Detecting Multi-Vector Attack Threats Using Multilayer Perceptron Network

IPOLE-ADELAIYE NANCY[1], FORI BARKA TATAMA[2], ONU EGENA[3], MAIKORI JENOM[4], LAWAL IBRAHIM[5]

[1, 2, 3, 4, 5] *Department of Computer Science, Bingham University, Karu, Nasarawa State, Nigeria.*

Abstract-* Multi-Vector Attack (MVA) is the utilization of various attack techniques and methods on a single target. The inability of existing traditional methods in mitigating this attack is a major problem, this poses a huge threat to individuals and organizations. This study improves the detection of MVA using a packet capture (PCAP) dataset through Multilayer Perceptron (MLP) Network. The proposed solution was implemented using python 3 programming language running on google Collaboratory GPU. This study uses a dataset containing 1,047,908 PCAP instances used in training the models. To evaluate the proposed solution, a comparative analysis of the proposed solution and three machine learning models were done based on training time, detection accuracy and F1-score. Despite the fact that the MLP model was train with input neuron, hidden neuron and output neuron of 150, 100 and 50 respectively over 100 epochs, the MPL classifiers was competitive to gradient boost, KNN and random forest machine learning algorithm in terms of detection accuracy. However, the MPL classifier struggles compared to the three machine learning algorithm in terms of training time. The evaluation result of the proposed solutions reports 99.85% detection accuracy, F1-Score of 99% which was verified using the multiclass confusion matrix.

***Indexed Terms-* Machine Learning, Anomaly Detection, Multi-Vector Attacks, Information Security, Intrusion Detection, Multilayer Perceptron.**

I. INTRODUCTION

With the increased reliance on information systems in our everyday living, there are concerns about the risks involved with the occurrence of an unexpected event. Sharing and representation of the information through the utilization of electronic media and devices exposes the data collected to remote systems thereby posing a threat to data confidentiality for humans and warrants an increase in security. The desired security level is the attainment of a state where information and information systems are devoid of undesired events. These unexpected and undesired events' effect includes loss of sensitive and confidential data, loss of finances, Negative effect on reputation, modification of data, loss of access amongst others. These attacks may be due to accidents or malicious activities perpetrated by adversaries.

In recent times, security concerns and attack has moved from attacks to a single node to distributed and multi-node attacks. Sequel to these adverse attacks not only affects the availability of these machines but also confidential data, financial losses, aerospace, defence, education, technological devices amongst others. Latterly, cyberattacks on information security systems have shown significant evidence in posing a very serious risk to humans, costing an estimated 7.2million dollars per organization for every successful attack (Brewer 2014, Mendez et al. 2017). A survey carried out by the United Kingdom government shows that it costs small and medium-sized enterprises (SMEs) between 75,000 and 311,000 pounds and large organizations between 1.46million and 3.14million pounds for a successful cybersecurity breach (Low, 2017).

A considerable amount of these attack methods have been characterized as special types of attacks. This is because of the increased complexity introducing improved difficulty in both preventing and detecting these types of attacks. These sophisticated attack methods involve multiple attack planes, with obfuscation techniques and also utilizing multi-attack vectors to improve success rates such as Advanced

Persistent Threat-like attacks (Krombholz, Hobel et al. 2015).

This research paper focuses on the detection of multi-vector attacks using multilayer perceptron networks and based on data traffic behavioural tendencies and patterns. The next section provides a detailed presentation of the problem this work aims to solve.

II. PROBLEM STATEMENT

The success of attacks on information systems have been of great concern to cyber security experts especially with the cost of an attack costing up to 3.14million pounds and 7.2 million dollars. This cost excludes the effect of the attack on trust and also on the organization's reputation.

Researchers have proposed several solutions to improving security in information systems. Due to the inability of traditional methods in preventing these attacks, have looked into the application of anomaly detection-based solutions majorly machine learning methods. These methods though show acceptable levels in accurately detecting attacks, they still present the possibility of the occurrence of false positive thereby leaving open a window for a successful attack. These misleading results can also reduce the administrator's response to flags and alerts generated by these proposed models.

This work focuses on the use of supervised learning techniques of artificial neural networks such as multilayer perceptron networks and also focusing not just on accuracy but using other test parameters to evaluate the successes of the proposed approach.

III. METHODOLOGY

This chapter describes procedures to be utilized in investigating, finding a solution to the research problem, and providing a detailed approach plan. The detailed plan and technical approach provided are about the inference, accuracy, and relevance for the recommendation and application of techniques in identifying, collecting, and analyzing information and data used in mastery and comprehension of the research problem. Hence, proving that the outcome of the research work is both reliable, valid, and reproducible. We are applying a waterfall model approach to meeting with the aim and objectives of this dissertation.

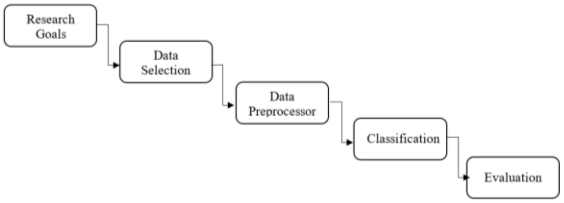

Figure 1 Adopted Waterfall Approach

Figure 1 Illustrates the project plan for this work. The first part identifying research goals, which has already been achieved in the previous chapter with the objectives and comparative evaluation review of related works. The data selection stage provides data samples for the machine learning stage. The machine learning group stage consists of four recursive stages that performs the learning operation using four algorithms in an attempt to select the best, based on accuracy and Area Under Curve (AUC). The output of this is feed to the development of an enhanced prediction model.

A. Data Selection (Dataset)

The dataset to be used is secondary data as it is already collected. The dataset provides a packet header details dataset for the implementation of the machine learning approach in meeting with the objectives of this study.

The dataset source is the cybersecurity research team at Coburg University, Germany. The dataset provides fields of data carrying basic network traffic information as seen in Table 1. This dataset was built through monitoring network traffic of a business organization for 1 week using open stack. This dataset called Coburg Intrusion Detection Dataset (CIDD) consists of over 1 million instances of data in a CIDDS-001-internal-week1.csv file. The dataset consists of 11 fields (Ring, Wunderlich, Grüdl, Landes, & Hotho, 2018).

Table 1: Attributes of CIDD dataset

Fields	Description
Duration	Duration of traffic flow
Protocol	Transport Protocol Used

Source IP Address	Source Port
Source Port No.	Source IP address
Destination IP Address	Destination IP address
Destination Port No.	Destination Port
Packets	Number of packets transmitted
Bytes	Number of Bytes transmitted
TOS	Type of Service
Class	Classification (Normal, Attacker and Victim)
Attack Type	Attack vector used
Attack ID	Unique identification for each attack vector type
Attack Description	Details about the attack parameters

The CIDDS-001 dataset is based on unidirectional data flow and for anomaly detection-based research towards mitigating information security breaches. The data was collected using OpenStack in a business environment, which consists of multiple clients and servers. OpenStack is a cloud-based service it is an efficient and flexible resource management with features for network monitoring and packet capture (PCAP). The environment is closely monitored and the data classified using labels based on the knowledge of the source, timestamp and attack destination. The dataset contains packet header details, each labelled in the class column, which is vital for the static rule-based anomaly detection using statistical analysis and machine learning based anomaly detection. The class column contains three distinct values: normal, victim and attacker. These values are allocated based on the direction of the traffic at that instance.

The choice of PCAP files is as result of the information contained being easily extractible from the packet header during data transmission. This can be done by utilizing off the shelf and cloud applications like Wireshark and OpenStack.

IV. RESULTS AND DISCUSSION

A. Data Presentation

The phases of implementation procedures are discussed alongside details of the data preparation process, which includes data cleaning, transformation, and splitting. The machine learning modeling process and the application of training, testing, and validation are also explained in detail. The evaluation procedures are presented alongside a summary of the performance metrics compared with each machine learning algorithm used in the study.

B. Experiment Environment Setup

The proposed research was conducted using a combination of software and hardware environments. The kernel convolution was set to three, and the dropout rate was 50%. Additionally, due to the number of records in the dataset, the experiment was run for 10 epochs. The tanh function was used as the activation function for the models.

C. System Requirements

All models were implemented on Google Colaboratory, a free cloud-based hardware-as-a-service platform made available by Google for research purposes. The platform provided GPU resources for the experiments.

D. Evaluation and Analysis of Data Processing on Proposed System

This section analyzes the observations made during the training of the proposed model on various machine learning algorithms. Figure 2 presents the correlation results of features of the dataset.

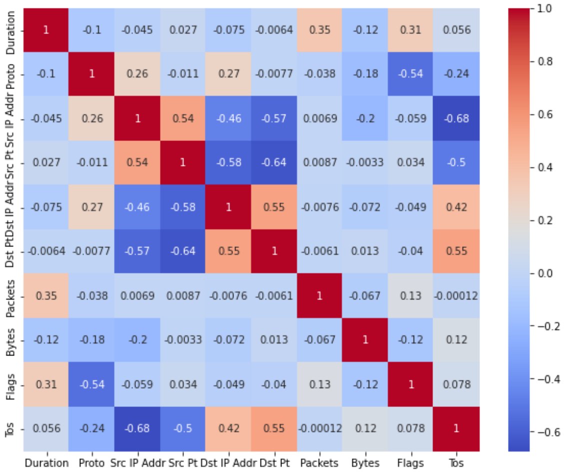

Figure 2: Correlation result for the dataset

Table 2 shows the time taken to train the algorithms on the dataset.

Table 2: Time Taken for Training Datasets on Existing System

Models	Processing Time (seconds)	Detection Accuracy (%)
Multilayer Perceptron (50 epochs)	238.19	93.88
Multilayer Perceptron (100 epochs)	2564.53	99.85
Random Forest	95.90	99.995 (1)
Gradient Boosting Classifier	79.65	99.995 (1)
KNN	2.30	99.87

E. Evaluation and Analysis of Confusion Matrix on Proposed System

Figure 3 presents the precision, recall, F1-score, and support for each model.

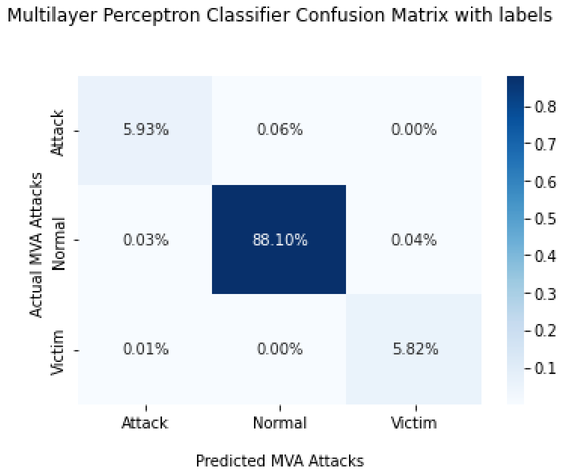
Multilayer Perceptron Classifier Confusion Matrix with labels

Figure 3: Confusion Matrix for MPN

F. Comparative Analysis

This section presents the results of the experiments across the four proposed models. Detection accuracy is presented first, followed by the ROC/AUC curve.

Table 3: Comparative Result for Detection Accuracy and ROC/AUC Across Algorithm

Algorithm	Detection Accuracy (%)	ROC/AUC (%)
Random Forest	100.0	100.0
Logistic Regression	60.7	49.1
KNN	88.8	93.3
Decision Tree	100.0	100.0

Table 3 shows a comparison of detection accuracy and ROC/AUC across the four proposed models. The results indicate that Random Forest and Decision Tree outperform Logistic Regression and KNN, with KNN performing better than Logistic Regression.

V. DISCUSSION

This work presents a system for detecting Multi-Vector Attacks (MVAs). Given the security challenges posed by MVAs to information systems, organizations, and nations, an improved machine learning and deep learning approach for mitigating this threat is presented. The approach and methodology adopted were derived from a comprehensive review of MVA attacks and existing popular mitigation techniques. An extensive review of the severity and impact of existing mitigation techniques and potential solutions was conducted. The review analysis revealed that machine learning techniques are the most recent and popular mitigation methods with evidence of effectiveness in mitigating the threat.

A modified waterfall approach was adopted for implementing the classification method, and a multi-vector attack dataset was acquired from Coburg University, Germany. The approach used machine learning and deep learning methods. Popular machine learning algorithms used in research aimed at mitigating advanced persistent threats (APTs) were evaluated, including K-Nearest Neighbors (KNN), Multilayer Perceptron Classifier, Gradient Boosting Classifier, and Random Forest.

CONCLUSION

In conclusion, the findings from this study demonstrate that the developed Multilayer Perceptron Classifier effectively mitigates Multi-Vector Attack threats. The model exhibits improved accuracy and effectiveness in preventing and detecting attacks. This achievement strengthens the fight against advanced persistent threats (APTs) and lays the groundwork for future research.

Furthermore, the success of this approach suggests a promising solution to the long-standing challenge of

MVAs for IT professionals. It is recommended that this method be evaluated using various network traffic scenarios to confirm its broader applicability.

REFERENCES

[1] Bann, L. L., Singh, M. M., & Samsudin, A. - Trusted security policies for tackling advanced persistent threat via spear phishing in BYOD environment. Procedia Computer Science, 72, 2015 pp129-136.

[2] Bhatt, P., Yano, E. T., & Gustavsson, P.- Towards a framework to detect multi-stage advanced persistent threats attacks. Paper presented at the Service Oriented System Engineering (SOSE), 2014 IEEE 8th International Symposium On, 2014 pp 390-395.

[3] Biener, C., Eling, M., &Wirfs, J. H.- Insurability of cyber risk: An empirical analysis. The Geneva Papers on Risk and Insurance-Issues and Practice, 40(1), 2015 pp131-158.

[4] Brahma, K. K., Sarmah, S., Kalita, C., & Ghosh, R.- Detection of Multi-Vector DDoS Attack. 2019

[5] Brewer, R. - Advanced persistent threats: Minimising the damage. Network Security, 2014(4), 2014 pp5-9.

[6] Low, P. - Insuring against cyber-attacks. Computer Fraud & Security, 2017(4), 18-20.

[7] Mitre Corporation. - Common vulnerabilities and exposures. 2017.

[8] Mendez, D.M., Papapanagiotou, I. and Yang, B., 2017. Internet of things: Survey on security and privacy. arXiv preprint arXiv:1707.01879, .

[9] Shatunova, O., Bozhkova, G., Tarman, B., & Shastina, E - Transforming the Reading Preferences of Today's Youth in the Digital Age: Intercultural Dialog. Journal of Ethnic and Cultural Studies, 8(3), 2021 pp62-73.

[10] Schroeder, R. - Social theory after the internet: Media, technology and globalization (p. 210). UCL Press. 2018

[11] Siadati, H., Nguyen, T., Gupta, P., Jakobsson, M., &Memon, N. - Mind your SMSes: Mitigating social engineering in second factor authentication. Computers & Security, 65, 2017 pp14-28.

[12] Tsvetanov, T., & Slaria, S. - The effect of the Colonial Pipeline shutdown on gasoline prices. Economics Letters, 209, 110122. 2021

[13] Virvilis, N., Vanautgaerden, B., & Serrano, O. S. - Changing the game: The art of deceiving sophisticated attackers. Paper presented at the Cyber Conflict (CyCon 2014), 2014 6th International Conference On, 2014 pp87-97.

[14] Vulnerabilities, C. - Exposures the MITRE Corporation. 2019