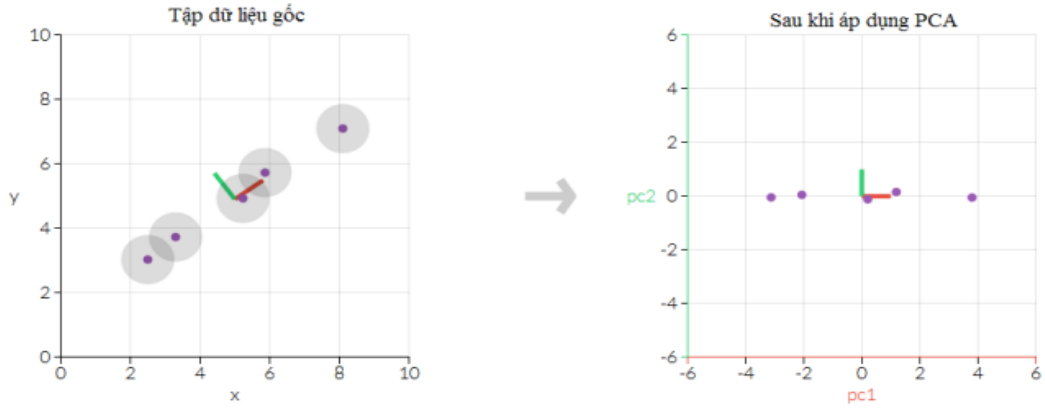
phương sai là một ma trận đối xứng. Nếu bạn tính hiệp phương sai giữa một chiều và chính nó, bạn sẽ có được phương sai. Ví dụ nếu bạn có một tập dữ liệu 3 chiều (x,y,z), sau đó bạn có thể đo được hiệp phương sai giữa chiều x và y, chiều x và z và chiều y và z. Đo hiệp phương sai giữa x và x, hoặc y và y, hoặc z và z sẽ cung cấp cho bạn phương sai của chiều x, 20 y và z tương ứng. Một tập dữ liệu 3 chiều x, y, z có thể thu được ma trận hiệp phương sai sau:

$$C = \begin{pmatrix} cov(x,x) & cov(x,y) & cov(x,z) \\ cov(y,x) & cov(y,y) & cov(y,z) \\ cov(z,x) & cov(z,y) & cov(z,z) \end{pmatrix}$$

Hiệp phương sai là độ đo sự biến thiên cùng nhau của hai biến ngẫu nhiên. Giải thích một cách đơn giản đó là nếu hiệp phương sai của chiều x và y là dương, nó cho biết giá trị của các chiều đó tăng cùng nhau (nghĩa là, khi một biến có giá trị cao hơn giá trị kỳ vọng thì biến kia có xu hướng cũng cao hơn giá trị kỳ vọng). Mặc khác, nếu hiệp phương sai của x và y có giá trị âm, thì nó cho biết giá trị chiều x nằm trên giá trị kì vọng còn chiều y có xu hướng nằm dưới giá trị kì vọng. Nếu giá trị hiệp phương sai bằng 0, nghĩa là giá trị x và y độc lập với nhau. Với ma trận hiệp phương sai n chiều chúng ta thu được trong bước cuối cùng, các véc tơ riêng n có thể được suy ra từ đó. Một véc tơ riêng v của ma trận hiệp phương sai T thỏa mãn phương trình sau:

$$T(v) = \lambda v$$

Nói theo cách khác, xác định một ma trận biến đổi T, có tồn tại véc tơ v không đổi phương hướng sau khi áp dụng bởi T. Biến đổi T có tỷ lệ véc tơ v không đổi bằng một số lượng λ. Số lượng λ trong trường hợp này gọi là giá trị riêng. Với một ma trận N x N, luôn luôn tồn tại n véc tơ riêng, ứng với mỗi trị riêng của nó. N các véc tơ riêng vuông góc với nhau vì vậy với một phép biến đổi thích hợp bộ dữ liệu gốc có thể được chiếu trên các chiều dữ liệu mới. Các giá trị riêng tương ứng với mỗi véc tơ riêng cho biết số lượng véc tơ riêng đặc trưng của dữ liệu hoặc có bao nhiêu phương sai của dữ liệu mà véc tơ riêng lẻ được giữ lại. Kết quả là, sau khi phân loại tất cả các véc tơ riêng dựa trên giá trị riêng của chúng, nó có khả năng phát hiện ra rằng có những véc tơ riêng giữ lại hầu hết phương sai dữ liệu (các giá trị riêng lớn nhất) và các véc tơ riêng khác giữ lại rất ít phương sai dữ liệu (các giá trị riêng rất nhỏ). Cuối cùng, với mục đích là giảm chiều dữ liệu, chúng ta có thể giữ lại các véc tơ riêng có giá trị riêng lớn nhất, các chiều quan trọng nhất và kẻ một đường thẳng dữ liệu gốc dựa trên trên các véc tơ riêng đã chọn. Hình ảnh 3 dưới đây là minh họa giảm chiều bằng cách áp dụng PCA với 5 điểm dữ liệu trong không gian 2 chiều, sau khi áp dụng PCA, trên một chiều pc1, chiều pc2 bị loại bỏ do nó ít quan trọng [6].

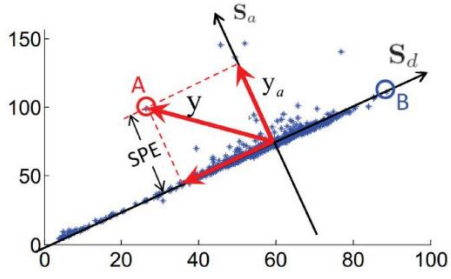


Hình 3. Áp dụng PCA trên dữ liệu 2 chiều để giảm xuống còn 1 chiều

Sau khi xác định vị trí các thành phần chính, chúng ta sẽ tách tập dữ liệu gốc ra thành 02 không gian con: các điểm dữ liệu bình thường 'normal' thường nằm gần một không gian con nào đó được tạo ra bởi các thành phần chính, trong khi các điểm dữ liệu 'abnormal' bất thường, khác biệt với các điểm dữ liệu bình thường 'normal' được tạo ra bởi các thành phần quan trọng khác, tức nằm xa không gian con đó. Hơn nữa, vì là 'abnormal' nên số lượng các sự kiện thuộc loại này là rất nhỏ so với 'normal'. Như vậy, chúng ta có thể áp dụng PCA trên toàn bộ dữ liệu để tìm ra các thành phần chính của dữ liệu, từ đó suy ra không gian con mà các điểm 'normal' nằm gần. Việc xác định một điểm là 'normal' hay 'abnormal' được xác định bằng cách đo khoảng cách từ điểm đó tới không gian con tìm được hoặc bất kỳ điểm dữ liệu nằm xa không gian con bình thường đều có thể xem là bất thường. Sau đây là công thức tính toán khoảng cách từ điểm dữ liệu y đến không gian con bình thường được tạo bởi chiều k [7]:

$$\| y.(I - V_{1:k} \,.\, V^{T}_{1:k}) \|^{2}$$

Trong công thức này, y là điểm dữ liệu (hoặc véc tơ), $V_{1:k}$ là ma trận được tạo bởi các véc tơ k chính đầu tiên (k nhỏ hơn n trong đó n là số chiều dữ liệu gốc) và $V^{T}_{1:k}$ là phiên bản nghịch đảo của ma trận $V_{1:k}$. I là ma trận đơn vị. Khoảng cách này được đặt tên là Sai số dự đoán toàn phương (Squared Prediction Error -SPE). Với SPE mỗi điểm dữ liệu được tính toán và quy luật để xử lý bất cứ điểm dữ liệu nào là bất thường nếu SPE của nó lớn hơn ngưỡng. Có nhiều cách để định nghĩa ngưỡng bất thường trong tình huống này, điều đơn giản nhất là chọn một điểm giá trị lớn từ tất cả giá trị SPE. Giả sử ta chọn điểm 99.99 của SPE khi là một ngưỡng như vậy điểm dữ liệu nào có SPE lớn hơn 99.99% SPE (ngưỡng) sẽ được xem là bất thường. Theo nghĩa đen, một điểm bất thường cách xa không gian bình thường hơn 99.99% các điểm dữ liệu khác. Hình 4 là minh họa SPE trên tập dữ liệu 2 chiều nơi không gian bình thường được tạo bởi một véc tơ Sd và không gian bất thường được thực hiện bởi các véc tơ khác Sa

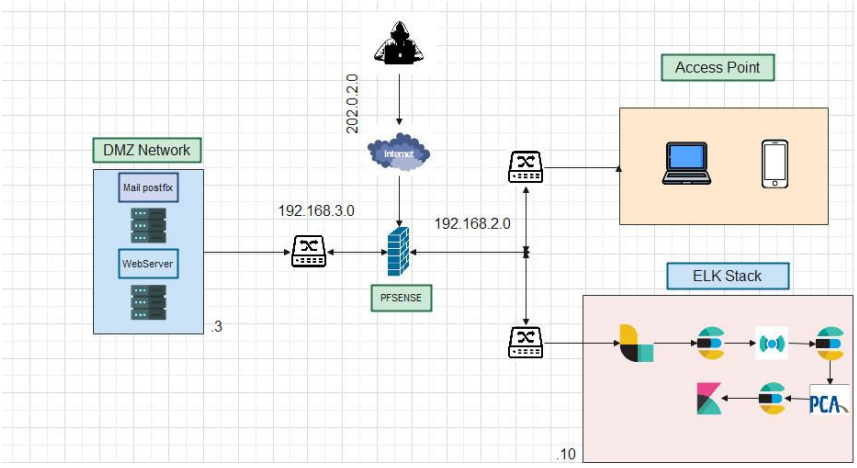


Hình 4. Tách biệt các điểm dữ liệu bất thường bằng cách tính khoảng cách SPE [7]

Hình 4 sau khi áp dụng PCA ta chọn tọa độ mới Sd và Sa , hầu hết chúng ta thấy như một đường thẳng, trực quan, một điểm dữ liệu xa Sd (chẳng hạn điểm A) cho thấy sự tương quan bất thường, và như vậy nó diễn tả sự bất thường, ngược lại điểm B nằm xa các điểm khác nhưng nó nằm trên trục Sd nên bình thường.

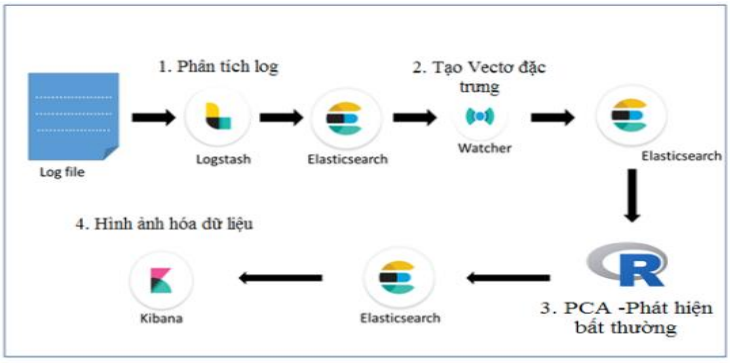
3. PHƯƠNG PHÁP PHÁT HIỆN BẤT THƯỜNG DỰA TRÊN ELK VÀ PCA

Phát hiện bất thường ngày càng được ứng dụng nhiều trong việc phát hiện xâm nhập, tấn công hệ thống mạng. Trong đó, các thuật toán phân lớp thường được sử dụng nhằm xây dựng các mô hình phát hiện xâm nhập trái phép, để dự đoán và phát hiện các tấn công mới khi có bất thường xảy ra. Tuy nhiên, trong bài báo này nhóm tác giả thực hiện bài toán phát hiện bất thường bằng phương pháp máy học dựa trên mô hình dưới đây:



Hình 5. Mô hình tổng quát phát hiện bất thường

Máy chủ ELK sẽ thu thập và xử lý dữ liệu từ log của máy chủ Mail postfix, sau đó áp dụng thuật toán PCA để phát hiện những điểm bất thường trong log (Hình 5).

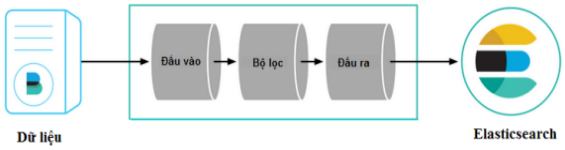


Hình 6. Mô hình thực nghiệm phát hiện bất thường

Bài toán phát hiện bất thường bằng phương pháp học không giám sát và máy học dựa trên 4 bước cơ bản: bước đầu tiên là thu thập và phân tích dữ liệu, tiếp theo tạo véc tơ đặc trưng lựa chọn các trường có thuộc tính quan trọng như các chương trình, giao thức, khoảng thời gian… Những thuộc tính quan trọng sau đó được lựa chọn dựa trên bộ công cụ Elastic Stack và sau đó sử dụng ngôn ngữ R áp dụng phương pháp giảm chiều và thuật toán PCA để phát hiện bất thường và cuối cùng là hình ảnh hóa dữ liệu bất thường (Hình 6).

3.1. Thu thập và phân tích log mail Postfix – Logstash

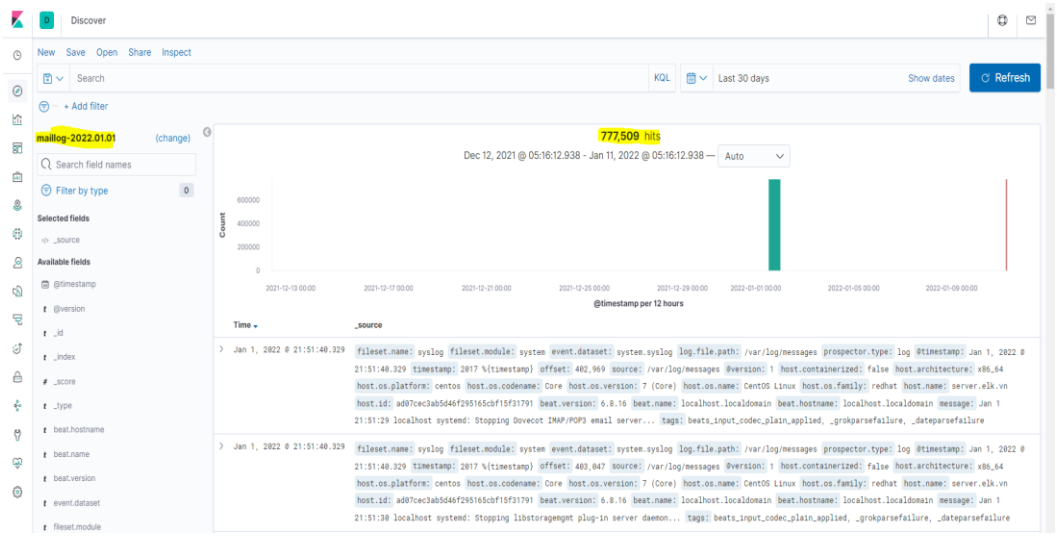
Logstash là một công cụ thu thập dữ liệu nguồn mở với khả năng xử lý chuỗi sự kiện (pipeline) dữ liệu theo thời gian thực. Logstash có thể tự động thu thập/tiếp nhận dữ liệu từ các nguồn khác nhau và chuẩn hóa dữ liệu thành các điểm đến mà bạn chọn. Chuỗi sự kiện (pipeline) Logstash có 03 giai đoạn: đầu vào, bộ lọc và đầu ra, 03 giai đoạn này xác định cách dữ liệu đầu vào, xử lý và đầu ra [8]. Hình 7 là hình ảnh đơn giản về chuỗi xử lý sự kiện Logstash.



Hình 7. Chuỗi xử lý sự kiện Logstach với 3 giai đoạn: đầu vào, bộ lọc và đầu ra

Chuỗi xử lý sự kiện logstash gồm 3 giai đoạn, việc cấu hình logstash cũng tương ứng với 03 thành phần chính là: đầu vào, bộ lọc và đầu ra, mỗi dòng log của logstash tất cả được lưu trữ dưới định dạng JSON (JavaScript Object Notation) , mỗi thành phần có thể hoạt động trong các phần bổ trợ (plugin) khác nhau. Các plugin sẽ xác định cách xử lý dữ liệu trong từng giai đoạn (nơi dữ liệu được thu thập, nơi dữ liệu được lưu trữ sau khi xử lý, cách dữ liệu được xử lý …).

Nhằm mục đích đánh giá phương pháp phát hiện bất thường, tác giả dựa vào tập dữ liệu thu thập được từ logmail Postfix. Tập dữ liệu log là bao gồm các thuộc tính từ các gói tin kết nối đến hệ thống như: thời gian, smtpd, sasl_method, sasl_username, qmgr, cleanup, saslauthd… Bằng cách sử dụng Logstash để phân tích và xây dựng cấu trúc log. Logstash thực hiện công việc phân tích cú pháp từ log mail gồm 03 giai đoạn: input, filter và ouput với các plugin phù hợp. Do mô hình thực nghiệm cài đặt Logstash và Elasticsearch trên cùng một máy chủ, nên thiết lập đầu ra của Logstash thông qua localhost để kết nối với Elasticsearch. Hình 8 cho thấy kết quả, có 777.509 hits được phân tích trong Elasticsearch.



Hình 8. Phân tích log trong Elasticsearch

3.2. Thực hiện tạo vector đặc trưng với watcher

Alerting còn được gọi là Watcher là một thành phần cảnh bảo và theo dõi được tính hợp trong Elasticsearch. Nó tập hợp các tính năng quản trị cho phép bạn xem các thay đổi hoặc bất thường trong hệ thống. Để cấu hình một Watcher, bao gồm 05 phần: trigger[9], input[10], condition[11], transform[12] và actions[13]. Các hành động xác định những gì cần phải được thực hiện khi điều kiện được đáp ứng, tất cả đều được định dạng JSON như sau:

```
{
trigger: {...},
input: {...},
condition: {...},
transform: {...},
actions: {...}
}
```

Hình 9. Các thành phần Watcher

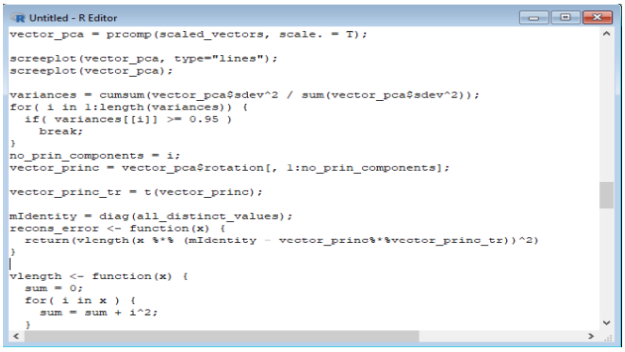
Trong nghiên cứu ngày nhóm tác giả sử dụng công cụ Watcher để tạo vector đặc trưng (vector tỷ lệ trạng thái) từ dữ liệu đã được phân tích và lưu trữ trong Elasticsearch của bộ công cụ ELK với Index là : maillog-2022.01.01. Wacher thực hiện thông qua 5 bước trigger, input, condition, transform và action. Trong nghiên cứu này nhóm tác giả thực hiện tạo vector mà không cần có bước transform, chọn khung thời gian ở đây là 10 giây và thực hiện đếm số lần xuất hiện mỗi chương trình trong 10 giây đó. Sau khi có kết quả cuối cùng thì vector tỷ lệ trạng

thái sẽ được lưu trữ trong Index: mail-program-watch-4. Kết quả sau khi thực hiện Watcher, từ 777.509 hít sẽ tạo ra 4097 vector đặc trưng và lưu trữ trong Elasticsearch.

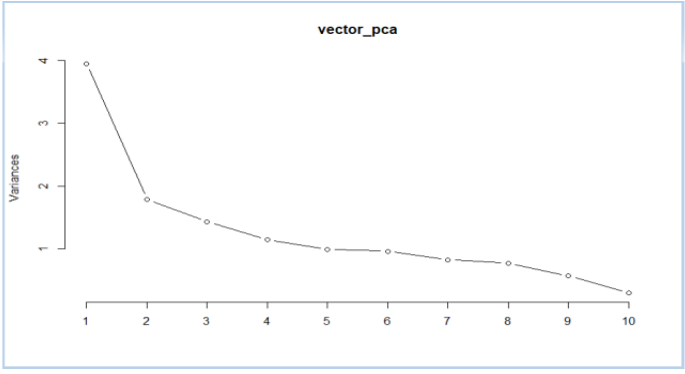
Hình 10. Watcher tạo vector đặc trưng trong Index mail-program-vector-4

3.3. Chương trình R và giải thuật PCA

Tại bước này, thực hiện áp dụng PCA trên tập hợp các véc tơ đặc trưng trong chương trình R. Sử dụng thư viện có tên elastic trong R để đọc các véc tơ từ Elasticsearch. Sau đó áp dụng một phép chuyển đổi đơn giản cho véc tơ sao cho tổng trung bình cộng bằng 0, rồi sử dụng PCA lên chúng bằng cách sử dụng hàm prcomp. Thuật toán PCA sẽ trích chọn ra các véc tơ đặc trưng tiêu biểu trong 4097 véc tơ đặc trưng. Sau đó, R sẽ tạo một Index gồm các véc tơ đặc trưng phát hiện bất thường và lưu trữ trong Elasticsearh, tác giả đặt trên index là maillog-anomaly-all-1s .



Hình 11. Chương trình R và áp dụng PCA



Hình 12. Phương sai của 10 thành phần đầu tiên được tạo từ vector đặc trưng mail log.

Sau đó, thực hiện lấy các thành phần chính đầu tiên có tổng phương sai lớn hơn 95% (> 95%) và thực hiện phát hiện bất thường từ những véc tơ đó. Hình 13 là độ lệch chuẩn và phương sai của các thành phần đầu tiên.

Standard deviations:

PC1	PC2	PC3	PC4	PC5	PC6	PC7	PC8	PC9	PC10	PC11	PC12	PC13
1.9854989	1.3367218	1.1965104	1.0717512	0.9971805	0.9808318	0.9103724	0.8800678	0.7580121	0.5511216	0.3792662	0.2948485	0.1479465

Variances:

0.3032466	0.1101259	0.0883577	0.0764899	0.0740023	0.0637521	0.0595784	0.0441986	0.0233642	0.0110648	0.0066873	0.0016837	0.0016837

Cumulative Porportion:

0.3032466	0.4406947	0.5508206	0.6391784	0.7156683	0.7896707	0.8534228	0.9130012	0.9571999	0.9805641	0.9916289	0.9983163	1.0000000

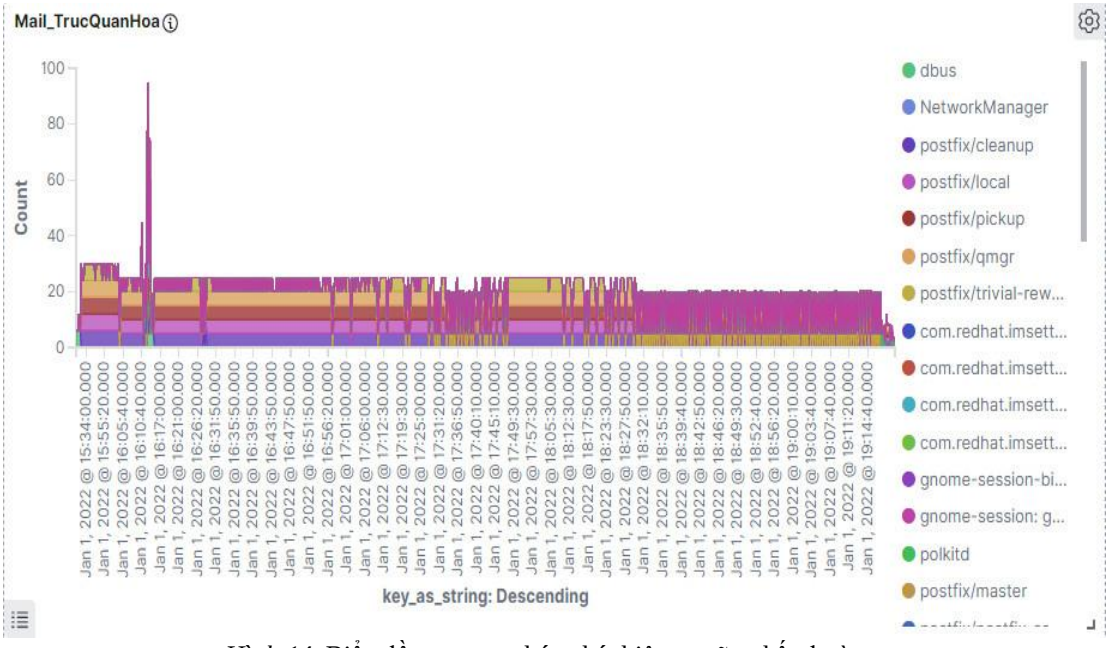
Hình 13. Độ lệch chuẩn của các thành phần đầu tiên

Thành phần chính đầu tiên là 30,32% phương sai, hai thành phần đầu tiên là 44,06% phương sai và ba thành phần đầu tiên là 55,08% phương sai, bốn thành phần đầu tiên là 63,91% phương sai, năm thành phần đầu tiên là 71,56% phương sai, sáu thành phần đầu tiên là 78,96% phương sai, bảy thành phần đầu tiên là 85,34% phương sai, tám thành phần đầu tiên 91.57% phương sai, chín thành phần đầu tiên là 95,71% phương sai lớn hơn 95% và tiếp tục..

Tác giả đặt ra các thành phần được chọn ít nhất 95% của phương sai dữ liệu, vì thế 9 thành phần đầu tiên được chọn, hành động này cũng có nghĩa là dữ liệu đã được giảm so với dữ liệu gốc. Sau khi có những chiều chính, sẽ thực hiện ánh xạ từ dữ liệu gốc vào các chiều mới, phát hiện các giá trị ngoại lệ, các điểm dữ liệu nằm xa các chiều dữ liệu chính. Sau đó, chọn 99,99 làm giá trị ngưỡng, nếu bất kỳ véc tơ nào có sai số thiết lập (reconstruction error) cao hơn ngưỡng này được xem là bất thường hoặc ngoại lệ

3.4. Trực quan hóa dữ liệu bất thường

Để trực quan hóa dữ liệu bất thường, tác giả thực hiện tạo ánh xạ Index maillog-anomaly-all-ls với Kibana của bộ công cụ ELK để trực quan hóa quá trình bất thường.



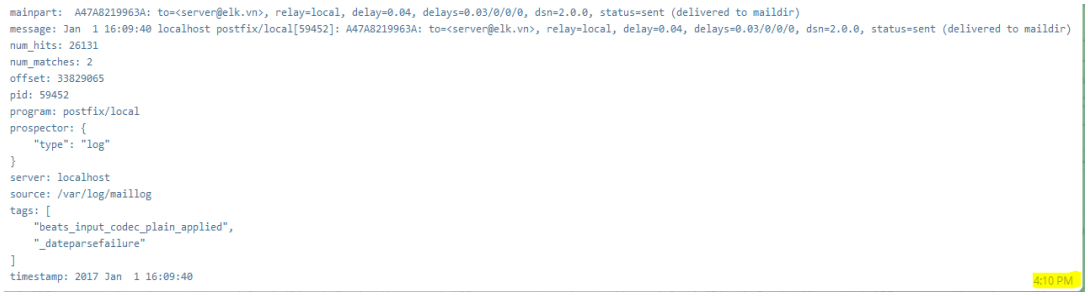
Hình 14. Biểu đồ trực quan hóa phát hiện ngưỡng bất thường

4. KẾT QUẢ VÀ THẢO LUẬN

4.1. Kết quả thực nghiệm

Bài báo đã trình bày một phương pháp phát hiện bất thường trong hệ thống mail dựa trên tập dữ liệu log mail. Hình 15 cho thấy các vector bất thường xảy ra vào lúc 16:10:40 ngày 1 tháng 1 năm 2022, khi so sánh kết quả với tình trạng của hệ thống mail thì vào thời điểm trên máy chủ mail Postfix nhận một lượng mail lớn. Đồng thời, hệ thống cũng gửi cảnh báo về Telegram tại cùng thời điểm với phát hiện vector bất thường (hình 16). Qua đó đã dự đoán được nguyên nhân hệ thống mail hoạt động chậm là do số lượng thư tăng đột biến ảnh hưởng đến hệ thống. Kết quả trên cũng chính là một giải pháp phát hiện và dự đoán tấn công các phần mềm của hệ thống mà tác giả đang hướng tới trong những nghiên cứu tiếp theo.

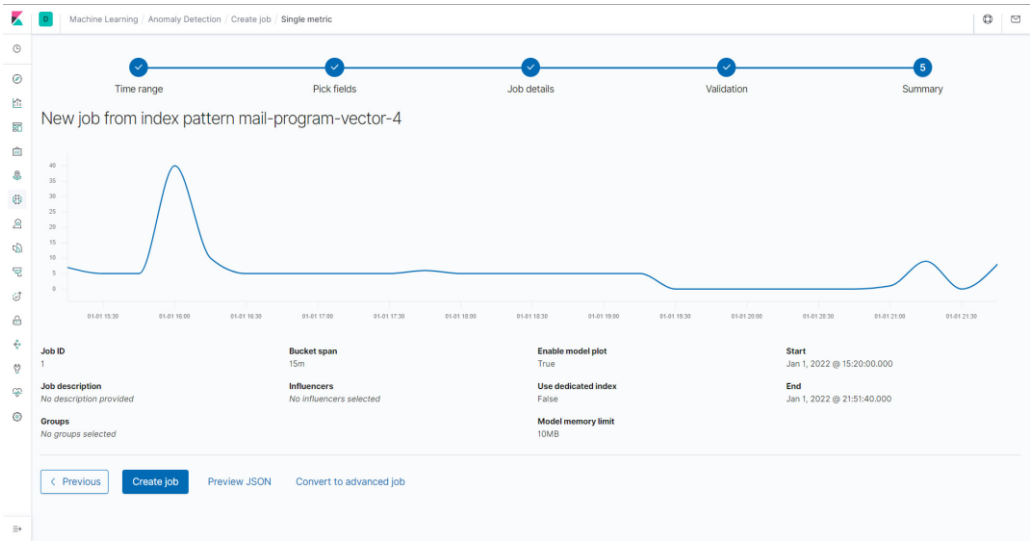
Hình 15. Hình ảnh về thời điểm xảy ra bất thường



Hình 16. Hình ảnh hệ thống gửi cảnh báo về Telegram

4.2. So sánh kết quả bài toán với học máy Elastic (Elastic Machine Learning)

Ở trong phần này, nhóm tác giả thực hiện so sánh kết quả giữa bài toán phát hiện bất thường đã trình bày ở trên với học máy Elastic được sử dụng trong bộ công cụ ELK Stack. . Học máy trong Elastic là phương pháp học không giám sát. Với một tập dữ liệu chuỗi thời gian và một hoặc nhiều biến được theo dõi, nó có thể phát hiện các điểm bất thường trong tập dữ liệu đó. Bỏ qua định nghĩa các quy tắc (rules), chỉ xác định ngưỡng hoặc xây dựng mô hình thống kế theo cách thủ công. Chỉ cần mô tả dữ liệu quan tâm cần phân tích và những thuộc tính khác có ảnh hưởng đến nó (máy chủ, địa chỉ IP, tên người dùng…). Mô hình bắt đầu từ một đường cơ sở (baselining) những gì là bình thường, vì vậy nó có thể phát hiện những gì là không bình thường. Học máy trong Elastic cung cấp 04 tùy chọn cho việc phát hiện bất thường: Single-metric, Multi-metric, Advanced, Population [14] .



Hình 17. Phát hiện bất thường trong máy học Elastic

Với Index maillog-anomaly-all-ls, sử dụng Single-metric job trong Elastic Machine Learning để phát hiện bất thường. Kết quả cho thấy giải pháp phát hiện bất thường, dự báo tấn công được đề xuất có kết quả giống với kết quả phát hiện bất thường trong máy học Elastic của ELK Stack. Qua phân tích các kết quả thực nghiệm đã khẳng định được tính đúng đắn của giải pháp được đề xuất trong nghiên cứu này với các hệ thống trên thực tế.

TÀI LIỆU THAM KHẢO

1. https://vi.wikipedia.org/wiki/Elasticsearch [Online; accessed Arpil, 18 , 2022]
2. Varun Chandola, Arindam Banerjee, and Vipin Kumar. "Anomaly Detection: A Survey". In: ACM Comput. Surv. 41.3 (July 2009), 15:1–15:58. issn: 0360- 0300. doi: 10.1145/1541880.1541882
3. Aaron Hart Michael Berthold Rosaria Silipo, Iris Adae. Seven techniques for dimensionality reduction. KNIME, 2014
4. Francisco Lima. Principal component analysis in r. https://www.rbloggers.com/principal-component-analysis-in-r/, 2018.
5. Machine Learning cơ bản (machinelearningcoban.com)
6. Lewis Lehe Victor Powell. Principal component analysis explained visually. http://setosa.io/ev/principal-component-analysis/
7. Wei Xu. System Problem Detection by Mining Console Logs. PhD thesis, University of California, Berkeley, 2010
8. Elastic. Logstash introduction. https://www.elastic.co/guide/en/ logstash/current/introduction.html.
9. Watcher. Triggers. https://www.elastic.co/guide/en/x-pack/current/triggerschedule.html
10. Watcher. Input. https://www.elastic.co/guide/en/x-pack/current/input.html
11. Watcher. Condition. https://www.elastic.co/guide/en/x-pack/current/ condition.html
12. Watcher. Transforms. https://www.elastic.co/guide/en/x-pack/current/ transform.html
13. Watcher. Action. https://www.elastic.co/guide/en/x-pack/current/ actions.html
14. Kibana. Machine Learning. https://www.elastic.co/products/stack/ machine-learning.

ABSTRACT

ANOMALY DETECTION METHOD FOR NETWORK ATTACK WARNING

Vu Duc Thinh*, Tran Thi Bich Van
Ho Chi Minh City University of Food Industry
*Email: *thinhvd@cntp.edu.vn*

In this study, the authors propose an anomaly detection method to warn of network attacks by using the Elastic Stack toolkit to collect and analyze log data of applications; then apply machine learning and PCA algorithm to detect behaviors, signs, anomalies in log data, thereby predicting user actions on applications that are attacks, invasions unauthorized entry or normal access; also compare the warning results of the proposed method with the Elastic machine learning technique being used in the Elastic Stack toolkit.

Keywords: Anomaly Detection, PCA, attack.