# USING MACHINE LEARNING ALGORITHMS FOR DETECTING CYBER ATTACKS

**Dr.Ayesha Banu[1] , Ranjith kanna Kanna[2], Jayalaxmi marripadagala[3], Veldandi Kiran[4]**

[1]Associate Professor, Department CSE(Data Science), Vaagdevi College of Engineering, Bollikunta, Warangal.
ayeshabanuvce@gmail.com

[2]Assistant Professor, Department CSE(Data Science), Vaagdevi College of Engineering, Bollikunta, Warangal.
ranjithkannakanna@gmail.com

[3]Assistant Professor, Department CSE(Data Science), Vaagdevi College of Engineering, Bollikunta, Warangal.
jaya.jhansi22@gmail.com

[4] Assistant Professor, Department CSE(Data Science), Vaagdevi College of Engineering, Bollikunta, Warangal.
veldandi.kiran.09@gmil.com

**ABSTRACT**

Internet has transformed the communications world predominantly making it a very important and useful means to connect to cyberspace via social networking websites. This increasing importance has directly lead to more number of cyber attacks and crimes. Developing effective techniques to combat these cyber attacks is of urgent demand in the domain of cyber security. The cyber security professionals focused their research on different algorithms to protect cyber space from such attacks. Machine learning(ML) algorithms started contributing in the fight against these attacks to prevent both the data and users. The effectiveness of the ML algorithms have very soon gained lot of importance for cyber security. The major areas addressed by these algorithms include malware classification, intrusion detection, identifying cyber attacks, spam and phishing detection and many more. This paper focus on the different possible cyber attacks and the system vulnerabilities. A study on machine learning algorithms for detecting cyber attacks is also focused with its challenges and future scope.

**Keywords: Cyber Space, Cyber Attacks, Machine Learning Algorithms, Security.**

## I. INTRODUCTION

The internet's inception resulted in numerous technological innovations showing a profound impact on human life. The capacity of systems to connect electronically worldwide has made human Interaction, teamwork, and data access much easier [1]. This impact has tremendously changed with the increase mobile devices supporting connect-from-anywhere terminals. Cloud services and the changes in network infrastructure has given rise to novel challenges to cyber security never like before[2]. Technological advancements always come with number of potential risks and challenges, which, if not addressed on time leads to great disasters. As the planet is rapidly being digitized - there is an urgent need for comprehensive and sophisticated algorithms to fight security threats and provide information security and privacy.

Nowadays, machine learning is employed in nearly every application domain to search for dangerous files and address cyber-security issues by identifying network risks and attacks, stopping data breaches, encrypting personal information, guarding against phishing, and other issues. Theoretically, clustering algorithms, boosting techniques like gradient boosting, regression models, statistical models like Random Forest and SVM, and linear algorithms are some of the categories into which machine learning algorithms in cyber security can be divided. models for neural

networks, particularly those utilizing deep learning [3]. This work focuses on the cyber-attack issues and the real necessity for dynamic detection techniques. It explores the different types of cyber-attacks and literature review on cyber attack detection techniques using machine learning algorithms.

## II. TYPES OF CYBER ATTACKS

Nowadays, machine learning is employed in nearly every application domain to search for dangerous files and address cyber-security issues by identifying network risks and attacks, stopping data breaches, encrypting personal information, guarding against phishing, and other issues. Theoretically, clustering algorithms, boosting techniques like gradient boosting, regression models, statistical models like Random Forest and SVM, and linear algorithms are some of the categories into which machine learning algorithms in cyber security can be divided. models for neural networks, particularly those utilizing deep learning .The different types of popular cyber attacks and the activity performed by the attacker are shown in Table 1 [4] [5].

| **Attack Name** | **Activity Performed by the Attacker** |
|---|---|
| 1. Malware | Intentionally written code for causing damage to a computer server. |
| 2.Denial-of-Service (DoS) Attacks | Computer or network is compromised which disable users to gain access to their own websites mails and online accounts. |
| 3. Phishing Attack | A scamming attempt to obtain private information, such account numbers or passwords, from users. |
| 4. Backdoor Trojan | Create a backdoor on the victim's computer so the attacker can get remote and total control. |
| 5. Ransom ware | A virus that, if a ransom is not paid, permanently prevents access to the victim's personal information. |
| 6.Distributed Denial-of-Service(DDoS) Attack | An attacker overloads a server with traffic, preventing users from accessing websites and online services that are connected. |
| 7.Man-in-the-middle (MitM) attack | The attacker assumes the identities of the client and the server in order to have access to the data shared between them. |
| 8.Drive-by- download attack | The attacker gains un authorized access to the network by disseminating malware. |
| 9. SQL Injection Attack | An attacker modifies the SQL query to take advantage of holes in a database. |
| 10. IoT-Based Attacks | Any cyber attack that goes after a network or device connected to the Internet of Things. |
| 11.sniffing or snooping attack | hacking information transmitted via digital gadgets. |
| 12. Cross-site scripting (XSS) attack | A malicious code is inserted by an attacker into a critical online application or a reliable website. |

Table 1: Types of Cyber Attacks

There are many more cyber attacks apart from the one mentioned in Table 1 that causes security risks in cyber space. The different cyber attacks their characteristics and classification based on purpose, scope, and severity of attack is discussed in [6].

## III. CYBER ATTACK DETECTION TECHNIQUES USING MACHINE LEARNING ALGORITHMS

This section includes a detail literature review of the various machine learning algorithms used for detection of different cyber-attacks.

The network infrastructure and information privacy can be greatly disrupted by the targeted cyber attacks. The hacker may employ botnets and a group of zombie computers, which provide initial access to the target system or network, to evade detection of this attack. In [7], a defence system against this kind of assault is put out. It extracts the sequences of reconnaissance attacks linked to the targeted attacks by analysing several network records. This method makes use of findings that demonstrate how effectively assaults can be identified in their early stages to stop additional network damage. Email-Spamming is a dangerous kinds of Cyber-attacks happening every day in cyber space where the spammers compromise the computers of the victims and send millions of spam emails. This type of cyber-attacks result in changing the cardinality of attack traffic. The scheme projected in [8] is capable of merging the information collected from multiple monitoring points to detect such large-scale spamming attacks.

In [9], a method for early DDoS attack detection is put out, and it is predicated on the DDoS traffic's steady upward trend. When an attacking packet lacks distinguishing characteristics, signatures, or conditions, this approach can nevertheless identify DDoS attacks. It works well in situations when attack rates are modest and progressively rising, and it can adjust to a variety of complex attacks. The method can extract attack characteristics such persistence features and increment trends, and it works with several DDoS packet types like ICMP, UDP, TCP-SYN, and source IP. Eleven distinct DDoS assaults are identified by a thorough analysis of six machine learning classification methods conducted on a number of datasets, with a focus on the CICDDoS2019 dataset obtained from the Canadian Institute of Cyber security [10]. Each attack is assessed based on how well the categorization techniques work.

The article [11] provides an explanation of an experimental analysis on phishing attack detection utilising machine learning algorithms: Support Vector Machines (SVM, Biassed SVM & Leave One Model Out), Neural Networks, Self Organising Maps (SOMs), and K-Means. This strategy makes advantage of a variety of features, such as HTML email, IP-based URLs, domain names, the quantity of domains and links, and keywords. This study demonstrated that LIBSVM outperformed all other ML algorithms, with an accuracy rate of 97.99%. There are number of variants of ransomware attacks that needs to be distinguished from the other malware types to protect users' machines from these attacks. A ransomware detection method proposed in [12] is proved to be capable of distinguishing ransomware files and benign files also the difference between ransomware and malware.

An SQL injection attack read, and copy ,modifies and deletes, data from database servers. This is treated as the damaging attack on web application causing damage of integrity, confidentiality and data availability. Promising results have been observed in the testing and application of machine learning techniques to control SQL injection attacks. [13] discusses pertinent work pertaining to several machine learning and deep learning models used to identify SQL injection attacks.

The different machine learning algorithms that can be used for detecting different kinds of cyber attacks is shown in Figure 1:

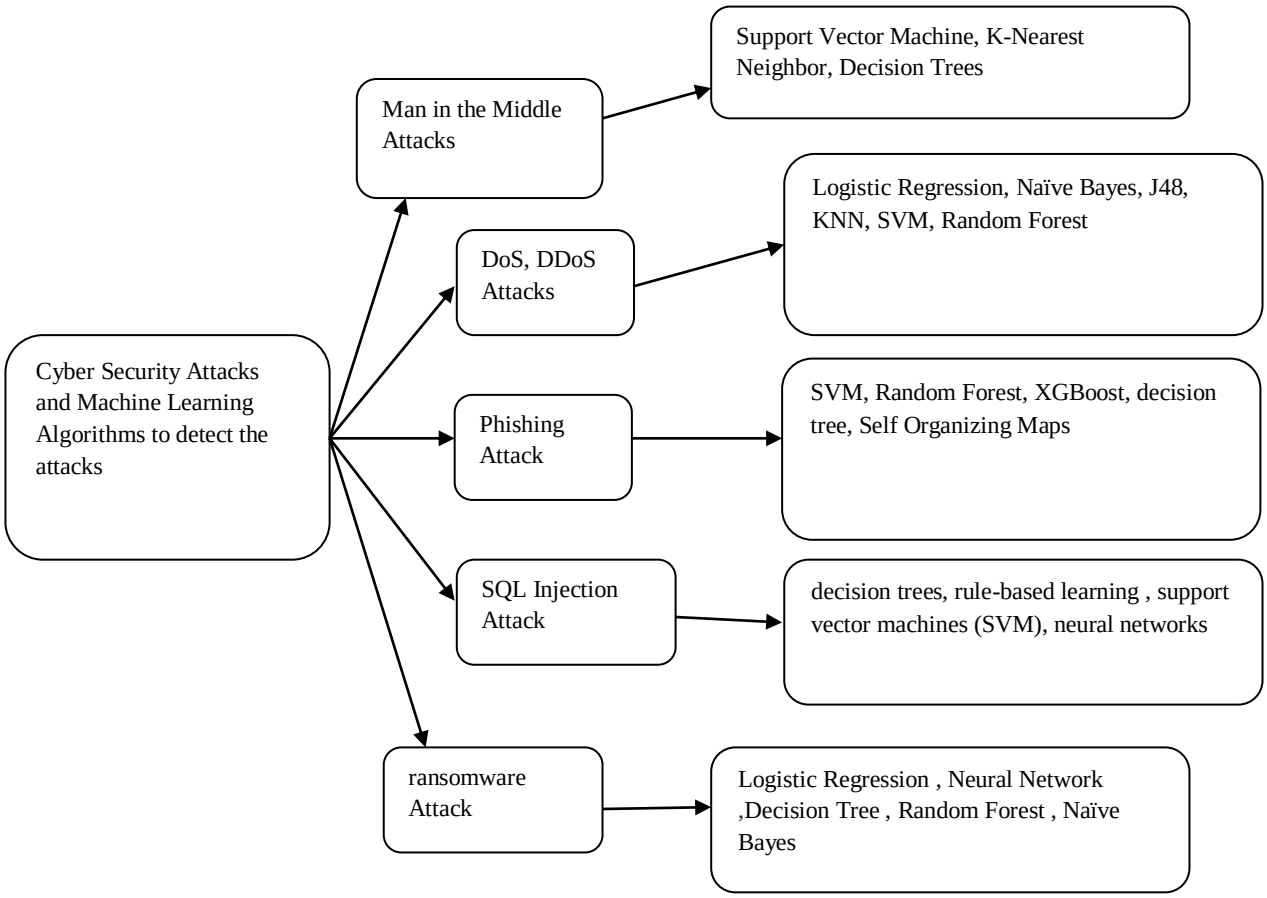


Figure 1: Cyber Security Attacks and Machine Learning Algorithms to detect the attacks

## IV. EFFECTIVENESS ANALYSIS OF ML-ALGORITHMS IN DETECTING CYBER ATTCKS

Owing to their capacity to spot patterns and abnormalities in huge, complicated datasets, machine learning algorithms are crucial instruments for identifying cyberattacks, as the literature review in Section III makes clear. The popular metrics to evaluate the functioning and effectiveness of machine learning algorithms include precision, recall and F-score. These metrics are used by many researchers for comparative analysis of different algorithms on a wide variety of datasets. A review critically examines the effectiveness of machine learning (ML) algorithms in cyber threat detection and mitigation, addressing the need for advanced cybersecurity measures in our interconnected digital landscape. Following Kitchenham's guidelines and utilizing the PRISMA model, the study analyzed 907 initial records from Science Direct, Google Scholar, IEEE Xplore, Springer, and ACM Digital Library, ultimately including only 15 studies that met stringent criteria. The thematic analysis revealed varying effectiveness of supervised learning (SVM and Random Forests) with accuracy rates of 85-90%, but with moderate false positive rates (15-20%). Unsupervised learning techniques (like K-means and DBSCAN) demonstrated lower accuracy (70-75%) yet excelled in detecting novel threats, albeit with higher false positive rates (25-30%). Reinforcement learning showcased adaptive defense capabilities but suffered from lower accuracy (65-70%) due to adversarial

manipulation. Deep learning methods achieved high accuracy (up to 99%) in specific tasks, yet faced challenges related to resource demands and limited interpretability[14].

A study done to evaluate the effectiveness of machine learning (ML) techniques in detecting cyber threats, focusing on supervised, unsupervised, and reinforcement learning models. Using datasets such as CICIDS2017, the study trains models including Random Forest, Support Vector Machines (SVM), and Neural Networks. The evaluation is based on accuracy, precision, recall, and F1-score metrics. The results demonstrate that the Random Forest model outperforms others with an accuracy of 92.5\%, a precision of 91.8\%, and an F1-score of 92.4\%. This superior performance highlights its potential for real-time threat detection, as evidenced by a case study where the model effectively identified previously undetected cyber threats in a large technology company's network. However, the study also acknowledges challenges such as data quality and the need for continuous model updates. The findings suggest that integrating ML models into cyber security frameworks can significantly enhance threat detection efficiency[15].

## IV. CONCLUSIONS AND FUTURE WORK

The primary objective of this study is to focus on the different types of cyber attacks which are threatening the privacy of users and security of data. The need for an effective Machine Learning algorithm for early detection of such cyber attacks is the most prominent research area today. This paper discuss the different types of cyber attacks and the system vulnerabilities. A detailed survey is also presented on the popular ML algorithms which have successfully identified the cyber attacks and contributed in securing the data and users. Future research may focus on developing adaptive algorithms, or machine learning algorithms that can modify their models in response to changing cyberthreats. This will guarantee long-term efficacy in cyberthreat detection and eliminate the need for manual or frequent retraining.

## REFERENCES


1. Rasha Al-majed, Amer Ibrahim, Abedallah Zaid Abualkishik, Nahia Mourad. “Using machine learning algorithm for detection of cyber-attacks in cyber physical systems”. Periodicals of Engineering and Natural Sciences .Vol. 10, No. 3, June 2022, pp.261-275.
2. Kozik, R., Choraś, M. (2014). Machine Learning Techniques for Cyber Attacks Detection. In: S. Choras, R. (eds) Image Processing and Communications Challenges 5. Advances in Intelligent Systems and Computing, vol 233. Springer, Heidelberg. https://doi.org/10.1007/978-3-319-01622-1_44.
3. A P Chukhnov and Y S Ivanov. Algorithms for Detecting and Preventing Attacks on Machine Learning Models in Cyber-Security Problems. Journal of Physics: Conference Series, Volume 2096, International Conference on Automatics and Energy (ICAE 2021) 7-8 October 2021, Vladivostok, Russia.
4. Simran Saini, Prof. Dr. Arvind Kalia. Detection of Cyber Attacks using Machine Learning. International Journal for Research in Applied Science & Engineering Technology (IJRASET) Volume 11 Issue IX Sep 2023.
5. Jibi Mariam Biju, Neethu Gopal, Anju J Prakash. CYBER ATTACKS AND ITS DIFFERENT TYPES. International Research Journal of Engineering and Technology (IRJET). Volume: 06 Issue: 03 | Mar 2019.
6. M. Uma and G. Padmavathi. A Survey on Various Cyber Attacks and Their Classification. International Journal of Network Security, Vol.15, No.5, PP.390-396, Sept. 2013.
7. C. -M. Chen, P. -Y. Yang, Y. -H. Ou and H. -W. Hsiao, "Targeted Attack Prevention at Early Stage," 2014 28th International Conference on Advanced Information Networking and Applications Workshops, Victoria, BC, Canada, 2014, pp. 866-870, doi: 10.1109/WAINA.2014.134.
8. W. Chen, Y. Liu and Y. Guan, "Cardinality change-based early detection of large-scale cyber-attacks," 2013 Proceedings IEEE INFOCOM, Turin, Italy, 2013, pp. 1788-1796, doi: 10.1109/INFCOM.2013.6566977.

9. Y. Huang, X. Fu, Q. Hou and Z. Yu, "The Early Detection of DDoS Based on the Persistent Increment Feature of the Traffic Volume," 22nd International Conference on Advanced Information Networking and Applications - Workshops (aina workshops 2008), Gino-wan, Japan, 2008, pp. 365-370, doi: 10.1109/WAINA.2008.160.
10. Kishore Babu Dasari, Nagaraju Devarakonda. Detection of Different DDoS Attacks Using Machine Learning Classification Algorithms. Ingénierie des Systèmes d'Information Vol. 26, No. 5, October, 2021, pp. 461-468.
11. Basnet, R., Mukkamala, S., Sung, A.H. (2008). Detection of Phishing Attacks: A Machine Learning Approach. In: Prasad, B. (eds) Soft Computing Applications in Industry. Studies in Fuzziness and Soft Computing, vol 226. Springer, Berlin, Heidelberg. https://doi.org/10.1007/978-3-540-77465-5_19.
12. M. Masum, M. J. Hossain Faruk, H. Shahriar, K. Qian, D. Lo and M. I. Adnan, "Ransomware Classification and Detection With Machine Learning Algorithms," 2022 IEEE 12th Annual Computing and Communication Workshop and Conference (CCWC), Las Vegas, NV, USA, 2022, pp. 0316-0322, doi: 10.1109/CCWC54503.2022.9720869.
13. Alghawazi, M.; Alghazzawi, D.; Alarifi, S. Detection of SQL Injection Attack Using Machine Learning Techniques: A Systematic Literature Review. *J. Cybersecur. Priv.* **2022**, *2*, 764-777. https://doi.org/10.3390/jcp2040039.
14. M. A. Adaji et al., "Effectiveness of Machine Learning Algorithms in Threat Detection and Mitigation in Cyberspace: A Systematic Review," 2024 IEEE 5th International Conference on Electro-Computing Technologies for Humanity (NIGERCON), Ado Ekiti, Nigeria, 2024, pp. 1-14, doi: 10.1109/NIGERCON62786.2024.10927069.
15. Khanza, Aulia & Yulian, Firdaus & Khairunnisa, Novita & Yusuf, Natasya & Nuche, Asher. (2024). Evaluating the Effectiveness of Machine Learning in Cyber Threat Detection. Journal of Computer Science and Technology Application. 1. 172-179. 10.33050/ysdncf05.