Tuijin Jishu/Journal of Propulsion Technology
ISSN: 1001-4055
Vol. 45 No. 3 (2024)

Computational Intelligence for Cyber Defense: A Review

Dr. Ravi Choubey*
**Ad hoc Lecturer in the Department of Computer Science.*
Government Girls P.G. College Ratlam,(M.P.), India.

Abstract: Cyber-attacks pose a continuous and escalating threat, demanding ever-more sophisticated defense mechanisms. Traditional signature-based detection methods struggle to adapt to the rapidly evolving attack landscape.[1] This paper explores the potential of machine learning (ML) as a powerful tool for cyber-attack detection. Review recent advancements in the field. The reviewed research highlights the effectiveness of various ML techniques, including deep learning models, for identifying anomalies and patterns indicative of malicious activity. The paper also discusses key challenges, such as the need for high-quality training datasets and the computational demands of certain ML algorithms. Finally, we explore promising future directions, including the integration of ML with other security solutions and the development of self-learning models that can autonomously adapt to evolving threats.[7] By leveraging the power of machine learning, we can significantly enhance our ability to detect and prevent cyber-attacks, safeguarding our digital infrastructure and fostering a more secure online environment.

***Keywords*:** Machine learning, Data Science, Cyber Attacks.

1. Introduction: Imagine a world where every click, every keystroke, every message zipping across the internet leaves a digital trail. This interconnectedness, a hallmark of our modern age, has revolutionized how we connect, conduct business, and access information at our fingertips. But this very connectivity, this kind of information exchange, has also become a playground for a new kind of bandit the "cyber-criminal". These digital world cyber criminals are everywhere on the web, constantly searching for new and sophisticated methods to exploit vulnerabilities, steal our data, and disrupt critical services. The cost of cybercrime is breaching privacy. the threat to national security ever-present. But fear not, for in the face of this evolving digital threat landscape, a new breed of hero emerges: the data scientist. Data science, a potent blend of statistics, computer science, and real-world knowledge, is becoming a crucial weapon in the fight against cybercrime.[2]

Imagine having a team of skilled detectives meticulously analyzing vast amounts of data, looking for even the smallest signs of trouble – a blip in network traffic, an unusual pattern in user behavior. One of the most powerful tools at their disposal is machine learning (ML). Think of ML as a highly advanced detective that not only examines data but also learns and evolves over time. ML algorithms can process extensive datasets of network activities, user behaviors, and historical cyber attacks. By uncovering intricate patterns and correlations hidden within this data, these algorithms can predict and prevent future attacks before they occur.[10]

Unlike traditional security measures that rely on predefined rules for known threats, ML can adapt and learn dynamically. It's like having a detective who not only recognizes a criminal's face but also detects suspicious behaviors like a change in demeanor or a nervous gesture – all potential signs of impending danger.

1.1 Types of Cyber Attacks:

Cyber attacks come in various forms, each targeting different vulnerabilities and aiming to exploit weaknesses in digital systems. Some common types of cyber-attacks include:

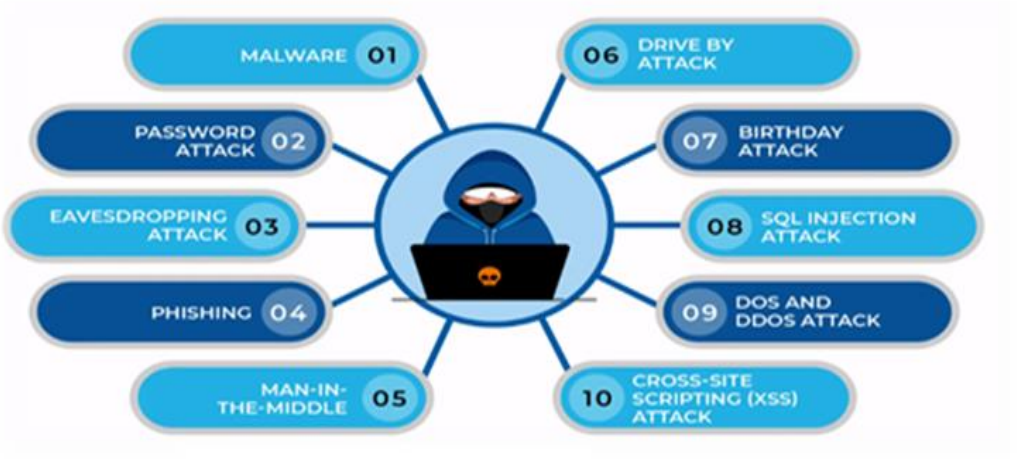

Fig.Types of Cyber Attacks [9]

- **Malware**: Malicious software designed to infiltrate and damage computer systems, such as viruses, worms, Trojans, and ransomware.
- **Phishing**: Deceptive techniques used to trick individuals into divulging sensitive information, often through fraudulent emails, messages, or websites.
- **Denial-of-Service (DoS) and Distributed Denial-of-Service (DDoS)**: Attacks that overwhelm a network or server with traffic, causing it to become unavailable to users.
- **SQL Injection**: Exploiting vulnerabilities in web applications by injecting SQL code to manipulate databases and gain unauthorized access.
- **Man-in-the-Middle (MitM)**: Interception of communication between two parties, allowing attackers to eavesdrop or manipulate the data transmitted. [8]

2. Literature Review

Deep Learning For Enhanced Cyber-Attack Detection,(S. N. A, B. K, G. E and M. I. C, "*2024)[3]:* In this paper uses an auto encoder to extract features from network traffic data, reducing processing costs. It then evaluates machine learning classifiers for attack detection, with K-Nearest Neighbor achieving a high 99.28% accuracy. DDoS Attack Detection Using Ensemble Machine Learning Models with RFE Algorithm(Tanut Visetbunditkun et.al 2022)[4]: In this paper focused on Distributed Denial of Service Attack (DDoS-Attack). This study proposes an ensemble machine learning approach with RFE for DDoS attack detection. It boasts high accuracy, reduced processing time, and lower CPU usage compared to traditional methods, making it a promising solution for resource-constrained environments. Cyber security using Machine Learning in the Digital Education industry(S.Shukla et.al, 2021)[5]: This paper explores these challenges and proposes leveraging machine learning, a powerful AI tool, to enhance threat detection in education, offering a significant advantage over traditional methods. Detection of Phishing Websites using Machine Learning Approaches(Farashazillah Yahya; Ryan Isaac W Mahibol, et.al. 2021)[6]:: This study explores using machine learning to identify phishing websites amid a rise in cyberattacks during the COVID-19 pandemic. Analyzing a dataset of over 11,000 websites, the research compared three models: Decision Tree, K-Nearest Neighbor (KNN), and Random Forest. While KNN achieved the highest accuracy (97.6%), Random Forest offered a lower false-negative rate, making it potentially better suited for real-world applications. Further investigation with different datasets and models is recommended.

Table 1: Comparison of Techniques

Title	Authors	Year	Focus	Techniques	Strengths	Limitations
Deep Learning For Enhanced Cyber-Attack Detection	Suhana Nafais A; Boomikka K. at.el	2024	Cyber Security	Supervised Machine Learning	- Effective for social IoT network attack detection	- Lacks details on specific deep learning architecture
DDoS Attack Detection Using Ensemble Machine Learning Models with RFE Algorithm	Tanut Visetbunditkun et.al	2022	DDoS Cyber Attack	Ensemble Machine Learning Algorithm	High Accuracy: The study suggests the approach achieves better accuracy.	**Black Box Nature of Ensembles:** Ensemble models can be complex and difficult to interpret
Cyber security using Machine Learning in Digital Education industry	S.Shukla et.al.	2021	Cyber Attacks in Digital Education Institute	Deep Neural Network, Supervised Machine Learning	99% accuracy to find Post Attack	Algorithm do not work on Real time

3. Key Findings and Discussion

The reviewed research highlights the promising potential of machine learning for cyber attack detection. Here are some key findings:

Machine learning algorithms can effectively identify patterns and anomalies indicative of various cyber attacks, including Denial-of-Service (DoS) attacks, malware infiltration, and unauthorized access attempts.

Supervised learning techniques, such as random forests and support vector machines (SVMs), demonstrate high accuracy in classifying network traffic as normal or malicious when trained on labeled datasets.

Unsupervised learning approaches, like anomaly detection algorithms, are valuable for identifying novel attacks unseen in training data.

Deep learning architectures, such as convolutional neural networks (CNNs) and recurrent neural networks (RNNs), can extract complex features from network traffic data, leading to improved attack detection accuracy.

4. Conclusion

In conclusion, this research explored the effectiveness of machine learning in detecting phishing websites. Three supervised learning models (Decision Tree, K-Nearest Neighbor, Random Forest) were evaluated, all achieving high accuracy (over 91%). While K-Nearest Neighbor exhibited the highest overall accuracy (97.6%), exceeding similar studies using autoencoders, Random Forest's potentially lower false-negative rate suggests it might be better suited for real-world applications where catching malicious websites is critical. This study aligns

with previous research highlighting the promise of machine learning for cyber threat detection. Further investigation with diverse datasets and models is recommended to solidify these findings and identify the optimal approach for phishing website detection. Overall, this research strengthens the argument that machine learning offers a powerful tool for website security, particularly relevant in the current digital landscape with its increased vulnerability to cyberattacks.

5. Future Work: Further investigations with diverse datasets and models are recommended to solidify these findings and explore the optimal approach for phishing website detection

References:

[1] F. Yahya, R. J. Walters and G. B. Wills, "Goal-based security components for cloud storage security framework: A preliminary study", *2016 Int. Conf. Cyber Secur. Prot. Digit. Serv. Cyber Secur. 2016*, 2016.

[2] L. Tang and Q. H. Mahmoud, "A Survey of Machine Learning-Based Solutions for Phishing Website Detection", *Mach. Learn. Knowl. Extr.*, vol. 3, no. 3, pp. 672-694, 2021.

[3] S. N. A, B. K, G. E and M. I. C, "Deep Learning For Enhanced Cyber-Attack Detection," 2024 International Conference on Cognitive Robotics and Intelligent Systems (ICC - ROBINS), Coimbatore, India, 2024, pp. 874-878, doi: 10.1109/ICC-ROBINS60238.2024.10533961.

[4] T. Visetbunditkun and W. Srichavengsup, "DDoS Attack Detection Using Ensemble Machine Learning Models with RFE Algorithm," 2022 7th International Conference on Business and Industrial Research (ICBIR), Bangkok, Thailand, 2022, pp. 269-273, doi: 10.1109/ICBIR54589.2022.9786423.

[5] S. Shukla and A. Sharma, "Cyber security using Machine Learning in Digital Education industry," 2021 International Conference on Innovative Computing, Intelligent Communication and Smart Electrical Systems (ICSES), Chennai, India, 2021, pp. 1-6, doi: 10.1109/ICSES52305.2021.9633786.

[6] F. Yahya *et al*., "Detection of Phising Websites using Machine Learning Approaches," *2021 International Conference on Data Science and Its Applications (ICoDSA)*, Bandung, Indonesia, 2021, pp. 40-47, doi: 10.1109/ICoDSA53588.2021.9617482.

[7] Gandotra Ekta and D. Gupta, "An Efficient Approach for Phishing Detection using Machine Learning" in Multimedia Security: Algorithm Development Analysis and Applications, Singapore:Springer Singapore, pp. 239-253, 2021

[8] J. Ma, L. K. Saul, S. Savage and G. M. Voelker, "Identifying suspicious URLs: an application of large-scale online learning", *Proceedings of the 26th annual international conference on machine learning*, pp. 681-688, 2009

[9] https://www.edoxi.com/studyhub-detail/top-most-common-cyber-attacks

[10] W. Bai, "Phishing Website Detection Based on Machine Learning Algorithm", *2020 International Conference on Computing and Data Science (CDS)*, pp. 293-298, 2020.