**Summaries**

[1], Adversarial Machine learning technique used to deceive the Deep Learning (DL) based NIDS that made DL-NIDS a vulnerable. So, instead of securing the network, the network will become more vulnerable due to deep learning infrastructure. There are two methods to secure deep learning models i.e. reactive and proactive. Defensive distillation and adversarial training are two proactive techniques while Pixel Defense is an example of reactive defense. An Open Source library Cleverhans is available for adversarial training. False positives detection increases the reliability of system while false negatives show the efficiency of system. There is a tradeoff between both of these values. There are two adversarial attacking objectives i.e. integrity violation exploited by false negative and availability violations exploited by false positive.

[2], NIDS are basically of 2 types: Signature based NIDS (SNIDS) and Anomaly Detection based NIDS (ADNIDS). SNIDS used for detecting the intrusion based on known features while ADNIDS is used for detecting unknown featured intrusions. In this paper, Self-Taught Learning (STL) and Non-symmetric Deep Auto-Encoder(NSDA) is used to learn patterns in unsupervised learning. Sparse auto-encoder will be used to learn the unknown patterns and then logistic regression function will be used to classify the user behavior learned by stack autoencoder. There are already many NIDS researched and implemented but a real time and more generic NIDS requires a lot of work yet. Total 115 features are considered here that are given as input to neural network. Deep network is made by stacking the autoencoders and logistic regression function is used to classify user as an intruder or normal user.

[3],This paper presents a novel deep learning technique for intrusion detection. Nonsymmetric deep autoencoder (NDAE) for unsupervised feature learning is proposed in this paper. This has been implemented using GPU enabled Tensor Flow with datasets KDD Cup ‘99 and NSL-KDD datasets. Most solutions are signature-based rather than anomaly based. Where signature based solutions are those solutions that detect an attack which is known .i.e. it belongs to a library/dataset of known attacks. On the other hand Behaviour or anomaly based as the name suggest is based upon the pattern of normal behaviour .i.e whenever an odd behaviour over a machine is observed the indication is made. Cetainly , the volume and diversity of network data is a challenge. However, here deep and shallow learning techniques are deployed. Particularly, Random Forest and NDAE are used. This paper focuses on nonsymetric data dimentionality reduction. For data dimensionality reduction the technique used is auto encoder. The input is first transformed into a typically lower-dimensional space (encoder), and then expanded to reproduce the initial data (decoder). Once a layer is trained, its code is fed to the next, to better model highly non-linear dependencies in the input. This paradigm focuses on reducing the dimensionality of input data. To achieve this, there is a special layer - the code layer , at the centre of the deep auto-encoder structure. This code layer is used as a compressed feature vector for classification or for combination within a stacked auto-encoder. If applied deeplearning to autoencoders it is termed as deep auto encoders or Stacked auto encoders. As for this paper NDAE Non symmetric deep auto encoder is used. Which learns the important features using similar strategy to that of deep auto encoder. Hidden input vector is given by hi = σ(Wi . hi−1 + bi) and “sigmoid function” is used for computing the actual output. To learn more complex features Stacked NDAE may be used. The stacked auto encoders with soft-max layer is not good at classification as compared to other classification algorithms so here stacked NDAE with shallow learning classifier is opted, .i.e Random Forest Classifier Algorithm.

[4], this paper proposed Anomaly-based Network Intrusion Detection System (A-NIDS) using Long Short Term Memory (LSTM) neural network architecture mostly used for sequence prediction problems, and One-class classification method Support Vector Data Description (SVDD) used for building a good data description vectors for normal data. This approach is used to tackle the time sequence attacks i.e. Dos, Probing, R2L and U2R etc. SVDD provides a best way to detect any anomalous activity because it generates a hyper sphere shape boundary across normal traffic data, and then classify any outlier data as anomalous. Network packets are fed to LSTM in form of sequence and the output of each sequence is averaged using mean pooling method. The LSTM model parameters are initialized randomly and then adjusted during training. Finally the output vectors of all sequences are fed to SVDD model, that convert them in a comparable form i.e. support vector classifier (SVC) and then make a hyper sphere shape space that will distinguish normal data from anomalous data. The new sequences will be input to SVDD Data Description model to determine a classification function y that will classify the sequence as normal or anomalous. For training, first order gradient descent approach is used due to its better results and high performance. In this way, parameters (c, R, theta) are optimized by joint structure of LSTM and SVDD infrastructure.

[5], Application of Deep Neural Networks for solution of Information security problems is relatively new area of research. However, most popular unsupervised learning technique is clustering in which the learning algorithm searches for similarities among instances of dataset to build group of instances called clusters. NSL KDD dataset has been used in this project. IDS problem in this study is treated as two-class problem where flows are either anomalous or normal. In general, learning algorithms benefit from standardization of the Dataset. Since different feature vectors of NSLKDD Dataset contained different numerical ranges, scaling is applied to convert raw feature vectors into more standardized representation for DCNN (Deep Convolutional Neural Network). As Datasets contained both normal and anomalous traffic, to avoid the negative influence of sample mean and variance, we used median and inter-quartile range (IQR) to scale the data for better results. We removed the median and scaled the data according to IQR. DCNNs accept input in form of images. Each NSLKDD training record from Training Dataset is shaped as 32x32 grayscale image. At first, the idea of converting a 41 feature input to a 32x32 2D array seems absurd but this approach has its merits. Arranging input features as 2D array helps to discover localized features which repeat themselves all over the input. So Proposed IDS approach uses a DCNN with an input layer, 3 pairs of conv-subsample layers, 3 fully connected layers and an output layer with one sigmoid unit

[6], This is actually a final year project dicussed by one of the students who have been part of it . So it starts with highlighting the fact that IDS is a variable sort of thing rather than static. Hence, approach used here is to detect anomaly. So it uses ISCX dataset by Canadian University for Cyber Security. An important step of Data pre-processing that enables “Deep learning” to be applied is that ISCX Flowmeter software has been used to convert “.PCAP” files to “.xml” format and finally to NumPy arrays. Essentially, these arrays act as images when given a visual form. Final product is an image, it makes sense that Convolutional Neural Network approach can be applied or generally Deep Learning. So VGG-19 model was used for this purpose. However, firstly anomaly dataset and Normal dataset individually were used for IDS as training data but there were discrepencies in the results. But when both Anomaly Data and Normal data were used the results improved substantially. And it became more like an outlier detection problem or in simple words classification problem. The system worked fine and to cope with various new types of attacks updating the dataset periodically ,as the new dataset by Canadian University for Cyber Securirty is launched makes system more efficient.

[7], As in most papers on this topic all start with mentioning the two types of Intrusion Detection techniques. That are 1. Signature Based 2. Anomaly Detection. Signature Based follow similar technique to that of a Virus Scanner. And as you know Virus Scanner needs to be updated periodically so is Signature based NIDS which require updating the datasets. While Anomaly Based works on analyzing the pattern of usage. Its ability to detect previously unknown (or variants of known) attacks when they appear is the biggest advantage of an Anomaly-based System. Self-Taught Learning is a deeplearning approach that consists of two stages for classification. In first stage un labeled data is used for feature learning i.e Unsupervised Feature Learning and this learnt representation in second step is applied to labelled data to carry out classification. The Sparse Auto-Encoder based feature learning is used for this work due to its easy implementation and good performance. As for dataset NSL KDD is used. One of the major drawback with the KDD Cup dataset is that it contains an enormous amount of redundant records both in the training and test data. This redundancy makes the algorithms biased towards frequent attacks and as a result does poor classification of infrequent harmful records. On the contrary NSL KDD dataset was more improved in a sense that it was less redundant hence making algorithms giving more accurate results. The dataset is preprocessed before applying self-taught learning on it. Nominal attributes are converted into discrete attributes using 1-to-n encoding The values in the output layer are computed by Sigmoid Function which gives values between 0 and 1 and then max min operations are performed to get a new list of attributes. The NSL-KDD training data without labels is used with the new attributes for the feature learning using sparse auto-encoder for the first stage of self-taught learning. In the second stage, the new learned features representation is applied on the training data itself for the classification using soft-max regression. In this implementation, both the unlabeled and labeled data for feature learning and classifier training come from the same source, i.e., NSL-KDD training data.

[8], So this report was important because we get to see how different ways can be used for NIDS and all through Deep Learning. 1.Vanilla Deep Neural Net 2. Self Taught Learning 3.Recurrent Neural Network are the three models of deep learning that primrarily are discussed in this report. The attacks which are on top of the list are DoS, Probe, R2L and U2R. KDD and NSL KDD datasets were used to observe difference in performances. Over 7 weeks’ network traffic collected was used for training. In all this a very important point is that “most novel attack are derived from known attacks” so it pretty much makes sense that deep learning can be applied for NIDS and to get effective results. Again as in one of the papers that I have researched on, here the fact is highlighted that KDD NSL dataset was prefered over KDD Cup due redundancies in the latter one. Simple deep neural network attained accuracy of 66 percent. It well classified the DoS and probe attacks but there was less success classifying normal non-threatning requests and U2R attacks. Then comes the STL(self taught learning). In steps STL works by first converting categorical features to numeric values. Then min max normalization takes place. Feature vector is passed to two layered stacked auto encoder. Results with this approach were pleasing with accuracy of 98.9 percent. Last but not the least Recurrent Neural Network take the input along with the previously perceived input instance. Problem with this model was vanishing gradient problem(when gradient is very small and weights remain same). Therefore the Long Short Term Memory Networks is a better version of RNN which eliminates the issue of vanishing gradient problem. Accuracy observed was 79.2 percent. Importantly the model failed to predict attacks other than DoS.

[9], This paper starts by discussing the Network and Network Intrusion Detection Systems. So amongst the existing system the Cross Layer Design is defined as: “Cross layer design, where the boundary among the protocol layers is a violated by sharing internal information, helping layers to become aware of the changes in the others and provide higher quality of services to the user.” Furthermore, the Network layers are discussed. So, important part is implementation. During the data transmission, packet drop process and packet delaying can be occurred due to the congestion and the collision along with the unavailability of the channel beau case of the hidden terminal and exposed terminal problem. This will lead to the false detection of the normal behavior as malicious behavior in the network environment. In order to handle this network dynamics, the learning system is employed based on the reinforcement learning system. So, behavioral prediction and operation of decision making system is carried by collected input during learning process. Secondly, the collaborated view of hidden layer is devised by **Bayesian network with Boltzmann input**. it is complex task to train a Deep Boltzmann machine (DBM) with **approximate maximum-likelihood learning** using the stochastic gradient unlike the restricted Boltzmann machines (RBM). DBM is a recently introduced variant of Boltzmann machines which extends widely used RBM to a model that has multiple hidden layers. There are some pros of DBM. DBM’s have the potential of learning internal representations that become increasingly complex, which is considered to be a promising way of solving object and speech recognition problems. Also high-level representations can be built from a large supply of unlabeled sensory inputs and very limited labeled data can then be used to only slightly fine-tune the model for a specific task at hand. As far as results are concerned, In case of Key Generation Delay, Machine **Learning Software Defined Network (MLSDN)** achieves higher performance by obtaining the lower delay. Similarly for **Key SharingDelay** MLSDN in lower latency compare to Software Defined Network (SDN). In case of **Hash Generation Delay**, MLSDN achieves lower delay while generating the hash code.

[10]  
In this paper by combining both NIDS and HIDS collaboratively, an effective deep learning approach is proposed by modeling a deep neural network (DNN) to detect cyberattacks proactively.  
An IDS system which uses system activities in the form of various log files running on the local host computer in order to detect attacks is called as HIDS. The log files are collected via local sensors. While NIDS inspects each packet contents in network traffic flows, HIDS relies on the information of log files which includes sensors logs, system logs, software logs, file systems, disk resources, users account information and others of each system. Many organizations use a hybrid of both NIDS and HIDS.  
Analysis of network traffic flows is done using:  
1. misuse detection,   
2. anomaly detection and/or   
3. stateful protocol analysis.

Most organizations tend to use both misuse detection and anomaly detection.   
Hence, after International Knowledge Discovery and Data Mining Tools Competition it was found that most of the published results of KDDCup 99 have used several feature engineering methods for dimensionality reduction.  
  
The proposed scalable architecture employs **distributed and parallel machine learning algorithms** with various optimization techniques that makes it capable of handling very high volume of network and host-level events.

Advanced machine learning embedded approach is deployed in this paper,owing to which the necessity of the feature engineering and feature extraction steps can be completely avoided. Along with advanced deeplearning text representation method have been used to extract contextual and sequence related information from system calls. (Bag of Words, N grams, Keras Embedding).

Computational model is based on Artificial Neural Network approach. More specific in terms , Multilayered Perceptron Learning which is sort of a FFN. Sigmoid , Tan h and softmax are the activation functions listed down with the ANN. Moreover, author states that “we employ DNNs as a more advanced model of the classical FFN with each hidden layer using the non-linear activation function, ReLU as it helps to reduce the **state of vanishing** and **error gradient issue**.” .

The DNN model was chosen by comprehensively evaluating their performance in comparison to classical machine learning classifiers on various benchmark IDS datasets. Overall, the performance can be further improved by training complex DNNs architectures on advanced hardware through distributed approach.

[11]

This paper explores how machines can learn algorithms involving a similar compositional structure. Arthimetic with simple operations is considered. However, the proposed model consists of an RNN-based controller that accesses the environment through a series of pre-defined interfaces. Each interface has a specific structure and set of actions it can perform. It consists of Input Tape, Input Grid and Output Tape. Where input tape reads one character at a time and can move left or right. Input Grid have additional up and down dimensions of movement. And Output tape is similar to Input tape except that it writes the character. To understand the behavior of this model and to provide an upper bound on performance, model is trained in a supervised setting, i.e. where the ground truth actions are provided. Note that the controller must still learn which symbol to output. But this now can be done purely with backpropagation since the actions are known.  
(*ground truth:* *accuracy of training set’s classification for supervised learning*)

Tasks involved are copy, reverse, walk , addition , 3 number addition and 1-digit multiplication. For the sake of comparision let us consider the fact that the simple feed-forward controller generalizes perfectly on the copy, reverse and walk tasks but completely fails on the remaining ones, due to a lack of required memory.

Second ML setting discussed is Q-learning which is unsupervised learning.  
the controller receives a reward of 1 every time it correctly predicts a digit (and 0 otherwise). Since the overall solution to the task requires all digits to be correct, a training episode is terminated as soon as an incorrect prediction is made. This learning environment is non-stationary, since even if the model initially picks the right actions, the symbol prediction is unlikely to be correct, so the model receives no reward. But further on in training, when the symbol prediction is more reliable, the correct action will be rewarded. This is important because reinforcement learning algorithms assume stationarity of the environment, which is not true in case of this model. Learning in non-stationary environments is not well understood and there are no definitive methods to deal with it.  
Another important set of experiments are ‘Reinforcement Learning Experiments’ discussed in this report. Enhancements had been applied to the six tasks in a series of experiments designed to examine the contribution of each of them. Performance of Reinforcement Learning being highly stochastic experiments were repeated a number of times with different random seed.  
  
Conclusively, they were not able to find a general controller that could solve all tasks.

[12]

There are two types Intrusion Detection Systems .The first one, **Host-based IDS** (HIDS), watches the host system operation or states. It detects system events such as unauthorized installation or access. The second one, Network-based IDS (NIDS) is placed on DMZ or choke point of the network edge. It observes a real-time network traffic and analyzes it for detecting unauthorized intrusions or the malicious attacks.  
Similarly, there are two types of detection techniques first one is behavior based intrusion detection called anomaly detection.While the second technique is a knowledge based intrusion detection called misuse detection. Long Short Term Memory (LSTM) to Recurrent Neural Network (RNN) have been applied in this paper and which it used for an IDS model. As proposed the Recurrent Neural Network is the effective model to training the sequence data. RNN has input , hidden and output units. Where as most important work is being done at hidden layer. Recurrent neural networks have introduced a directional loop that can memorize the previous information and apply it to the current output, which is the essential difference from traditional Feed-forward Neural Networks(FNNs).The preceding output is also related to the current output of a sequence, and the nodes between the hidden layers are no longer connectionless. Not only the output of the input layer but also the output of the last hidden layer acts on the input of the hidden layers. On the other hand Long Short-Term Memory (LSTM) networks are a type of recurrent neural network capable of learning order dependence in sequence prediction problems. LSTM is composed of a cell which is responsible for remembering values over arbitrary time intervals.  
***LSTM networks are well-suited to classifying, processing and making predictions based on time series data, since there can be lags of unknown duration between important events in a time series.*** To minimize LSTM's total error on a set of training sequences, iterative gradient descent such as back propagation through time can be used to change each weight in proportion to its derivative with respect to the error.As for Datasets a test dataset is independent of the training dataset, but follows the same probability distribution as the training dataset.   
During the first epoch in the learning process they obtained the lower efficiency rate at a range of 70%. When training the dataset at more number of iteration the error rate get decreased and the efficiency get increased. Efficiency reached the maximum of 93%

[13]

Various different techniques are available for IDSs’ to distinguish an attack, such as anomaly detection or signatures of attack. Intrusion detection based on ANN is built by using gathered features about several types of attacks. The problem in this paper has been formulated as an optimization problem.   
More specifically, the problem is how to find the optimal values of the hidden layer neurons in both Single Hidden Layer Feedforward Neural Network (SLFN), and Fast Learning Network (FLN) in order to maintain highest accuracy of testing.   
As the topic of this report goes the focus is on **Particle Swarm Optimization** (PSO). The PSO algorithm’s performance is greatly influenced by the included tuning parameters, often referred to as the **exploration– exploitation** tradeoff.  
Exploration: ability to assess certain regions in problem space to an attempt to specify the good optimum.   
Exploitation: describes the ability to focus the search within vicinity of a promising particular solution, to effectively and quickly locate the optimum.  
Each particle saves its position, composed of the candidate solution and its evaluates fitness, and its velocity.

As for the **Fast Learning Network** , it is a parallel connection of an SLFN and a 3 layer FNN: input, hidden and output layer.  
  
The overall accuracy of the ANN depends on how well the weights are selected. So **PSO-Based optimized FLN** is trained based on selecting weights using particle swarm optimization. Problem with optimizing is that 1. selecting the number of neurons in hidden layer for better accuracy 2. selecting weight values. To cope with this problem maximum no. of neurons are considered.

It can be concluded that the proposed PSO-FLN outperformed other learning approaches in the testing accuracy of the learning.   
Another finding is that the accuracy improved for all models with increasing the number of hidden neurons.

[14]

In this paper End-End Adversial learning approach has been proposed for anomaly based Network Intrusion Detection. It is a sort of semisupervised solution.  
It has been aimed to generate simulated anomalous flows, inspired by the Generative Adversarial Networks (GANs). Using GAN, it has been proposed that an end-to-end deep network for IDS which is able to effectively detect the network intrusions, even against unforeseen and new ones. The proposed method is composed of two main modules, Reconstructor network (R), and Anomaly detector network (A). However, the key idea of the proposed method is to solve this problem by simulating anomalous packet flows (PFs) using original normal traffic.

The **Reconstructor Network** generates simulated anomalous PFs by reconstructing normal traffic (to remove the need for the presence of anomaly class in training phase.). Where the purpose of the **Anomaly Detector Network** detects whether the incoming traffic is normal or not.

How is the Generative Adversial Network (GAN) different is that the simulated anomalies should have some deviation from the normal traffic, otherwise, anomalous PFs are not properly generated.  
  
Two Networks are used in GAN setting:

**1. Reconstructor Network:** has simulationly and adverserially generated anomalous traffic in the stage of training by reconstructing normal incoming PFs.   
This network gradually and in competition with Anomaly Detector Network, learns to generate flows similar to normal ones.

**2. Anomaly Detector Network:** acts as a classifier to distinguish between the representation of simulated traffic i.e., abnormal/fake flows, generated by Reconstructor Network and normal traffic i.e., real flows.

The proposed method has been evaluated on NSL-KDD dataset and the results suggest that this method has better performance compared to the other state-of-the-arts.

[15]

**References:**

[1] 27 March,2019. Link: <https://arxiv.org/pdf/1903.11688.pdf>

[2] March 2019. Link: <https://search.proquest.com/openview/ab6d5a2cbbb23e2c3cc10af0093a3134/1?pq-origsite=gscholar&cbl=2026671>

[3] February 2018: <https://blogs.qub.ac.uk/netsec/wp-content/uploads/sites/153/2019/02/08264962.pdf>

[4] May 2019: <https://arxiv.org/ftp/arxiv/papers/1906/1906.05277.pdf>

[5] , Enhanced Network Intrusion Detection using Deep Convolutional Neural Networks:2018 Link:<http://www.itiis.org/digital-library/manuscript/2163>

[6] Building Intrusion Detection System using Deep Learning year: 2018

link: <https://towardsdatascience.com/building-an-intrusion-detection-system-using-deep-learning-b9488332b321>

[7], Detecting Network Intrusion through a Deep Learning Approach:2018

Link:<https://www.researchgate.net/publication/322572874_Detecting_Network_Intrusion_through_a_Deep_Learning_Approach>

[8], Comparative Study of Deep Learning Models for Network Intrusion Detection:2018.

url: [https://scholar.smu.edu/datasciencereview/vol1/iss1/8/?%20utm\_source=scholar.smu.edu%2Fdatasciencereview%20%2Fvol1%2Fiss1%2F8&utm\_medium=PDF&utm\_campaign=PDFCoverPages](https://scholar.smu.edu/datasciencereview/vol1/iss1/8/? utm_source=scholar.smu.edu%2Fdatasciencereview %2Fvol1%2Fiss1%2F8&utm_medium=PDF&utm_campaign=PDFCoverPages)

[9], Optimized Intrusion Detection System using Deep Learning Algorithm:2019

Link: <https://www.academia.edu/39171572/Optimized_Intrusion_Detection_System_using_Deep_Learning_Algorithm>

[10], 3rd April, 2019: <https://ieeexplore.ieee.org/abstract/document/8681044>

[11], <https://arxiv.org/pdf/1511.07275.pdf>

[12] http://ajast.net/data/uploads/4093.pdf

[13] https://ieeexplore.ieee.org/abstract/document/8326489

[14] <https://arxiv.org/pdf/1904.11577.pdf>

[15] <http://ijsrst.com/paper/5345.pdf>