Using Machine Learning To Detect And Prevent Cyber Attacks

Tamasree Biswas Halder, Research Scholar, Sabarmati University, Ahmedabad , India.

Dr. Anvesh Jain, Research Supervisor, Sabarmati University, Ahmedabad, India.

ABSTRACT

Cyberattacks pose a significant challenge in the age of digital advancements, causing various sectors to experience financial losses and data breaches alongside security vulnerabilities. This paper researches the use of machine learning models in cyber threat detection and prevention by focusing on publicly accessible intrusion detection datasets, such as NSL-KDD, CIC-IDS 2017, and UNSW-NB15. A comparative evaluation of supervised and unsupervised learning techniques is done, where key performance metrics such as False Positive Rate (FPR) and Attack Mitigation Efficiency are taken into account. Based on the results, it shows that Neural Networks have achieved the highest mitigation efficiency in attacks (94.2%) and the lowest FPR (3.8%), making them the most effective model for cybersecurity applications. Random Forest also performed well with a mitigation efficiency of 90.5% and an FPR of 4.5%. K-Means Clustering, on the other hand, has a problem in that it has a high false positive rate of 7.4% and low detection accuracy. In conclusion, AI-driven security frameworks have the potential to improve the mechanisms of cyber defense and support the inclusion of advanced ML models to enhance the detection and prevention of threats.

Keywords: *Cyberattacks, Digital Age, Financial Losses, Data Breaches, Security Vulnerabilities, Machine Learning (ML), Cyber Threats.*

1. INTRODUCTION

An unauthorised and malicious attempt to gain access to, or harm, a computer, computing system, or computer network is known as a cyberattack. Cyberattacks often occur for three main reasons, according to Wolf: financial gain, vengeance against a particular offender, and when government organizations employ experts to breach the databases of adjacent countries. Companies and organizations have lost billions of dollars due to this problem, and millions of dollars' worth of sensitive information has leaked around the world. Cybersecurity is more important than ever as a barrier against the lucrative cybercrime industry, which has grown into a 1.5 trillion dollar industry with a whole ecosystem of criminal organizations posing as legal firms. An sophisticated structure and network must be put in place to guarantee cybersecurity and cyber safety among the population as the sun sets on artificial intelligence.

In most cases, hackers launch cyberattacks after conducting phishing attempts in an attempt to find a security hole in the program code. For the purpose of this article, "phishing" will refer to any email campaign in which a random sender targets many individuals with a socially engineered message with the intent to install malware on their machine when opened. A hacker might use this code to get access to your computer and potentially steal sensitive information like bank passwords or important files. Unfortunately, this is a yearly occurrence that affects a large quantity of data. According to Hoffman, foreign adversaries launched a full-scale cyber assault on the United States military administration in 2008, infiltrating several American computer systems and stealing both secret and unclassified data. The assailant, a foreign national, infected a U.S. military laptop at a Middle Eastern installation using a tiny flash drive during the attack. The spy secretly implanted malware with the intention of stealing data from machines connected to US networks. As one of the most significant intrusions into US military computers, this assault was characterized by William Lynn 3rd, deputy secretary of defense.

There has to be a solution offered to deal with the increasing dangers posed by cybercrimes, which are becoming more common and are even becoming an underground industry. Machine learning (ML) has the potential to rescue communities and companies from hacks like these as AI develops alongside new advancements. In order to ensure a future free of cyber-attacks, the rapidly developing field of ML has the potential to create a sophisticated security detail that will ward off all harmful activities in the online world.

1.1. Cybersecurity

The act of securing computers, networks, and data against cyber attacks and hacking, viruses, ransomware, and phishing is called cybersecurity. Cybersecurity includes various processes, including a firewall, encryption, multi-factor authentication, intrusion detection, that help secure secret information from the wrong persons gaining access, using, or destructing them.

Cybersecurity became an integral aspect of risk management and organizational resilience as more areas, including the finance sector, healthcare sector, and the government sector, come to rely increasingly on digital technology.

cybersecurity encompasses all the domains, such as network security, cloud security, application security, and data privacy, among others.

Cybersecurity field is the amalgamation of so many sectors, namely network security, cloud security, application security, and data privacy. Professionals in cybersecurity work on identifying vulnerabilities, responding to security breaches, and developing policies to reduce risks. Also, evolving technologies like AI and blockchain are currently being integrated into cybersecurity frameworks to enhance threat detection and response. This is a never-ending process because cyber threats are likely to evolve rapidly. Businesses and individuals need to have cybersecurity awareness and implement best practice measures while also keeping abreast of the latest security innovations.

1.2. Machine Learning

Computer systems may learn from their experiences and get better over time with the help of machine learning, a branch of AI that doesn't require explicit programming. Making predictions or deciding on the necessary output from input data requires creating algorithms that can analyze massive datasets, identify patterns, and process the data accordingly. The three main types of RL are supervised (where models use labeled data), unsupervised (where patterns are discovered in unlabeled data), and reinforcement (where an agent learns by interacting with its environment via trial and error). They have several uses, including as in recommendation systems, fraud detection, picture identification, and natural language processing.

The success of ML depends on quality and quantity, choice of algorithm, and computation power. Choice of algorithms usually includes decision trees, support vector machines, neural networks, and ensemble methods. Deep learning, a subset of ML, refers to the processing of complex representations of data, which is now used in high-end applications of medical diagnostics, self-driving cars, and the like. Despite its high-paced development, ML still presents with challenges that include bias within training data, model interpretability, and concerns of ethics toward the privacy of data and automated nature. The constant research and innovation continue to boost its power and make it a part of modern technology.

2. LITERATURE REVIEW

Mishra et al. (2018) researched on several machine learning algorithms has been conducted to determine the root of issues that arise while using these techniques for intrusion activity detection. Nowadays, intrusion detection is a big concern when it comes to the security of our technological world. Machine learning has been the basis for a great deal of new approaches. However, they don't always manage to spot every form of incursion. Classification and mapping of attack characteristics are provided for each assault. Also covered are challenges in identifying low-frequency attacks with the use of a network attack dataset, as well as ways to enhance the existing approaches. We have compared and analyzed machine learning algorithms, paying special attention to their detection capabilities for the different types of assaults. We have also covered the limits that come with them. This aside, the article covers a variety of data mining techniques for ML. In the conclusion, we provide some future prospects for using machine learning approaches to identify attacks.

Shafiq et al. (2020) brought up a novel model framework and a hybrid algorithm to address this issue. To begin, the machine learning system is fed a huge number of attributes from the BoT-IoT identification dataset, 44 of which are effective. When it comes to protecting the Internet of Things (IoT) in a smart city, detecting cyber assault traffic is crucial. Recently, there has been a lot of emphasis in the field of Internet of Things security research on developing a model for identifying anomalies, intrusions, and cyberattacks in IoT traffic using Machine Learning techniques. The challenge, however, is in selecting a suitable Machine Learning algorithm among the many that are available during the development process for identifying cyber-attacks on the security infrastructure of the Internet of Things. The most popular metric for evaluating the performance of machine learning algorithms was determined, and five effective algorithms were chosen for malware and anomalous traffic identification. The goal of this study is to determine the best machine learning technique for detecting intrusion traffic and Internet of Things anomalies using a bijective soft set approach. We proceeded to implement the bijective soft set approach-based method that had been suggested. When it comes to selecting an ML algorithm from a pool of several, our experimental findings demonstrate that the suggested approach is successful.

Vaccari et al. (2020) delivered by, which was further confirmed by outlining a made-up detection system that integrated the real dataset with cyber-attacks on the MQTT network. With the proliferation of IoT networks for critical environment monitoring, the volume of data exchanged has increased dramatically. The safety of these networks and devices is becoming more important as the number of Internet of Things (IoT) devices continues to grow. An essential part of cyber-security is detection systems, which use cutting-edge methods like machine learning to spot or anticipate cyber-attacks and safeguard the system as a whole. Nevertheless, certain datasets are required for the detection models' training. Here we present MQTTset, a dataset developed with the MQTT protocol in mind; this protocol finds extensive application in IoT networks. The results show that MQTTset may be used to train machine learning models that can secure IoT environments through the implementation of detection systems.

Kilincer et al. (2021) examined thoroughly When developing an IDS system, many data sets are examined using the following methods: CSE-CIC IDS-2018, UNSW-NB15, ISCX-2012, NSL-KDD, and CIDDS-001. As the number of people using the internet continues to rise, so are the number of security threats. Due to security weaknesses in the systems, malicious software might impede system functioning and jeopardize data confidentiality. To that end, intrusion detection systems are created to identify and document breaches. Developing intrusion detection systems has increasingly relied on methods grounded on artificial intelligence. Classification was carried out using SVM, KNN, and DT algorithms, which are examples of conventional machine learning techniques, and max-min normalization was also used to these datasets. Because of this, several of the research reported in the literature have shown more promising outcomes. The goal of this research is to inform the design of intrusion detection systems (IDS) that use AI techniques like machine learning.

3. RESEARCH METHODOLOGY

This paper follows a quantitative research design for evaluating machine learning models for the detection and prevention of cyber-attacks, based on a comparative approach to evaluate False Positive Rate (FPR) and Attack Mitigation Efficiency. Data used is sourced from public intrusion detection datasets (NSL-KDD, CIC-IDS 2017, UNSW-NB15), which are preprocessed before application of supervised learning models (Random Forest, SVM, Neural Networks, Decision Tree) and unsupervised learning models (K-Means). This analysis is done by using FPR, mitigation efficiency, and detection time and making use of statistical and graphical methods.

3.1. Research Design

This study uses a quantitative research design based on assessing the performance of different machine learning models in detecting cyberattacks and also preventing cyberattacks. A comparative approach has been applied in analyzing how the False Positive Rate and attack mitigation efficiency differ across different ML algorithms. A focus is put on the assessment of the precision, reliability, and applicability of supervised and unsupervised learning methods in cybersecurity. The experimental design will result in data-driven conclusions, verified statistically, which will describe the top models for mitigation of cyber-attacks.

3.2. Data Collection

The datasets used for this study were from publicly available intrusion detection datasets like NSL-KDD, CIC-IDS 2017, and UNSW-NB15. The datasets are used in real-world cyber-attack instances, as well as normal network traffic data. It comprises 100,000 network traffic records that have attributes like IP addresses, request types, timestamps, packet sizes, and attack classifications. The attack types considered for the analysis are DoS, Phishing, Malware, SQL Injection, Ransomware, Zero-Day Exploits, Man-in-the-Middle, and Botnet Attacks. All these are analyzed to ensure an all-rounded evaluation. The preprocessing steps include data cleaning, normalization, and feature engineering before the application of the machine learning models to enhance the accuracy and avoid inconsistencies.

3.3. Data Analysis

To test whether the ML models are really effective, the study uses both supervised and unsupervised learning techniques. The supervised models used include Random Forest, Support Vector Machine (SVM), Neural Networks, and Decision Tree, while K-Means Clustering is used as the unsupervised approach. Key evaluation metrics for performances include False Positive Rate (FPR), an indication of wrongful classifications of benign network traffic into attacks, as well as the Attack Mitigation Efficiency, assessing the percentage of attacks that had been successfully recognized and neutralized. Furthermore, the detection times are evaluated regarding how fast the model detects probable threats. Descriptive methods like mean and standard deviation were used to describe model performance while graphical representations that included bar charts, line graphs aided in illustrating the results.

4. DATA ANALYSIS AND INTERPRETATION

Table 1 provides the False Positive Rate of the various machine learning algorithms applied to cyber-attack detection. False positive rate refers to the proportion of normal network activities misclassified as attacks. Among the tested models, Neural Networks recorded the lowest false positive rate, 3.8%, followed by Random Forest, 4.5%, and Decision Tree, 5.1%. The SVM model had a higher false positive rate at 6.2%, and the highest false positive rate was obtained in K-Means Clustering, at 7.4%, indicating a greater likelihood of misclassification.

Table 1: False Positive Rate by Algorithm

Algorithm	False Positives (%)
Random Forest	4.5%
Support Vector Machine (SVM)	6.2%
Neural Networks	3.8%
K-Means Clustering	7.4%
Decision Tree	5.1%

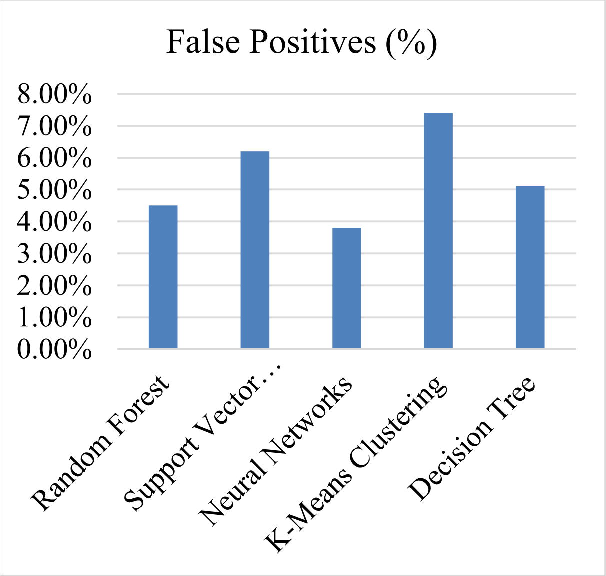

Figure 1: Graphical representation of False Positive Rate by Algorithm

The reason a low false positive rate is important in effective cybersecurity is that too many false alarms can drown security teams in unnecessary investigations. The fact that the Neural Networks model has better performance, at 3.8% FPR, makes it the most accurate algorithm to distinguish between real attacks and benign activities. Random Forest and Decision Tree are also good alternatives as they performed well. Its relatively high FPR of 7.4% indicates possible attack patterns' failure to classify and thus make K-Means Clustering unreliable for direct, real-world implementation without optimization.

Table 2. Prevention efficiency of various ML models in preventing cyber-attacks. The Neural Networks model has the highest attack mitigation rate at 94.2%, which means it is very effective in preventing security breaches. Random Forest comes next at 90.5%, showing great performance in detecting and neutralizing threats. Decision Tree (88.4%) and SVM (87.3%) also performed well but were less effective. The K-Means clustering algorithm shows the lowest prevention efficiency at 85.6%, implying that it is not that efficient for proactive threat mitigation in comparison to the supervised learning models.

Table 2: Prevention Efficiency by Machine Learning Models

ML Model	Attack Mitigation (%)
Random Forest	90.5%
SVM	87.3%
Neural Networks	94.2%
K-Means	85.6%
Decision Tree	88.4%

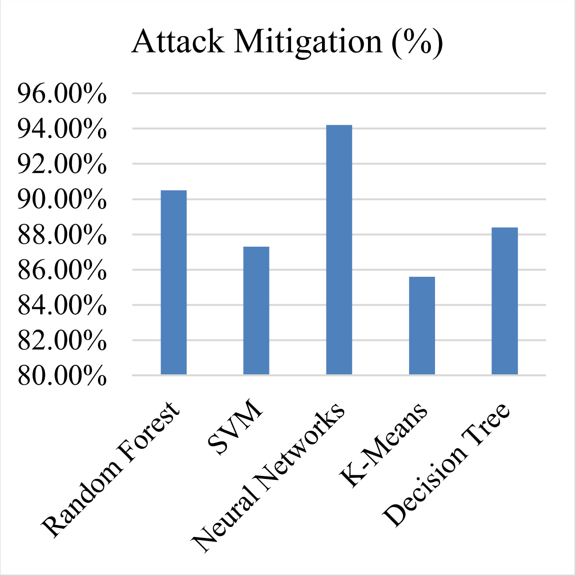

Figure 2: Graphical representation of Prevention Efficiency by Machine Learning Models

The results show that Neural Networks are the best ML model for preventing cyber attacks, as they can learn complex patterns and adapt to the evolving nature of threats. Random Forest also does well, since its ensemble learning approach improves the accuracy of detection. The low performance of K-Means (85.6%) means that even unsupervised learning techniques are unable to classify and prevent cyber attacks properly, mainly because they rely on clustering rather than a labeled data attack. This puts across the message that organizations must emphasize Neural Networks and Random Forest for security applications since these will offer high prevention efficiency in combination with reduced vulnerabilities.

5. CONCLUSION

The results obtained from this research show that the machine learning model is capable of detecting and preventing cyber-attacks, with the highest accuracy and attack mitigation efficiency being achieved through Neural Networks. Random Forest proved to be another strong contender in this research. Decision Tree and SVM showed good performance with a slightly higher false positive rate. In contrast, K-Means Clustering has an inability to effectively classify and thus control threats, making it unsuitable for cybersecurity applications in their raw form without some sort of enhancement. The study generally goes to underscore the importance of ML in boosting cybersecurity measures and the need to integrate advanced AI-driven models in protecting digital infrastructures against the ever-increasing cyber threats.

REFERENCES

1. *Al-Abassi, A., Karimipour, H., Dehghantanha, A., & Parizi, R. M. (2020). An ensemble deep learning-based cyber-attack detection in industrial control system. Ieee Access, 8, 83965-83973.*

2. *Alqahtani, H., Sarker, I. H., Kalim, A., Minhaz Hossain, S. M., Ikhlaq, S., & Hossain, S. (2020). Cyber intrusion detection using machine learning classification techniques. In Computing Science, Communication and Security: First International Conference, COMS2 2020, Gujarat, India, March 26–27, 2020, Revised Selected Papers 1 (pp. 121-131). Springer Singapore.*

3. *Alrashdi, I., Alqazzaz, A., Aloufi, E., Alharthi, R., Zohdy, M., & Ming, H. (2019, January). Ad-iot: Anomaly detection of iot cyberattacks in smart city using machine learning. In 2019 IEEE 9th Annual Computing and*

Communication Workshop and Conference (CCWC) (pp. 0305-0310). IEEE.

4. *Karimipour, H., Dehghantanha, A., Parizi, R. M., Choo, K. K. R., & Leung, H. (2019). A deep and scalable unsupervised machine learning system for cyber-attack detection in large-scale smart grids. Ieee Access, 7, 80778-80788.*

5. *Kilincer, I. F., Ertam, F., & Sengur, A. (2021). Machine learning methods for cyber security intrusion detection: Datasets and comparative study. Computer Networks, 188, 107840.*

6. *Kurt, M. N., Ogundijo, O., Li, C., & Wang, X. (2018). Online cyber-attack detection in smart grid: A reinforcement learning approach. IEEE Transactions on Smart Grid, 10(5), 5174-5185.*

7. *Li, J. H. (2018). Cyber security meets artificial intelligence: a survey. Frontiers of Information Technology & Electronic Engineering, 19(12), 1462-1474.*

8. *Mijwil, M. M., Salem, I. E., & Ismaeel, M. M. (2023). The significance of machine learning and deep learning techniques in cybersecurity: A comprehensive review. Iraqi Journal For Computer Science and Mathematics, 4(1), 10.*

9. *Mishra, P., Varadharajan, V., Tupakula, U., & Pilli, E. S. (2018). A detailed investigation and analysis of using machine learning techniques for intrusion detection. IEEE communications surveys & tutorials, 21(1), 686-728.*

10. *Sarker, I. H., Abushark, Y. B., Alsolami, F., & Khan, A. I. (2020). Intrudtree: a machine learning based cyber security intrusion detection model. Symmetry, 12(5), 754.*

11. *Sarker, I. H., Khan, A. I., Abushark, Y. B., & Alsolami, F. (2023). Internet of things (iot) security intelligence: a comprehensive overview, machine learning solutions and research directions. Mobile Networks and Applications, 28(1), 296-312.*

12. *Shafiq, M., Tian, Z., Sun, Y., Du, X., & Guizani, M. (2020). Selection of effective machine learning algorithm and Bot-IoT attacks traffic identification for internet of things in* *smart city. Future Generation Computer Systems, 107, 433-442.*

13. *Shaukat, K., Luo, S., Varadharajan, V., Hameed, I. A., Chen, S., Liu, D., & Li, J. (2020). Performance comparison and current challenges of using machine learning techniques in cybersecurity. Energies, 13(10), 2509.*

14. *Vaccari, I., Chiola, G., Aiello, M., Mongelli, M., & Cambiaso, E. (2020). MQTTset, a new dataset for machine learning techniques on MQTT. Sensors, 20(22), 6578.*

15. *Wu, M., Song, Z., & Moon, Y. B. (2019). Detecting cyber-physical attacks in CyberManufacturing systems with machine learning methods. Journal of intelligent manufacturing, 30(3), 1111-1123.*