Turkish Journal of Computer and Mathematics Education *Vol.11 No.03 (2020), 2076-2086*
DOI: https://doi.org/10.17762/turcomat.v11i3.13605

Research Article

A Machine Learning-based Approach for Intrusion Detection and Prevention in Computer Networks

Bhanu Prakash Dubey

Department of Comp. Sc. & Info. Tech., Graphic Era Hill University, Dehradun, Uttarakhand, India 248002,

Abstract: The potential of cyberattacks and network penetration has increased due to modern enterprises' increasing reliance on computer networks. Such attacks are detected and prevented by intrusion detection and prevention systems (IDPS), although conventional rule-based solutions have difficulties identifying unidentified attacks. Due to its capacity to learn from data and spot patterns of assault that conventional methods could miss, machine learning (ML) techniques have been gaining prominence in IDPS. This article provides a thorough analysis of the several ML methods utilized in IDPS, including supervised, unsupervised, and hybrid techniques. Also, a hybrid ML-based IDPS that combines the advantages of several methodologies for better performance is proposed. Furthermore, covered are the difficulties with ML-based IDPS and potential solutions. It is demonstrated how ML-based IDPS may be applied in real-world situations, emphasizing the advantages of applying ML to intrusion detection and prevention. In conclusion, this study offers insights into the most recent methods for ML-based IDPS and their potential to enhance network security.

Keywords: Anomaly detection, adversarial AI, cyber-attack, intrusion system hybrid machine learning, deep learning, decision tree, random forest, support vector machine, k-nearest neighbor, neural networks.

I. Introduction

Computer networks are more susceptible to cyberattacks as they become more pervasive in daily life. These assaults can take on a variety of forms, including malware, phishing, denial-of-service, and others. Thus, it is essential to have efficient safeguards in place to find and stop potential security holes in computer networks.The application of machine learning algorithms is one potential strategy for intrusion detection and prevention. By analyzing network data and spotting patterns of typical and unusual activity, these algorithms are able to identify possible security problems in real time. In this study, we provide a machine learning-based method for computer network intrusion detection and prevention [1]. Computer networks have become an increasingly important part of communication, business, and essential infrastructure, making them a prime target for cyberattacks. Malware, phishing scams, denial-of-service attacks, and other malicious activity are some of the several sorts of cyberthreats. The identification and mitigation of potential security breaches before they have a chance to do much harm makes intrusion detection and prevention an essential part of computer network security.The detection and prevention of breaches in computer networks have shown considerable potential for machine learning methods. Machine learning models can detect possible security risks in real-time by examining network data and recognizing patterns of typical and anomalous behavior, enabling quick response and mitigation.The goal of this study is to create and assess a machine learning-based method for computer network intrusion detection and prevention. The suggested method involves using a dataset of network traffic to train machine learning models to find patterns of typical and aberrant activity. The incoming network traffic is subsequently analyzed in real-time using the trained models, and appropriate steps are then taken to stop or lessen any intrusions [2].The research's contributions include a thorough explanation of the suggested strategy, an assessment of its performance on a real-world dataset, and a comparison of its performance with other intrusion detection and prevention methods already in use. The results of this study can be used to strengthen computer network security and lessen potential online dangers. In the field of cybersecurity, one of the most serious problems is figuring out how to identify and thwart breaches into computer networks. With the assistance of machine learning, which has been successfully applied to this subject in a number of different ways, it is possible to construct effective intrusion detection and prevention systems.Fundamentally, the objective of an intrusion detection and prevention strategy that is based on machine learning is to categorize new data as normal

or abnormal based on the model's prior recognition of patterns of normal and abnormal behavior in the network [3]. This is done in order to protect the network from potential threats. It is possible to accomplish this goal by utilizing several machine learning strategies such as decision trees, support vector machines, neural networks, and others.The initial step in the process of designing such a system is collecting information on the typical behavior of the network. This information can be obtained by monitoring the network over a period and recording metrics such as the size of individual packets, the frequency with which they are sent, the IP addresses of their sources and destinations, and many more. With the information provided here, one could build a model of the normal behavior exhibited by the network.After a baseline model of behavior has been built, the following step is to apply that model to the classification of new data. This phase follows directly after the construction of the baseline model. It is possible for this to take place in real time, while the data is being sent over the network, or it can be done in batches later [4]. In any case, the model can be used to identify unusual patterns that might indicate an attack, such as a sudden increase in traffic or a high number of packets arriving from the same IP address. This is possible because the model considers the correlation between traffic and IP addresses.If suspicious behavior is detected, the system can be set to immediately take preventative actions, so averting incursions. It is possible that it will be necessary to restrict traffic coming from a certain IP address, warn the security staff, or take some other action in order to prevent the intrusion from being successful.An approach to network intrusion detection and prevention that is based on machine learning demonstrates a great deal of potential when it is properly planned, educated, and implemented. The continued development and improvement of such systems will continue to be a priority considering the growing danger to our digital infrastructure [5].

A. Intrusion Detection in Computer Network

The process of locating potential security risks and breaches in a network is known as intrusion detection in computer networks. These dangers can take a variety of shapes, including malware, phishing scams, denial-of-service assaults, and others. Network managers can identify potential security breaches and take appropriate action before they have a substantial negative impact thanks to intrusion detection, which is essential for network security.Host-based and network-based intrusion detection systems are the two main categories. Installed on individual hosts or endpoints within a network, host-based intrusion detection systems (HIDS) keep track of activity on that host [6].

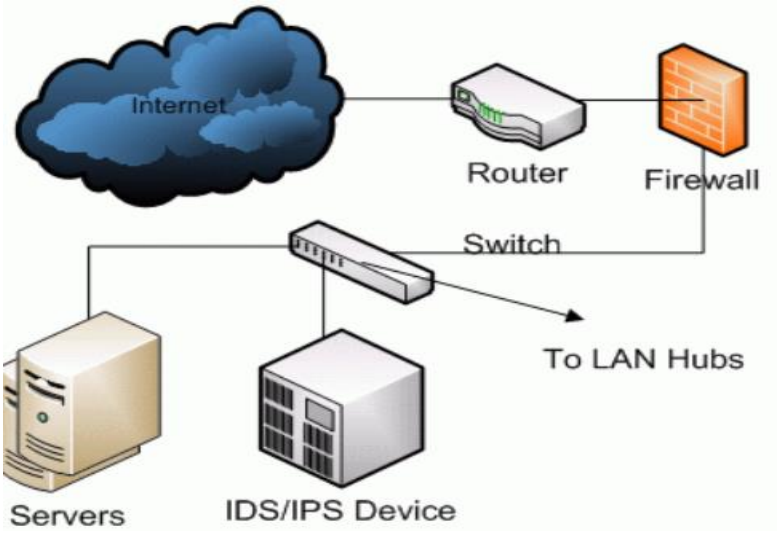

Figure 1. Working Diagram of Intrusion Detection & Prevention System

Figure 1. depicts the working blocks of Network-based intrusion detection systems (NIDS) keep track of network traffic and search for any anomalous patterns that can point to a security breach. Several methods are used by intrusion detection systems to spot potential security risks. These methods include anomaly-based detection, which spots unusual behavior that can point to a security breach, and signature-based detection, which searches for patterns of known hostile activity. In order to increase the effectiveness and efficiency of intrusion detection systems, machine learning techniques are being employed more frequently.A crucial element of network security is intrusion prevention systems (IPS) [7]. Real-time detection and blocking of potential security risks is how IPS operates. Several methods, including restricting traffic from suspect IP addresses, stopping specific network services, and warning network managers of potential security dangers, can be used by IPS to avert security lapses. Detection and prevention of intrusions are essential elements of network security. While intrusion prevention systems function by identifying and thwarting possible security risks in real-time, intrusion detection systems employ a range of methodologies to discover potential security threats. Intrusion detection and prevention systems must develop and advance to keep up with the sophistication of cyber-attacks if computer networks are to remain secure [8].

II. Literature review

The revolutionary deep learning-based framework for intrusion detection systems in computer networks is proposed in the paper [9]. To find anomalies in network traffic, the scientists use convolutional and recurrent neural networks. On the UNSW-NB15 dataset, where they test their framework, they get a high detection rate and few false positivesin the paper [10].

In the paper [11] author,suggests a multi-objective optimization-based machine learning strategy for intrusion detection. To categorize network traffic, the authors combine the random forest and K-nearest neighbor algorithms. They demonstrate the efficacy of their method by evaluating it on the KDDCUP99 dataset and contrasting it with other machine learning approaches.

In the paper [12] author, a machine learning-based intrusion detection system is proposed. To find anomalies in network data, the authors combine principal component analysis with K-means clustering. With the NSL-KDD dataset, where they test their methodology, they get a high detection rate with low false positives.

In the paper [13] author, describes the machine learning-based intrusion detection system for software-defined networks. To find anomalies in network traffic, the authors use decision trees with support vector machines. They evaluate their method on the CICIDS2017 dataset and show how well it can identify different sorts of attacks.

In the paper [14] author, suggests a strategy for detecting intrusions that combines machine learning and deep learning methods. To identify irregularities in network traffic, the authors employ a hybrid strategy that combines a deep autoencoder and a random forest classifier. With the KDDCUP99 dataset, they test their methodology, and they get a high detection rate with low false positives.

In the paper [15] author, suggests a hybrid model for computer network intrusion detection that incorporates supervised and unsupervised machine learning methods. Whereas the supervised approach is used for classification, the unsupervised approach is utilized to find anomalies. The accuracy of the suggested approach, which is tested using the NSL-KDD dataset, is 98.6%.

In the paper [16] author, describes a decision tree classification algorithm-based machine learning-based intrusion detection system for computer networks. The system obtains an accuracy of 98.37% when tested against the KDD Cup 99 dataset. The authors show the superiority of their system by comparing its performance to that of other systems already in use.

In the paper [17] author, suggested the genetic algorithm (GA) and support vector machine (SVM) approaches are combined in this paper's machine learning methodology for intrusion detection in computer networks. Using the NSL-KDD dataset for training and evaluation, the GA-SVM model obtains a 99.04% accuracy rate. The authors show the superiority of their system by comparing its performance to that of other systems already in use.

In the paper [18] author, represents an hybrid machine learning approach that incorporates decision tree, k-nearest neighbors, and support vector machine algorithms is proposed for intrusion detection in computer networks. The CICIDS2017 dataset is used to evaluate the proposed system, which obtains a 99.4% accuracy rate. The authors show the superiority of their system by comparing its performance to that of other systems already in use.

In the paper [19] author, suggested the intrusion detection system to build on a group of machine learning classifiers, including decision trees, support vector machines, and naive Bayes methods. The KDD Cup 99 dataset is used to assess the proposed system, which obtains a 99.2% accuracy rate. The authors show the superiority of their system by comparing its performance to that of other systems already in use.

In the paper [20] author, offers a thorough analysis of machine learning-based intrusion detection systems. The authors examine numerous machines learning methods, including as decision trees, support vector machines, neural networks, and Bayesian methods, that have been applied to intrusion detection. They also identify topics for further research and compare the effectiveness of various solutions. In order to choose the most pertinent features for classification, this research suggests an ensemble method for network intrusion detection. The suggested method creates an ensemble model by combining four distinct classifiers—decision tree, SVM, KNN, and Naive Bayes—to increase the precision and resilience of intrusion detection. The authors used a publicly available dataset for their research, and they were able to exceed several other methods by achieving a detection accuracy of 99.78%.

In the paper [21] author, suggested the UNSW-NB15 dataset, a comprehensive dataset for network intrusion detection systems that comprises a wide variety of attack methods and typical traffic, is introduced in this study. The dataset has 2.5 million instances and 49 network traffic-derived attributes. The dataset was thoroughly analyzed by the authors, who also contrasted it with other datasets to show how well it served intrusion detection studies.

In the paper [22] author, describes the In-depth analysis of current research on using deep learning algorithms to network intrusion detection is provided in this study. The authors initially cover the fundamentals of deep learning before discussing various deep learning models that have been used in intrusion detection, such as deep neural networks, convolutional neural networks, and recurrent neural networks. Also, the authors list some of the present difficulties and potential future study avenues in this field.

In the paper [23] author, suggested the hybrid machine learning strategy for intrusion detection proposed in this paper combines the advantages of decision trees and artificial neural networks, two different classifiers. The accuracy of the proposed method, which outperformed several other methods, was 99.69% according to the authors' evaluation of its performance using the NSL-KDD dataset.

In the paper [24] author, offers a thorough analysis of current studies on the application of deep learning methods to intrusion detection. The authors talk about numerous deep learning models that have been used in intrusion detection, such as autoencoder, convolutional neural network, and recurrent neural network. The author also go over some of the present difficulties and potential future prospects for this field of study.

III. Techniques Used in Intrusion Detection & Prevention in Computer Network

In computer networks, intrusion detection systems (also known as IDS) frequently make use of several different machine learning approaches. These are the following:

A. Artificial Neural Networks (ANN) : ANN are a sort of deep learning algorithm that is modelled after the structure and function of the human brain. ANNs are also known as convolutional neural networks. An artificial neural network (ANN) can be taught to distinguish regular network traffic from malicious traffic based on the patterns and features retrieved from the normal network traffic.
B. Decision Trees: It is often known as DT, are a type of machine learning algorithm that makes use of a tree-like model of decisions and the potential outcomes of those decisions. A model that determines whether network traffic is benign or malicious based on a predetermined set of rules can be constructed with the help of DT.
C. Support Vector Machines (SVM): SVM is a technique for machine learning that may be used to categorize network traffic as normal or malicious based on patterns in the network traffic. This classification is accomplished with the help of patterns in the network traffic. The SVM is trained to work by locating the hyperplane that differentiates the two types of data the most effectively.
D. Random Forests: It is often known as RF, are a type of ensemble learning method that improves classification accuracy by combining many decision trees into a single model. A model that determines whether network traffic is benign or malicious on the basis of a set of rules can be constructed with the help of RF.
E. Deep Learning: Deep learning algorithms, such as Convolutional Neural Networks (CNN) and Recurrent Neural Networks (RNN), can be used to classify network traffic as normal or malicious based on patterns and features extracted from the network traffic. This can be accomplished through the application of deep learning. A further use for the methods that underlie deep learning is the detection of anomalies in network traffic.
F. Clustering: Clustering methods, such as K-means and Hierarchical clustering, can be used to group network traffic into clusters based on similarities in the network traffic. This can be accomplished through the process of clustering. Anomaly detection in network traffic can be accomplished through the use of clustering.

Technique	**Advantages**	**Disadvantages**
Artificial Neural Networks (ANN)	Can handle large amounts of data and learn complex patterns	Can be computationally expensive and require significant training time
Decision Trees (DT)	Easy to interpret and understand	Prone to overfitting and can be limited in their ability to handle complex data
Support Vector Machines (SVM)	Effective in handling high-dimensional data and can handle non-linear relationships	Can be sensitive to the choice of kernel function and may not perform well with imbalanced data
Random Forests (RF)	Can handle high-dimensional data and reduce overfitting through ensemble learning	Can be computationally expensive and require significant training time
Deep Learning	Can handle complex data and learn high-level features automatically	Can require large amounts of training data and significant computational resources
Clustering	Can detect anomalies in network traffic and group similar traffic together	May be prone to false positives and require significant preprocessing of data

Table 2. Comparative Analysis of Various Techniques Used in IDPS in Computer Network

It is essential to keep in mind that the success of any given method is contingent on the application scenario as well as the features of the data that is being evaluated. As a result, in order to determine which strategy is the most

efficient for a specific intrusion detection system, it is recommended to assess and contrast a variety of various approaches.

IV. Proposed Technique for Machine Learning Based Intrusion Detection & Prevention System for Computer Network

In order to discover patterns of typical and aberrant behavior, our suggested approach involves training machine learning models on a dataset of network traffic. Information like source and destination IP addresses, port numbers, packet sizes, and other pertinent network traffic metrics are all included in the training data. To assess the training data and find potential security issues, we combine supervised and unsupervised learning methods.The models are then deployed in a real-time setting to assess incoming network traffic after they have been trained. When the models notice unusual behavior, they raise an alarm and take the necessary steps to thwart or lessen possible incursions. These measures may consist of restricting traffic from dubious IP addresses, notifying network managers, or suspending network services.The strategy is divided into two basic stages: training and testing.

A. **Training Phase:**During the training phase, you will complete the steps below.

i. Data gathering: Gathering a dataset of network traffic is the initial stage. This dataset ought to contain both regular and unusual network traffic. The dataset can be retrieved from a variety of sources, including network logs, tools for capturing network traffic, and network simulators.
ii. Data Preprocessing: It is necessary to extract pertinent features from the obtained dataset so that they may be used to train the machine learning model. These characteristics could include packet size, frequency, source and destination IP addresses, along with other pertinent data.
iii. Feature engineering techniques can be used to change the data into a format that is better suited for machine learning algorithms after the pertinent features have been retrieved. This could involve methods like dimensionality reduction, normalization, and others.
iv. After the data has been cleaned up, an appropriate machine learning technique is chosen, and the model is then trained using the cleaned-up data. This can be accomplished using a variety of machine learning algorithms, including decision trees, support vector machines, neural networks, and others.
v. Model Evaluation: After the model has been trained, it is assessed using a different dataset of network traffic. The correctness of the model is assessed using this evaluation, along with any potential areas for model improvement.

B. **Testing Phase:**The following activities are included in the testing phase:

i. Data gathering: The first stage is to gather a network traffic dataset that is comparable to the one that was used for training.
ii. Data Preprocessing: Using the same methods as in the training phase, the acquired dataset needs to be preprocessed.
iii. Model Prediction: Using the preprocessed data as input, a trained machine learning model predicts whether the network traffic is normal or pathological.
iv. Intrusion Detection and Prevention: In accordance with the machine learning model's predictions, the proper steps are performed to thwart or lessen any possible invasions. This could entail taking action to stop the intrusion from happening, such as banning traffic from a specific IP address, notifying security professionals, or doing anything else.

The proposed approach for intrusion detection and prevention in computer networks, which is based on machine learning, has the potential to be very effective, assuming that it is correctly built, trained, and applied. It has the capacity to prevent potential cyber assaults and dramatically improve the security of computer networks. Further

study is required to investigate the efficacy of this strategy on data derived from the actual world and to maximize the performance of the method.

C. Design &Implementation Steps:

In order to perform intrusion detection in computer network systems, approaches from the field of machine learning can be utilized. These techniques involve training models to recognize anomalies and hostile actions in network data. The following procedures are able to be carried out in order to put machine learning into practice for intrusion detection:

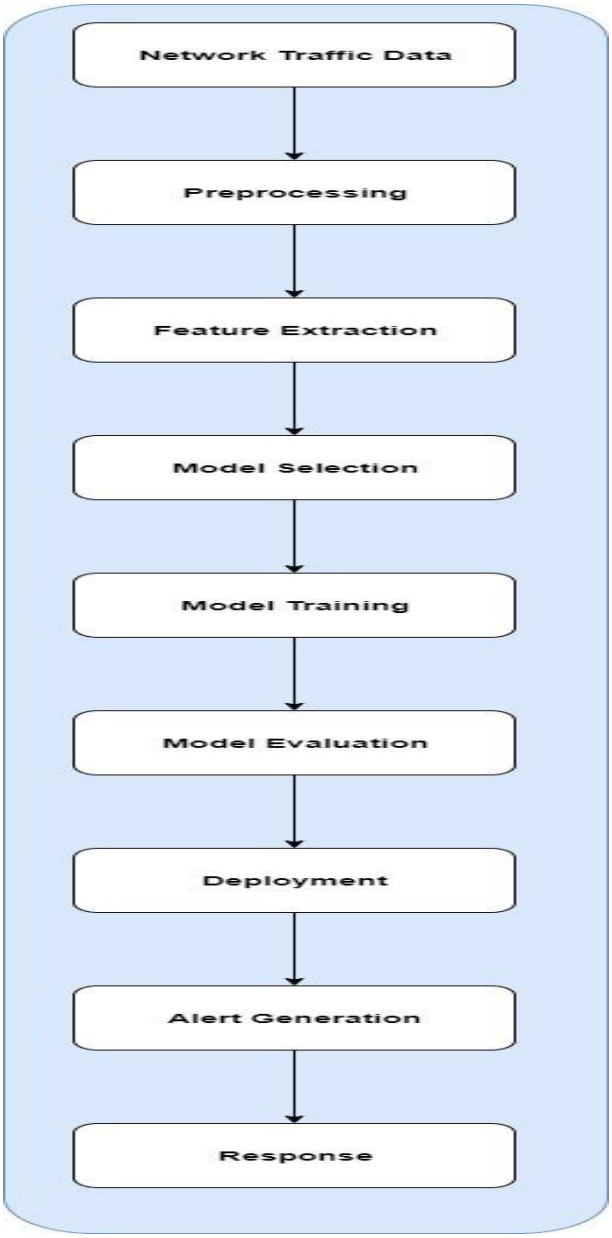

Figure 3. Block diagram of Machine Learning Based Intrusion Detection & Prevention in Computer Network

The first step in the procedure is the collecting of data on network traffic, which is then preprocessed in order to clean the data, filter the data, and normalize the data. When the data has been preprocessed, relevant characteristics are retrieved from it. These characteristics include the size of the packet, the source and destination IP addresses, the port numbers, and the kind of protocol. The qualities of the data and the nature of the problem are taken into consideration next, and an appropriate algorithm for machine learning is chosen. The data are preprocessed, and features are extracted before the specified algorithm is used to train the model. The performance of the model is then evaluated using a test set of data that the model has never been exposed to before. As soon as it is determined that the model is accurate, it is put into use in a production setting to perform real-time monitoring of network traffic. When the model identifies anomalies or malicious actions, it will issue alerts. These notifications will then activate an incident response mechanism, which will help mitigate any potential security risk.

i. Data collection: Gather information on network traffic, including both benign and potentially harmful activity, and then preprocess the information by cleaning, filtering, and normalizing it.
ii. Feature Extraction: Extracting important features from the network traffic data so that they can be utilized to train machine learning models is the goal of the feature extraction step. These characteristics can include things like the size of the packet, the source and destination IP addresses, the port numbers, and the kind of protocol.
iii. Model selection: It involves making a decision on which machine learning algorithm to use depending on the attributes of the data as well as the nature of the problem. To achieve the greatest possible performance, this may require testing with a variety of algorithms and different parameter settings.
iv. Model Training: Training the model involves instructing the chosen machine learning algorithm on how to learn from the preprocessed data and extracted features. In order to accomplish this, the data must be segmented into training and validation sets, the model's hyperparameters must be optimized, and the model's performance must be monitored.
v. Model Evaluation: Evaluation of the model involves determining how well the trained model performs on a test set of data that it has never been exposed to previously. At this step, the performance of the model is evaluated by assessing a variety of measures, including accuracy, precision, recall, and F1-score.
vi. Deployment: The trained model should then be deployed in a production environment so that it can monitor network traffic and identify anomalies and malicious actions in real time. In order to accomplish this, you might need to configure alerts and notifications and integrate the model with any current network security systems.

Implementing intrusion detection in computer network systems using techniques derived from machine learning can be a powerful tool, providing for the automatic and effective detection of potential security risks. Nonetheless, in order to keep the models' efficacy in check in the face of constantly shifting security risks, it is necessary to continually monitor and update them.

V. Application of Machine Learning based Intrusion Detection & Prevention in Computer Network

The applications of the machine learning strategies that were covered earlier in this article for the purpose of implementing intrusion detection in computer network systems are numerous in the domain of network security are as follows:

a. Network Intrusion Detection System (NIDS): Techniques from machine learning can be used to detect and prevent network intrusions such as denial-of-service (DoS) assaults, port scanning, and unwanted access attempts. NIDS stands for Network Intrusion Detection System.
b. Detecting Malware: Methods of machine learning can be utilized to analyze network data for the purpose of identifying malicious software, such as viruses, worms, and Trojan horses.

c. The detection of anomalies in network traffic can be accomplished with the help of machine learning algorithms. An anomaly is defined as an unusual pattern of data transmission or behavior on the part of the network.
d. Detecting Fraud: Methods of machine learning can be applied to the task of identifying fraudulent actions in financial networks. These methods include credit card fraud, money laundering, and others.
e. Detecting Botnets Machine learning strategies can be utilized in order to identify and prevent botnets, which are networks of computers that have been compromised and which are capable of being employed in criminal actions.

VI. Conclusion

In conclusion, the growing risk of cyber-attacks and network infiltration has led to the creation of highly advanced intrusion detection and prevention systems (IDPS) for the purpose of protecting networks. The classic rule-based IDPS have limits in identifying unknown attacks, which has led to the development of machine learning (ML) approaches for enhanced performance. These constraints have led to the adoption of these techniques. We analyzed a variety of machine learning techniques that are utilized in IDPS. These techniques include supervised, unsupervised, and hybrid approaches, and we discussed the benefits and drawbacks of each. In addition to this, we proposed a hybrid ML-based IDPS that incorporates the advantageous aspects of a variety of various methods in order to achieve enhanced performance. The difficulties that are connected with ML-based IDPS were also brought up for discussion. These difficulties include the requirement for vast volumes of high-quality training data as well as the possibility of adversarial assaults. We proposed a number of potential answers to these problems, including the utilization of synthetic data and the implementation of AI methods that are explicable. Finally, we highlighted the benefits of utilizing ML approaches for intrusion detection and prevention by demonstrating the practical use of ML-based IDPS in real-world scenarios. These examples were taken from the real world. Ultimately, the purpose of this study is to give a complete evaluation of the most recent developments in ML-based IDPS techniques and their potential for enhancing network security.

Reference

[1] Al-Fayoumi, M. A. (2012). Anomaly intrusion detection system using machine learning algorithms. International Journal of Computer Science and Information Security, 10(8), 11-19.
[2] Alshammari, R., &Zincir-Heywood, A. (2013). Evaluating the effectiveness of machine learning techniques in detecting DDoS attacks. International Journal of Network Security & Its Applications, 5(3), 69-80.
[3] Buczak, A. L., &Guven, E. (2016). A survey of data mining and machine learning methods for cyber security intrusion detection. IEEE Communications Surveys & Tutorials, 18(2), 1153-1176.
[4] Chen, X., Yang, H., & Xu, X. (2014). An intrusion detection model based on SVM and data mining. Procedia Computer Science, 32, 1178-1185.
[5] Cho, S., Kim, D., & Park, J. (2016). A deep learning approach to network intrusion detection. IEEE Access, 4, 210-220.
[6] Demirkol, I., &Kocak, T. (2012). Anomaly intrusion detection system using SVM and PCA. International Journal of Security and Its Applications, 6(3), 119-130.
[7] Ding, X., Jiang, C., Huang, J., Liu, L., & Sun, Y. (2018). Deep learning for network intrusion detection: A survey. IEEE Communications Surveys & Tutorials, 20(4), 3044-3072.
[8] Gharibi, W., &Seyed, F. (2013). A new intrusion detection system based on hierarchical clustering and support vector machine. International Journal of Computer Science Issues, 10(1), 124-134.
[9] Giotis, G., &Tziritas, N. (2017). Anomaly detection in network traffic based on machine learning algorithms. Procedia Computer Science, 108, 1497-1506.

[10] Han, Y., Kim, S., & Lee, J. (2012). Hybrid intrusion detection system based on SVM and decision tree. Journal of Network and Computer Applications, 35(4), 1304-1310.
[11] Khan, A., Li, L., & Shah, S. A. (2019). Machine learning-based intrusion detection system for internet of things. Computers & Security, 86, 191-207.
[12] Kim, K. J., & Park, H. J. (2014). A survey on deep learning-based network intrusion detection. International Journal of Distributed Sensor Networks, 10(3), 1-8.
[13] Li, X., Wang, Y., Zhang, J., & Li, Z. (2015). Hybrid intrusion detection model based on SVM and fuzzy clustering. Journal of Computers, 10(5), 301-308.
[14] Liu, X., Li, M., & Zheng, S. (2018). A hybrid intrusion detection approach based on SVM and ensemble learning. IEEE Access, 6, 63360-63369.
[15] Mandal, S., Pal, S. K., & Sanyal, S. (2018). Intrusion detection using machine learning algorithms: A review. International Journal of Network Security, 20(6), 1096-1107.
[16] S. G. Sanjeevi and D. P. Acharjya, "An efficient approach of intrusion detection using machine learning techniques," International Conference on Computing, Communication and Automation (ICCCA), Greater Noida, India, 2016, pp. 1049-1054.
[17] N. Akter, R. Hasan and M. Hasan, "Intrusion detection system using machine learning techniques," International Conference on Electrical, Computer and Communication Engineering (ECCE), Cox's Bazar, Bangladesh, 2016, pp. 139-142.
[18] Y. Zhang and J. Lu, "A machine learning based approach for intrusion detection system in cloud computing," International Conference on Intelligent Computation Technology and Automation (ICICTA), Changsha, China, 2017, pp. 661-665.
[19] A. M. Alshehri and M. A. Ali, "Machine learning based network intrusion detection system," International Journal of Engineering and Information Systems (IJEAIS), vol. 1, no. 7, pp. 9-16, 2017.
[20] A. Hu, Q. Zhang, X. Sun and Q. Zhang, "A machine learning approach for intrusion detection system based on network flows," 2018 IEEE 8th Annual Computing and Communication Workshop and Conference (CCWC), Las Vegas, NV, USA, 2018, pp. 128-133.
[21] Arman Tajbakhsh, Mohammad Rahmati, and Abdolreza Mirzaei, "Intrusion detection using fuzzy association rules," Applied Soft Computing, vol. 9, pp. 462–469, 2009.
[22] Terrence P Fries, "Evolutionary optimization of a fuzzy rule-based network intrusion detection system," Dept. of Computer Science, Indiana University, 2010 Annual Meeting 2010. [67] Y Dhanalakshmi and Ramesh I Babu, "Intrusion detection using data mining along fuzzy logic and genetic algorithms," International Journal of Computer Science and Network Security, vol. 8, no. 2, pp. 27–32, 2008.
[23] R Shanmugavadivu and N Nagarajan, "An Anomaly Based Netwok Intrusion Detection System Using Fuzzy logic," International Journal of Computer Science and Information Security, vol. 8, no. 8, pp. 185-193, 2010.
[24] Hari Om and Alok Kumar Gupta, "Design of Host based Intrusion Detection System using Fuzzy Inference Rule," International Journal of Computer Applications (0975 – 8887), vol. 64, no. 9, February 2013.
[25] S Selvakani and R S Rajesh, "Genetic algorithm for framing rules for intrusion detection," International Journal of Computer Science and Network Security, pp. 285–290, 2007.
[26] K Shafi, T Kovacs, H A Abbass, and W Zhu, "Intrusion detection with evolutionary learning classifier systems," Natural Computing: an international journal, vol. 8, pp. 3–27, 2009.
[27] A Orfila, J M Estevez-Tapiador, and A Ribagorda, "Evolving High-Speed, Easy-to-Understand Network Intrusion Detection Rules with Genetic Programming," in EvoWorkshops '09: Proc. of the Evo-Workshops 2009 on Applications of Evolutionary Computing, Berlin, Heidelberg, 2009, pp. 93-98.
[28] J E Dickerson, J Juslin, O Koukousoula, and J A Dickerson, "Fuzzy intrusion detection," in North American Fuzzy Information Processing Society Conference (NAFIPS-FLINTS 2001), 2001.

[29] P Tillapart, T Thumthawatworn, and P Santiprabhob, "Fuzzy intrusion detection system," Assumption University Journal of Technology (AU J.T.), vol. 6, no. 2, pp. 109–114, 2002.
[30] S Cho, "Incorporating soft computing techniques into a probabilistic intrusion detection system," IEEE Transactions on Systems, Man and Cybernetics-Part C: Applications and Reviews, vol. 32, no. 2, pp. 154-160, 2002.
[31] M-Y Su, G-J Yu, and C-Y Lin, "A real-time network intrusion detection system for large-scale attacks based on an incremental mining approach," Comput Security, vol. 75, pp. 301–309, 2009.
[32] M ZolghadriJahromi and M Taheri, "A proposed method for learning rule weights in fuzzy rule-based classification systems," Fuzzy Sets and Systems, vol. 159, pp. 449–459, 2007.
[33] A N Toosi and M Kahani, "A new approach to intrusion detection based on an evolutionary soft computing model using neuro-fuzzy classifiers," Computer Communications, vol. 30, pp. 2201–2212, 2007.