NETWORK INTRUSION DETECTION SYSTEMS AND SECURITY UPGRADES USING MACHINE LEARNING TECHNIQUES

Abstract

Machine learning (ML) is a modern image-processing technique with high potential. It has recently entered the networking field since it has been eminently used in various areas. Currently, Machine learning is a new technology that can be used in the modern networking and communication sector; it's applied to enhance the productivity and security of the privacy - Artificial Neural Networks (ANNs), now one of the most widely-known approaches to computational intelligence. IDS improves network security by aiding in the prevention of an increasing variety of attacks. NIDS can be categorised as either signature-based or anomaly-based. The anomaly-based NIDS, based on machine learning models and can identify attacks with high accuracy, is the most prominent type of NIDS. In recent years, artificial neural networks have various advantages in pattern recognition and machine learning. Machine learning is successful because it can quickly and efficiently find patterns and predict problems with enormous amounts of information. By automating the analysis, cyber teams may immediately identify threats and isolate situations that require additional human investigation. The network security environment has extensively used machine learning techniques, supervised learning, unsupervised learning, and reinforcement learning. Additionally, it provides concise explanations of each ML technique, often utilised security datasets, required ML tools, and assessment metrics for classification model evaluation. The issues of using ML approaches to cyber security are finally explored. This chapter on the application for machine learning in

Authors

R. Ramya
Assistant Professor
Department of ECE
K.S. Rangasamy College of Technology
Tiruchengode, Tamil Nadu, India.

P. Kumar
Professor
Department of ECE
K.S. Rangasamy College of Technology
Tiruchengode, Tamil Nadu, India.

C. Saranya
Assistant Professor
Department of ECE
K.S. Rangasamy College of Technology
Tiruchengode, Tamil Nadu, India.

computer networking in the real-world framework. It provides classification techniques like neural networks (RNNs, CNN) other methods (SVM, KNN, and Decision Tree). It supplies the reader with knowledge of present and emerging mode in ML applications research and area of focus for researchers. Labeling network traffic or designing access control policies aims to fine-tune the many aspects of pertinent security procedures to mitigate a specific attack. This chapter is conducted research efforts that employ various neural networks such as convolution neural networks (CNN), which constitute a specific class of ML, applied to other networking and security issues challenges.

Keywords: Networking, Cyber Security, machine learning, CNN, Supervised techniques, AI, PerformanceEvaluation

I. INTRODUCTION

More time is spent online due to advancements in computer technology, the Internet, and mobile phones. Millions of different networks, networks, and connected devices make up the global Internet. Internal errors in configuring and implementing computer systems and networks expose them to threats and cyberattacks. Information network system problems include poor architecture, a lack of appropriate protocols, and untrained or inexperienced workers [1]. Networks are growing, and as systems get more challenging to control, the risk of cyberattacks rises. Cyberattacks begin with analysing the target and using vulnerabilities to carry out malicious activities. It is software that maintains track of multiple sources and identifies system intrusions. IDS has gained the attention of numerous researchers due to its success in identifying intrusions. Using independent ML techniques to detect new and undiscovered crimes is one of the most effective and advantageous ways to accomplish this goal [2]. We can recognise spam, spot fraud, malware, or deep websites, and find breaches with machine learning tools.

An extensive range of variables are included in cyberspace, such as the Internet, competent users, system assets, data, and non-technical individuals. Worldwide access to knowledge and resources is made possible by cyberspace. With rapidly expanding losses and rewards, cyberspace plays a leading role in data transfer and information sharing.

According to the study, artificial neural networks with feedforward and feedback propagation patterns perform better when used to address network problems. As a result, we now suggested ANNs for all applications that can be evaluated based on feedforward and feedback propagation neural network patterns for research focus based on data analysis parameters like classification accuracy, processing speed, latency, scalability, data standardization, type of data inputs, performance, and validation. In addition, we recommend that future research focus on integrating ANN models into a single network-wide application rather than adopting a single approach. For instance, the author analyzed data related to cyber security to draw results and then used those conclusions to create an automated and data-driven intelligent application for cyber security [2]. Industry 4.0 optimises typical industrial and manufacturing processes by applying machine learning, regarded as smart technology, and used for exploratory data processing. Therefore, machine learning algorithms are essential to developing intelligent real- time engineering applications for real-world situations by intelligently analyzing the data. The many machine learning approaches are unsupervised, supervised learning, and reinforcement [3].

For intrusion detection in Android mobile devices, authors in developed a statistical semi-supervised machine learning algorithm. Cybercrimes will also rise due to the increase in data transmission. Therefore, more sophisticated machine learning methods to detect malicious behaviors are required to defend Android mobile devices against sophisticated cybercrimes [4].

To evaluate how effectively machine learning approaches perform in identifying some well-known cybercrimes, we have offered a thorough analysis of the frequently utilized methods. The decision tree, neural network, and support vector machine are three crucial machine learning algorithms that we have examined. But three significant cyber-related risks have been taken into account. This study includes into consideration malware, spam, and intrusion detection.

II. RELATED WORKS

The authors of provided an overview of some research on applying machine learning models for enhancing cyber security. To identify appropriate datasets with the highest effectiveness for a particular security issue, they tackled specific, often encountered challenges to machine learning approaches [5].

The following cyber security fields, including intrusion detection, deep web sites, extortion, identifying malware, fraud detection , and spam classification, make significant use of machine learning methods. Utilising reliable and cutting-edge techniques is required to solve the challenges associated with cyber security. Machine learning is appropriate for evolutionary threats since it allows for experience-based understanding.

Apruzzese et al. have reviewed machine learning approaches used in cybersecurity to identify spam, malware, and intrusions [6]. It stated that all methods are still working to overcome all the constraints and challenges and that machine learning techniques are exposed to cyber threats. The problem is that the same classifier is frequently used to categorise several safety issues. Finding a proper classifier for a specific safety concern is essential. It also emphasised the need to seriously treat all of the machine learningtechniques' shortcomings because cyber attackers are making the most of them.

The goal of this paper is to address the knowledge gap that exists between operational MLusage in cybersecurity and empirical studies. We accomplish this by integrating all of the advantages, drawbacks, and expected challenges of ML in cybersecurity into one article. Any reader who is interested in machine learning and how it relates to cybersecurity should be able tounderstand what we have to say. Researchers and engineers are interested in developing novel MLapproaches toward cybersecurity, enhancing present ML systems, and minimising certain drawbacks. Future ML for cybersecurity advances should be based on this article's unresolved problems and challenges.

III. MACHINE LEANING IN CYBERSECURITY

It will eventually make cybersecurity an effective tool. As it is present everywhere, people continue to be the most essential and irreplaceable asset in security. Cybersecurity currently reliesprimarily on humans, but robots are quickly acquiring the ability to carry out important duties. Technology can assist workers with their regular responsibilities more and more as it progresses. A key aspect of ML is using previously observed patterns of behaviour to infer results and predictthe future. In terms of artificial intelligence-based cyber defence, ML has so far emerged as the most significant industry. Figure 1 depicts many forms of cyber security in the field of networking.

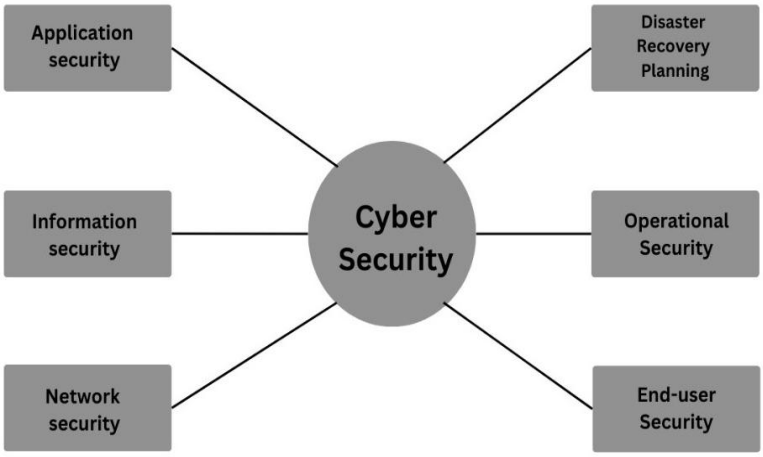

Figure 1: Various types of Cybersecurity in Networking

1. **Role of ML used in Present Research and Applications in Cybersecurity:** In order to attain high levels of accuracy, machine learning is essential to success. This shows that ML can pick up new abilities from datasets optimised for particular tasks. The technique concludes by identifying the most effective method to complete the given work. The decision that makes the most sense in considering the available information will be chosen, even if it is not the most appropriate. There are several machine learning applications in cybersecurity, each providingunique benefits.

    - **Data Classification:** Data classification involves grouping records according to established norms. A key initial phase towards developing a profile of threats, vulnerabilities, and other proactive safety features is locating these areas. This is a crucialaspect of the association between ML and cyber security.

    - **Prediction:** This benefit is due to the ability to predict foreseeable occurrences using historical data. This is a crucial part of numerous endpoint prediction systems and is frequently applied to risk the modelling process, fraud prevention, and data intrusion prevention. It’s the most cutting-edge method of machine learning.

    - **Data Clustering:** When data are clustered, data that don't fit a certain set of parameters arecombined with unexpected or related data. Analysing data sets may provide a more profound knowledge of what was attacked, how it was attacked, and what was left vulnerable.

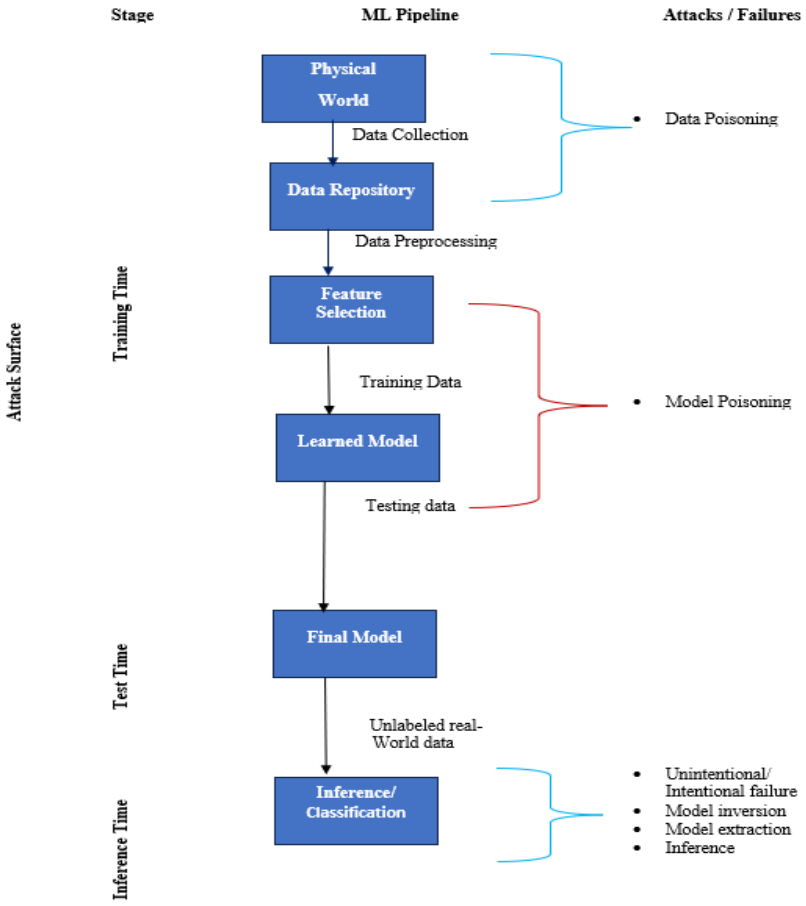

Figure 2: Cyberattacks Workflow with Machine Learning

2. **Potential Use Cases:** Over the last few years, machine learning techniques have been successfully applied to many kinds of issues in several application domains about cybersecurity. Figure 2 shows the overall ML framework, including prospective threats at every phase [17]. Applications for detecting intrusions, malware analysis and detection, spam filtering, fraud, and anomaly detection, cyberbullying detection, IoT assaults, and threat analysis, among many more, are all available.With machine learning, defenders can more precisely identify and rank potential threats. Withthe aid of ML algorithms, a wide variety of specialised work, including different kinds of vulnerability identification, deception, and attack interruption, may be fully or substantially automated. B Below, we look at a few ML-related cybersecurity applications. Below we discussed several potential applications in cybersecurity.

   - **Ranking and Prioritising Network Risk:** Machine learning includes analysing previous cyber threat data sets to identify the most commonly attacked network components. Data from recent cyberattacks can be analysed using machine learning techniques to determine which network segments were most frequently targeted by a given attack. This score, which determines the likelihood and impact of an attack on a particular network area, may help industries minimisetheir risk of becoming the target

of such attacks. Cyber experts have evaluated each network component and are now prioritising their efforts to concentrate on the most significant threats [7].

- **Identify Intrusions and Response:** Since machine learning models can detect, evaluate, and defend against various cyber threats in real-time, organisations may respond to breaches as soon as they occur.

- **Identifying Malware:** By utilising patterns identified in prior attacks, cyber analysts may predict malware attacks and lower the risk at a rate not feasible with manual operations.

- **Cyber Multi-Attack Detection and Classification:** Machine learning can analyse enormous amounts of data rapidly and efficiently, exceeding human risk detection speed. Machine learning uses behavioural analysis and dynamic parameters to detect anomalies that could indicate an attack. Developing security models based on machine learning that evaluate numerous cyberattacks or abnormalities and ultimately detect or forecast the risks may result in intelligent security services.

- **Access Management and Smart Authentication**: Authentication technology verifies that a user's credentials match those stored in the system of approved users or a data authentication server to enable system access control. Machine learning is used in adaptive authentication to determine whether to request multi-factor authentication from users. Machine learning can be used to perform advanced authentication by monitoring real-time user authentication behaviour and identifying irregularities and hazards simultaneously.

- **Automation Tasks:** Automating repetitive and time-consuming operations, such as vulnerability assessments, malware analysis, and network traffic analysis, and intelligence evaluation, is one of machine learning's primary advantages in cyber security. By including machine learning in the security workflow, industries may complete activities more quickly and respond to threats and problems at an unattainable rate with just manual human experience.By automating routine processes, firms can swiftly grow, or contract without changing the workers needed.

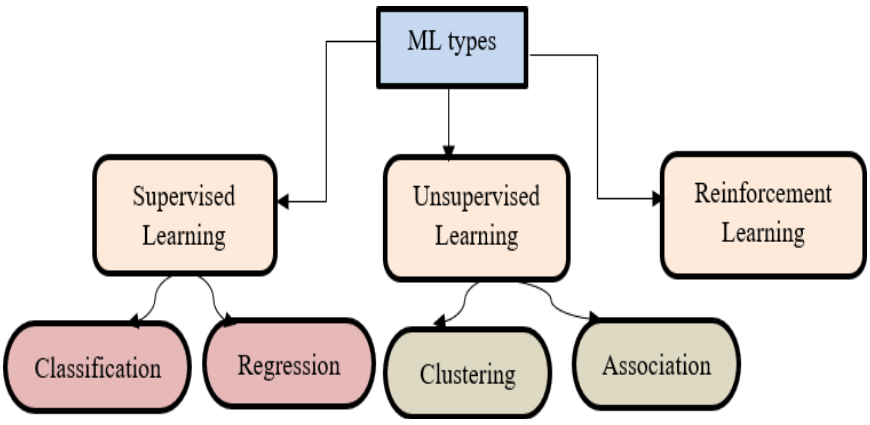

Figure 3: ML Types

Figure 3 shows types of ML. The term labels, which refers to the target value for a prediction function on an instance, is essential to the design of ML models. ML techniques can be divided into supervised and unsupervised categories depending on the availability of labels. Training data with labels is a requirement for supervised algorithms. Otherwise, obtaining labels requires specialised individual examination. While the output value for classification is discrete, the output value for regression is continuous [8]. On the other hand, unsupervised techniques either don't need labelling or have little oversight. Forinstance, the ML model is created using a fully automated feedback mechanism in reinforcement learning.

IV. MACHINE LEARNING TECHNOLOGIES

The most prevalent machine learning algorithms, regularly used ML techniques, processing time,and pros and cons are all discussed in this article.

1. **Support Vector Machine (SVM):** SVMs are considered the most widely used and effective ML method for systems that identify invasions. Figure 4 shows how SVM categorized and classified the two data classes based on labeling the margins on either side of the hyperplane.

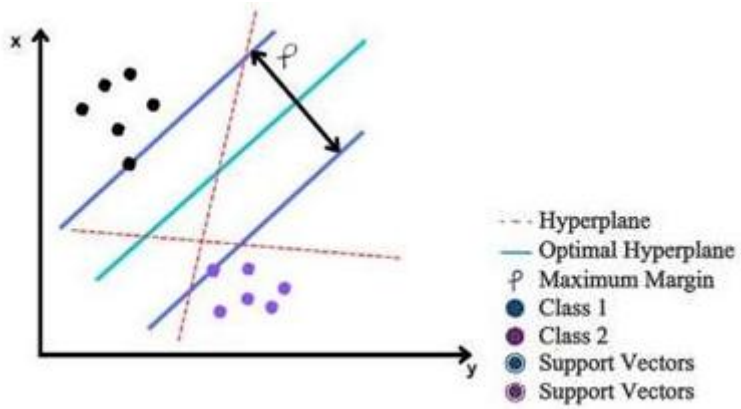

Figure 4: SVM

Expand the region between the margins and the hyperplanes to get more accurate results. At the edge of the hyperplane are data points known as support vector points. The SVM, a supervised learning algorithm, is included in the category of classifying systems. Applying a training data set, this binary categorization technique predicts the optimal hyperplane in n- dimensional space. The SVM algorithm is used to classify data in multidimensional hyperplanes and two-dimensional planes. Multidimensional hyperplanes classify multidimensional data using a "kernel." Use should be given to the maximal spacing or margins between data points of the hyperplanes. The boundary line dividing a plane is known as a hyperplane. As multidimensional data is classified using SVMs, the hyperplane is a straight line with two inputs and a 2D plane with threeor more information. Although it can be used for regression analysis, the SVM algorithm uses it primarily for classification [9].

A classification algorithm examines the training data to predict the outcome. A regressionmethod is used to determine the relationship between the independent variables and to predict theoutcome. There are two significant groups of SVMs. Depending on the kernel function, it could be linear or nonlinear. Depending on the type of recognition, there may be one or more classifications. SVM is trained with various training intervals to provide better results when learning dynamic usage patterns. The performance of the classifier is additionally affected by kernel functions and parameters.

2. **Decision Tree (DT):** The technique can be applied to predict reliable outcomes from unreliable information or to rectify regression errors. The simplicity of analysis and comprehension of the decision-making process are the main benefits of using a decision tree in ML. Root or intermediate nodes, processes, and leaf nodes form DT, as shown in figure 5. The tree's root or intermediary nodes represent variousobjects or properties.

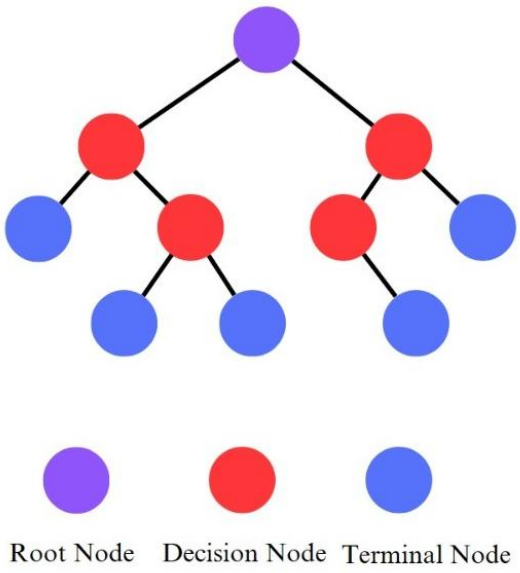

Figure 5: Decision Tree

Each branching path in the tree reveals a potential parent node value. Nodes with a leaf have associations with predicate categories or characteristics. Another technique to express the generated tree is with if-then rules. When we build the tree using heterogeneity and additional information variables, the most suitable routing data is chosen.

3. **Random Forest:** It is a type of ensemble learning that uses several categorization models to produce a scientific consensus regarding a problem and assemble typical results. Usually, an RF includes a variety of forecasting results produced from various decision trees. The literature utilizes random forest for problems like intruder recognition and analysing spam volumes. In the model training phase, it improves nonlinear problem performance while consuming fewer computing resources. Although knowing that random forest can predict a variety of decision trees, the technique of decision trees must be chosen to be considered during the prediction step. Many decision trees' forecast outputs are used for predicting the outcome rather than a single one. Random Forest is an

excellent option for effectively detecting attacks in the cloud and on a network because the approach depends on the ensemble concept. Random forests are utilised as examples for network intrusion detection [10][19].

4. ANN CNN

- **Artificial Neural Network –ANN:** ANNs are trained using both the forward and backward propagation cycle approaches. The feed-forward mechanism delivers data to each node in the hidden layer. The initiation factor is calculated for each node in the output layer and concealed layer[11]. Activation functions have an impact on classifier performance. Error is calculated by contrasting the network output with the desired value. The back propagation algorithm sends the change appropriate to the input layer and uses the Guardian Descent algorithm to modify the values between hidden and output nodes. This procedure is repeated until the desired level is reached. ML techniques, particularly artificial neurons, were used in this investigation to predict outcomesin the future. Overall, the study found that while neural networks may be used for predictionmore effectively, they still have a lot of limitations. The user's actions weren't always reasonable, partly because the participants were mainly from the information technology field [12].

- **Convolutional Neural Network (CNN)**

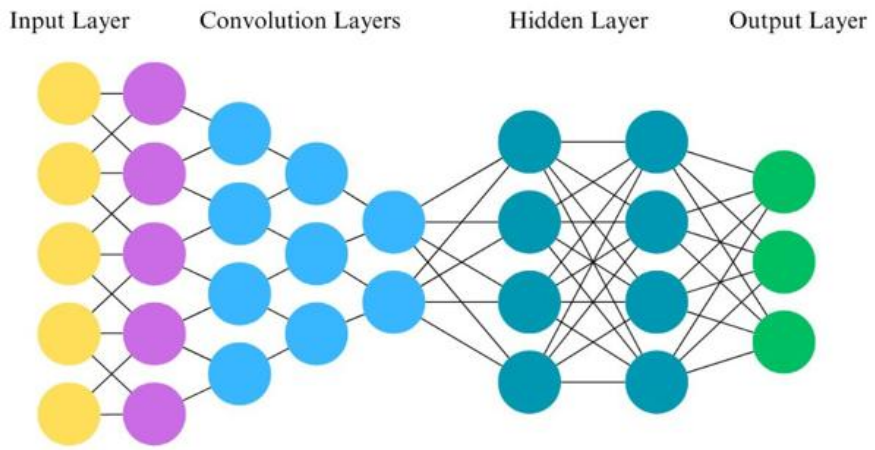

Figure 6: CNN Model

Neural Network method for training image datasets, a CNN-aided intrusion detection model. Here integrated convolutional neural layers with max-pooling layers to develop a CNN-based intrusion detection system (IDS) [20]. CNN, a multi-layer feed-forward ANN, also uses neural networks, as shown in figure 6. It comprises a convolutional layer, one or more fully interconnected layers,and pooling layers, as shown in Figure 5. Extraction of intricate, high-resolution features followed by processing into complicated parts [13]. To distinguish between regular passengers and potential terrorists, deep neural networks (DNNs) are used in aircraft passenger profiling. Extraction of intricate, high-resolution features followed by processing into complicated parts. To

distinguish between regular passengers and potential terrorists, deep neural networks (DNNs) are used in aircraft passenger profiling [14]. The parameters of the network model are modified by the CNN model's back propagation method. The performance of the network model is measured using the test data's classification results after the relevant model parameters have been identified.

5. **Intrusion Detection by Using ML:** For intrusion detection systems, there are three main categories of cyber analysis. These detections are hybrid, anomaly- and exploit-based. Known attacks are to be discovered through exploit-based detection. Anomaly detection retains a close watch on the ordinary network and system activity and detects abnormal network and system behaviour. A hybrid-based detection technique combines exploit-based and anomaly-based strategies to enhance identification outcomes. Attackers can successfully exploit the ubiquity of these conventional defenses' faults. Consequently, it has become challenging to protect consumers from evolving hazards. In cyberinfrastructure, there is a tremendous amount of data [15]. Figure 7 shows different cyber-attacks.

Thus, ML algorithms significantly impact the real-time detection and forecasting of upcoming attacks and invasions. ANNs, SVMs, decision trees, and statistical models are typical methods utilised in ML techniques frequently used to detect intruders.

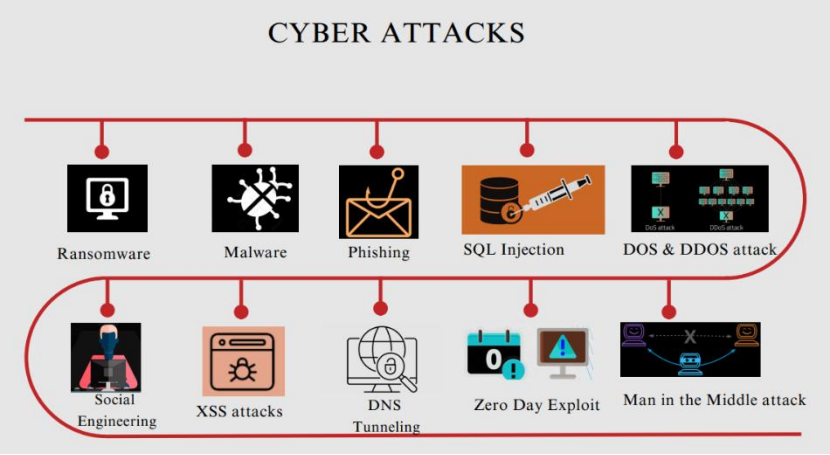

Figure 7: Cyber Attacks

V. CLUSTERING IN CYBERSECURITY

Another typical approach used in machine learning for processing cybersecurity data is clustering, categorised as unsupervised learning. Based on metrics of similarity and dissimilarity in security data from many sources, it can cluster or group a set of data points. Clustering may assist in identifying hidden patterns and structures that can be used to discover anomalies or incursions in data. Data can be clustered using various methods, including partition, hierarchy, fuzzy theory, and density.

Popular clustering algorithm concepts include K-means, K-medoids, single linkage, complete linkage, agglomerative clustering, DBSCAN, Gaussian Mixture Model, etc. The

unlabeled dataset is split into K clusters by an unsupervised iterative method called the K means clustering approach [19]. It introduced a bottom-up clustering technique that takes behaviour analysis into the assessment. Numerous cybersecurity issues can be solved using these clustering strategies. For instance, the k-Means technique profiles devices' abnormal behaviour. The researchers use a dynamic threshold-based approach to identify outliers or noisy events in data. In general, clustering techniques are advantageous for obtaining pertinent information or understanding from system log data for cybersecurity applications [16]. By exposing hidden patterns and structures in cybersecurity data and assessing behavioural similarity or dissimilarity, clustering techniques may assist in the solution of various security issues, including outlier detection, anomaly detection, signature extraction, fraud detection, cyber-attack detection, and others. Therefore, for further research in next-generation cybersecurity, clustering-based unsupervised learning, including building efficient algorithms, may be an essential field.

VI. RESULTS AND DISCUSSION

The SVM structural risk minimization framework reduces generalisation error for unobserved data. The margin that separates the data points affects how many free parameters the SVMs employ. Using a kernel function, the SVM provides a general technique for fitting the hyperplane's surface to the input data. During the SVM's training process, we used the Gaussian Kernel function, which chooses the support vectors along the function's surface. A broader spectrum of issues can be classified thanks to this ability. The data has been divided into two categories using the SVM and Improved Support Vector Machine. The iSVM has a higher rate of cyber threat detection than the conventional SVM [18]. As a result, the random forest is preferable to other approaches in terms of classification. While performing similarly to different classifiers for intrusion detection, the random forest model takes more time. Because of that, Random Forest isn't an appropriate option for real-time intrusion detection applications in real-world environments [19].

Table 1: An Overview of Cybersecurity-Related Machine Learning Applications

Name of the approach	Purpose
SVM	Classifying cyberattacks using labels such DoS, U2R, R2L, and Probing
	choosing security features, recognising and categorizing attacks
ANN and SVM	modelling and developing network intrusion detection systems
K-means	Designing intrusion detection system
Decision Tree	designing an effective network intrusion detectionsystem and integrating safety features solving the minor disjunct issue while developing a tree-based IDS
RF	Identify cyber anomalies, DoS attack detection, and systems to detect intrusions
CNN	LAN Intrusion Detection

Table 1 shows an overview of ML-based techniques used in cybersecurity applications. Extracting features is essential in all AI/ML-based methods to provide reliable outcomes, ML -K-means, CNN and ensemble-based methods suggested almost identical results above 99%. By eliminating undesirable and redundant features from the dataset, CNN often uses the feature selection approach to identify the optimal feature subset for improving system performance [21]. The analysis only addressed typical assaults and security risks, including DoS, Probe, R2L, and U2R. The Machine learning-based techniques are evaluated using just the accuracy estimates. Future research work has to contrast the other evaluation criteria, such as detection and False rates. Additionally, considering the present network and cloud architecture, we will evaluate the potential benefits of AI, ML-based intrusion detection systems for a broader range of the most recent attacks in the future.

VII. CONCLUSION AND FUTURE SCOPE

By including machine learning in the security workflow, industries may complete activities more quickly and respond to threats and problems at an unattainable rate with just manual human experience. By automating routine processes, firms can swiftly grow, or contract without changing the workers needed. An analysis of cyberattacks against machine learning algorithms is currently available. Clearly, there isn't a single, generalised defence mechanism that prevents all types of attacks against ML. It has risks that are more closely related to the structure and content of the system. According to CNN-based study results, the method enhances network traffic identification and categorization and cuts down on categorization time, enabling the system to satisfy full-time commitments. Building a cyber-attack detection system that integrates various class-specific cyber-attack detection systems will be part of future work, as may analysing the economics and potential of utilising this method in a real-time cyber-attack detection system. This system will provide an altogether detection rate for all classes.

REFERENCES

[1] Kamran Shaukat et al., “Cyber Threat Detection Using Machine Learning Techniques: A Performance Evaluation Perspective”, IEEE Conference Paper · October 2020 DOI: 10.1109/ICCWS48432.2020.9292388.
[2] I. H. Sarker, A. S. M. Kayes, S. Badsha, H. Alqahtani, P. Watters, and A. Ng, “Cybersecurity data science: an overview from machine learning perspective,” Journal of Big Data, vol. 7, no. 1, pp. 41–29, 2020.
[3] B. Slusarczyk, “Industry 4.0 - are we ready?” Polish Journal of Management Studies, vol. 17, no. 1, pp. 232–248, 2018.
[4] J. Ribeiro, F. B. Saghezchi, G. Mantas, J. Rodriguez, S. J. Shepherd, and R. A. Abd-Alhameed, "An autonomous host-based intrusion detection system for android mobile devices," Mobile Networks and Applications, vol. 25, no. 1, pp. 164-172, 2020.
[5] H. Jiang, J. Nagra, and P. Ahammad, "Sok: Applying machine learning in security-a survey," arXivpreprint arXiv:1611.03186, 2016.
[6] Apruzzese, G.; Colajanni, M.; Ferretti, L.; Guido, A.; Marchetti, M. On the effectiveness of machine and deep learning for cyber security. In Proceedings of the 2018 10th International Conference on Cyber Conflict (CyCon), Tallinn, Estonia, 29 May–1 June 2018; pp. 371–390.
[7] Sarker IH (2021) Machine learning: algorithms, real-world applications and research directions. SN Comput Sci 2(3):1–21.
[8] Rutvij H. Jhaveri, et at., “A Review on Machine Learning Strategies for Real-World engineering Applications”, Review Article, Volume 2022, Article ID 1833507 | https://doi.org/10.1155/2022/1833507.
[9] S. T. Miller and C. Busby-Earle, “Multi-perspective machine learning a classifier ensemble method for intrusion detection,” in Proc. Int. Conf. Mach. Learn. Soft Comput. (ICMLSC), 2017,pp. 7-12.

[10] K. He, X. Zhang, S. Ren, and J. Sun, "Deep residual learning for image recognition," in Proc. IEEE Conf. Comput. Vis. Pattern Recognit. (CVPR), Jun. 2016, pp. 770-778.
[11] R. U. Khan, X. Zhang, M. Alazab, and R. Kumar, "An improved convolutional neural network model for intrusion detection in net- works," in Proc. Cybersecurity Cyberforensics Conf. (CCC), May 2019, pp. 74-77.
[12] S. Smadi, N. Aslam, and L. Zhang, "Detection of online phishing email using dynamic evolving neural network based on reinforcement learning," Decis. Support Syst., vol. 107, pp. 88-102, Mar. 2018.
[13] MXNET An Efficient Library for Deep Learning. Accessed: Aug. 13, 2020. [Online]. Available: https://mxnet.apache.org/versions/1.6/.
[14] N. F. Shah and P. Kumar, "A comparative analysis of various spam classifications," in Progress in Intelligent Computing Techniques: Theory, Practice, and Applications. Singapore: Springer, 2018, pp. 265-271.
[15] J. M. Torres, C. I. Comesana, and P. J. Garcıa-Nieto, "Machine learning techniques applied to cybersecurity," Int. J. Mach. Learn. Cybern., vol. 10, no. 10, pp. 2823-2836, 2019. Difference Between Threat and Attack. Accessed: Jun. 3, 2020.
[16] Landauer M, Skopik F, Wurzenberger M, Rauber A (2020) System log clustering approaches for cyber security applications: a survey. Comput Secur 92:101739.
[17] Chakraborty, A.; Alam, M.; Dey, V.; Chattopadhyay, A.; Mukhopadhyay, D., "Adversarial attacks and defences: A survey", arXiv 2018, arXiv:1810.00069.
[18] Shailendra singh et al. "Improved Support Vector Machine for Cyber-attack detection", Proceedings of the World Congress on Engineering and Computer Science 2011 Vol I WCECS 2011, October 19-21, 2011, San Francisco, USA.
[19] Sowmya T et al., "A comprehensive review of AI based intrusion detection system", Measurement: Sensors, Volume 28, August 2023, 100827.
[20] Hanan Zaine, Cemal Koçak, "LAN Intrusion Detection Using Convolutional Neural Networks", Appl. Sci. 2022, 12, 6645.
[21] Dong, R.H.; Yan, H.H.; Zhang, Q.Y., "An Intrusion Detection Model for Wireless Sensor Network Based on Information Gain Ratio and Bagging Algorithm", Int. J. Netw. Secur. 2020, 22, 218–230.

