Machine Learning: Enhancing Cybersecurity through Attack Detection and Identification

Darshana Pandya [1*], Abhijeetsinh Jadeja [2], Madhavi Bhuptani[3], Vandana Patel[4], Kinjal Mehta[5], Dipal Brahmbhatt[6]

Associate Professor, Shri C. J Patel College of Computer Studies (BCA), Sankalchand Patel University, Visnagar[1]
Professor, Department of Engineering, Darshan University, Rajkot, Gujarat [2]
Assistant Professor, Silver Oak College of Computer Applications, Silver Oak University, Ahmedabad, Gujarat [3, 4, 5, 6]

ddpandya.fcs@spu.ac.in[*1], abhijit.highereducation@gmail.com[2], madhavibhuptani.ca@silveroakuni.ac.in[3]
vandanapatel1011@gmail.com[4], sk19990711@gmail.com[5], hockeydeepal@gmail.com[6]

Abstract: Securing data and the systems that manage or store it is known as cyber security. Cyber security violations are the most frequent crime performed by online attackers using one or more systems on one or more networks or systems. These cyberthreats can rapidly steal or lose data, as well as partially or totally shut down network systems. Because cyber-attacks are always developing, manually detecting them can be time-consuming and expensive. Consequently, they may be found and classified using machine learning approaches. This study focuses on a survey of the current algorithms for machine learning research in cyber security.

Keywords: Machine Learning, Cyber Security, IoT, Cyber attacks

I. INTRODUCTION

The internet is influencing more and more people's social lives and habits on a daily basis. The Internet's role in society is progressively expanding as a result of globalization. The Internet is interwoven with crucial governmental infrastructure, and it is quickly emerging as one of the most significant engines of socioeconomic development. The Internet's developing and deepening structure exposes us to new dangers, whose variety is continually expanding. One of the most crucial problems in modern cyber-security is how these risks might be found in network traffic. A system called cyber-security was created to safeguard the network's hardware, programs, and data from unwanted access and manipulation.

Mathematical models have been used in machine learning (ML) algorithms for classification, clustering, regression, and other tasks [1]. Using a machine-learning procedure called training; data samples are processed to construct a machine-learning model. Then, this model can be put to a variety of uses. The performance of a computer learning model is dependent upon the traits chosen from the educational data as well as on other elements like the machine learning method utilized. The efficiency of a machine learning model is assessed by how well it can categorize, cluster, or predict desired values. By using more data or by transforming the data into different formats, the model's accuracy can be improved [2].

Numerous security weaknesses have also been brought about by increased internet use. Several technologies, like as firewalls, data encryption, and user authentication, are used to address these security flaws. These safety precautions protect against a variety of attacks. However, thorough packet analysis is not possible with these security technologies. They are unable to identify attacks at the desired level as a result. Systems for intrusion detection and prevention (IDS) have been created to fill in the gaps left by these security measures. Thanks to their algorithms, which include machine learning, deep learning, and artificial intelligence, these systems are able to analyze data more thoroughly than other security systems [3].

II. IMPORTANT FIGURES & PARTS

The potent powers of machine learning are equally applicable to cybersecurity. Machine learning is being used in cybersecurity to enhance malware detection, priorities events, locate breaches, and notify enterprises of security risks. Machine learning may identify sophisticated threats and targeting, including infrastructure vulnerabilities, organizational profiling, and potentially interconnected vulnerabilities and exploits [5].

Adapting IoT to everyday lives has been a great threat due to (DoS) Denial of Service and Scattered Disowning of Service attacks (DDoS). DoS attacks are cyber-attacks in which the attacker floods the network with massive spam requests that exceed the server's handling capacity, preventing legitimate network requests from being processed. In a

DoS attack, the attacker temporarily or permanently disables a resource/device from its intended users. In a DDoS attack, the incoming traffic flooding the resource/device comes from a variety of sources, making it difficult to pinpoint the source of these attacks. Since the first incident of Scattered Denial of Service (DDoS), the majority of DoS attacks have been distributed in nature. [6] Some of the IOT characteristics and challenges [7] are listed in table 1.

TABLE I
CHARACTERISTICS AND CHALLENGES IN IoT

Properties of IoT	• IoT applications' cybersecurity issues
Large-scale adoption	• Multiple devices are used to distribute data. • Network overhead; • Device individual protection.
Number of variables	• Equipment with a wide range of capabilities. • The requirement for various solutions to secure various devices.
Minimal rates and resources communications	• IoT equipment has high energy requirements. • A strong mechanism for assuring dependable communication is absent from networking protocols. • Distributed cybersecurity solutions for IoT applications should take into account unstable connections.
Low latency	• Time constraints may apply to IoT applications. • Delays will be added for complex cybersecurity solutions.

Because of the large and quick expansion of technology computer network attacks, network traffic anomaly detection is critical in cyber security. Indeed, as new Internet-related technologies are developed, the more sophisticated the attacks become. One of the most challenging problems is preventing dictionary-based brute-force attacks (BFA). in today's high-level attacks. We must create effective methods for detecting and mitigating such brute-force attacks in real-time, and hence we use machine learning algorithms. [10] The entire computing paradigm has changed as a result of improvements in information and communication technology. These developments have led to the development of IoT communication. The IoMT allows medical devices to communicate with one another and exchange private data security issues, including password guessing, man-in-the-middle attacks, denial of service attacks, remote hijacking, and impersonation. Critical IoT connectivity data may be exposed, changed, or even made unavailable to authorized users in the case of such attacks. Protecting the IoMT is essential because distributed denial-of-service (DDoS) attacks have cost businesses and governments throughout the world a large amount of money. These figures are consistent with the increasing number of Internet of Things-enabled devices paradigm, which is characterized by the idea of linking everything, anywhere, at any time. The DDoS volumetric attack, which accounts for more than 65% of all such attacks, is one of the most hazardous harmful traffic on the Internet. A volumetric DDoS assault aims to overwhelm the target's computing capacity or nearby network links by coordinating the coordinated delivery of a massive number of meaningless materials.

Ransomware prevents If a ransom is not paid, the hacker gains access to the victim's data and threatens to delete it. The Trojan horse is the riskiest type of malware since it impersonates useful and common software with the primary goal of stealing financial data. It's common to launch a drive-day attack to spread malware. Any user activity must enable these data. After visiting a seemingly innocent website, users' computers are secretly infected, turning them into IFrames that direct the victim's browser to an attacker-controlled website. The goal of SQL injection (SQLI) modifies information from a back-end database that wasn't meant to be displayed by using malicious code. By entering malicious code into a search field on a susceptible website, attackers might execute a SQL injection. The threat posed by an unidentified security flaw for which a fix has not yet been made available or about which the software creators are in the dark is referred to as a zero-day exploit attack. The developers need to be always alerted in order to recognize this threat.

DNS tunnelling sends HTTP and other protocol traffic across the DNS protocol to convey non-DNS traffic over port 53. Since employing DNS tunnelling is a frequent and acceptable practice, its usage for nefarious purposes is frequently disregarded. Attackers are able to mask outbound traffic as DNS, hiding shared data via an internet connection.

1. User-to-Root-Attack (U2R): This type of attack begins with the perpetrator seeking to obtain a client's prior access and then takes advantage of the gaps to seize root control.
2. Remote-to-Local-Attack (R2L): This interruption occurs when the aggressor can send data packets to the target but does not have a client account on that machine. In this interruption, the aggressor tries to exploit a flaw to gain access to the area by pretending to be the target machine's current client.
3. Probing-Attack: This type of attack involves the perpetrator trying to gather information about the company's PCs

with the clear intention of getting past the firewall and gaining root access.

III. REVIEW OF EXISTING ML TECHNIQUES IN CYBER SECURITY ISSUES

A. Using machine learning, effectively classify secure and insecure bug reports

Traditionally, human classification of bugs is based on severity. It becomes a very tedious process to classify the bugs manually because of the very high growth rate of internet usage and bugs related to it. Hence an automated way of classifying bugs is defined using Natural Language Processing (NLP) or pre-processing and then Artificial Neural Networks (ANN) for classifying them to secure and non-secure bugs [4].

1) Shortcomings identified from previous research: Previous research limited the research to supervised learning algorithms to classify the bugs which have a very limited scope in the ever-developing internet world. The classifier can predict accurately only the bugs that were defined in the datasets feed to them for training. Newer bugs are found every day. If they are to be fed to the classifier, the whole process from pre-processing to the training and testing should be done again which is not practical.
2) Recommended Solution: The performance of the classifier can be improved by improving the data used for building the classifier. Instead of using a supervised learning algorithm for classification, Reinforcement learning [7] can be used since bugs keep evolving and varieties come in day by day. The study itself says that the labelled datasets have many errors caused by the manual labelling of the data.

Hence using them can never be a perfect solution for classification problems like this. The skewed real-world data cannot be solved using conventional classification algorithms. [8]. Solutions like the Markov Decision Process (MDP) can be used in the classifier part of the proposed algorithm instead of stacked Naive Bayes. Here the RL classifier starts with zero knowledge in the field and the environment gives an immediate reward when the prediction is correct and returns a punishment when it predicts wrongly. For a problem which has tremendous datasets and sufficient people to guide, the algorithm keeps learning from the data which will make it as powerful as the supervised learning algorithm in the existing research. When it starts to learn from newer data that it encounters after deployment, it finds overhead over conventional supervised learning algorithms.

The common family of algorithms for determining the best course of action for finite states and actions Storage is needed for MDPs value V, which holds real values, and policy, which holds actions, is two arrays that are indexed by state. The answer and the discounted sum of the benefits that, on average, can be obtained by implementing that answer from states will be contained in V(s) at the conclusion of the algorithm. The algorithm consists of two parts a value change and a policy update, respectively. Until no more changes are made, each of these processes is repeated for each state in the specific order made. Using an earlier estimation of those values, both recursively update new estimates of the ideal state value and policy:

$$V(s) := \sum_{s'} P_{\pi(s)}(s,s') \left(R_{\pi(s)}(s,s') + \gamma V(s') \right)$$

$$\pi(s) := \operatorname{argmax}_a \left\{ \sum_{s'} P_a(s,s') \left(R_a(s,s') + \gamma V(s') \right) \right\} \tag{1}$$

Depending on the algorithm variant, one can perform them in a specific order Alternatively, more frequently to some states than others, state by state. The algorithm will eventually reach the right answer as long as no state is permanently excluded from either of the phases.

B. Use of Using machine learning to identify intrusions IoT

Three approaches were developed. The first approach is anomaly detection, for which a training dataset was tested against five classifiers - Decision trees, SVMs, neural networks, and random forests are examples of and K-nearest. The accuracy percentages varied from 0.999 to 0.991. The second method involved utilizing ML to find DDoS. using Software-defined Networks (SDN). NMETA2 was used to implement the ML algorithm. False positive rates were less than 0.3%. The third approach used artificial neural networks. False-negative results were higher. [6]

1) Shortcomings identified from previous research: Accuracy rates for the three models were pretty same but detection rates for neural networks had higher potential. The models gave high false positives and false negatives as well.
2) Recommended Solution: By increasing the training data volume, the results can be improved in terms of accuracy and replicability.

C. Machine learning to detect cyber-attacks inside of technologically technologies

Systems that are computer security are a combination of digital and physical systems. Attacks are focused on it. We begin by pulling data from the CPS database and then normalizing the data to remove errors and duplicate entries. The characteristics are obtained through the use of a technique known as (LDA). The Heuristic Multiswarm Ant colony

Optimization process is used in conjunction with it to optimize the system's Fuzzy Logic-based Hidden Markov Model. The normalization of data using the formula:

$$\text{value after normalization} = \frac{\text{value before normalization}}{\text{max - min}} \tag{2}$$

Results were recorded thereafter. A histogram was plotted using the data on the x-axis and the y-axis as their instances or occurrences. Existing and proposed techniques were compared in terms of precision, true positive frequency, and false positive rate, threshold decisions, ROC curve (FPR versus detection rate for changing predefined threshold values).

1) Shortcomings identified from previous research: It has been hampered by performance constraints caused by massive computer processes.
2) Recommended Solution: To research and find better algorithms that could reduce the computations.

D. Using Genetic Programming, a Pragmatic Optimal Approach for Cyberattack Detection

Approaches used are Data collection, where a new dataset containing modern types of DDoS attacks is used. There were 2,160,668 instances in the dataset. Preprocessing, in which PCA was used on the Modern DDoS Dataset to reduce the features to 8, 16, and 20 major components. And finally, The Implementation of Genetic Programming (GP). [11]

1) Shortcomings identified from previous research: The GP model's performance was quite low compared to using either the mutation or crossover techniques.
2) Recommended Solution: Look for more efficient and usable resources that can help make the model be used for the detection of more complex attacks.

E. Cyber-attacks on the Machine Learning-Based Internet of Things Detection

This article explains how machine learning techniques are used in IoT network threats. can be used to prevent them. They evaluated seven popular machine learning classifiers using the Bot-IoT dataset, including Quadratic Discriminant Analysis, Random Forest, AdaBoost, K-Nearest Neighbors, Iterative Dichotomiser, Multilayer Perceptron, and Nave Bayes. Here, feature extraction, data preprocessing, data splitting, feature selection, and machine learning algorithm implementation are the five crucial processes for assessment. After analyzing the data, it was discovered that the accuracy of the f-measure was 0.99 for the k nearest neighbours. [13]

1) Shortcomings identified from previous research: Accuracy rates of all machine learning models were different, and Naive Bayes has the lowest accuracy (0.77) f- measures.

2) Recommended Solution: using the Feature selection step's top seven features to apply machine learning methods to the whole data set. This makes the Naïve Bayes and random forest algorithm running time is reduced and performance is increased slightly.

F. Detecting cyber-attacks in an intelligent grid using Machine learning algorithms

In this paper, RFC model outstrips all the other models therefore it was considered as best. It was chosen as the base model because of its robustness and design. The goal of this research was to create a sequential model with improved precision and accuracy at a cheap computational cost. There are two layers to this model. The first level of the problem categories events into natural and attack events. In detecting a natural event, this layer has a 99% accuracy rate. The data is sent on to the lower-level sub-problem, which categories the data based on 27 classifications of attacks, if the upper level qualifies the data as an attack event. The model's total accuracy is 95.44%. [14]

$$\text{Accuracy} = \frac{\text{TP} + \text{TN}}{\text{TP} + \text{FP} + \text{FN} + \text{TN}} \tag{3}$$

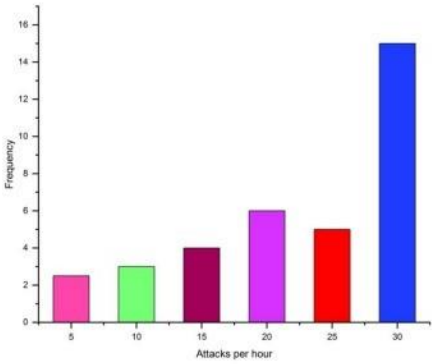

Figure 1: Attacks per Hour vs Frequency plot

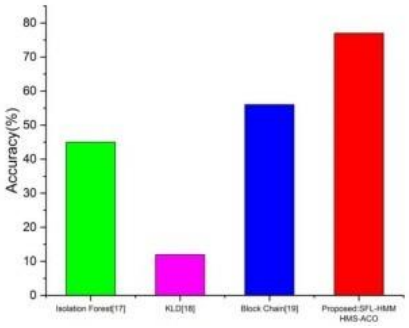

Figure 2: Existing techniques comparison based on Accuracy

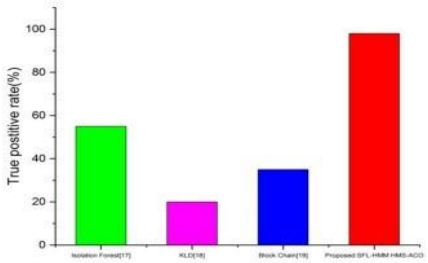

Figure 3: Existing techniques comparison based on TPR

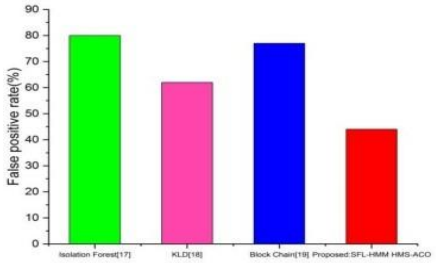

Figure 4: Existing techniques comparison based on FPR

1) Shortcomings identified from previous research: The deep learning model has various restrictions, such as the limited amount of accessible time attack data, which makes it difficult for deep learning to function well. Another problem with the attack datasets now in use is a class imbalance that causes model training to disproportionately favour the normal state over the strike condition.
2) Recommended Solution: The performance of existing models like the can be improved by training the model using class balancing techniques. Random forest classifier model. Which works better and at a low cost?

G. Machine Learning for SCADA Systems' Reliable Network Attack Detection

The increasing adoption of connection and the standardization of open SCADA protocols have led to an increase in the frequency and variety of malicious breaches. The detection of attacks that do not already exist in databases is impossible with outdated intrusion detection systems. In this article, Mississippi State University real-time data sets from the gas pipeline system are used to evaluate machine learning for intrusion detection in SCADA systems. Four techniques are used to estimate missing data and two techniques are used to normalize data. Results demonstrate that Random Forest effectively detects intrusions, with an F1 score greater than 99%. [12]

1) Shortcomings identified from previous research: When dealing with categorical variables, random forests are found to be biased. It has a slow training time and is unsuitable for linear methods with a large number of sparse features.
2) Recommended Solution: Additionally, the Kernel Principal Component Analysis (KPCA) and Support Vector Data Description can be applied. Machine learning techniques used to forecast the manner of a cyber-attack and its perpetrator.

One of the major concerns in the world now is cyber-attacks. Every day, they seriously harm people and nations' economies. Cybercrime is also on the rise along with cyber-attacks. This study used machine learning to analyze two alternative models of cybercrimes and forecast the impact of specific attributes on the identification of attack vectors and perpetrators. It arrived at this conclusion after using eight machine learning techniques in its approach. Static Vector Machine With an accuracy rate of 95.02%, linear was discovered to be the most effective cyber-attack detection technique. The first model was able to accurately anticipate the kinds of attacks that victims are most likely to experience. With an accuracy of 65.42%, Logistic Regression was the second-best method for identifying attackers. Whether offenders might be recognized by comparing their traits was predicted by the second model. The findings indicated that as victims' levels of education and income rise, the risk of cyber-attack declines. Here it suggests a technique that anticipates and identifies cyber-attacks that make use of both data from earlier cybercrime incidents and machine learning techniques [17].

1) Defects discovered from earlier study Support vector machine techniques are unsuitable for large data sets. [18] It performs poorly when the target classes overlap and there is greater noise in the data set. When there are more attributes for each data point than there are training data samples, the support vector machine will not perform well. The support vector classifier inserts data points above and below the classifying hyper plane, therefore there is no probabilistic justification for the classification.
2) Recommended Solution: In order to avoid SVM overfitting, a novel sparse-coding kernel method is used. Gene-Switch-Marker (GSM) uses SVM overfitting on single genes to capture relevant biomarkers. ML-based method for detecting and notifying cyberattacks.

Cybercrime is on the rise and takes use of a variety of computer environment flaws. It is crucial to develop effective methods in the field of cyber security. The bulk of IDS strategies in use today can't handle how dynamic and complex computer network threats are. The success of machine learning in resolving cyber security problems, it has recently taken on a significant role in the field. [19] Major cyber security concerns like Machine learning techniques have been used to combat intrusion detection, malware categorization and detection, spam detection, and phishing detection. Here, the main goal is to fundamentally differentiate the process of identifying attacks from these other applications, which makes it much harder for the intrusion detection community to properly use machine learning. The bulk of IDS strategies in use today can't handle how complicated and dynamic computer network threats are. [20] Consequently, efficient adaptive strategies, including various machine learning approaches, can result in decreased false alarm rates, higher detection rates, and appropriate computing and communication costs. Here are a few significant machine learning-based

intrusion detection algorithms discussed. IDSs can be designed with ML techniques that have a high rate of detection, low percentage of false positives, and ability of system to quickly adjust to evolving harmful behaviour. IDS use a range of machine learning techniques, such as Random Forest, Decision Tree, and Deep Learning, to enhance performance in different dimensions. Logistic Regression. In accordance with the requirements, an IDS need to offer the most effective solution [21].

1) Shortcomings identified from previous research: Here, it is impossible to predict when, when, or how an attack would occur, therefore complete protection from them is not yet possible.
2) Recommended Solution: Forecast future attacks, Audit data protection techniques, Optimize and reduce costs, detect unknown threats, and detect unknown threats.

IV. SUMMERY

This study's primary objective was to apply machine learning (ML) techniques to perform early cyber-attack detection on the physical system. We researched and looked at several alternative methods for launching a cyber-attack. The methods used to launch cyber-attacks have changed dramatically in recent years. There is a constant need for new varieties of detection systems because those who engage in cybercrime are constantly coming up with new ways to get around security measures. The identification of cyber attackers required the adoption of ML techniques due to the enormous amount of information that had to be gathered from a variety of different sources.

REFERENCES

[1] Huseyin Ahmetoglu and Resul Das, A thorough study on the detection of cyber-attacks: Data sets, methodologies, difficulties, and future research directions, Internet of Things, Volume 20, 2022, 100615, ISSN 2542-6605, https://doi.org/10.1016/j.iot.2022.100615.

[2] Umer Farooq, Noshina Tariq, Muhammad Asim, Thar Baker, and Ahmed Al-Shama'a, "Machine learning and the Internet of Things security: Solutions and open challenges," Journal of Parallel and Distributed Computing, Volume 162, Issue 2, 2022, pp. 89–104, ISSN 0743–7315, doi: 10.1016/j.jpdc.2022.01.015.

[3] N. Mane, A. Verma, & A. Arya (2020, November). a realistic best practice for applying genetic programming to detect cyberattacks. IEEE's 20th International Symposium on Computational Intelligence and Informatics (CINTI) will take place in 2020. (pp. 71-76). IEEE.

[4] Detection of Cyber Attack in Network Using Machine Learning Techniques by Diwakar Reddy M, Bhoomika T Sajjan, Anusha M, SyedJafar Sadiq B M, and Shambulingappa H S (2021).

[5] Sanjay Gaur, Darshanaben Dipakkumar Pandya (2019), Closest Fit Approach for Pattern Designing to Recovered Anomalous Values in Data Mining, 2018 Second World Conference on Smart Trends in Systems, Security and Sustainability (WorldS4), 308-312 IEEE Xplore, DOI: 10.1109/WorldS4.2018.8611610

[6] Sanjay Gaur, MS Dulawat (2011), Improved Closest fit Techniques to handle missing Attribute values, Journal of Computer and Mathematical Sciences Vol-2, no-2, 170-398.

[7] Y. Wang, G. Zha, R. Li, and S. Yu, "Intrusion Detection Systems in the Era of Big Data: A Review," IEEE Access, Volume 6, 2018, pp. 68732-68749, DOI: 10.1109/ACCESS.2018.2880687.

[8] F. Xiao, "Internet of Things: Security and privacy in a connected world," Communications of the ACM, Volume 61, Issue 9, 2018, pp. 26-28, DOI: 10.1145/3241035.

[9] K. K. Singh and N. Sharma, "Survey on Machine Learning Techniques for Intrusion Detection Systems," International Journal of Advanced Research in Computer and Communication Engineering, Volume 5, Issue 3, 2016, pp. 1035-1038.

[10] J. Zhang and M. Zulkernine, "A Machine Learning-Based Intrusion Detection System," International Journal of Network Security, Volume 8, Issue 2, 2009, pp. 105-111.

[11] N. A. Bhuiyan, M. S. A. Hossain, and M. I. A. Aziz, "A Comprehensive Study of Cyber-Physical System and Its Security: Vulnerabilities, Threats, Attacks, and Tools," IEEE Access, Volume 9, 2021, pp. 29703-29722, DOI: 10.1109/ACCESS.2021.3058525.

[12] T. M. Mitchell, "Machine Learning," McGraw-Hill Education, 1997, ISBN: 978-0070428072.

[13] L. Breiman, "Random Forests," Machine Learning, Volume 45, 2001, pp. 5-32, DOI: 10.1023/A:1010933404324.

[14] R. Duda, P. Hart, and D. Stork, "Pattern Classification," Wiley-Interscience, 2000, ISBN: 978-0471056690.

[15] I. Goodfellow, Y. Bengio, and A. Courville, "Deep Learning," MIT Press, 2016, ISBN: 978-0262035613.

[16] M. S. A. Hossain, "IoT and Cloud Computing: A Deep Dive into the Cyber-Physical Systems," IEEE Transactions on Industrial Informatics, Volume 14, Issue 9, 2018, pp. 4256-4266, DOI: 10.1109/TII.2018.2829996.

[17] J. Quinlan, "C4.5: Programs for Machine Learning," Morgan Kaufmann Publishers Inc., 1993, ISBN: 978-1558602380.

[18] N. Cristianini and J. Shawe-Taylor, "An Introduction to Support Vector Machines and Other Kernel-based Learning Methods," Cambridge University Press, 2000, ISBN: 978-0521780193.

[19] D. Barber, "Bayesian Reasoning and Machine Learning," Cambridge University Press, 2012, ISBN: 978-0521518147.

[20] T. Hastie, R. Tibshirani, and J. Friedman, "The Elements of Statistical Learning: Data Mining, Inference, and Prediction," Springer, 2009, ISBN: 978-0387848570.

[21] P. Domingos, "The Master Algorithm: How the Quest for the Ultimate Learning Machine Will Remake Our World," Basic Books, 2015, ISBN: 978-0465065707.