# A Review on Attack Detection On Software Define Network

Jatin Nimade, Namita Tiwari**, Meenu Chawla**

*Research Scholar, **Professor*
*Maulana Azad National Institute of Technology, Bhopal, India*
*Jatinnimade05@gmail.com,*
*namitatiwari21@rediffmail.com, chawlam@manit.ac.in*

**Abstract**

To gain cost efficiency and network flexibility, most businesses are converting their traditional networks to Software-Defined Networks (SDN). However, we have seen recent security breaches and attacks against SDN which have shown that technology's security flaw. On a software-defined network, attack detection is an essential part of the infrastructure for security management(SDN). Advancement in machine learning has benefited a variety of fields with also including security.Anomaly-based intrusion detection systems are trained using machine learning approaches to detect even unknown threats. We can undertake a complete review of many various types of research related to ML-based Attack Detection systems using NSL-KDD dataset.

**Keywords:** NSL-KDD, IDS.

## 1 Introduction

Based on the detecting mechanism, the IDSs are divided into two categories. Anomaly-based and misuse-based detection are two of these types of detection. The usual type of traffic is modeled in anomaly-based detection frameworks. Any departure from the model is considered an attack. With innovative attacks, this method of detection offers

*River Journal,* 1–6.

an advantage. Misuse-based detection systems, on the other hand, we have coordinated the particular signatures for threats that have already been detected. There are various types of traffic who are associated with the preset assaults are regarded as normal. Based on the detecting mechanism, Two types of IDS-based detection are anomaly-based and misuse-based detection. The usual type of traffic is modeled in anomaly-based detection frameworks. Any departure from the model is considered an attack. With innovative attacks, this method of detection offers an advantage. Misuse-based detection systems, on the other hand, coordinate specific signatures to pre-detected threats.

Machine Learning (ML) technologies examine large data sets and predict the Variables of interest's future values using mathematical methods. Machine learning approaches are also used to train and assess the Intrusion Detection System(IDS) in the area of cyber security on dataset related to the security. An IDS that has been properly trained can identify unauthorized network activity as well as new assaults, such as zero-day attacks, forecast and detect.

We have examined many works with our related to Attack detection using the Network Security and Data Mining (NSLKDD) data set in this paper.The remainder of this work is divided into the following sections: NSLKDD data set is described in section 2 . We outline the various studies on ML-based IDS and their accuracy of different algorithm in section 3. and finally we have to conclude the paper in section 4.

## 2 NSL-KDD Data set

.

The NSL-KDD is a more comprehensive version of the KDD dataset that incorporates information from the KDD cup 99 data sets. The collection includes records of internet traffic detected by the simplified intrusion detection network and encountered by the genuine intrusion detection system. Each record in the dataset has 43 features, 41 of which are related to the input traffics and labels such as normal or assault, as well as the input, traffics' violence. In the dataset, there are four main types of assaults.: DoS, Probing, U2R, R2L.

Tavallaee et al. [13] conducted the usage of the KDDCUP'99 data set resulted in a poor anomaly detection evaluation, according to sta-

tistical analysis. They proposed the NSLKDD dataset, on the basis of original KDD dataset, to fix the issues.

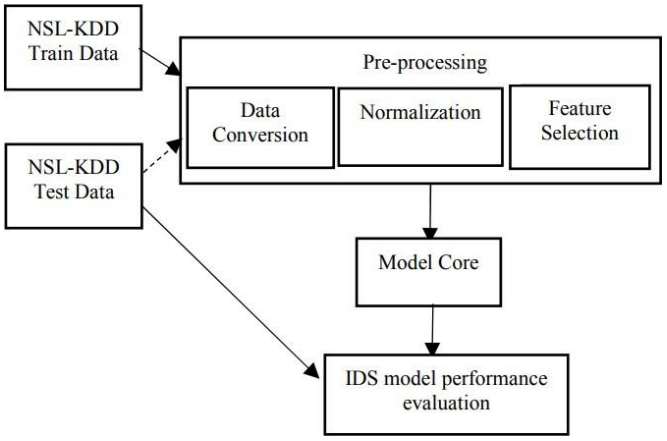


Figure 1 Flow of attack detection research efforts utilising the NSL-KDD dataset.

## 3 Related Work

In this section review and comparison of different Attack Detection in literature is done. Also tables(3.1) are included in this review which further describes and compares literature studied. 3.1 gives insights to various algorithm and some datsets used in different literature, datasets and compares different Attack Detection classification methods used and achieved accuracy on respective dataset.

### 3.1 Literature review

In the study, SHAHZEB HAIDER et al., [1] developed We used benchmark ensembles of deep learning and hybrid state-of-the-art methodologies to evaluate a framework for deep CNN ensembles that is both efficient and scalable for detecting the most common and sophisticated DDoS attacks in SDNs, and we put it through its paces on an SDN dataset based on flow. Both detection accuracy and computational complexity have improved with the suggested technique. this DDos attack detection achieved an accuracy level of 99.45

Table 1 Compression Of Different Paper

| Ref | Algorithms | Detection | Data sets | Classes | Accuracy |
|---|---|---|---|---|---|
| [1] | RNN & RNN<br>RNN & LSTM<br>LSTM & LSTM<br>CNN & CNN | DDos Detction | NSL-KDD | 2 | RNN-98.16%<br>RL-98.75%<br>LSTM-98.17%<br>CNN-99.45% |
| [2] | DL-CNN | Attack Detection | NSL-KDD | 2 | 98.43% |
| [3] | Ensemble voting<br>Multi Tree<br>DNN | Intrusion Detection | NSL-KDD | 5 | Ensemble voting-85.2%<br>Multi Tree-84.23%<br>DNN-81.61% |
| [4] | SAE -SVM<br>SAE-SVM | Intrusion Detection | NSL-KDD | 2<br>5 | SAE-SVM-99.14%<br>SAE-SVM-80.48% |
| [5] | RNN | Attack Detection | NSL-KDD | 2 | RNN-84.56% |
| [6] | Auto Encoder | Intrusion Detection | NSL-KDD | 2 | AN-90.61% |
| [7] | CM-KNN<br>DPTCM-KNN | Anomaly Flow Detection | Real Time Traffic | 2 | TCM-KNN-92.03%<br>DPTCM- KNN-97.88% |
| [8] | SVM and K-Means | Attack Detection | KDD-99 | 2 | SVM &<br>K-means - 92.86% |
| [9] | Multi DT's Algorithm and DNN, KNN Classifier | Attack Detection | NSL-KDD | 2 | Multi DT's- 85.2% |
| [10] | NB-SVM | Attack Detection | Real Organization Traffic | 2 | NB- SVM - 95.96% |
| [11] | LOA+CNN | DDos | NSL-KDD | 2 | LOA+CNN -98.2% |
| [12] | KNN+ELM | Intrusion Detection | NSL-KDD | 5 | KNN+ELM -84.29% |
| [13] | CNN | Intrusion Detection | NSL-KDD | 5 | CNN-79.48% |

In study X. Gao et al., [4] presented DT, DNN, and KNN classifiers are used in ensemble voting adaptive algorithms, as well as a ensemble voting adaptive algorithms with DT, DNN, and KNN classifiers and multi-tree approach with multiple Decision Trees (DTs). This IDS is validated using the NSLKDD dataset. The accuracy achieved was 85.2 %.

In P. Pokhrel et al., [9] proposed an Attack Detection that relies It was tested on two firms' traffic after integrating NB and SVM.. On two separate kinds of traffic, this IDS obtained accuracy scores of 95 % and 96 %.

Majd et al., [5] proposed in order to get better the system's overall accuracy, On the basis of flow statistics, a 5-level hybrid categorization system was presented. They use k-Nearest Neighbor technique (kNN) for the first level, and Extreme Learning Machine(ELM) for the second

. In order to avert irreversible harm as a result of a cyberattack, This IDS Acchived accuracy level of 84.29 % on five different classes of the dataset

KEHE WU et al., [6]To handle the problem of an imbalanced data collection, CNN was used to automatically determine the ach class's weight coefficient is based on its numbers in the cost function by extracting traffic attributes from a raw data collection. This IDS Achieved an accuracy level of 79.48 % on five different classes of the dataset.

D. Arivndainabi et al., [7] presented an DDos attack Detection using a loin optimizer algorithm with CNN classifiers. The NSL-KDD dataset was used to validate DDos Attack detection, with an accuracy of 98.2% on two different classes of dataset.

XIANWEI GAO et al., [11] suggested a paradigm for adaptive ensemble learning The model's main idea is to use ensemble learning to combine the benefits of various techniques. To boost the detection effect. It has been demonstrated showing our ensemble model improves detection accuracy effectively when compared to other research articles. The proposed algorithm has an accuracy of 85.2% on five different classes of detaset.

JULIAN JANG-JACCARD et al., [14] present a new 5-layer AE-based model that is superior at detecting abnormal network traffic. Our proposed model's major components and architecture are the outcome of a thorough and thorough investigation into the impact of major AE model performance indicators on detection accuracy.The accuracy of our proposed 5-layer architectural model is unsurpassed. That is 90.16. %

## 4 Conclusion

In this Study the advent of ML new ideas for Attack Detection in Software Define Network(SDN) has been implemented by various researcher and different form of classification model has been developed.We almost present a review of over 13 papers providing alternative approaches for implementing Attack Detection in this work.For the development of an IDS, a variety of machine learning algorithms were used. With all of the potential combinations of feature selection techniques. The most extensively used datasets in this domain are the KDD99 and NSL-KDD datasets. Ensemble and hybrid classifiers out-

perform single classifiers in terms of efficiency, resulting in a a high rate of detection and forecast accuracy.

## References

[1] Haider, S., Akhunzada, A., Mustafa, I., Patel, T., Fernandez, A., Choo, K. & Iqbal, J. A deep CNN ensemble framework for efficient DDoS attack detection in software defined networks. *Ieee Access*. 8 pp. 53972-53983 (2020)

[2] Sallam, Y., Ahmed, H., Saleeb, A., El-Bahnasawy, N. & Abd El-Samie, F. Implementation of Network Attack Detection using Convolutional Neural Network. *2021 International Conference On Electronic Engineering (ICEEM)*. pp. 1-6 (2021)

[3] Peng, H., Sun, Z., Zhao, X., Tan, S. & Sun, Z. A detection method for anomaly flow in software defined network. *IEEE Access*. 6 pp. 27809-27817 (2018)

[4] Gao, X., Shan, C., Hu, C., Niu, Z. & Liu, Z. An adaptive ensemble machine learning model for intrusion detection. *IEEE Access*. 7 pp. 82512-82521 (2019)

[5] Latah, M. & Toker, L. An efficient flow-based multi-level hybrid intrusion detection system for software-defined networks. *CCF Transactions On Networking*. 3, 261-271 (2020)

[6] Wu, K., Chen, Z. & Li, W. A novel intrusion detection model for a massive network using convolutional neural networks. *Ieee Access*. 6 pp. 50850-50859 (2018)

[7] Arivudainambi, D., KA, V. & Chakkaravarthy, S. LION IDS: A meta-heuristics approach to detect DDoS attacks against software-defined networks. *Neural Computing And Applications*. 31, 1491-1501 (2019)

[8] Al-Qatf, M., Lasheng, Y., Al-Habib, M. & Al-Sabahi, K. Deep learning approach combining sparse autoencoder with SVM for network intrusion detection. *IEEE Access*. 6 pp. 52843-52856 (2018)

[9] Pokhrel, R., Pokharel, P. & Timalsina, A. Anomaly-based–intrusion detection system using user profile generated from system logs. *International Journal Of Scientific And Research Publications (IJSRP)*. 9 (2019)

[10] Li, Z., Rios, A., Xu, G. & Trajković, L. Machine learning techniques for classifying network anomalies and intrusions. *2019 IEEE International Symposium On Circuits And Systems (ISCAS)*. pp. 1-5 (2019)

[11] Gao, X., Shan, C., Hu, C., Niu, Z. & Liu, Z. An adaptive ensemble machine learning model for intrusion detection. *IEEE Access*. 7 pp. 82512-82521 (2019)

[12] Ravale, U., Marathe, N. & Padiya, P. Feature selection based hybrid anomaly intrusion detection system using K means and RBF kernel function. *Procedia Computer Science*. 45 pp. 428-435 (2015)

[13] Tavallaee, M., Bagheri, E., Lu, W. & Ghorbani, A. A detailed analysis of the KDD CUP 99 data set. *2009 IEEE Symposium On Computational Intelligence For Security And Defense Applications*. pp. 1-6 (2009)

[14] Xu, W., Jang-Jaccard, J., Singh, A., Wei, Y. & Sabrina, F. Improving performance of autoencoder-based network anomaly detection on nsl-kdd dataset. *IEEE Access*. 9 pp. 140136-140146 (2021)