**Definition:**

An Intrusion Detection System (IDS) is a system that monitors a network for any abnormal activity and alerts the administrator if such activity happens. There are 4 main types of IDS:

* Network intrusion detection system (NIDS)
* Host intrusion detection systems (HIDS)
* Signature-based intrusion detection
* Anomaly-based intrusion detection system

A well known NIDS is **Snort**.

**Properties:**

* Monitoring the operation of routers, firewalls, key management servers and files.
* Providing administrators a way to tune, organize and understand relevant operating system.
* Providing a user-friendly interface.
* Including an extensive attack signature database against which information from the system can be matched.
* Reporting when the IDS detect that data files have been altered.
* Generating an alarm and notifying.
* Reacting to intruders by blocking them.

**Literature Review:**

In [1], the researchers used the Self-Taught Learning (STL) approach which consist of two stages i.e. first, Unsupervised Feature Learning (UFL) for feature learning from an unlabeled data and second, applying these learnt features on labeled data for its classification. For UFL, it used Sparse Autoencoder Neural Network that contains an input layer, a hidden and an output layer that set their respective weights by back propagation. We applied this technique on NSL-KDD dataset which is an advanced and improved version of KDD-99 dataset. The dataset is also pre-processed, before applying the above mentioned technique, in which one attribute is deleted due to its constant value for all instances of data. Total 121 attributes are processed. The dataset is divided into training and test data. This approach gave better results as compared to previously used approaches.

In [2], the researchers used Convolution Neural Network (CNN) which is basically used for image feature learning due to its better results in image processing. So, the dataset (NSL-KDD) is first preprocessed and total 121 attributes are used, which then are reformed into 2D dataset of size 11\*11 that will be processed as image by CNN. After one or more convolution layers, a pooling layer was included. The Rectified Linear Unit (ReLU) activation function is used in all layers except last one, in which softmax activation function is used. This report shows the feasibility of applying CNN in NDIS by modifying dataset in 2D form.

[3] The network intrusion detection system is an important tool for protecting computer networks against threats and malicious attacks. Many techniques have recently been proposed; however, these face significant challenges due to the continuous emergence of new threats that are not recognized by existing systems. DNN is used hence in the initial stage, network traffic can be classified into normal or abnormal with a probability score value. This value is used as an additional feature to train the final decision stage for normal and multi-class attack classification. Classification is performed by Soft-max classifier. Data processing consists of data-conversion and data-resampling task. Using 10-fold cross validation method each dataset is divided into ten parts, one of which is used as a testing dataset while the remaining nine are used as a training dataset. This method is repeated 10 times, and the results are then averaged to yield a single estimation. The advantage of this evaluation is that all observations are employed for both training and testing, and each observation can be used exactly once for testing the trained model. In this context, we demonstrate the results of each stage of the TSDL model. The results of the evaluation measures are demonstrated for both initial and final decision stages. The initial stage is responsible for normal and abnormal state classification, whereas the final decision stage is used for multi-class classification (normal state and other types of attacks). This implies that the TSDL model is a flexible FIGURE 6. Area under curve of normal and abnormal classification of KDD-99 dataset. . Confusion matrix of normal and abnormal classification for KDD-99 dataset. Evaluation measures of normal and abnormal classification for KDD99 dataset. intrusion detection model with two options, as requested by the user.

[1] Q. Niyaz, Weiqing Sun, Ahmad Y Javaid, and Mansoor Alam,“ A Deep Learning Approach for Network Intrusion Detection System” Link: <https://eudl.eu/pdf/10.4108/eai.3-12-2015.2262516>

[2] Leila Mohammadpour, Teck Chaw Ling, Chee Sun Liew and Chun Yong Chong.

Link: [journals.sfu.ca/apan/index.php/apan/article/download/239/pdf\_147](https://www.google.com/url?sa=t&rct=j&q=&esrc=s&source=web&cd=8&ved=2ahUKEwjV2sqk5YTjAhW-AmMBHRPFCssQFjAHegQICBAC&url=http%3A%2F%2Fjournals.sfu.ca%2Fapan%2Findex.php%2Fapan%2Farticle%2Fdownload%2F239%2Fpdf_147&usg=AOvVaw3Aln-0xprJZ39jrTTf5JFK)

[3] A Novel Two-Stage Deep Learning Model for Efficient Network Intrusion Detection Link:https://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=8643036