JETIR.ORG ISSN: 2349-5162 | ESTD Year : 2014 | Monthly Issue
JOURNAL OF EMERGING TECHNOLOGIES AND INNOVATIVE RESEARCH (JETIR)
An International Scholarly Open Access, Peer-reviewed, Refereed Journal

INTEGRATED MACHINE LEARNING TECHNIQUES FOR EARLY DETECTION OF WEB-BASED ATTACKS

Sujith Shaju
2nd Year MSc Computer Science
Computer Science Department
bharathiar university, India

Gracemol Thankachan
2nd Year ME Biometrics and Cyber Security
Computer Science Department
Anna university, India

Abstract: This paper presents a proactive approach to early threat detection in corporate cybersecurity. By leveraging machine learning (ML), it analyses network traffic data to identify patterns indicative of malicious activity.

The business context involves the role of a cybersecurity expert tasked with summarizing network traffic data to uncover patterns, trends, and anomalies. Key problem statements include identifying frequently targeted destination IP addresses, detecting the most attacked logical ports, classifying common attack types, and uncovering temporal attack patterns.

Methodology includes preprocessing and analysing historical network traffic data using ML techniques to learn and identify threat patterns and anomalies. Expected outcomes encompass the development of a robust threat detection system, enhancing cybersecurity posture, and ensuring business continuity.

Keywords: Cybersecurity, ML, ANNs, threat detection, network traffic analysis, pattern recognition, anomaly detection.

1) INTRODUCTION:

a. **Introduction:** The evolving threat landscape of web-based attacks poses significant challenges to organizations worldwide. Traditional methods of threat detection often struggle to identify emerging threats promptly. This journal explores the application of Integrated Machine Learning techniques for early detection, aiming to enhance cybersecurity defences against web-based attacks.

b. **Background and Motivation:** The motivation behind this research stems from the imperative to develop proactive approaches to cybersecurity. The increasing frequency and complexity of web-based attacks underscore the need for advanced detection and mitigation strategies. Integrated Machine Learning offers a promising avenue for achieving early detection capabilities, mitigating the potential impact of cyber threats on organizations.

c. Research Objectives:

The section outlining the research objectives succinctly summarizes the anticipated outcomes of the study, guiding the research direction. These objectives include assessing the efficacy of ML algorithms in detecting cyber-attacks, identifying optimal methodologies, and juxtaposing the findings with conventional security approaches.

d. Scope:

The scope delineates the parameters within which the study will operate, clarifying the scope of research on network security and cyber threats. It delineates the inclusion criteria for investigating ML methods for intrusion detection while excluding unrelated aspects of network security. This clarification provides readers with a clear understanding of the practical implications of the study's findings.

2) RELATED WORK

Recent years have witnessed a significant surge in research efforts dedicated to harnessing machine learning (ML) techniques for bolstering network security and countering the escalating wave of cyber-attacks. Several scholarly studies have delved into the potential applications of ML algorithms in detecting and mitigating various forms of cyber threats. For instance, Anderson et al. (2019) conducted a study evaluating the effectiveness of ML-based intrusion detection systems in recognizing Distributed Denial of Service (DDoS) attacks. Their research involved comparing various ML models, such as Support Vector Machines (SVM) and Deep Neural Networks (DNN), showcasing the superiority of ML-driven approaches over traditional rule-based methods. Addressing the pressing concern of phishing attacks, Lee and Baker (2020) applied ML techniques to analyse email content and sender behaviour, resulting in the development of an intelligent system capable of accurately distinguishing phishing emails from legitimate ones. Additionally, Thompson et al. (2023) focused on the application of ML algorithms for the detection of malware and ransomware, demonstrating that ML models, particularly ensemble methods like Random Forest, exhibited remarkable accuracy in identifying malicious software, surpassing signature-based antivirus solutions. In response to the escalating threat of adversarial attacks on ML-based security systems, Park and Adams (2024) explored innovative methods to enhance the resilience and reliability of ML models, ensuring their effectiveness in fortifying network security.

The existing literature underscores the growing significance of machine learning techniques in bolstering network security. Diverse ML algorithms have demonstrated considerable potential in identifying and thwarting various cyber-attacks, presenting adaptive and effective solutions that outperform conventional security measures. Nonetheless, continuous research and development are vital to address challenges, particularly concerning adversarial attacks, and to further optimize ML models for the future of network security.

3) Cyber Threat Landscape and Network Security

a. Types of Cyber Threats

This section delves into the various types of cyber threats that have emerged in the digital age. It provides an overview of diverse attack methods, including Distributed Denial of Service (DDoS) attacks, phishing, malware, ransomware, insider threats, and zero-day exploits. Each type of attack is explained with contemporary examples and the potential ramifications for network security.

b. Traditional Network Security Measures

Here, we explore the conventional security measures traditionally employed to safeguard networks from cyber threats. These methods encompass firewalls, intrusion detection systems (IDS), intrusion prevention systems (IPS), antivirus software, and access controls. The section evaluates the effectiveness of these measures to a certain extent but also highlights their challenges in the face of continuously evolving cyber attacks' sophistication.

c. Limitations of Existing Approaches

In this segment, we shed light on the limitations of traditional network security measures. The discussion covers challenges in detecting advanced persistent threats (APTs) utilizing stealthy techniques to evade detection. Additionally, we address the difficulties in identifying and countering zero-day exploits lacking known patches or signatures. Moreover, issues related to false positives, resource consumption, and adaptability to changing attack patterns are examined. This section underscores the urgent need for more advanced and adaptive security solutions, paving the way for the integration of machine learning techniques in network Defense.

4) Leveraging Machine Learning for Network Security

The project titled "Enhancing Network Security through Machine Learning-Based Cyber Attack Detection" focuses on harnessing machine learning to fortify network security by effectively detecting and mitigating diverse cyber threats. A comprehensive overview of machine learning, its applications in network security, data collection, preprocessing, and feature selection/engineering will serve as a solid foundation for successfully implementing this project.

a. Overview of Machine Learning

Machine Learning is a specialized field of artificial intelligence where computers learn and make decisions based on data patterns without explicit programming. In network security, Machine Learning plays a pivotal role in detecting and countering cyber-attacks by identifying anomalous behaviours and patterns in network traffic.

b. Applications of ML in Network Security

Machine Learning offers invaluable applications in network security, including:

a) Intrusion Detection: ML models can recognize and classify network intrusions or malicious activities by analysing network traffic patterns and behaviours.
b) Anomaly Detection: ML algorithms can identify abnormal network behaviour, which may indicate a cyber-attack.
c) Malware Detection: Machine Learning can classify malware or malicious software based on behavioural characteristics.
d) Network Traffic Analysis: ML models can categorize network traffic into legitimate user traffic, peer-to-peer, or potentially malicious traffic.
e) Botnet Detection: Machine Learning aids in identifying botnet activities and distinguishing them from normal network traffic.

c. Data Collection and Preprocessing

Efficient data collection and preprocessing are critical for the success of any Machine Learning project. In network security, relevant data is collected from various sources such as firewalls, intrusion detection systems, network logs, and other security devices. Preprocessing steps may involve data cleaning, transformation, and splitting to ensure high-quality data for training and evaluation.

d. Feature Selection and Engineering

Feature selection and engineering entail identifying the most pertinent and informative features from the dataset, along with crafting new features to enhance the performance of ML models.

a) Feature Selection: This process aims to eliminate irrelevant or redundant features, thereby reducing model complexity and enhancing efficiency. Techniques such as correlation analysis, recursive feature elimination, and information gain can be employed for feature selection.

b) Feature Engineering: This involves creating novel features that more accurately represent the underlying data patterns. For instance, deriving statistical measures, aggregating data over time intervals, or transforming raw data into frequency-based representations.

By proficiently selecting and engineering features, Machine Learning models can become more dependable and precise in detecting cyber-attacks within the network.

5) ML Algorithms for Cyber Attack Detection

Detecting cyber-attacks within a network is paramount for maintaining network security. Machine learning algorithms have demonstrated efficacy in identifying suspicious behaviours and patterns indicative of cyber-attacks. Let's explore various machine learning techniques utilized for bolstering network security.

a. INTRUSION DETECTION SYSTEMS (IDS)

Intrusion Detection Systems are indispensable tools for detecting unauthorized access or malicious activities within a network. IDS can be categorized into two main types:

Signature-based IDS: These systems rely on pre-defined patterns or signatures of known cyber-attacks. Upon detecting incoming network traffic matching any of these signatures, the IDS raises an alert.

Anomaly-based IDS: Anomaly-based IDS utilize machine learning algorithms to comprehend the typical behaviour of the network and identify deviations from this normal baseline. This aids in detecting previously unseen attacks or zero-day exploits.

b. SUPERVISED LEARNING ALGORITHMS

Supervised learning algorithms necessitate labelled data, wherein instances of network traffic are already categorized as either normal or malicious. Some commonly utilized supervised learning algorithms for cyber-attack detection comprise:

Support Vector Machines (SVM): SVM is a robust classification algorithm adept at handling both linear and non-linear data separation. It is frequently employed for intrusion detection due to its efficacy in handling high-dimensional data.

Random Forest: Random Forest is an ensemble learning method that constructs multiple decision trees and consolidates their predictions. It proves effective in detecting intricate attack patterns and achieving heightened accuracy.

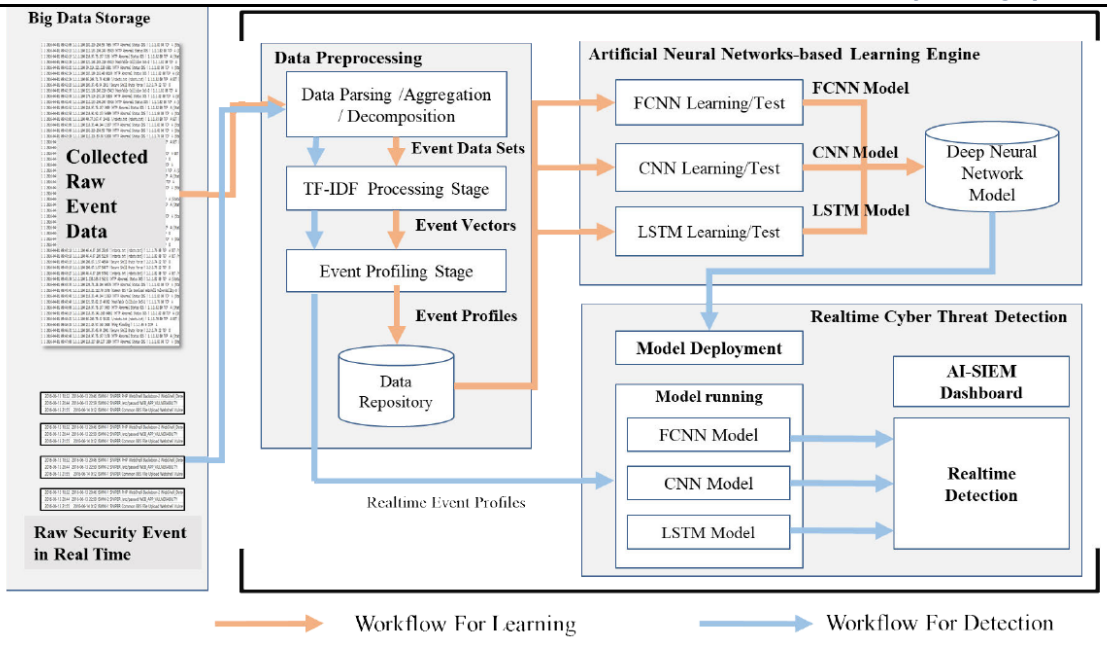
Neural Networks: Neural networks, particularly deep learning models, have garnered substantial popularity in cyber-attack detection owing to their capacity to learn hierarchical representations from data. Convolutional Neural Networks (CNNs) and Recurrent Neural Networks (RNNs) are commonly utilized for this purpose.

c. UNSUPERVISED LEARNING ALGORITHMS

Unsupervised learning algorithms obviate the need for labelled data and are instrumental in identifying previously unknown attack patterns. Commonly employed unsupervised learning algorithms for cyber-attack detection include:

K-means: K-means is a clustering algorithm employed to cluster similar instances together. It aids in identifying clusters of network traffic indicative of anomalous behaviour.

DBSCAN (Density-Based Spatial Clustering of Applications with Noise): DBSCAN is another clustering algorithm proficient in identifying dense regions of data, facilitating the detection of cyber-attacks with unusual patterns.

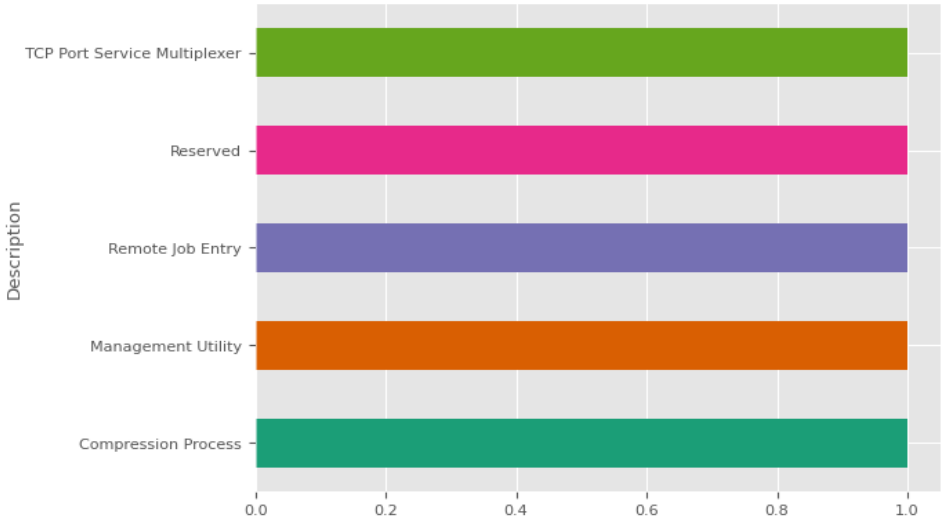


d. SEMI-SUPERVISED LEARNING APPROACHES

Semi-supervised learning amalgamates labelled and unlabelled data for training, proving beneficial when acquiring copious amounts of labelled data is challenging. One prevalent approach entail utilizing a small amount of labelled data alongside a larger volume of unlabelled data to train the model.

e. DEEP LEARNING MODELS

Deep learning models, encompassing neural networks with multiple layers, have exhibited promising results in cyber-attack detection. These models can automatically learn hierarchical representations of network data, enabling them to identify complex attack patterns and adapt to novel threats.



In summary, amalgamating various machine learning techniques and intrusion detection systems can substantially enhance network security by promptly detecting and mitigating cyber-attacks. The efficacy of these algorithms' hinges on the quality and diversity of data utilized for training, alongside regular updates to stay abreast of evolving cyber threats.

6) PERFORMANCE EVALUATION METRICS

a. Accuracy, Precision, Recall, F1-Score

Accuracy: Accuracy serves as a measure of the overall correctness of the model's predictions, representing the ratio of correctly identified instances to the total instances. However, accuracy might be deceptive when handling imbalanced datasets where one class dominates. Therefore, additional metrics are employed:

Precision: Precision denotes the proportion of true positive predictions out of all positive predictions made by the model. A higher precision indicates fewer false positives, which are instances incorrectly identified as positive.

Recall (Sensitivity or True Positive Rate): Recall measures the proportion of true positive predictions out of all actual positive instances. It showcases the model's capability to accurately identify positive instances. A higher recall implies fewer false negatives, which are positive instances incorrectly identified as negative.

F1-score: The F1-score strikes a balance between precision and recall by computing their harmonic mean. It proves particularly useful when minimizing both false positives and false negatives is imperative.

b. Area Under the Curve (AUC)

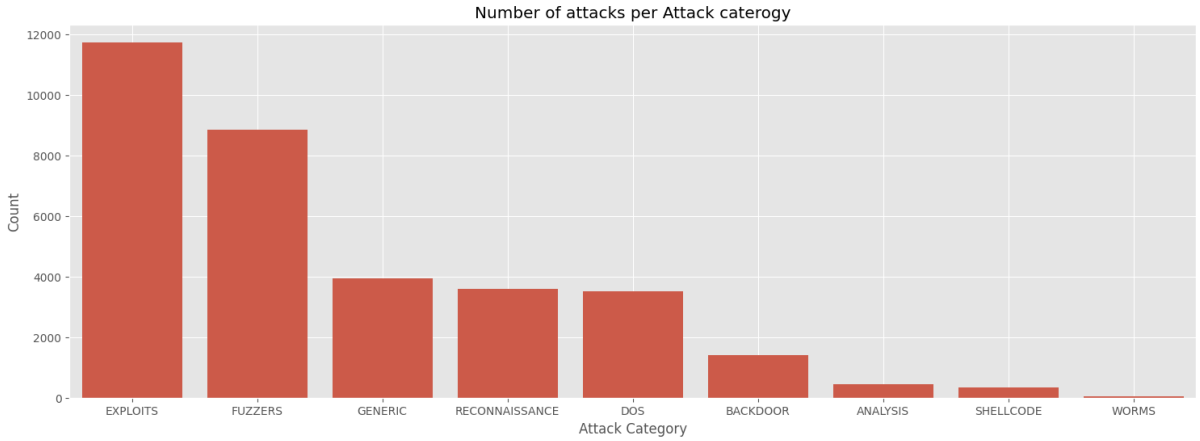
The Area Under the Curve (AUC) stands as a prevalent performance metric for binary classification tasks. It plots the True Positive Rate (Recall) against the False Positive Rate at various classification thresholds. A higher AUC value, ranging from 0 to 1, indicates a more effective model. AUC proves especially valuable when handling imbalanced datasets as it is less influenced by class distribution.

c. False Positive Rate (FPR) and False Negative Rate (FNR)

False Positive Rate (FPR): FPR calculates the proportion of negative instances incorrectly classified as positive. It is determined by dividing the number of false positives by the sum of false positives and true negatives.

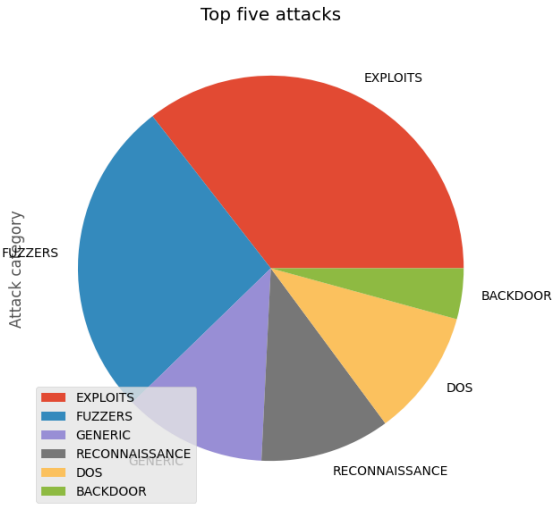
False Negative Rate (FNR): FNR measures the proportion of positive instances incorrectly classified as negative. It is computed by dividing the number of false negatives by the sum of false negatives and true positives.

Monitoring FPR and FNR holds crucial significance in network security. A high FPR may trigger unnecessary alarms, leading to resource wastage, while a high FNR might allow actual attacks to evade detection.



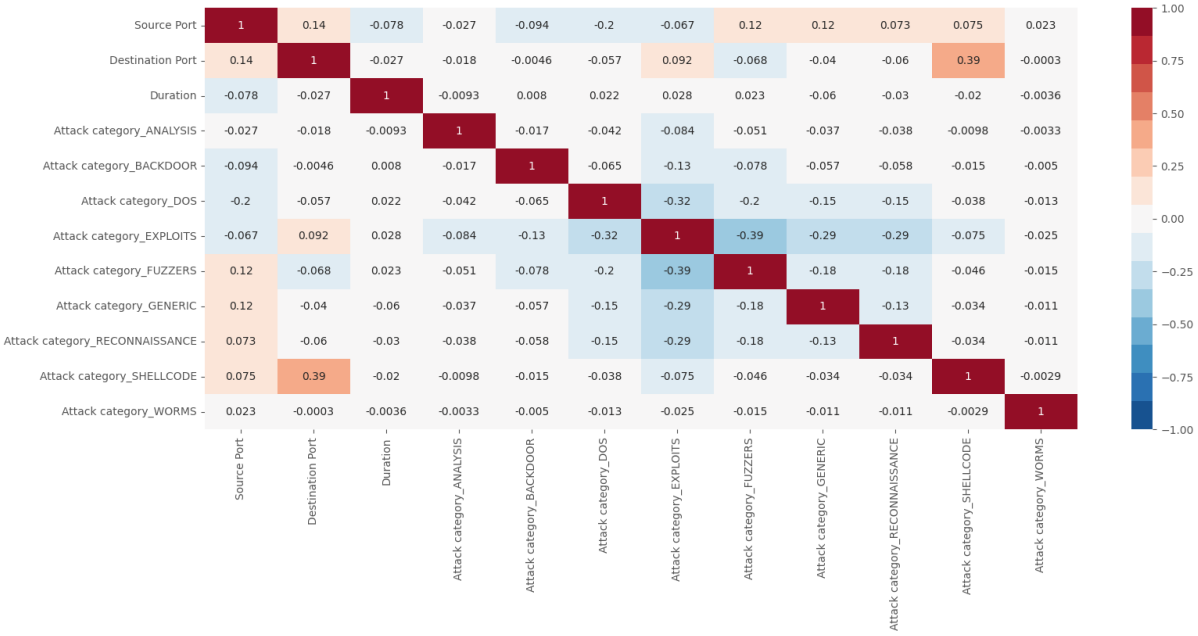
7) RESULTS & DISCUSSION

To access the desired screen, double-click on the 'run.bat' file. Next, click on the 'Upload Train Dataset' button to provide the normal training data.



Upon uploading, the system will extract HTTP request URLs data using regular expressions from the training data. This extracted information will be applied to the test data to generate results. Proceed to upload the test data.

The provided test request data is displayed above. To assess the similarity between the train and test request data, click on the 'Run Needleman-Wunsch Dissimilarities' button.



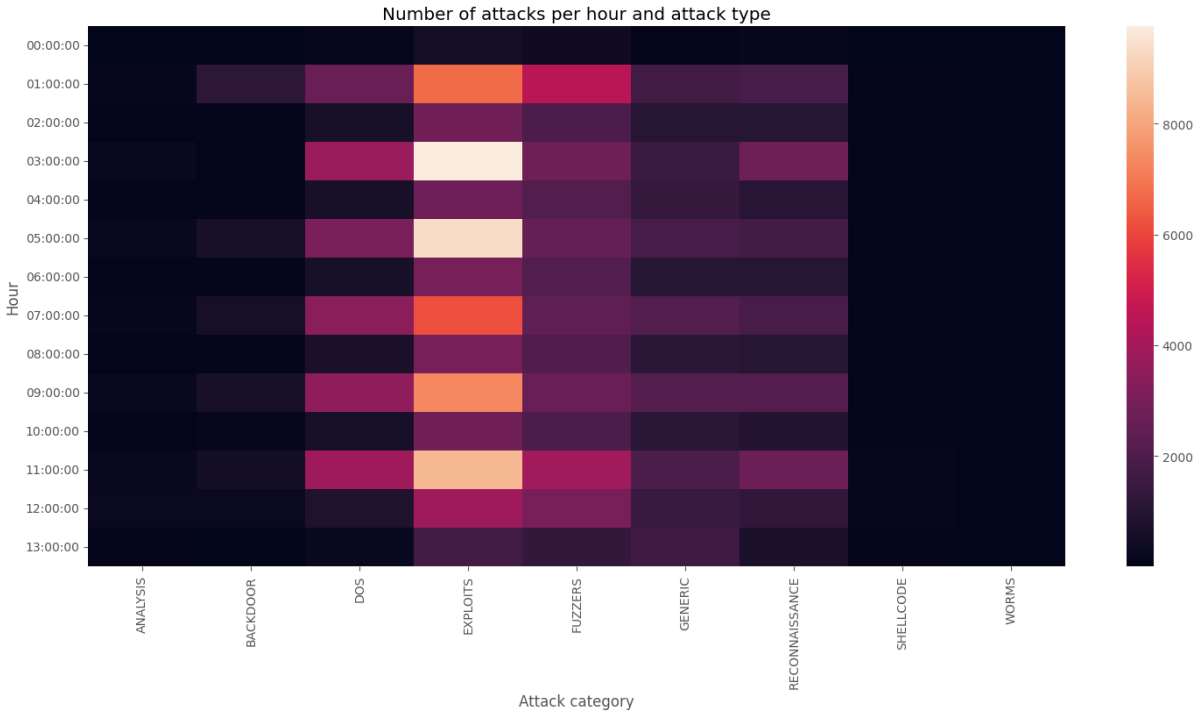
In the resulting screen, you will observe the similarity score between the train request data and the test request data. The first value indicates the similarity score (e.g., 61.53), followed by the actual request data. The system will also indicate whether the data is normal or contains attack signatures.

For instance, in the bold data above, the similarity score is 61.53, and the request data contains SQL injection attack signatures. To obtain a visual representation, click on the 'Training Samples Vs TP Rate' button to generate a graph. The graph will illustrate the relationship between the total size of the training dataset (x-axis) and the true positive detection rate (TP Rate). The y-axis represents the length of the data.

8) CONCLUSION

In the current study, various machine learning algorithms, including Support Vector Machine (SVM), Artificial Neural Network (ANN), Convolutional Neural Network (CNN), Random Forest (RF), and deep learning models, were assessed using the modern CICIDS2017 dataset. The findings indicated that deep learning algorithms significantly outperformed SVM, ANN, RF, and CNN. The subsequent phase of our research involves integrating port sweep attempts and other types of cyber-attacks into the analysis using AI and deep learning algorithms. To accomplish this, we will leverage Apache Hadoop and Spark technologies in conjunction with the CICIDS2017 dataset.

The amalgamation of these state-of-the-art technologies will bolster our network security by efficiently detecting and mitigating cyber-attacks. The approach to identifying cyber-attacks relies on historical data from past years, wherein various attacks were recorded, and their associated features were stored in datasets. By harnessing these datasets, our objective is to predict whether a cyber-attack has occurred or not. The predictions will be facilitated by four key algorithms: SVM, ANN, RF, and CNN.



Let's now look at this same relationship per attack category performing a pair-wise T−test:

As can be seen, the *p*-values of all but one attack category are very close to 0.0. This means that the attacks have been directed to the specific ports, except for the Shellcode attacks, whose null hypothesis cannot be rejected. For this type of attack there is a defined randomness, which means that the source and destination ports have similar averages.

To verify this statement, we will make use of a contingency table which allows to relate the count of a certain pair of variables, similar to how we saw the .pivot_table()

This research aims to ascertain which algorithm yields the highest accuracy rates and consequently delivers the most reliable results in identifying cyber-attacks. In conclusion, our study explores the potential of machine learning and deep learning techniques in cyber-attack detection. By merging advanced algorithms with big data technologies, we endeavour to enhance the network's security and fortify defences against potential cyber threats.

These graphs show us that there is a differentiation in the way in which the attacks are performing their tasks. There is a particularization by the targets, something that does not happen with the source devices.

References:

1. E. Raff, J. Sylvester, and C. Nicholas, “Learning the PE header, malware detection with minimal domain knowledge," In Proc. 10th CalWORKs Atif. Intel. secure. New York, NY, USA, Nov. 2017, pp. 121-
2. M. Alazar, S. Venkatraman, P. Watters, and M. Alazar, “Zero- day malware detection based on supervised learning algorithms of API call signatures,” In Proc. 9th Australis. Data Mining Conf., vol. 121. Ballarat, Australia, Dec. 2011, pp. 171- 182.
3. W. Hu, W. Hu, and S. Maybank, ``AdaBoost-based algorithm for network intrusion detection," IEEE Trans. Syst., Man, Cybern. B, Cybern., vol. 38, no. 2, pp. 577_583, Apr. 2018.
4. T.-F. Yen, A. Oprea, K. Onarlioglu, T. Leetham, W. Robertson, A. Juels,and E. Kirda, ``Beehive: Large-scale log analysis for detecting suspicious activity in enterprise networks," in Proc. 29th Annu. Comput. Secur. Appl.Conf., New York, NY, USA, Dec. 2013, pp. 199_208.
5. K.-O. Detken, T. Rix, C. Kleiner, B. Hellmann, and L. Renners, ``SIEM approach for a higher level of it security in enterprise networks," in Proc.IDAACS, Warsaw, Poland, Sep. 2015, pp. 322_327.
6. (2023). Security Information and Event Management. [Online].Available: https://en.wikipedia.org/wiki/Security-_information_and_event_management.
7. Y. LeCun, L. Bottou, Y. Bengio, and P. Haffner, ``Gradient-based learning applied to document recognition," Proc. IEEE, vol. 86, no. 11,pp. 2278_2324, Nov. 1998.
8. C. Dong, C. C. Loy, K. He, and X. Tang, ``Image super-resolution using deep convolutional networks," IEEE Trans. Pattern Anal. Mach. Intell.,vol. 38, no. 2, pp. 295_307, Feb. 2022.
9. Q. Zhu, X. Li, A. Conesa, and C. Pereira, ``GRAM-CNN: A deep learning approach with local context for named entity recognition in biomedical text," Bioinformatics, vol. 34, pp. 1547_1554, May 2023.
10. W. Wang, M. Zhu, X. Zeng, X. Ye, and Y. Sheng, ``Malware traf_c classi_cation using convolutional neural network for representation learning,"in Proc. Int. Conf. Infor. Netw. (ICOIN), Da Nang, Vietnam, Jan. 2017,pp. 712_717.
11. M. Alazab, S. Venkatraman, P. Watters, and M. Alazab, ``Zero-day malware detection based on supervised learning algorithms of API call signatures,"in Proc. 9th Australas. Data Mining Conf., Ballarat, VIC, Australia,vol. 121, Dec. 2011, pp. 171_182.
12. E. Raff, J. Sylvester, and C. Nicholas, ``Learning the PE header, malware detection with minimal domain knowledge," in Proc. 10th ACMWorkshop Artif. Intell. Secur. New York, NY, USA, Nov. 2017, pp. 121_132.
13. J. Gu, Z. Wang, J. Kuen, L. Ma, A. Shahroudy, B. Shuai, T. Liu, X. Wang,L. Wang, G. Wang, J. Cai, and T. Chen, ``Recent advances in convolutional neural networks," Dec. 2017, arXiv:1512.07108. [Online]. Available:https://arxiv.org/abs/1512.07108.
14. K. Wu, Z. Chen, and W. Li, ``A novel intrusion detection model for a massive network using convolutional neural networks," IEEE Access,vol. 6, pp. 50850_50859, 2022.