International Research Journal of Engineering and Technology (IRJET) e-ISSN: 2395-0056
Volume: 09 Issue: 03 | Mar 2022 www.irjet.net p-ISSN: 2395-0072

Network Intrusion Detection System using Machine Learning

Prof. Vrushali V. Kondhalkar[1], Swapnil Shende[2], Abhishek Patwari[3], Pranav Ovhal[4]

[1]Prof. Vrushali V. Kondhalkar, Dept. of Computer Engineering, JSCOE, Pune, Maharashtra, India
[2]Swapnil Shende, Dept. of Computer Engineering, JSCOE, Pune, Maharashtra, India
[3]Abhishek Patwari, Dept. of Computer Engineering, JSCOE, Pune, Maharashtra, India
[4]Pranav Ovhal, Dept. of Computer Engineering, JSCOE, Pune, Maharashtra, India
Department of Computer Engineering, Jayawantrao Sawant College of Engineering, Pune

---

Abstract - *Machine Learning Algorithms-based "Network Intrusion Detection System" is a soft device that monitors computer networks to detect malicious activity that is intended to steal confidential information or damage / hack network agreements. The technologies used in today's IDS cannot deal with Dynamic Complex types. security Cyber Attack on Computer Networks Login activity is primarily based on accuracy.*

The accuracy of the input should reduce false alarms and increase the availability of alarms. To improve

performance, various techniques have been used in recent activities. Analyze large network traffic data is the main function of the access system.

A well-planned separation method is needed to overcome this problem. Machine learning method such as Vector Machine support (SVM) and Naive bars used to test IDS. NSL-KDD information using acquisition data set, accuracy and distortion level is calculated.

Key Words: NIDS, Machine Learning, KDD

1.INTRODUCTION

To detect unusual malicious activity on a network or system by attackers Through Machine learning "In today's world one of the most dangerous things in the security of com puter or network security is illegal access to a computer system. As network applications are growing rapidly, new types of network attacks are on the rise. To manage suspicious activities our system needs to be reformed. Once an attack is identified or unusual behavior is detected, a notification can be sent to the director's strator. Access access systems (IDS) take the path based on the network or host by detecting and diverting attacks. In any case, these products are subject to attack signatures often indicate a malicious or suspicious intent. When the ID is checked these patterns in network traffic are then derived from the network.

Most of the techniques used in modern IDs they cannot manage the flexible and complex environment of Internet attacks on computer networks. So, effectively again using adaptive mechanisms that lead to high detection levels, low false alarm levels. Methods of machine learning provide appropriate accounting and communication costs. Matching pattern is fast enough to check the presence of a signature in the order of the incoming package and acquires a malicious behavior and must meet both your expansion signature number and link speed. There are several ways to use IDS.

This study describes the behavior of the machine learning to identify intruders. This is very helpful in preventing interference with some kind of related attack. The model can also reach real time identification entry based on size reduction and simple separator.

This study aims to increase focus on a number of points:

• selecting the appropriate algorithm for the appropriate tasks depending on the data types, size and network behavior and requirements.

• Implement a well-developed development process by preparing and selecting benchmark data set to build a promising NIDS system.

• Data analysis, acquisition, modeling, and engineering key features, are used several processing techniques by putting them together in a smart order for best accuracy with low data representation size and size.

• propose integration and a complete development process using these algorithms and strategies from database selection to testing algorithms used a different metric. What can be expanded to other NIDS applications are governed by an Intellectual body and they select the most suitable paper for publishing after a thorough analysis of submitted paper. Selected paper get published (online and printed) in their periodicals and get indexed by number of sources.

1.1 Background and Related Work

Integrating machine learning algorithms into SDN has attracted significant attention . A solution was solved to solve the problems in the KDD Cup 99 by making a plan extensive exploratory research, using the NSL-KDD data set to achieve excellent accuracy entry discovery. The experimental study was performed on five well-known and well-performing individuals machine learning algorithms

(RF, J48, SVM, CART, and Naïve Bayes). Relationships the feature selection algorithm was used to reduce the complexity of the features, which led to Only 13 features in the NSL-KDD database.

A dynamic model of the "Intelligent Access Acquisition System" proposed based on a specific AI method of access acquisition. Strategies that integrate neural networks and abstract thinking have a network profile, using simple data mining techniques to process network data. The program includes confusing, abuse and host-based acquisitions. Simple comprehensive rules allow for rules that reflect common ways to define security attacks. There have been a number of methods used by machine learning applications to address the problem of selecting features for access. In the author used PCA to identify space features in the main character area and select features that correspond to high eigen values using the Genetic Algorithm.. The same models were re-trained using 13 reduced features to achieve an average accuracy of 98%, 85%, 95%, 86%, and 73% in each model. A deep neural network model was proposed to detect and detect SDN intrusion.

1.2 Algorithms

1)Support Vector Machine:-

The Vector Support Machine (SVM) machine falls under a supervised learning method, where different types of data are trained from different subjects. In the upper part, SVM creates multiple hyperplanes or hyperplanes. A hyperplane that properly separates data assigned to different categories over a wide range, is considered a leading aircraft. To test genes between hyperplanes, the indirect detector uses a variety of kernel functions. Genetic enhancement among hyperplanes is the main goal of these kernel functions such as linear, polynomial, radial basis, and sigmoid. Due to the growing attention in SVMs, outstanding applications have been developed by developers and researchers. SVM plays a major role in image processing and pattern recognition applications.

2)Naive Bayes:-

Bayesian classifiers are statistical classifiers. They are capable to forecast the probability that whether the given model fits to a particular class. It is based on Bayes' theorem. It constructed on the hypothesis that, for a given class, the attribute value is independent to the values of the attributes. This theory is called class conditional independence.

$$P(H|\mathbf{X}) = \frac{P(\mathbf{X}|H)\ P(H)}{P(\mathbf{X})}$$

2. Literature Survey

1. Ahmad et al [1] analyze well-known machine learning methods namely. support vector method and advanced reading machine. NSL data set and data mining data are taken to assess the detection method. In their analysis results, it was concluded that ELM is more accurate than RF, SVM in whole data samples, and SVM is more accurate in part samples, except that in quarterly data SVM is better. Advanced Intelligent Access Acquisition System Using Machine Learning 2178 Published Blue Eyes Intelligence Engineering and Copy Recovery Science Number: H6932068819 / 19 © BEIESP DOI: 10.35940 / ijitee.H6932.078919

2. M. Al-Qatfet al [4] proposed an IDS approach that uses self-study (STL) which is an effective in-depth learning technology for learning feature and size. This is done using a scant auto encoder device which is a great way to learn how to rearrange the drawing of a novel feature in an uncontrolled manner. The paper currently improves the accuracy of SVM sections as well as training times and test times quickly. In addition, it produces accurate statistics in two categories and five categories. The highest level of precision in the five-phase division is achieved in this way compared to other shallow subdivisions such as J48, Naive Bayesian, RF, and SVM.

3. C. Xu et al [5] introduced the IDS reading comprehension study using an output feature that enhances the in-depth learning model. Proposed interventions that include a continuous neural system consisting of duplicate units (GRU), multilayer perceptron (MLP), softmaxmodule. The study is based on both the KDD database and the NSL-KDD data sets. This paper concludes that the effect of BGRU and MLP in combination with KDD 19 and NSL-KDD data is better.

4. Naseer et al [6] investigated a suitable IDS-based approach that is based on a variety of deep emotional networks such as convolutional neural systems, autoencoders, and periodic sensory systems. These were competent in the NSLKDD database and rated on the NSLKDDTest + and NSLKDDTest21 and operated on a GPU-based test bed using the non-backed Keras. In this case, the test was performed using organizational metrics namely. receiver performance indicator, curve area, memory recall curve, intermediate accuracy and deep separation precision and standard machine learning methods.

3. FUTURE SCOPE

Future work deals with large volume of data, a hybrid multi-level model will be constructed to improve the accuracy.

It deals with building an more effective model based on well. It deals with building an more effective model based

on well- organised classifiers which are capable to categorise new attacks with better performance.

4. SYSTEM ARCHITECTURE

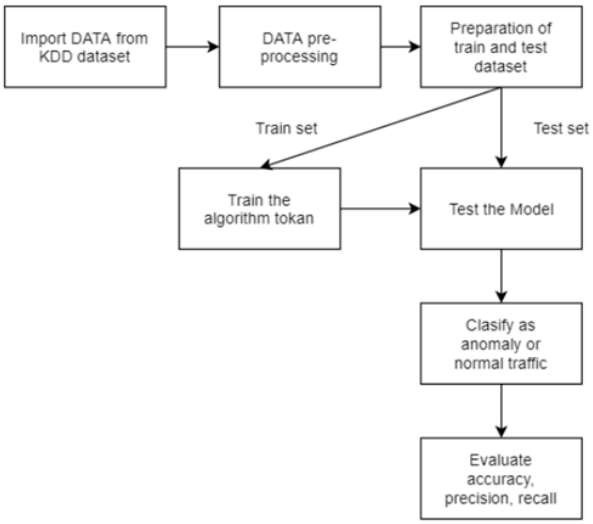

Figure 4.1: System Architecture

5. CONCLUSIONS

IDS is designed to provide basic acquisition strategies to protect existing systems on networks directly or indirectly online. But finally at the end of the day to the Network Administrator to make sure his network is out of danger.

Many different methods have been used in the screening process. Among them machine learning plays a vital role. This analysis works with machine learning algorithms such as KNN, DTC and Naïve Bayes.

This does not completely protect the network from attackers, but IDS helps the Network Administrator track down the bad guys on the internet whose purpose is to bring your network into a hotspot and make it vulnerable to attack.

REFERENCES

1. Hurley, T.; Perdomo, J.E.; Perez-Pons, A. HMM-Based Intrusion Detection System for Software Defined Networking. In Proceedings of the 2016 15th IEEE International Conference on Machine Learning and Applications (ICMLA), Anaheim, CA, USA, 18–20 December 2016; pp. 617–621.

2. Shone, N.; Ngoc, T.N.; Phai, V.D.; Shi, Q. A Deep Learning Approach to Network Intrusion Detection. IEEE Trans. Emerg. Top. Comput. Intell. 2018, 2, 41–50.

3. Gómez, J.; Gil, C.; Baños, R.; Márquez, A.L.; Montoya, F.G.; Montoya, M.G. A Pareto-based multi-objective evolutionary algorithm for automatic rule generation in network intrusion detection systems. Soft Comput. 2013, 17, 255–263.

4. Sangeetha, S.; Gayathri devi, B.; Ramya, R.; Dharani, M.K.; Sathya, P. Signature Based Semantic Intrusion Detection System on Cloud. In Information Systems Design and Intelligent Applications; Mandal, J.K., Satapathy, S.C., Kumar Sanyal, M., Sarkar, P.P., Mukhopadhyay, A., Eds.; Springer: New Delhi, India, 2015; pp. 657–666.

5. Dey, S.K.; Rahman, M.M. Effects of Machine Learning Approach in Flow-Based Anomaly Detection on Software-Defined Networking. Symmetry 2020, 12, 7.