International Journal of Science and Research Archive

eISSN: 2582-8185

Cross Ref DOI: 10.30574/ijsra

Journal homepage: https://ijsra.net/

(REVIEW ARTICLE)

Check for updates

Machine learning based Cyber Attack detection on Internet Traffic

A. Sathiya Priya and A. Sandhiya *

Department of Information Technology, Dr.N.G.P. Arts and Science College, Coimbatore, TamilNadu, India.

International Journal of Science and Research Archive, 2024, 11(02), 619–624

Publication history: Received on 09 February 2024; revised on 16 March 2024; accepted on 19 March 2024

Article DOI: https://doi.org/10.30574/ijsra.2024.11.2.0459

Abstract

Cyber attacks on the internet have become increasingly sophisticated and frequent, posing significant challenges to cybersecurity. Traditional rule-based methods for detecting these attacks often struggle to keep pace with the evolving tactics of malicious actors. In this context, machine learning (ML) techniques have emerged as a promising approach for cyber attack detection due to their ability to analyze large volumes of data and identify patterns indicative of malicious behavior. The proposed framework for utilizing machine learning in cyber attack detection on the internet. The framework integrates various ML algorithms, including supervised, unsupervised, and reinforcement learning techniques, to enhance the detection capabilities against different types of cyber threats. Moreover, the framework incorporates feature engineering and selection methods to optimize the performance of ML models in identifying malicious activities.

Keywords: Cyber Attack; Support Vector Machine; Convolutional Neural Networks; Cyber threats; Machine Learning

1. Introduction

The purpose of the study is to differentiate between normal and abnormal network data and how they differ from each other. Machine Learning techniques are being used to train and diagnose if a computer intrusion or hack has occurred. Every classification model can then be used to determine whether the attack is a Distributed denial of service attack. Paxson V. (2020), Support vector machine (SVM) Algorithm, a collaborative learning approach that collects information and identifies trends or can cluster features based on commonality, is an instance of a classification model. Since we can't predict where, how or when a threat will strike, a full-stack intrusion prevention isn't always possible. Hence, our best bet for the time being is early diagnosis that can mitigate the danger of irreversible damage caused by such attacks.

2. Cyber Attack

In the digital age, where interconnectedness prevails, cyber-attacks pose a significant threat to individuals, organizations, and even governments. These attacks can manifest in various forms, from sophisticated hacking endeavors orchestrated by skilled cybercriminals to simple yet effective phishing emails targeting unsuspecting users. Regardless of their complexity, cyber-attacks aim to compromise the integrity, confidentiality, or availability of digital assets.

2.1. Issues Surrounding Cyber Attacks

The prevalence of cyber-attacks underscores several pressing issues:

* Corresponding author: A. Sandhiya

- Technological Vulnerabilities: Software bugs, misconfigurations, and inadequate security measures create entry points for attackers to exploit. As technology advances, new vulnerabilities emerge, challenging cybersecurity professionals to keep pace with evolving threats.
- Human Factors: Despite the deployment of robust cybersecurity tools, human error remains a significant factor in cyber-attacks. Employees falling prey to phishing scams, neglecting security protocols, or inadvertently disclosing sensitive information can inadvertently facilitate cyber breaches.
- Global Impact: Cyber-attacks transcend geographical boundaries, posing a global threat to governments, businesses, and individuals alike. The interconnected nature of cyberspace means that an attack targeting one entity can have cascading effects, impacting numerous interconnected systems.
- Resource Constraints: Addressing cybersecurity concerns requires substantial resources, including financial investments in cutting-edge technologies, skilled personnel, and ongoing training programs. However, many organizations, particularly smaller ones, struggle with limited resources, making them more vulnerable to cyber-attacks.
- Regulatory Compliance: Governments and regulatory bodies worldwide have introduced cybersecurity regulations and standards to mitigate cyber risks. Compliance with these regulations adds another layer of complexity for organizations, necessitating investments in compliance efforts and risk management strategies.

2.2. Types of Cyber Attacks

Cyber-attacks encompass a broad spectrum of tactics and techniques, each tailored to exploit specific vulnerabilities. Some common types of cyber-attacks include:

- Phishing: Attackers use deceptive emails, messages, or websites to trick individuals into divulging sensitive information or downloading malware.
- Malware: Malicious software, including viruses, worms, trojans, and ransomware, is designed to infiltrate systems, steal data, or cause damage.
- Denial-of-Service (DoS) and Distributed Denial-of-Service (DDoS): These attacks overwhelm targeted systems or networks with excessive traffic, rendering them inaccessible to legitimate users.
- Man-in-the-Middle (MitM): Attackers intercept and potentially alter communications between two parties without their knowledge, enabling eavesdropping or data manipulation.
- SQL Injection: By exploiting vulnerabilities in web applications, attackers inject malicious SQL code to gain unauthorized access to databases or execute arbitrary commands.
- Cross-Site Scripting (XSS): Attackers inject malicious scripts into web pages viewed by other users, enabling them to steal information or execute unauthorized actions.
- Ransomware: This type of malware encrypts files or systems, demanding payment for their decryption, thereby extorting victims for financial gain.
- Social Engineering: Attackers manipulate individuals into divulging confidential information or performing actions that compromise security through psychological manipulation tactics.
- Zero-Day Exploits: Attackers leverage previously unknown vulnerabilities (zero-day vulnerabilities) in software or hardware to launch targeted attacks before patches or fixes are available.
- Credential Reuse Attacks: Cybercriminals exploit stolen credentials from one service to gain unauthorized access to other accounts where users have reused the same credentials.

3. Cyber attack detection process

In my research work some of the processing steps involved in cyber attack detection through internet are:

3.1. Data collection

- **Step 1:** Identify relevant data sources: These could include network logs, system logs, intrusion detection system (IDS) alerts, firewall logs, etc.
- **Step 2:** Collect raw data: Obtain data from the identified sources. This could involve setting up data collection agents, tapping into network traffic, or accessing log files.
- **Step 3:** Ensure data quality: Check for completeness, consistency, and accuracy of the collected data. Remove or correct any anomalies or errors.

3.2. Data preprocessing

- **Step 1: Data cleaning:** Handle missing values, outliers, and noisy data. Techniques like imputation, filtering, and smoothing can be used.
- **Step 2: Feature selection/extraction:** Identify relevant features that are informative for distinguishing between normal and malicious activities. This could involve domain knowledge or statistical methods.
- **Step 3: Feature scaling/normalization:** Scale numerical features to a similar range to avoid dominance by features with larger scales.
- **Step 4: Handling categorical variables:** Encode categorical variables into numerical representations using techniques like one-hot encoding or label encoding.
- **Step 5: Dimensionality reduction:** Reduce the number of features to decrease computational complexity and potential overfitting. Techniques like Principal Component Analysis (PCA) or feature importance ranking can be applied.
- **Step 6: Data balancing:** If there's an imbalance between normal and attack instances, apply techniques like oversampling, under sampling, or generating synthetic samples to balance the dataset.
- **Step 7: Temporal data handling:** For time-series data, consider techniques like windowing, resampling, or feature lagging to extract relevant temporal patterns.

3.3. Machine learning models for cyber-attack detection:

There are several machine learning models and techniques commonly used for cyber-attack detection. These models leverage various algorithms and approaches to analyze patterns, anomalies, and signatures within network traffic, system logs, and other relevant data sources.

- **Random Forest:** A versatile ensemble learning technique that can be used for classification tasks in cyber-attack detection.
- **Support Vector Machines (SVM):** Effective for both classification and regression tasks, SVM can be used for detecting anomalies or classifying network traffic.
- **Convolutional Neural Networks (CNNs):** Effective for analysing sequential data such as network traffic flows or time-series data from system logs.
- **Recurrent Neural Networks (RNNs):** Useful for capturing temporal dependencies in sequential data, which is crucial for detecting complex cyber-attacks.
- **Autoencoders:** A type of neural network used for learning efficient representations of data, which can be utilized for anomaly detection in network traffic or system logs.
- **Ensemble Methods:** Ensemble methods, such as AdaBoost and Gradient Boosting Machines (GBM), combine multiple weak learners to create a strong classifier. They are effective in improving the overall performance and robustness of cyber-attack detection systems.
- **Hybrid Models:** Hybrid models combine multiple machine learning techniques, such as combining traditional statistical methods with deep learning approaches or combining supervised and unsupervised learning methods, to leverage the strengths of each approach for improved detection accuracy.

3.4. Evaluation metrics

When evaluating machine learning models for cyber-attack detection, it's crucial to consider metrics that reflect both the model's ability to detect attacks accurately and its performance in real-world scenarios. Here are some common evaluation metrics used in machine learning-based cyber-attack detection:

- **Accuracy:** Accuracy measures the proportion of correctly classified instances out of all instances. While accuracy is important, it might not be sufficient on its own, especially in imbalanced datasets where the number of attack instances is much smaller than normal instances.

$$ACC = \frac{tp + tn}{tp + fp + tn + fn}$$

- **Precision:** Precision measures the proportion of true positive predictions (correctly identified attacks) out of all instances predicted as attacks. It indicates the model's ability to avoid false alarms.
- **Recall (Sensitivity):** Recall measures the proportion of true positive predictions out of all actual attack instances. It indicates the model's ability to capture all attacks, minimizing false negatives.

- **F1 Score:** F1 score is the harmonic mean of precision and recall, providing a balance between the two metrics. It's particularly useful when there's an uneven class distribution.
- $$F_{beta} = (1+\beta^2)\frac{precision * recall}{\beta^2 * precision + recall}$$
- **False Positive Rate (FPR):** FPR measures the proportion of false alarms (instances incorrectly classified as attacks) out of all actual negative instances. It's complementary to specificity and helps in understanding the rate of false alarms generated by the model.
- **False Negative Rate (FNR):** FNR measures the proportion of missed attacks (instances incorrectly classified as normal) out of all actual attack instances. It complements recall and indicates the model's ability to detect attacks accurately.

Table 1 Comparison and analysis of machine learning models

ML Models	Accuracy %	Precision %	Recall %	F1-score %
Random Forest	93.92	94.41	93.92	94.1
CNN	89.5	71.73	76.24	72.69
SVM	95.02	95.43	95.03	95.16
RNN	81.77	81.79	81.77	81.23
Autoencoders	92.26	92.3	92.27	92.28
Ensemble Methods	94.48	94.48	94.48	94.48
Hybrid Models	93.36	92.75	92.82	92.76

Among these seven machine learning model analysis SVM works best and gives the accuracy of 95.16%.

4. Challenges and future directions

4.1. Challenges

- **Data Quality and Quantity:** ML algorithms require large amounts of high-quality data for effective training. However, obtaining labelled datasets for cyber-attacks can be challenging due to the rarity of attacks and the need to ensure data privacy.
- **Imbalanced Datasets:** Cyber-attack datasets are often highly imbalanced, with the number of normal instances far outweighing the number of attack instances. This can lead to biased models that perform poorly on minority classes.
- **Adversarial Attacks:** Attackers can manipulate data to evade detection systems by adding perturbations or crafting adversarial examples. ML models need to be robust against such attacks.
- **Interpretability and Explainability:** Many ML models used in cyber-attack detection, such as deep neural networks, are often considered as black boxes, making it challenging to interpret their decisions. Explainable AI techniques are needed to enhance trust and understanding of model outputs.
- **Generalization to New Attacks:** ML models trained on historical attack data may not generalize well to new and unseen attack patterns. Continuously updating and retraining models with new data is essential to maintain effectiveness.
- **Real-Time Processing:** Effective cyber-attack detection often requires real-time or near-real-time processing of large volumes of network traffic data. ML algorithms must be efficient enough to handle this high computational demand.
- **Privacy Concerns:** Sharing sensitive data for model training purposes raises privacy concerns. Federated learning and other privacy preserving techniques can mitigate these risks.

4.2. Future directions

- **Enhanced Feature Representation:** Developing more sophisticated feature representations, such as incorporating temporal and spatial information, can improve the accuracy of cyber-attack detection systems.

- **Deep Learning Architectures:** Further exploration of deep learning architectures, including recurrent neural networks (RNNs) and graph
- neural networks (GNNs), can lead to more effective detection of complex attack patterns.
- **Transfer Learning and Domain Adaptation:** Transfer learning techniques can be used to transfer knowledge from related domains to improve model performance in cyber-attack detection tasks. Domain adaptation methods can also help in adapting models trained on one network environment to another.
- **Ensemble and Hybrid Models:** Combining multiple ML models into ensembles or hybrid models can enhance detection accuracy and robustness by leveraging the strengths of different algorithms.
- **Active Learning:** Incorporating active learning techniques can help in reducing the labelling effort by selecting the most informative instances for manual annotation, thereby improving the efficiency of model training.
- **Unsupervised Learning Approaches:** Unsupervised learning techniques can be explored for anomaly detection without the need for labeled data, thus addressing the challenge of data scarcity.
- **Explainable AI (XAI):** Integrating XAI techniques into ML models can enhance their interpretability, allowing security analysts to understand the rationale behind model predictions and trust the decisions made by automated detection systems.

5. Conclusion

In conclusion, machine learning presents a promising avenue for enhancing cyber-attack detection on internet traffic. However, the evolving landscape of cyber threats calls for a proactive and adaptive approach to model development and deployment. By addressing the challenges and seizing the opportunities identified in this research, the cybersecurity community can better safeguard digital assets and infrastructure against the ever-present threat of cyber-attacks.

Compliance with ethical standards

Disclosure of conflict of interest

No conflict of interest to be disclosed.

References

[1] IBM (2022), IBM Cloud Pak for Data, IBM Documentation for SPSS, https://www.ibm.com/docs/en/cloud-paks/cp-data/4.6.x

[2] Chou D. (2022), A survey on data driven network intrusion detection, ACM Computing Survey, https://doi.org/10.1145/3472753

[3] S. Dolev and S. Lodha, In Proceedings of the First International Conference, CSCML 2017, Beer-Sheva, Israel, June 29-30, (2017).

[4] Aljabri, M.; Aljameel, S. S., Mohammad, R. M. A., Almotiri, S. H., Mirza, S., Anis, F. M, Altamimi, H. S. (2021). Intelligent Techniques for Detecting Network Attacks: Review and Research Directions. Sensors, 21(21), 7070.

[5] Najafabadi M, Khoshgoftaar T, Calvert C, Kemp k, (2020) Middle traffic detecting man using Header packet information, published by reliability and quality International Conference

[6] Shiravi A, Shiravi H, Tavallaee M, and Ghorbani A. (2021), Toward mounting a logical method to make usual datasets for imposition detection, security, and computers.

[7] Sommer R and Paxson V. (2020). Freestanding the locked world. On expanding machine learning aimed at network imposition discovery, published by Security and Privacy.

[8] Yadav S, Selvakumar S. (2020). DDoS application layer Detection attacked by exhibiting user conduct using logistic deterioration. Published by Optimization and Infocom

[9] Zhao, J.; Jing, X.; Yan, Z.; Pedrycz. W. (2021). Network traffic classification for data fusion: A survey. Inf. Fusion 2021, 72, 22–47

[10] Xie, M.; Hu, J.; Slay, J. Evaluating host-based anomaly detection systems: Application of the one-class SVM algorithm. In Proceedings of the 2014 11th International Conference on Fuzzy Systems and Knowledge Discovery (FSKD), Xiamen, China, 19–21 August 2014

[11] Churcher, A.; Ullah, R.; Ahmad, J.; Ur Rehman, S.; Masood, F.; Gogate, M.; Alqahtani, F.; Nour, B.; Buchanan, W.J. An experimental analysis of attack classification using machine learning in IoT networks. Sensors 2021, 21, 446

[12] Rahman, R.U.; Tomar, D.S. (2018). Security attacks on wireless networks and their detection techniques. In Emerging Wireless Communication and Network Technologies: Principle, Paradigm and Performance; Springer: Singapore, 2018; pp. 241–270. ISBN 9789811303968

[13] Tuor, A.; Kaplan, S.; Hutchinson,, S. (2017). Deep learning for unsupervised insider threat detection in structured cybersecurity data streams. In Proceedings of the Artificial Intelligence for Cyber Security Workshop (AAAI-2017), San Francisco, CA, USA, 4–5 February 2017; pp. 224–234 .