European Journal of
Technology
(EJT)

Machine Learning in Cybersecurity: Techniques and Challenges

Jasmin Praful Bharadiya

European Journal of Technology
ISSN 2520-0712 (online)
Vol.7, Issue 2, pp 1 - 14, 2023

www.ajpojournals.org

Machine Learning in Cybersecurity: Techniques and Challenges

Jasmin Praful Bharadiya[1*]
[1]Doctor of Philosophy Information Technology, University of the Cumberlands, USA
[*]Corresponding Author's Email: jasminbharadiya92@gmail.com

Article history
Submitted 25.05.2023 Revised Version Received 30.05.2023 Accepted 02.06.2023

Abstract

In the computer world, data science is the force behind the recent dramatic changes in cybersecurity's operations and technologies. The secret to making a security system automated and intelligent is to extract patterns or insights related to security incidents from cybersecurity data and construct appropriate data-driven models. Data science, also known as diverse scientific approaches, machine learning techniques, processes, and systems, is the study of actual occurrences via the use of data. Due to its distinctive qualities, such as flexibility, scalability, and the capability to quickly adapt to new and unknowable obstacles, machine learning techniques have been used in many scientific fields. Due to notable advancements in social networks, cloud and web technologies, online banking, mobile environments, smart grids, etc., cyber security is a rapidly expanding sector that requires a lot of attention. Such a broad range of computer security issues have been effectively addressed by various machine learning techniques. This article covers several machine-learning applications in cyber security. Phishing detection, network intrusion detection, keystroke dynamics authentication, cryptography, human interaction proofs, spam detection in social networks, smart meter energy consumption profiling, and security concerns with machine learning techniques themselves are all covered in this study. The methodology involves collecting a large dataset of phishing and legitimate instances, extracting relevant features such as email headers, content, and URLs, and training a machine-learning model using supervised learning algorithms. Machine learning models can effectively identify phishing emails and websites with high accuracy and low false positive rates. To enhance phishing detection, it is recommended to continuously update the training dataset to include new phishing techniques and to employ ensemble methods that combine multiple machine learning models for better performance.

Keywords: *Security, Machine Learning, Survey, Machine Learning, Intrusion Detection, Spam Cybersecurity.*

European Journal of Technology
ISSN 2520-0712 (online)
Vol.7, Issue 2, pp 1 - 14, 2023

1.0 INTRODUCTION

In this age, the cyberspace is growing faster as a primary source for a node to node information transfer with all its charms and challenges. The cyberspace serves as a significant source to access an infinite amount of information and resources over the globe. In 2017, the internet usage rate was 48% globally, later it increased to 81% for developing countries. The vast range of cyberspace encompasses a lot more than just the internet, including users, system resources, participant technical expertise, and much more. Additionally, the cyber sphere significantly contributes to the countless vulnerabilities to cyberthreats and attacks. Cybersecurity is a collection of many strategies, tools, and procedures intended to protect cyberspace against threats and cyberattacks. Cybercrimes are expanding more quickly than the current cybersecurity system in the modern world of computers and information technology. A computer system's vulnerability to threats can be attributed to a number of factors, including a weak system configuration, untrained staff, and a dearth of techniques. More progress must be made in creating cybersecurity techniques due to the expanding cyber threats.

Attack strategies are advancing quickly to penetrate systems and elude generic signature-based defenses, much as web and mobile technologies are doing the same. Due to their ability to quickly adapt to novel and unknowable circumstances, machine learning techniques present prospective answers that can be used to resolve such difficult and complex issues. Many different machine learning techniques have been successfully used to tackle a variety of issues in computer and information security. This paper covers and emphasizes several machine-learning applications in cyber security. Machine learning: One of the primarily used advanced methods for cybercrime detection is machine learning techniques. Machine learning techniques can be applied to address the limitations and constraints faced by conventional detection methods.

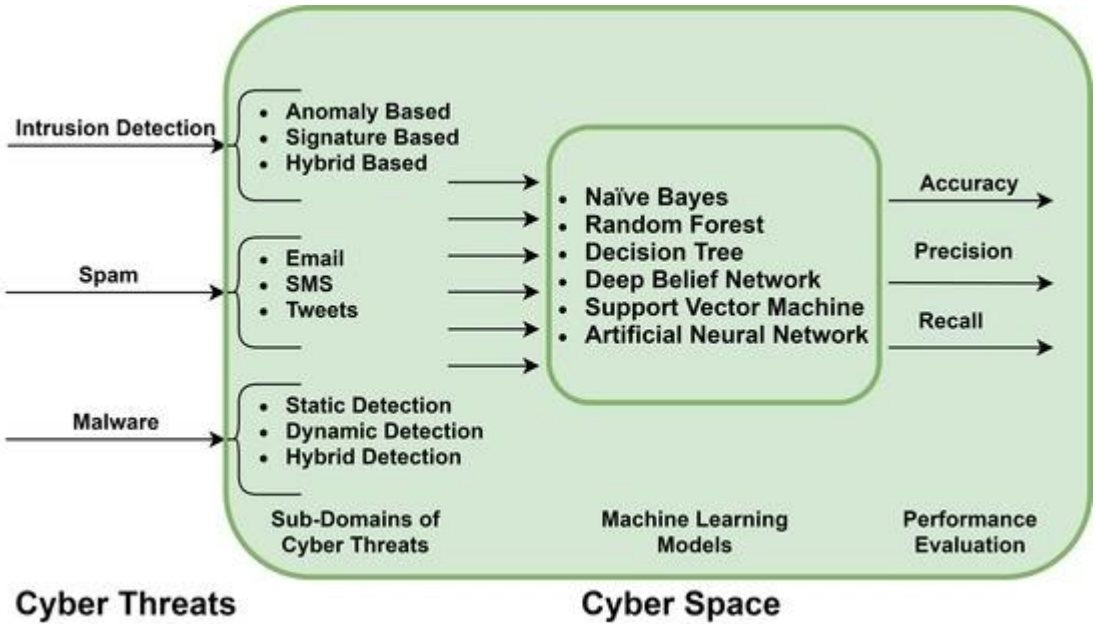

Figure 1: Cyber Threats in the Cyber Space

Cybersecurity's role as a machine learning capabilities and functions-

Machine Learning in Cyber Security

Cyber threats: Machine learning techniques are playing a vital role in fighting against cybersecurity threats and attacks such as intrusion detection system, malware detection, phishing detection, spam detection, and fraud detection to name a few. We will focus on malware detection, intrusion detection system, and spam classification for this review. Malware is a set of instructions that are designed for malicious intent to disrupt the normal flow of computer activities. Malicious code runs on a targeted machine with the intent to harm and compromise the integrity, confidentiality and availability of computer resources and services. Saad et al. in discussed the main critical problems in applying machine learning techniques for malware detection. Sad et al. argued that machine-learning techniques have the ability to detect polymorphic and new attacks. Machine learning techniques will lead to all other conventional detection methods in the future. The training methods for malware detections should be cost-effective. The malware analysts should also be able to keep with the understanding of ML malware detection methods up to an expert level. Ambalavanan et al. in described some of the strategies to detect cyber threats efficiently. One of the critical downsides of the security system is that the security reliability level of the computing resources is generally determined by the ordinary user, who does not possess technical knowledge about security.

Attacks such as replay, man-in-the-middle (MiTM), impersonation, credentials leakage, password guessing, session key leakage, unauthorised data update, malware injection, flooding, denial of service (DoS) and distributed denial of service (DDoS), among others, can be carried out against connected systems in the cyberspace. Therefore, in order to recognize and stop these assaults, we need some sort of security standard. Through the offered pre-processed dataset, the machine learning models (ML algorithms) may learn about various cyber assaults in the offline and online modes. The machine learning algorithms identify any indication of an incursion (a cyberattack) in real time, or in online mode.

Cybersecurity

Over the last half-century, the information and communication technology (ICT) industry has evolved greatly, which is ubiquitous and closely integrated with our modern society. Thus, protecting ICT systems and applications from cyber-attacks has been greatly concerned by the security policymakers in recent days. The act of protecting ICT systems from various cyber-threats or attacks has come to be known as cybersecurity. Several aspects are associated with cybersecurity: measures to protect information and communication technology; the raw data and information it contains and their processing and transmitting; associated virtual and physical elements of the systems; the degree of protection resulting from the application of those measures; and eventually the associated field of professional endeavor. Overall, cybersecurity concerns with the understanding of diverse cyber-attacks and devising corresponding defense strategies that preserve several properties.

- **Confidentiality** is a property used to prevent the access and disclosure of information to unauthorized individuals, entities or systems.
- **Integrity** is a property used to prevent any modification or destruction of information in an unauthorized manner.

- **Availability** is a property used to ensure timely and reliable access of information assets and systems to an authorized entity.

2.0 METHODOLOGY

In the world of cybersecurity, the use of machine learning techniques has grown in value, allowing for more efficient threat detection and response. The approaches used to use machine learning in cybersecurity are thoroughly reviewed in this article, with emphasis on their advantages, disadvantages, and practical applications.

Data Collection and Preprocessing

Acquisition of Relevant Data: Identifying and gathering cybersecurity datasets for model training and evaluation. Data Cleaning and Transformation: Preprocessing techniques to handle missing values, outliers, and ensure data quality. Feature Extraction and Engineering: Selecting informative features and creating new representations to enhance model performance.

Model Selection and Evaluation

Algorithm Selection: Choosing appropriate machine learning algorithms, such as decision trees, support vector machines, or neural networks, based on the problem and data characteristics. Training and Testing: Splitting the dataset into training and testing sets, ensuring appropriate sample sizes, and assessing model generalization. Performance Metrics: Determining evaluation metrics like accuracy, precision, recall, F1-score, and area under the curve (AUC) to measure the effectiveness of the models.

Model Training and Optimization

Model Training Techniques: Employing supervised, unsupervised, or semi-supervised learning approaches based on the availability and labeling of data. Hyperparameter Tuning: Optimizing model parameters to enhance performance using techniques like grid search, random search, or Bayesian optimization. Regularization and Overfitting Prevention: Applying techniques like L1 and L2 regularization, dropout, and early stopping to prevent overfitting.

Deployment and Integration

Real-time Monitoring: Implementing models into live systems for continuous monitoring and immediate response to cyber threats. Integration with Security Infrastructure: Incorporating machine learning models into existing security systems, such as intrusion detection or firewall systems. Model Updates and Maintenance: Establishing mechanisms to update models with new data and adapting to changing threat landscapes.

Spam

This process involves training a machine learning model on a dataset of labeled emails, where each email is categorized as either spam or non-spam. During training, the machine learning model learns patterns and characteristics that distinguish spam emails from legitimate ones. These patterns can include specific words or phrases commonly found in spam emails, the presence of certain types of attachments or URLs, or characteristics of the email sender. Once the model is trained, it can be deployed in a production environment, where it can analyze incoming emails and predict whether they are spam or legitimate. The model evaluates various features extracted from the email, such as the subject line, sender's address, content, and other relevant metadata. Based on the model's prediction, the email can be categorized accordingly. Spam emails can be filtered

out, preventing them from reaching users' inboxes, while legitimate emails can be allowed to pass through. It's important to note that the machine learning model needs to be regularly updated and maintained to adapt to new spamming techniques and patterns. As spammers continually evolve their tactics, the model must be retrained with fresh data to ensure its accuracy and effectiveness in categorizing spam.

Phishing Detection

Phishing is aimed at stealing personal sensitive information. Researchers [2] have identified three principal groups of anti-phishing methods: detective (monitoring, content filtering, anti-spam), preventive (authentication, patch and change management), and corrective (site takedown, forensics) ones.

Table 1: Principal Groups of Anti-Phishing Methods

Detective Solutions	Preventive Solutions	Corrective Solutions
• Monitors account life cycle • Brand monitoring • Disables web duplication • Performs content filtering Anti-Malware • Anti-Spam	• Authentication • Patch and change management • Email authentication • Web application security	• Phishing site takedown • Forensics and investigation

A comparison of phishing detection methods is presented, and it is found that many of the solutions being considered for phishing detection have a high percentage of missed detection. Researchers compared six machine learning classifiers, including Logistic Regression (LR), Classification and Regression Trees (CART), Bayesian Additive Regression Trees (BART), Support Vector Machines (SVM), Random Forests (RF), and Neural Networks (NNets), using 1,171 raw phishing emails and 1,718 genuine emails. Here is a summary of the error rates for each of the classifiers listed above.

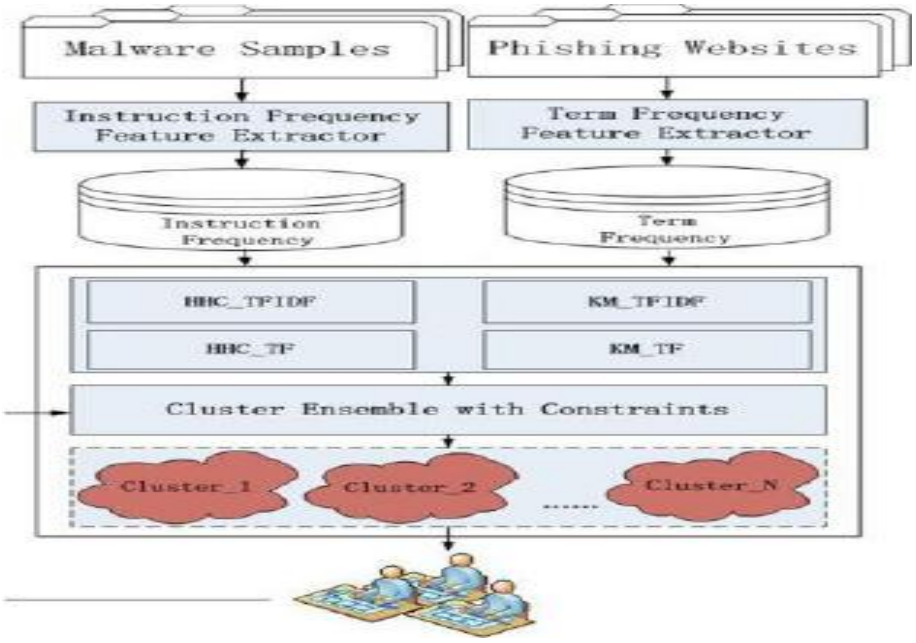

Figure 2: The Architecture of ACS

For experimentation, text indexing techniques were used for parsing the emails. All attachments were removed, "header information of all emails and html tags" from the emails' bodies as well as their specific elements were extracted. Afterwards, a stemming algorithm was applied and all the irrelevant words were removed. Finally, all items were sorted according to their frequency in emails. As a result of this work, it can be concluded that LR is a more preferable option among users due to low false positive rate (usually, users would not want their legitimate emails to be misclassified as junk). Also, LR has the highest precision and relatively high recall in comparison with other classifiers under contemplation

Breaking Human Interaction Proofs

Chellapilla and Simard [16] discuss how the Human Interaction Proofs (or CAPTCHAs) can be broken by utilizing machine learning. The researchers experimented with seven various HIPs and learned their common strengths and weaknesses. The proposed approach is aimed at locating the characters (segmentation step) and employing neural network [17] for character recognition. Six experiments were conducted with EZ-Gimpy/Yahoo, Yahoo v2, mail blocks, register, Ticketmaster, and Google HIPs. Each experiment was split into two parts: (a) recognition (1,600 HIPs for training, 200 for validation, and 200 for testing) and (b) segmentation (500 HIPs for testing segmentation). On the recognition stage, different computer vision techniques like converting to grayscale, thresholding to black and white, dilating and eroding, and selecting large CCs with sizes close to HIP char sizes were applied.

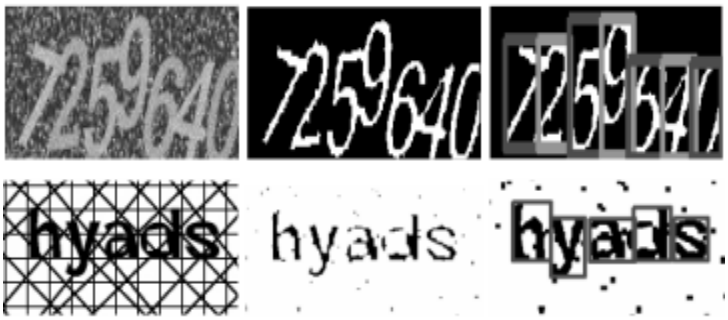

Figure 3: Types of Alphanumerical CAPTCHA

Intrusion Detection

Machine learning plays a significant role in cybersecurity intrusion detection. By leveraging its capabilities, machine learning algorithms can analyze large volumes of data, detect anomalies, and identify potential security breaches in real-time. Here's an overview of how machine learning is applied in cybersecurity intrusion detection:

Data Collection

Machine learning models require data to learn patterns and make predictions. In cybersecurity, relevant data sources include network traffic logs, system logs, user behavior data, and security event information from various sensors.

Feature Extraction

Once the data is collected, relevant features need to be extracted to represent the characteristics of normal and abnormal behavior. These features could include network traffic patterns, application usage, login activities, file access patterns, and more.

Model Training

The extracted features are then used to train machine learning models. Commonly used algorithms include decision trees, random forests, support vector machines, and deep learning techniques like neural networks. The models are trained on labeled datasets, where instances of normal and malicious behavior are properly classified.

Anomaly Detection

After training, the machine learning models can identify deviations from normal behavior. When deployed in a real-time environment, they continuously monitor network traffic and system logs, comparing incoming data against the learned patterns. Unusual patterns or behaviors are flagged as potential security threats or intrusions.

Alert Generation

When an anomaly is detected, the system generates an alert or notification to security analysts or administrators. The alert includes details about the detected anomaly, such as the type of intrusion, affected systems, and severity level. Analysts can then investigate and respond accordingly.

Model Adaptation

Cybersecurity threats are dynamic and constantly evolving. Machine learning models need to be regularly updated and retrained to adapt to new attack techniques. This involves incorporating new

data, adjusting model parameters, and fine-tuning the algorithms to maintain their effectiveness over time.

Collaborative Intelligence

Machine learning models can benefit from collaborative intelligence, where multiple models or systems work together to enhance intrusion detection capabilities. By sharing information and insights, models can improve their accuracy and identify sophisticated attacks that may involve multiple stages or components.

Cybersecurity Advance Techniques

Machine learning has proven to be a powerful tool in bolstering cybersecurity defenses by detecting and mitigating cyber threats. This article provides a comprehensive overview of various machine-learning techniques employed in cybersecurity, highlighting their capabilities and applications.

Anomaly Detection

Unsupervised Learning: Utilizing algorithms like k-means clustering, DBSCAN, or Isolation Forest to detect deviations from normal patterns and identify anomalous behavior. One-Class Classification: Employing techniques such as support vector machines (SVM) or auto encoders to build models that classify instances as normal or anomalous.

Intrusion Detection

Supervised Learning: Training models, such as decision trees, random forests, or support vector machines, to classify network traffic as normal or malicious based on labeled datasets. Deep Learning: Utilizing deep neural networks, such as convolutional neural networks (CNN) or recurrent neural networks (RNN), to analyze network traffic and detect intrusions.

Malware Detection

Signature-based Detection: Using pattern matching techniques to compare file or code signatures against known malware signatures. Behavior-based Detection: Employing machine learning models to analyze the behavior of files or code and identify suspicious or malicious activities.

Threat Intelligence

Text Mining and Natural Language Processing: Extracting valuable information from textual sources, such as security reports or social media, to identify emerging threats or vulnerabilities Sentiment Analysis: Analyzing sentiments expressed in cybersecurity-related data to gauge public opinion or detect potential risks.

User Behavior Analytics

Sequential Pattern Mining: Identifying patterns in user behavior sequences to detect abnormal or potentially malicious activities. Clustering and Profiling: Grouping users based on their behavior characteristics and detecting deviations from their normal patterns. Adversarial Machine Learning: Generative Adversarial Networks (GANs): Employing GANs to generate adversarial examples and evaluate model robustness against malicious attacks. Defensive Distillation: Implementing techniques to make machine learning models more resilient against adversarial manipulation.

Explainable AI in Cybersecurity

Interpretable Models: Developing machine learning models that provide transparent explanations for their decisions, enabling better understanding and trust in the system's outputs. Rule Extraction Techniques: Extracting human-readable rules from complex machine learning models to facilitate comprehensibility and explain ability.

Federated Learning for Privacy-Preserving Collaborative Security

Collaborative Threat Intelligence: Leveraging federated learning techniques to enable multiple organizations to share insights about emerging threats while preserving data privacy. Privacy-preserving Model Training: Training machine learning models on decentralized data sources without sharing raw data, thus maintaining data confidentiality.

Integration of Machine Learning with Big Data and Iota Security

Data Fusion and Analysis: Harnessing the power of big data to improve the accuracy and effectiveness of machine learning models in detecting and mitigating cyber threats. Secure Iota Ecosystems: Developing machine learning-driven solutions to enhance security measures and anomaly detection in vast Iota networks.

Context-aware and Adaptive Security

Context-aware Threat Detection: Developing machine learning models that consider contextual information, such as user behavior, network conditions, and system configuration, to improve threat detection accuracy. Adaptive Defense Systems: Creating dynamic defense systems that can adapt and evolve in real-time based on changing threat landscapes, leveraging machine learning to detect and respond to new attack vectors.

Human-in-the-Loop Machine Learning

Augmented Threat Intelligence: Combining human expertise with machine learning algorithms to enhance threat intelligence capabilities, leveraging human insights for model training and validation. User-Centric Security: Incorporating user feedback and behavior analysis to personalize security measures and provide proactive defense against targeted attacks.

Cybersecurity Challenges

Machine learning (ML) has been increasingly used in cybersecurity to detect and prevent various types of cyber threats. While ML offers numerous advantages, it also poses several challenges in the context of cybersecurity. Here are some key challenges associated with machine learning in cybersecurity:

Adversarial Attacks

Adversaries can attempt to manipulate or deceive ML models by exploiting vulnerabilities. Adversarial attacks include techniques like data poisoning, evasion attacks, and adversarial examples, where slight modifications to input data can mislead the ML model and compromise its effectiveness. Lack of labeled training data: Building accurate ML models requires large amounts of high-quality labeled training data. In the cybersecurity domain, obtaining such data can be challenging due to the limited availability of real-world cyber attack data, as well as the difficulty in labeling it correctly.

Imbalanced Datasets

Cybersecurity datasets often suffer from class imbalance, where the occurrence of positive (attacks) and negative (normal) instances is disproportionate. Imbalanced datasets can lead to biased ML models that perform poorly in detecting minority classes or exhibit high false-positive rates.

Interpretability and Explain Ability

Many ML algorithms, particularly deep learning models, are often considered "black boxes" due to their complex architectures. This lack of interpretability makes it difficult to understand the reasoning behind ML model decisions, hindering the ability to trust and explain their predictions, which is crucial in cybersecurity.

Concept Drift and Evolving Threats

The cybersecurity landscape is constantly evolving, with new threats and attack techniques emerging regularly. ML models trained on historical data may struggle to adapt to novel attacks or changing patterns, as they might not have encountered such instances during training.

Scalability and Performance

ML models in cybersecurity should be capable of handling large-scale, real-time data streams with low latency. Ensuring high performance and scalability can be a challenge, especially when dealing with computationally intensive ML algorithms or when operating in resource-constrained environments.

Privacy and Data Protection

ML models often require access to sensitive and private data for training and inference, raising concerns about data privacy and compliance with regulations like GDPR. Protecting the confidentiality of user information and preventing unauthorized access to ML models and their training data is crucial. Addressing these challenges requires ongoing research and development efforts to improve the robustness, resilience, and effectiveness of ML-based cybersecurity systems. Solutions may involve developing robust ML algorithms, designing resilient architectures, enhancing data collection and labeling techniques, incorporating explain ability methods, and adapting models to changing threats through continuous learning and monitoring.

3.0 CONCLUSION AND RECOMMENDATIONS

Conclusion

In conclusion, machine learning techniques are becoming quite useful in the cybersecurity industry. Traditional detection techniques have shown to be insufficient in addressing the developing nature of cybercrimes, given the rapid increase of cyber threats and attacks. By creating automated and intelligent systems that can analyse massive amounts of data, spot patterns, and spot potential security breaches in real-time, machine learning provides a solution. This article has covered a number of machine learning applications in cybersecurity, such as spam classification, malware detection, intrusion detection, and more. These software programmes make use of machine learning methods to improve threat detection and reaction times. Machine learning algorithms can learn to distinguish between legitimate and harmful activity by being trained on labelled datasets, making it possible to identify cyber threats and attacks. Yet, there are difficulties in applying machine learning to cybersecurity. The caliber and variety of the training data have a

significant impact on how well machine-learning models perform. Finding pertinent and representative information can be difficult, especially given how quickly cyber risks are developing. In order to adapt to new attack strategies, verify their correctness, and maximize their efficacy, machine-learning models also need to be continually updated and retrained. Using machine learning with big data and iota security also raises privacy and security issues. While using large data to boost the effectiveness of machine learning models, data privacy and confidentiality must be upheld. The development of methods like federated learning has made it possible to collaborate on threat intelligence while protecting the privacy of raw data.

Further developments in machine learning algorithms and methods will significantly improve cybersecurity precautions. AI that is interpretable and comprehensible will help people better comprehend and trust machine learning models' judgements. Additionally, combining machine intelligence with cutting-edge innovations like blockchain can improve cybersecurity systems' security and transparency. Overall, machine learning has enormous potential for tackling the intricate and constantly changing issues in cybersecurity. By utilizing its capabilities, enterprises may fortify their defenses, more effectively detect and address cyber threats, and safeguard vital systems and data in the digital age.

Recommendations

Some additional recommendations specific to machine learning techniques applied to cybersecurity:

Feature Selection and Engineering

In the field of cybersecurity, feature selection and engineering play a crucial role in identifying relevant features that can improve the performance of machine learning models. Look for resources that delve into techniques for selecting and engineering features specific to cybersecurity datasets.

Adversarial Machine Learning

Adversarial machine learning focuses on developing techniques to detect and defend against adversarial attacks aimed at manipulating or deceiving machine-learning models. Explore resources that discuss adversarial attacks and defense mechanisms in the context of cybersecurity.

Intrusion Detection Systems (IDS)

IDS is an important application of machine learning in cybersecurity. Look for resources that cover machine learning algorithms and approaches used in building effective IDS systems, such as anomaly detection or behavioral analysis.

Malware Detection and Classification

Machine learning can be applied to detect and classify malware based on its behavior, code analysis, or other features. Seek resources that provide insights into machine learning techniques used for malware detection and classification in cybersecurity.

Network Traffic Analysis

Analyzing network traffic data can help identify anomalies, detect intrusions, and prevent cyber-attacks. Look for resources that discuss machine-learning methods applied to network traffic analysis for cybersecurity purposes.

Threat Intelligence and Security Analytics

Machine learning can be leveraged for analyzing large volumes of security data and extracting meaningful insights. Explore resources that focus on applying machine learning techniques to threat intelligence and security analytics, enabling proactive identification and response to cyber threats.

REFERENCES

Anti-Phishing Working Group, "Phishing and Fraud solutions". [Online]. Available: http://www.antiphishing.org/. [Accesses: April 4, 2013].

Bharadiya, J. P. (2023). A Comprehensive Survey of Deep Learning Techniques Natural Language Processing. European Journal of Technology, 7(1), 58 - 66. https://doi.org/10.47672/ejt.1473

Bharadiya, J. P. (2023). Convolutional Neural Networks for Image Classification. International Journal of Innovative Science and Research Technology, 8(5), 673 - 677. https://doi.org/10.5281/zenodo.7952031

Bharadiya, J. P., Tzenios, N. T., & Reddy, M. (2023). Forecasting of Crop Yield using Remote Sensing Data, Agrarian Factors and Machine Learning Approaches. Journal of Engineering Research and Reports, 24(12), 29–44. https://doi.org/10.9734/jerr/2023/v24i12858

Densham B. Three cyber-security strategies to mitigate the impact of a data breach. Netw Secur. 2015;2015(1):5–8.

Hariri RH, Fredericks EM, Bowers KM. Uncertainty in big data analytics: survey, opportunities, and challenges. J Big Data. 2019;6(1):44.

Knowledge Discovery and Data Mining group, "KDD cup 1999". [Online]. Available: http://www.kdd.org/kddcup/index.php. [Accessed: March 3, 2013].

L. F. Cranor, S. Egelman, J. Hong, and Y. Zhang, "Phinding phish: An evaluation of anti-phishing toolbars", Technical Report CMUCyLab-06-018, CMU, November 2006.

Nallamothu, P. T., & Bharadiya, J. P. (2023). Artificial Intelligence in Orthopedics: A Concise Review. Asian Journal of Orthopaedic Research, 6(1), 17–27. Retrieved from https://journalajorr.com/index.php/AJORR/article/view/164

Qiao L-B, Zhang B-F, Lai Z-Q, Su J-S. Mining of attack models in ids alerts from network backbone by a two-stage clustering method. In: 2012 IEEE 26th international parallel and distributed processing symposium workshops & Phd Forum. IEEE; 2012. p. 1263–9.

S. Abu-Nimeh, D. Nappa, X. Wang, and S. Nair, "A Comparison of Machine Learning Techniques for Phishing Detection", APWG eCrime Researchers Summit, October 4-5, 2007, Pittsburg, PA.