# COMP8325 GROUP PROJECT REPORT

# APPLICATIONS OF ARTIFICAL INTELLIGENCE FOR CYBER SECURITY

Aprajita Shrivas - 46124780

Bhavya Gundlapally - 46124780

Nivedita Rajendra Kumar - 46176594

Vinay Kumar Attapuram - 46330674

## Table of Contents

# 1. Introduction

Our society has become more and more reliant on information and digital services, but the possibility of cyber-attacks has also increased. Emerging and destructive cyberattacks highlight the need of having a solid cybersecurity strategy in place. Hackers are present on all platforms of today's communication technologies, including wired, wireless, remote, and distant access, to corrupt system functionality, evade security measures, and gain unauthorized access. [1] With the rise of internet devices and digital devices, malware threats such as metamorphic malware, zero-day attacks, and code obfuscation have become more prevalent. [2] Attackers use a variety of approaches, including port scanning and distributed denial of service (DDoS) assaults. Machine learning is one of the most important techniques available today for finding the best answers to a variety of real-world issues using a computational intelligence methodology. The goal of this work is to review and categorize the existing research on machine learning-based systems on Intrusion Detection systems, Malware Detection, and Port Scanning detection.

Intrusion Detection Systems (IDS) are used to detect malicious behavior by routing traffic. Intrusion detection systems and IDS solutions are frequently compared to intruder alarms, in that they alert you to any behavior that could compromise your data or network.[3] IDS is basically classified in two different ways,

i) **Passive - IDS:** This sort of IDS simply collects and analyzes traffic, informing the admin of assaults and vulnerabilities and the

ii) **Active - IDS:** These IDS work in the same way as passive IDS, but they also prevent attacks by restricting malicious traffic. Intrusion detection systems employ two basic approaches to identifying threats to inform network managers of signals of a threat: signature-based and anomaly-based. It works by employing a list of common threats and associated indicators of compromise that has been pre-programmed (IOCs). As packets traverse the network, a signature-based IDS compares them to a list of identified IOCs or attack indicators to identify any suspicious behavior.

Anomaly-based intrusion detection systems, on the other hand, can warn you about unusual behavior. An anomaly-based detection system uses machine learning to educate the detection system to recognize a normalized baseline rather than searching for known threats.

Before launching more invasive attacks, an attacker will use a variety of scanning techniques to gather information about network topologies, server implementations, and potential vulnerabilities. [8] HIDS (Host Intrusion Detection System), IDS (Intrusion Detection System), and IPS (Intrusion Prevention System) are some of the tools that can help with network server monitoring. Their function is to make comparisons of network packets in a cyber risk database containing signatures of attacks that the network administrator has already recognized.

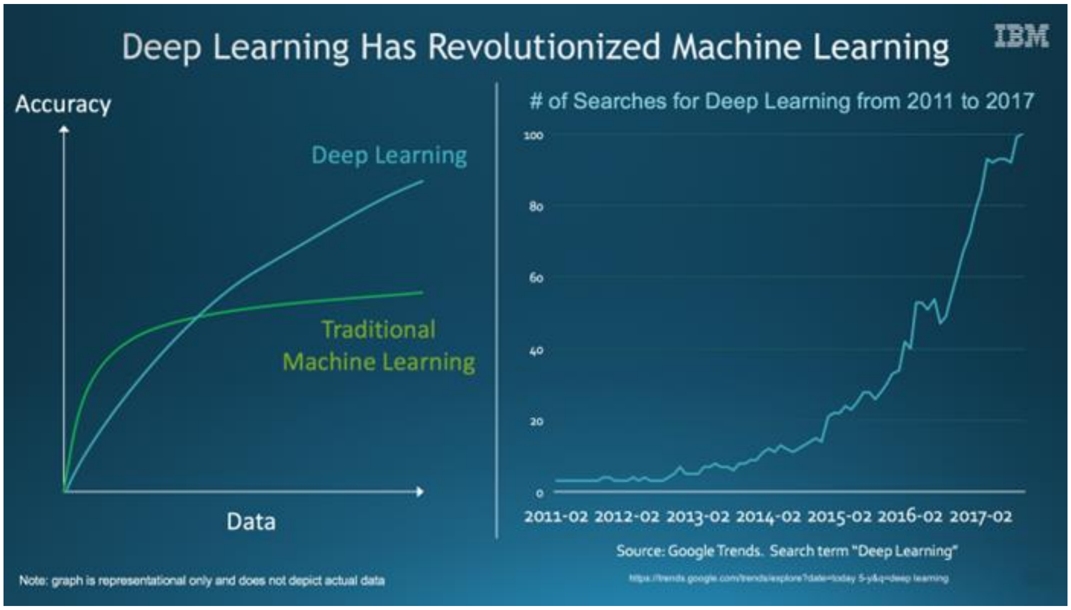

Figure 1. Deep Learning Trends [IBM]

## 1.1 Methodology

The collection of the Port Scan, Network Intrusion Detection, and Malware Detection datasets are the intended network datasets, the first step in the development of our system. Gaussian Naive Bayes, Decision Tree, Random Forest, Logistic Regression, and KNN are five different ML classifiers that are dynamically trained using the training dataset in the system described. After that, the datasets are compared using the test and training accuracy to determine which algorithm is the most accurate. Once we have the most precise model, we connect the processed data to it in order to assess the consequences, whether they are normal or harmful.
Some of the classifiers are:

### 1.1.1 Decision Tree:

A D-tree is a tree-like network containing core blocks that represent a feature test, routes that reveal test results, and leaf nodes that provide a class label. The path from the root node to the branch is what determines categorization rules. The root node is chosen first since it is the most critical attribute for splitting and separating data. [9]

### 1.1.2 KNN Classifier:

KNN is a case-based learning approach for classification that maintains all the training data. Its status as a slow learning approach precludes it from being used in a variety of applications, such as dynamic web mining for a big repository. Finding some representatives to represent the entire training data for classification, i.e., creating an implicit learning approach from the training dataset and utilizing this model(representatives) for classification, is one technique to increase its efficiency.[10]

### 1.1.3 Findings:

By using these methodologies on the above mentioned three datasets we have calculated the training time, testing time, and accuracy whereas KNN classification distributes the data points based on the similarity.

# 2. Literature Review

## 2.1 Methods of cybersecurity intrusion detection based on machine learning:

To address the difficulties of cyber threats and create solutions for intrusion detection, researchers are employing a variety of machine learning approaches. Deep learning is one of the most important techniques available today for finding optimal solutions to a variety of real-world issues, such as cyber security, using a soft computing approach. The main technical challenges of IDS, which are feature extraction, classifier design, and sequential pattern prediction, are viewpoints on technological challenges in IDSs based on machine learning.

To detect patterns from attacks and create improved anomaly detection tools, researchers have used cognitive theories such as analytics, deep learning, information extraction, pattern recognition, and spectral theory. Many experts plan to employ Big Data approaches to develop intrusion detection systems that are both fast and accurate. [4] The author has used techniques of cluster machine learning. To assess whether network traffic was an attack or not, the authors employed the k-Means method in Spark's machine learning library. For training and testing, the KDD Cup1999 was used. The authors did not employ a feature selection methodology to choose the associated characteristics in this proposed model.

[5] IDS clustering approach based on Mini Batch K-means and principal component analysis was proposed (PCA). To minimize the dimension of the processed dataset, the principal component

analysis approach is utilized, followed by the mini-batch K-means++ method for data clustering. [4] In an IoT environment, the author presented an IDS system based on decision trees. The researchers devised a pretreatment technique to determine the strings in a training sample and then normalize the data to verify the input data's quality, hence increasing detection efficiency. For IDS, they employed the decision tree method and compared it to the Nave Bayesian and KNN methods. The results of the experiments on the KDDCUP99 dataset revealed that the proposed strategy is both efficient and exact. [6] Using Apache Spark, Belouch examined the performance of the IDS classification methods SVM, Nave Bayes, Decision Tree, and Random Forest. The accuracy, training time, and prediction time of the overall performance comparison on the UNSW-NB15 dataset are examined.

Feature selection and extraction are regarded as key activities for minimizing computing costs and detecting data trends to develop a valid ID system model. From the original feature, the feature selection is used to choose a subset of the most important features. The feature extraction is required for reducing the dimensionality of input data. [7] For extracting the features and selection, several approaches such as the Genetic Algorithm, variance of network features, Partial Least Square, and Kernel Principal Component Analysis can be utilized. When using feature extraction, it's crucial to assess whether the original input data's qualities are passed on to the obtained new feature sets.

[11] For addressing massive data in cloud computing systems, the CADF Collaborative Anomaly Detection Framework was proposed. They offered the framework's technical functionality as well as the deployment method for various settings. The suggested system consists of three modules: gathering and monitoring network data, pre-processing this data, and a new Decision Engine for detecting assaults that uses a Gaussian Mixture Model with a lower–upper Interquartile Range threshold.

Deep learning algorithms are used to develop cybersecurity solutions, which is one of the most popular and important applications. This paper discusses how machine learning can be utilized as a useful tool in various aspects of information security, such as assessing protocol implementation, developing authentication systems, profiling advanced metering data, and assessing the security of human interaction proofs, among other things. It also explains what Network Intrusion Detection Systems (NIDS) are and how they are utilized in organizations to detect suspicious network activities. [12] With track hyperparameters across several trials with a deep learning platform, initiate experiments automatically, and save money on pricey on-premises GPU clusters or cloud-based GPU services while also saving time.

## 2.2 Methods of Cybersecurity malware detection based on machine learning:

Malware (malicious software) is software that is specifically designed to harm a server, computer, or client. Its goal is to cause damage to both computer systems and networks, hence digital attacks have become a big worry in recent years.

Malware attacks have become increasingly complicated in recent years. Despite advancements in malware detection and classification into appropriate malware family classes over time, as well as ongoing malware evolution, the malware remains the most effective danger to the cyber world. Malware detection and categorization are critical because it determines which malware family it belongs to, allowing malware mitigation or anti-malware solutions to be built with a distinctive signature to identify it.

Machine learning is essential. Antivirus software mostly detects malware based on signatures. These signatures for identifying malware are obtained from malware samples collected earlier. These signature-based methods function effectively if the malware has been previously identified, but they are unable to detect new samples if the malware has not been previously identified. As a result, signature-based solutions aren't always enough. There are a lot of false positives and negatives. New detection systems are required to tackle the threat of enhanced malware versions. Signature-based analysis can be combined with machine learning approaches to achieve more accuracy than a single signature-based strategy for detection [14].

The operational flow consists of four stages:

1. Data Collection: Due to the lack of a comprehensive dataset for malware analysis, we created our own. We'll use this dataset to conduct more malware analysis utilizing machine learning algorithms. We gathered malware and clean files containing windows PE header files from the Virus Share and Virus Total websites. The processing of these files with Cuckoo Sandbox is described in the following subsection.
2. Analysis Phase: All the files are evaluated in Cuckoo Sandbox, which occurs during the execution of each file, evaluates all its run-time activity, and generates thorough analysis results that characterize the malware's behaviors as it runs inside a newly installed operating system.
3. Feature Extraction and Selection Module: A python module was created for feature extraction, feature selection, and the development of training and testing datasets in our proposed system. This Python module accepts JSON (JavaScript Object Notation) formatted analysis reports provided by Cuckoo Sandbox as input and returns features in feature representation form. This module collects the features that are important for detection and classification from analysis reports.
4. Detection and Classification: For malware identification and classification, we employed the Scikit-Learn package in our proposed methodology. Marco dataset and Micro dataset are the two datasets created by combining feature extraction and feature selection. Micro datasets are utilized for classification while Macro datasets are used for detection [15].

## 2.3 Methods of Cybersecurity port scanning based on machine learning:

Identifying vulnerable hosts and possible victims is the first step in launching a network assault. The port scanning attack is a common method used mostly by attackers to determine the extent of vulnerability in their targets. This is a reconnaissance attack that allows the attacker to collect information about receiving hosts' port numbers, network setups, server implementations, operating systems, and potential service vulnerabilities.

Port scanning corresponds to a substantial fraction of today's malicious actions taking place via the internet due to the huge range of network protocols and many implementations of each. As a result, detecting the presence of a port scan attack and distinguishing it from the normal transmission is critical [16].

## 2.4 Security issues in Machine Learning models

Machine learning applications have exploded in popularity in recent years in a variety of fields. Machine learning has become mainstream in many applications that have helped society in many ways, thanks to the increasing rate of data collection and recent breakthroughs in big data analytics. However, as the multitude of machine learning applications grows, so does the number of bad actors who target them. In machine-learning-based systems, security concerns become more sophisticated and diversified.

### 2.4.1 DISCUSSION ABOUT ATTACKS:

Most machine learning attacks in the recent decade were competitive example attacks, with the other four forms of attacks being far less common. Adversarial example studies on images make up most of them, whereas adversarial example investigations on speech and text make up the minority. Recent years have seen a rise in privacy-related attacks, which have gotten a lot of attention. The following are the treads of machine learning threat:

1) **IP Providers -** The IP provider is another untrustworthy actor in the manufacturing cycle since it can contaminate the training datasets and modify baseline ML models/architectures or other hyper-parameters that are not accessible to 3P cloud providers.

2) **3$^{rd}$ Party (3P) Cloud Platforms** - Third-party (3P) cloud platforms are utilized when IP providers or manufacturers do not have adequate computer capabilities to meet the demands of larger datasets and neural networks, such as ResNet. It does, however, include security flaws, such as IP theft, manipulation of the training dataset, and models/architectures. As a result, cloud systems can be considered untrustworthy under the following two scenarios.

3) **The following security weaknesses can still be exploited after the implementation of ML-based systems:**

   i. Side-channel assaults, i.e., trained ML algorithms, can be used to obtain the IP address.

   ii. By changing the inference data or their associated hardware during inference, attackers can affect the security of the ML-based system [17].

# 3. Conclusion

The goal of this study was to determine the utility of machine learning approaches for classifying software requirements, which was motivated by the unique applications of machine learning in Requirements Engineering. Furthermore, a wide range of machine learning techniques for needs categorization was investigated in the literature, implying numerous preprocessing techniques for text processing. In this report, we included ML concepts like classification, regression, KNN, D-tree, i-forest, Local outlier factor and deep belief network in our literature review. With several machine learning algorithms, a survey on security concerns has been offered in this report. Furthermore, from this report we can conclude that machine learning and artificial intelligence play an important role in computer system security.

# References

[1] X. Liu, Y. Lin, H. Li, and J. Zhang, “A novel method for malware detection on ML-based visualization technique,” *Computers & Security*, vol. 89, p. 101682, Feb. 2020, doi: 10.1016/j.cose.2019.101682.

[2]M. Aamir, S. S. H. Rizvi, M. A. Hashmani, M. Zubair, and J. A. . Usman, “Machine Learning Classification of Port Scanning and DDoS Attacks: A Comparative Analysis,” *January 2021*, vol. 40, no. 1, pp. 215–229, Jan. 2021, doi: 10.22581/muet1982.2101.19.

[3]T. Saranya, S. Sridevi, C. Deisy, T. D. Chung, and M. K. A. Ahamed. Khan, “Performance Analysis of Machine Learning Algorithms in Intrusion Detection System: A Review,” *Procedia Computer Science*, vol. 171, pp. 1251–1260, 2020, doi: 10.1016/j.procs.2020.04.133.

[4] F. Karataş and S. A. Korkmaz, “Big Data: Controlling Fraud by Using Machine Learning Libraries on Spark,” *International Journal of Applied Mathematics Electronics and Computers*, vol. 6, no. 1, pp. 1–5, Mar. 2018, doi: 10.18100/ijamec.2018138629.

[5] K. Peng, V. C. M. Leung, and Q. Huang, “Clustering Approach Based on Mini Batch Kmeans for Intrusion Detection System Over Big Data,” *IEEE Access*, vol. 6, pp. 11897–11906, 2018, doi: 10.1109/access.2018.2810267.

[6] M. Belouch, S. El Hadaj, and M. Idhammad, “Performance evaluation of intrusion detection based on machine learning using Apache Spark,” *Procedia Computer Science*, vol. 127, pp. 1–6, 2018, doi: 10.1016/j.procs.2018.01.091.

[7] S.-Y. Ji, B.-K. Jeong, S. Choi, and D. H. Jeong, “A multi-level intrusion detection method for abnormal network behaviors,” *Journal of Network and Computer Applications*, vol. 62, pp. 9–17, Feb. 2016, doi: 10.1016/j.jnca.2015.12.004.

[8] Carlos A. C. Tojeiro*, Carlos J. Reis, Kelton A. Costa, Thiago J. Lucas, “*Port Scan Identification Through Regression Applying Logistic Testing Methods to Balanced Data*”

[9] K. Rai, M. S. Devi, and A. Guleria, “Decision Tree Based Algorithm for Intrusion Detection,” vol. 07, no. 04, p. 7, 2016

[10] G. Guo, H. Wang, D. Bell, Y. Bi and K. Greer, "KNN Model-Based Approach in Classification", On The Move to Meaningful Internet Systems 2003: CoopIS, DOA, and ODBASE, pp. 986-996, 2003.

[11]Moustafa N, Creech G, Sitnikova E, Keshk M. Collaborative anomaly detection framework for handling big data of cloud computing. In: 2017 military communications and information systems conference (MilCIS). IEEE; 2017

[12]"5 Amazing Applications of Deep Learning in Cybersecurity", *Datto.com*, 2022. [Online]. Available:https://www.datto.com/au/blog/5-amazing-applications-of-deep-learning-in-cybersecurity.

[13] D. P Vinchurkar and R. Alpa, "A Review of Intrusion Detection System Using Neural Network and Machine Learning Technique", *research gate*, 2022. [Online]. Available: https://www.researchgate.net/profile/Alpa-Reshamwala/publication/233943805_A_Review_of_Intrusion_Detection_System_Using_Neural_Network_and_Machine_Learning_Technique/links/02bfe50d2f409cdafa000000/A-Review-of-Intrusion-Detection-System-Using-Neural-Network-and-Machine-Learning-Technique.pdf.

[14] Choudhary, S., & Sharma, A. (2020, February). Malware detection & classification using machine learning. In 2020 International Conference on Emerging Trends in Communication, Control and Computing (ICONC3) (pp. 1-4). IEEE.

[15] Sethi, K., Kumar, R., Sethi, L., Bera, P., & Patra, P. K. (2019, June). A novel machine learning-based malware detection and classification framework. In 2019 International Conference on Cyber Security and Protection of Digital Services (Cyber Security) (pp. 1-4). IEEE.

[16] Al-Haija, Q. A., Saleh, E., & Alnabhan, M. (2021, December). Detecting Port Scan Attacks Using Logistic Regression. In *2021 4th International Symposium on Advanced Electrical and Communication Technologies (ISAECT)* (pp. 1-5). IEEE.

[17] Khalid, F., Hanif, M. A., Rehman, S., & Shafique, M. (2018, December). Security for machine learning-based systems: Attacks and challenges during training and inference. In *2018 International Conference on Frontiers of Information Technology (FIT)* (pp. 327-332). IEEE.