INTRUSION DETECTION AND PREVENTION SYSTEM

Sharanya Emmadisetty
Department of CSE
VNRVJIET
Hyderabad, India
emmadi.sharanya@gmail.com

M Sree Pranav Reddy
Department of CSE
VNRVJIET
Hyderabad, India
sreepranav2002@gmail.com

Chandana Sankarapuram
Department of CSE
VNRVJIET
Hyderabad, India
chandanasankarapuram@gmail.com

Sreya Tirumalaraju
Department of CSE
VNRVJIET
Hyderabad, India
sreyatirumalaraju@gmail.com

N Sandeep Chaitanya
Assistant Professor
Department of CSE, VNRVJIET
Hyderabad, India
sandeepchaitanya_n@vnrvjiet.in

Abstract—**The rapid growth of technology in different fields has led to a great need for various services as they are an essential component in any domain's operation and performance. With this advancement, there's a huge rise in the effects caused by cyber-attacks. There's a burning need to prevent this type of attacks and intrusions and its after affects. An essential instrument for monitoring, identifying and preventing intrusion threats is the INTRUSION PREVENTION SYSTEM (IPS).With a focus on datasets, ML methods, and metrics, this study tries to analyze recent Intrusion Prevention System research using a Machine Learning approach.**

An intrusion detector needs to be built to distinguish between safe normal connections and bad intrusions or attacks. The system's prevention model takes necessary action to reduce or restrict the extent to which the intrusion can damage the system. However, the dynamic and complex nature of cyber-attacks on computer networks cannot be handled by most techniques used in today's Intrusion Detection & Prevention System. Therefore, higher detection rates, lower false alarm rates and low computation and communication costs can be achieved by efficient adaptive methods such as various machine learning techniques.

Keywords— Intrusion prevention system, Random Forest, K Nearest Neighbors, Naïve Baye's theorem.

I. INTRODUCTION

With the shift towards distributed work environments, the threat landscape has become more expansive, and hackers are increasingly targeting remote workers' systems. As a result, more personal and confidential data is accessible online than ever before, which is of significant value to malicious actors. Unfortunately, no firewall or network is completely secure, and hackers are continually developing new tactics and techniques to bypass defenses. Typically, social engineering and malware are employed to obtain user credentials, granting the attacker access to sensitive information. Malicious attacks have become more sophisticated, and attackers are using evasion techniques to hide their activities and avoid detection by intrusion detection systems (IDS). The primary objective of IDS is to detect intrusions which are novel in nature. An IDS is a software designed to monitor individual computers may be targeted towards stealing, censoring, or corrupting information or network protocols. The primary goal of an IDS is to detect and respond to any malicious traffic, which is crucial for network security. By monitoring the inbound and outbound traffic on the network and data transfers between devices, an IDS can provide IT professionals with advance warning of possible attacks or network intrusions. Its role is to ensure that network security is maintained by keeping IT professionals informed about potential threats.Intrusion Detection System is not same as the firewall. An Intrusion Detection System detects and reports intrusions on a network, whereas a firewall would block and filter the network

II. LITERATURE SURVEY

The paper "Flexible Network-based Intrusion Detection and Prevention System on Software-defined Networks" by An Le, Hoa Le, et. al proposes an IDS/IPS system that uses the ability of centralization in SDN environment. The system consists of five main modules - SDN controller, OpenFlow switch, Feature Extractor, Data Classifier and Log Module. SDN controller manages the flow control in a software defined networking (SDN) environment. OpenFlow switch provides an pen protocol to program the flow table in different switches and routers. Based on a TCP connection, the Feature Extractor extracts some features from the header. Data Classifier detects whether it is an attack or not using machine learning. Log module saves information of the attacks and creates data for training process. It reduces the cost of specialized hardware and software required in traditional IDPS while maintaining the same performance. Accuracy(64.3%).

The paper "A Proposed Wireless Intrusion Detection Prevention and Attack System" by Jafar Abo Nada and

Mohammad Rasmi proposes a system that analyses data traffic. This system is based on collecting data traffic from "management frames" which are specific to wireless networks that work within IEEE 802.11 frequency. The system analyzes the users' behavior and the networks that they are using. In addition, the system updates the system's database. All these actions are supervised by the system's administrator. **I**t increases the effectiveness of the system in the work environment where the system is able to monitor most of the attacks and the system can Defend the network from counterfeit networks by attacking the attacker and cut the path towards the attacker and protect the staff from being scammed. Accuracy (68.1%).

The paper proposes a packet-based approach to network intrusion detection and prevention. The proposed system describes a network where every node contains the system installed in it. The main idea is to maintain a server node where every node will write the exceptional packet behaviors (performed by the intrusion packets) after it detects an exceptional packet. After a certain period of time every node in the network will read this exceptional behavior profile from the server and store these exceptional behaviors of the intrusive packets within them. This system is capable of coping with multiple intrusive packets unlike other systems and is less time consuming than currently existing IDS s. Accuracy(69.4%).

The paper " An instant approach to network intrusion detection and prevention" proposes an intrusion prevention system based on DoS attacks. The proposed system describes a network where every node contains the system installed in it. The main idea is to maintain a centralized database where every node will write the address of the intruder after it recovers from the intrusion. whenever any resource is unavailable, detect it as a DoS attack and freeze the link with the node from which the last instruction has come. In a network, a node is connected with several other nodes. It is capable of coping with multiple intrusions unlike other systems. It has a accuracy of 70.5%

The paper "Intrusion Detection and Prevention System Using Deep Learning" proposes an IDS/IPS system that uses deep learning algorithms for network traffic analysis. The system consists of two main modules: the intrusion detection module and the intrusion prevention module. The intrusion detection module uses a deep neural network to identify anomalous traffic patterns and classify them as normal or attack traffic.The system can detect a wide range of attacks, including both known and unknown attacks, and can also distinguish between different types of attacks.The use of deep learning algorithms can improve the accuracy of the system, reducing the number of false positives and false negatives. It has a accuracy of 90.2%.The system may be vulnerable to adversarial attacks that can manipulate or evade the deep neural network model, leading to false classifications and potentially compromising the security of the system.

The paper "NIDS: A network based approach to intrusion detection and prevention" proposes a network-based approach to intrusion detection and prevention using a combination of signature-based and anomaly-based techniques. The system uses real-time traffic analysis to detect known attack signatures and anomalous traffic patterns, and can respond to detected threats by blocking traffic, generating alerts, or triggering other security measures. The system proposed in the paper is based on a combination of signature-based and anomaly-based techniques, which can improve the accuracy and efficiency of threat detection and reduce the likelihood of false positives and false negatives. Accuracy(85.4%)

The paper “A Hybrid Intrusion Detection and Prevention System Using Machine Learning”proposes a hybrid intrusion detection and prevention system (IDPS) for IoT networks that uses machine learning algorithms to detect and prevent attacks. The system consists of three main components: a data pre-processing module, an intrusion detection module, and an intrusion prevention module. The data pre-processing module cleans and filters incoming data, the intrusion detection module uses machine learning algorithms to identify anomalous traffic patterns, and the intrusion prevention module takes action to block malicious traffic. The hybrid approach, which combines both intrusion detection and prevention capabilities, makes the system more robust and effective in mitigating attacks with a accuracy of 75.2%.The system may require significant computational resources, especially if the machine learning models are large and complex.

The paper "Intrusion Prevention System Design" by Xinyou Zhang proposes an intrusion prevention system (IPS) design based on a combination of signature-based and anomaly-based detection techniques. The proposed IPS consists of three modules: the packet analysis module, the signature matching module, and the anomaly detection module. The packet analysis module captures and analyzes network packets, while the signature matching module compares the captured packets against a database of known attack signatures. The anomaly detection module identifies anomalous network behavior by using machine learning algorithms**.** The use of machine learning algorithms allows for the detection of previously unknown attacks, improving the accuracy of the IPS to around 71.4%.

The paper proposes a practical approach for network-based intrusion detection and prevention. The authors describe a system that is capable of monitoring network traffic and detecting malicious activities in real-time. The proposed system consists of three main components: a data capture module, a data analysis module, and an action module.

The data capture module is responsible for capturing network traffic and storing it in a database. The data analysis module analyzes the captured data using a set of predefined rules and machine learning techniques to detect anomalous activities. The action module takes action on the detected malicious activities by blocking the traffic or alerting the system administrators. The system may require frequent updates to stay current with the latest threats and attack techniques. It has a accuracy of 68.6%.

III. EXISTING MODEL

Some existing intrusion detection systems such as Snort apply signatures of well known DoS and DDoS attacks to identify them. Signatures are modeled and created though the analysis of each individual attack in order to uniquely label the malicious traffic. Others monitor the changes in the normal behavior of host and network and any deviation will be detected and reported as an attack. Another existing systems such as Check Point embeds their Quantum IPS into their next generation firewall (NGFW) solutions to scan packets passing through the device. This device can replace a variety of other devices (firewalls, VPNs, etc.) and provides both IDS and IPS functionality. It uses both signature and anomaly detection. The disadvantage is that the support for distant or cloud resources that are not routed through the gateway is not available and for protection, internal network traffic must go through the gateway.

IV. PROPOSED SOLUTION

Our model aims to build a real time intrusion detection and prevention system that continuously runs in the background. This model tries to overcome the drawbacks of few of the existing systems such as the large number of false positives, The inability to detect unknown attacks and the need for a stable connection between client and server. It keeps on checking the internal state of the system through various classifiers like Naïve Bayes, Support Vector Machine and K Nearest Neighbors. When an intrusion is detected, the system will save the current works and automatically shuts down the system to prevent the spread of malware or any other intrusions.

Our main objectives are:

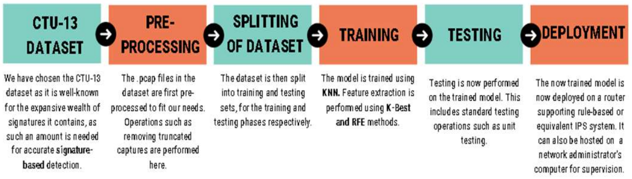
- To develop an effective Intrusion Prevention System.
- To provide reliable protection with minimal false-positives.
- To reduce processing times in order to not hinder network latencies.

V. METHODOLOGY

Our methodology focuses on building a modular model trainer, whose classifier and geature selection mechanisms can be selected by the user themselves through a GUI. We give them the option to choose between the aforementioned 3 classifiers and feature selectors. Hence, it makes for a more controllable training experience, as it is not given that each and every system will be able to perform the most resource-intensive training mechanism (a combination of Support vector Machine and Recursive Feature Elimination in this case).

Although the dataset featured has a certain affinity towards a combination of K-Nearest Neighours and Recursive Feature Elimination models, we are of the belief that these IDS/IPS programs we are buildin today are not build-once-use-anytime. We believe that as newer and newer cybersecurity threats are discovered, the models should be able to add the new data into their detection apparatus (through more training) and continue to be as effective, regardless of the novelty of the threat detected.

The suggested system relies on data and is based on Anomaly-based Intrusion Detection, which leverages machine learning to train the detection system to identify normal patterns of behavior instead of specific known threats. This system compares all network activity to the baseline that represents the usual system behavior. Instead of searching for known IOCs (Indicators of Compromise), the Anomaly-based IDS (Intrusion Detection System) detects any unusual behavior that triggers alerts. In summary, the proposed system uses a data-driven approach that relies on Anomaly-based IDS and machine learning to identify any anomalous activity that may pose a threat to the system.



We have chosen the CTU-13 dataset as it is well-known for the expansive wealth of signatures it contains, as such an amount is needed for accurate **signature-based** detection.

The .pcap files in the dataset are first pre-processed to fit our needs. Operations such as removing truncated captures are performed here.

The dataset is then split into training and testing sets, for the training and testing phases respectively.

The model is trained using **KNN.** Feature extraction is perfomed using **K-Best and RFE** methods.

Testing is now performed on the trained model. This includes standard testing operations such as unit testing.

The now trained model is now deployed on a router supporting rule-based or equivalent IPS system. It can also be hosted on a network administrator's computer for supervision.

Dataset

The TON_IoT datasets are new generations of Industry 4.0/Internet of Things (IoT) and Industrial IoT (IIoT) datasets for evaluating the fidelity and efficiency of different cybersecurity applications based on Artificial Intelligence (AI), i.e., Machine/Deep Learning algorithms. The datasets can be used for validating and testing various Cybersecurity applications-based AI such as intrusion detection systems, threat intelligence, malware detection, fraud detection, privacy-preservation, digital forensics, adversarial machine learning, and threat hunting. The datasets have been called 'ToN_IoT' as they include heterogeneous data sources collected from Telemetry datasets of IoT and IIoT sensors, Operating systems datasets of Windows 7 and 10 as well as Ubuntu 14 and 18 TLS and Network traffic datasets. Hence, it can be trained on and used for a wide variety of operating systems and client-side machines, considering the processes to obtain an intrusion into these systems are not too dissimilar.

Intrusions

In this project, we are focused on protecting the system against the most prominent types of network intrusions, namely: DDoS attacks, SQL injections, HTTP hijacking and such. As the peculiar signatures these actions produce int the system performance spectrum can be evidence enough of the intrusions themselves, we have opted to catch detect and/or prevent them by looking for the same. . Our model get the Windows metrics from the system, aggregates them into a query and makes a prediction based on the same. The model then forwards the prediction onto the system module, which makes the appropriate action hard-coded into it, logging the data and shutting the system down int this case.

Feature Selection:

Feature selections is performed using K Best and Recursive Feature Elimination.

K Best Selector

Based on the k highest score the features are chosen using SelectKBest. By modifying the 'score_func'value this approach can be applied to both regression and classification data.Choosing right features is a crucial process when we prepare a huge data set for training.

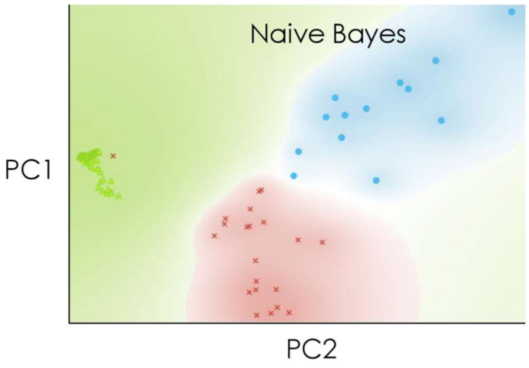
Recursive Feature Elimination

The recursive feature elimination (RFE) technique is used to select features in a model. Until the desired number of features is obtained it removes the weakest feature or features.The purpose of RFE is to eliminate any dependencies and collinearity that may exist in the model. The technique iteratively deletes a fixed number of features every iteration based on the model's coef_ or feature_importances_ characteristics.

Classifiers:
Naïve Baye's, K-Nearest Neighbors and Support Vector Machine is considered for this application.

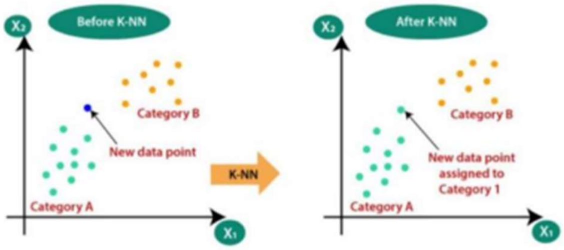
Naïve Bayes Classifier

A group of uncomplicated probabilistic classifiers, known as Naive Bayes classifiers, utilize Bayes' theorem and naive independence hypothesis between the features. The number of parameters required by these classifiers is linearly related to the number of variables (features/predictors) in a learning problem, making them scalable. During the training process, a closed-form expression is evaluated using maximum-likelihood, which takes linear time and is less expensive compared to the iterative approximation used in other types of classifiers. To summarize, simple and efficient probabilistic models are used by Naive Bayes classifiers. These models are scalable, and the training algorithms are straightforward and based on Bayes' theorem and naive independence assumptions.



K-Nearest Neighbours Classifier

The k-Nearest Neighbors (k-NN) algorithm was initially developed in 1951 by Evelyn Fix and Joseph Hodges, with additional enhancements by Thomas Cover. It is a non-parametric supervised learning technique that can be applied to both regression and classification tasks. The algorithm works by taking the k closest training samples from a given dataset as input. For k-NN classification, the output is determined by a majority vote among the k nearest neighbors, which results in the class membership of the object being classified. When k equals 1, the object is simply assigned to the class of its closest neighbor. For k-NN regression, the output is the property value for the object being predicted, which is the average of the values of the k nearest neighbors. In summary, k-NN is a powerful but straightforward algorithm that is useful for various supervised learning tasks..



Support Vector Machines

Support Vector Machines (SVMs), also known as support vector networks, are supervised learning models combined with learning algorithms that are used for both regression and classification tasks. They are considered to be one of the most reliable methods of prediction.The statistical learning frameworks or VC theory form the basis for SVMs. In summary, SVMs are supervised learning models that use statistical learning frameworks or the VC theory to analyze data for classification and regression tasks, and they are regarded as one of the most reliable prediction methods.

VI. EXPERIMENTAL RESULTS

The algorithm has been tested for different combinations of feature selectors and classifiers. Recursive feature elimination and K Best selector are used as Feature selectors. Naïve Baye's, K Nearest Neighbors and Support Vector Machine are used as classifiers.

		Precision	**Recall**	**F Beta**	**Accuracy**
Recursive Feature Elimination	KNN	0.9746	0.9742	0.974301	97.4%
	SVM	0.5130	0.7088	0.592452	60.1%
	Naïve Baye's	0.8205	0.4856	0.48225	48.2%
K Best Selector	KNN	0.9661	0.9662	0.966072	96.6%
	SVM	0.5201	0.1636	0.602629	60.2%
	Naïve Baye's	0.8638	0.7102	0.75559	75.5%

The maximum accuracy is obtained when K Nearest Neighbors is used with RFE feature selector. Hence it is used most to detect intrusions in the system. This application runs constantly in the background and when an intrusion is detected in the system it automatically saves the ongoing processes and shuts down the system thus preventing it from being attacked and malfunctioning.

VII. CONCLUSIONS

Our application works on the principle of Anomaly-based Intrusion Detection System. It is much more efficient than the existing Intrusion Detection Systems as our application can predict novel attacks and zero-day attacks. In our application, various machine learning models and procedures have been tested to come up with an IDS ML Model which predicts intrusions with a good accuracy. The IDS ML model using KNN as a classifier has performed the best. The other competitors were SVM and Naïve Bayes models. Based on the accuracy scores of the KNN model, it can be said that the Model is reliable enough to predict intrusions. Using RFE for feature selection has improved the accuracy of the KNN model by ~1.5%. A python-based script for windows systems to collect Network and System metrics has been developed. These metrics are then used by the IDS ML model to predict intrusions.

This application only works on Windows machines compatible with the win32pdh package as that is the only OS dependency. We aim to further add support to Linux and other Operating Systems by supporting a wider array of OS-level drivers. And overall this IPS system can be upgraded to capture device information from connected enterprise-level systems, but that would require access to said machines. We could also keep these machines up-to-date by providing Over-The-Air(OTA) updates that include updated models that are trained on newer vulnerabilities. Since the models aren't too big (<50 Mb), this can be achieved with moderate ease.We hope to provide an all-encompassing solution by more research and improving out codebase.

This project tries to tackle the problem of detecting intrusions using machine learning. The following points describe the extent to which the project deals with this problem: • The application module in this project only works on Windows machines (Windows 10 or 11) as it uses Windows-specific win32pdh API for extracting required network and system metrics • The application module can be modified in the future to function with other operating systems as well • This IDS model can also be upgraded into a much more comprehensive system which can also block and prevent detected intrusions

VIII.REFERENCES

1. Xianwei Gao et al. propose an adaptive ensemble machine learning model for intrusion detection.
2. Ansam Khraisat et al. survey intrusion detection systems, including techniques, datasets, and challenges.
3. Ravipati Rama Devi and Munther Abualkibash review different machine learning algorithms for intrusion detection, focusing on the KDD-99 and NSL-KDD datasets.
4. Abiodun Ayodeji et al. suggest a new perspective for developing robust intrusion detection systems for industrial control systems using data-driven approaches.
5. Jia dong Ren et al. propose a hybrid data optimization-based intrusion detection system that uses machine learning algorithms.
6. Abdullah Alsaedi et al. present a new dataset for data-driven intrusion detection systems in IoT and IIoT called TON_IoT Telemetry Dataset.
7. Zeeshan Ahmad et al. conduct a systematic study of machine learning and deep learning approaches for network intrusion detection systems.
8. M. Akshay kumaar et al. propose a hybrid framework that uses deep learning for intrusion detection in healthcare systems.
9. Chuanlong Yin et al. use recurrent neural networks for intrusion detection in a deep learning approach.
10. B. Ida Seraphim and E. Poovammal analyze intrusion detection systems using machine learning techniques.
11. Jianwei Hu et al. propose an improved convolutional neural network approach for network intrusion detection systems.
12. Hanan Hindy et al. develop a Siamese network for intrusion detection systems.