Survey of Deep Learning Based Intrusion Detection Systems for Cyber Security

Riyaz Jamadar[1],Shreyas Ingale[2], Anuj Panhalkar[2],Anup Kakade[2],Mohit Shinde[2]

[1]Assistant Professor AISSMS's Institute of Information Technology, Pune ,India

[2]Student AISSMS's Institute of Information Technology, Pune ,India

Abstract: Due to rapid growth of Internet and increasing complexity of cyber attacks, the need of cyber security has increased. There has been an extensive research in developing efficient and cost-effective solutions for intrusion detections. The latest research leverages machine learning and deep learning algorithms to provide most efficient solutions. In this paper an effort is made to prepare a survey report that describes some of the literature work carried out for developing network intrusion detection systems. The limitation of existing work along with advantages is been discussed with further research direction and scope. The primary objective of this survey is provide with a researcher, the state of the art work already carried out in this field of research.

Index Terms: **Deep learning, Intrusion detection, accuracy, precision**

I. INTRODUCTION:

With the increasingly in-depth integration of the Internet and social life, the Internet is changing how people learn and work, but it also exposes us to increasingly serious security threats. How to identify various network attacks, particularly not previously seen attacks, is a key issue to be solved
urgently.

Cybersecurity is a set of technologies and processes designed to protect computers, networks, programs and data from attacks and unauthorized access, alteration, or destruction [1]. A network security system consists of a network security system and a computer security system. Each of these
systems include firewalls, antivirus software, and intrusion detection systems (IDS). Currently, network intrusion detection systems (NIDS) offer a better solution to the security problem compared with other traditional network defence technologies, such as firewall systems. NIDS helps network administrators detect attacks, vulnerabilities, and breaches inside an organization's network [2].

There are three main types of network analysis for IDS: misuse-based, also known as signature-based, anomaly-based, and hybrid. Misuse-based detection techniques aim to detect known attacks by using the signatures of these attacks[3]. They are used for known types of attacks without generating a large number of false alarms. However, administrators often must manually update the database rules and signatures. New (zero-day) attacks cannot be detected based on misused technologies. Anomaly-based techniques study the normal network and system behaviour and identify anomalies as deviations from normal behaviour. They are appealing because of their capacity to detect zero-day attacks. Another advantage is that the profiles of normal activity are customized for every system, application, or network, therefore making it difficult for attackers to know which activities they can perform undetected. Additionally, the data on which anomaly-based techniques alert (novel attacks) can be used to define the signatures for misuse detectors. The main disadvantage of anomaly-based techniques is the potential for high false alarm rates because previously unseen system behaviour can be categorized as anomalies. Hybrid detection combines misuse and anomaly detection [4]. It is used to increase the detection rate of known intrusions and to reduce the false positive rate of unknown attacks. Most DL methods are hybrids.

This paper presents a literature review of deep learning (DL) methods for cybersecurity applications. The purpose of this paper is for those who want to study network intrusion detection in DL.

II. EXISTING WORK CARRIED-OUT IN NETWORK INTRUSION DETECTION SYSTEMS:

a) A Deep Learning Approach for Intrusion Detection using Recurrent Neural Networks:

In this paper[5], a deep learning approach for intrusion detection using Recurrent Neural Network (RNN-IDS) is proposed. RNN helps in improving the accuracy of classifier to achieve effective intrusion detection. It can remember previous information and can apply it to the current output which makes it damn effective than previous DL approaches like Feed Forward Neural Networks. The performance of proposed approach is evaluated using NSL-KDD dataset and is studied on binary and multi-class classification and compared with other ML based approaches like J48,SVM,ANN etc. Effects of different learning rate and number of neurons are also studied. Results have shown that

using RNN for classification increases the accuracy effectively and that its performance is superior to traditional machine learning classification methods in both binary and multi-class classification.

Traditional shallow machine learning approaches cannot solve the problem of massive amount of intrusion data classification that arises in real time network.Also,they cannot perform intelligent analysis and forecasting requirement required in massive data. Deep Learning approaches are able to extract better representations. But previous approaches have used deep learning in the pre-training phase only which doesn't make greater impact. Due to the dynamic growth of datasets, multiple classification tasks will decrease accuracy. Thus, proposed approach uses RNN for classification rather than pre-training., which has shown greater accuracy.

This approach has accuracy of 83.28% in KDD-Test and 68.55% in KDD-Test-21 for binary classification, slightly higher than traditional ML approaches on 80 hidden nodes and 0.1 learning rate and has accuracy of 81.29% in KDD-Test and 66.67% in KDD-Test-21 for binary classification,significantly higher than traditional ML approaches on 80 hidden nodes and 0.5 learning rate.

Although, this approach requires significant training time and has the problem of exploding and vanishing of the gradients used. Also, it cannot be stacked into deeper models.

b) An Effective Deep Learning Based Scheme for NIDS using Denoising Auto-encoder:

In this work[6], a deep learning-based approach for network intrusion detection using denoising auto-encoder (DAE) is implemented. A weight loss function is included which helps in selecting a limited number of important features for reducing feature dimensionality. The selected data is then classified using multilayer perceptron (MLP) as classifier. Experiments are conducted using UNSW-NB dataset. Results show that the feature selection yields satisfactory detection performance with low memory and computing power requirements.

Denoising auto-encoder is a special auto-encoder which receives corrupted data as input and is trained to predict original data as its output. Proposed approach consists of two deep learning-based components to perform feature selection and classification. The selection is performed by DAE where a key process is to add weights to its loss function which improves selection results by placing more emphasis on attack samples. The classification is done by MLP with the help of minimized number of parameters while still achieving high performance.

Main advantage is that firstly, feature selection for IDS is improved using weighted loss function since features that characterize attack samples are selected intelligently giving better detection performance. Secondly, the classifier i.e. MLP is used because after feature selection feature dimensionality is reduced significantly and hence strategic use of MLP (first deep MLP is implemented to maximize performance and then 2 hidden layers with 16 and 4 hidden units are used to minimize computation requirements) gives high performance even with a smaller number of parameters.

Overall accuracy of the approach is high 98.80 % with F-score of 0.952, precision of 95.98 % and recall of 94.43 %. The feature selection ratio is of 5.9% selecting 12 out of 202 features of which 2 belong to same class making the selected features to be 10.

c) Cloud-based Real-time Network Intrusion Detection Using Deep Learning:

This paper [7]investigates the capability of using deep learning models for network intrusion detection in real-time. A cloud hosted prototype system was developed that combines a deep learning binomial classification model to predict if there is an intrusion, with a multinomial model to identify the attack category. The prototype system integrates deep learning models built using the H2O framework, as well a messaging service to alert the network administrator. An evaluation study was carried out using the well-known benchmarked NSL-KDD dataset to compare the H2O deep learning models with models built using DeepLearning4J, Lib-SVM, Random Forest, Logistic Regression and Naive Bayes. The results showed that H2O deep learning models generally outperformed the other models, achieving over 99.5% accuracy using cross-validation on the training dataset and over 83% accuracy on the test dataset, for both binomial and multinomial classification.

The prototype system that was implemented in order to showcase the real-time network intrusion detection capability of deep learning using cloud computing. A web application was developed for network monitoring, which integrates two deep learning models: binomial classification model to identify if there is an intrusion or not, and multinomial model to detect the attack class in case of an intrusion. The application is hosted in AWS and communicates with the deep learning POJO models generated by H2O using API calls. The H20 environment was configured in AWS EC2.Proposed real-time network intrusion monitoring and alert system using Deep Learning. Instance and the deep learning models were deployed in the cloud environment if an intrusion is detected, the application shows live alerts in the web interface. Moreover, Twilio API is integrated for sending real-time notifications to the mobile phone of the network administrator, thus enabling the admins to take quick actions even if they are not with the monitoring system.An evaluation study was carried out using the benchmark NSL-KDD dataset which consists of normal traffic record as well as intrusions grouped into four classes U2R, Probe, R2L and U2R.

The evaluation study compared deep learning models built using H2O and DeepLearning4J libraries, with other commonly used machine learning models such as SVM, Random Forest, Naive Bayes and Logistic Regression. The results showed that the choice of the deep learning library is an important factor to consider for real-time applications, as using default settings H2O outperformed DL4J in terms of accuracy and detection rates, and was faster to train and build the models. In terms of accuracy the H2O deep learning based binomial and multinomial models also outperformed the other machine learning models. The H2O binomial model also provided better detection rates than the other models. However, for multinomial classification no model provided consistent and best performance for all intrusion classes. One limitation of this study is the use of the NSL-KDD dataset, thus other future work directions would be to use datasets with other intrusion types and/or real-time network traffic metrics.

d) Firefly algorithm-based Feature Selection for Network Intrusion Detection:

In this work[8] not all attributes are needed for detecting attacksreduced number of features can decrease the detection rate or increase the detection.Hence, we combine filter and wrapper-based approach to select appropriate feature for IDS.The extended work is in progress using GPU facilities to decrease the time taken for computation and improved results. Using this approach, we combined filter and wrapper-based approach to select appropriate features for detecting Network Intrusion. The motivation of the work is in reducing the number of features with improved performance for an uncompromised detection rate. The proposed work focuses on NIDS. Though various techniques exist in the literature for NIDS in terms of selection of features, classifiers, the proposed work concentrates on the Meta heuristic approach called firefly technique for feature selection and C4.5 classifier and compared with Bayesian network classifier.

In their work, instead of constructing a large number of features from massive network traffic, the authors aim to select the most prominent features and use them to detect intrusions in a fast and effective.Filter based feature used the information gain to select important feature based on relevance between an attributes and class and important feature are selected based on rank. Wrapper based feature selection used some searching methods to select subset of the features and selected subset is evaluated using C4.5 and Bayesian network. In this approach we used KDDCUP 99[9] data set which consist of total 22 normal and attack types.

Most of the existing NIDS detect attacks by using all attributes constructed from network trafficbut not all attributes are needed for detecting attacksreduced number of features can decrease the detection rate or increase the detection.Hence, we combine filter and wrapper-based approach to select appropriate feature for IDS.The extended work is in progress using GPU facilities to decrease the time taken for computation and improved results. Using this approach, the improved accuracy for the attack Dos,Probe,R2L and U2R are: 99.98%,93.42%,98.73%,68.97% and improved false positive rate are:0.01,0.01,0,0 respectively.

e) Fast Activation Function Based Deep Learning Approach:

In this work[10], we propose a novel fast activation function, namely the Adaptive Linear Function (ALF) to increase the convergence speed and accuracy of the deep leaning structure for real-time applications. The ALF reduces the saturation effects caused by the soft activation functions and the vanishing gradient caused by the negative values of the ReLU. We evaluate the training method for an online anomaly intrusion detection system using Deep Belief Network (DBN)and simulating four benchmark datasets.The activation function increases the convergence speed of the DBN, with the entire training time reduced 80% compared to the sigmoid, ReLU, and tanh activation functions.In ALF we expand our training method that combine generative part of tanh and ReLU to compress the input vector for fast training.

To evaluate the efficiency of this approach we design deep belief network and apply it to task of online anomaly detection using four benchmark datasets:CSIC HTTPKDDCUP99,NSL-KDD and Kyoto datasets. We demonstrate the improved DBN unsupervised training method using the ALF outperformed the sigmoid, ReLU and tanh activation functions for the task of online anomaly intrusion detection using four benchmark datasetsand proposed training method requires an average of only 3 epochs to converge for the four datasets compared to 25 epochs using SSAELM structure and achieves a testing speed of 0.325ms during online detection.

Previous experiments with deep belief network for anomaly detection focused on measuring the performance of the network for offline detection. Common nonlinear activation functions used in neural networks such as the tanh and the sigmoid activation functions suffer from saturation during training. The saturation behaviour causes the problem of vanishing stochastic gradient decent. Another drawback of the sigmoid function is that it causes most of the neurons to activate, which makes training the deep structure slow and costly for real-time applications. On the other hand, the ReLU activation function increases the sparsity of the neurons in the network, which reduces the number of neurons that can activate during deep learning training. compare to other activation function the performance of ALF is higher in accuracy and over all convergence speed and testing time DBF,decrease the false positive rate.

In this approach,the method achieves an accuracy rate of 98.59% on the total 10% KDDCUP'99 test dataset, 96.2% on the NSL-KDD dataset, 98.4% on the Kyoto dataset,and 96.57% on the CSIC-HTTP dataset.

f) A Deep Auto-Encoder Based Approach for Intrusion Detection System:

The proposed deep learning approach for Intrusion Detection Systems (IDS) uses Deep Auto-Encoder(DAE) model[11]. Deep Auto-Encoder is one of the most well-known deep learning models for addressing the network security problems. This DAE model is trained in greedy layer-wise fashion for avoiding problems like overfitting and local optima.KDD-CUP'99 dataset is used for experimental results. This result shows that the proposed approach provides significant improvement over other deep learning-based approaches concerning accuracy, detection rate and false alarm rate.

Deep Auto-Encoders (DAEs) are created by daisy chaining auto-encoders together. The proposed Deep Auto-Encoder based IDS consists of four auto-encoders. Here the output of each auto-encoder in the current layer is used as the input of the auto-encoder in the next layer. SoftMax classifier is used which classifies the attack classes from input dataset in the last hidden layer of model. Therefore DAE-IDS performs unsupervised feature learning, supervised fin-tuning, and thus intrusion detection. For solving the Intrusion detection problem, Deep Auto-Encoder based IDS runs in two phases: training and testing. Firstly, in training phase, the system uses a training dataset and creates a model based on proposed DAE model. Then the system employs the model for identifying the label of unseen data (test dataset) in the testing phase to estimate the performance of the system if is used on-line. Various experiments are performed on KDD-CUP'99 which is widely used standard dataset for evaluation of IDSs. Experimental results show that the proposed approach can produce low false negative rate (0.42%), high accuracy (94.71%), and high detection rate (94.53%).

g) Deep Learning Approach Combining Sparse Autoencoder with SVM for Network Intrusion Detection:

It proposes an effective deep learning approach[12], self-taught learning (STL)-IDS, based on STL framework which is formed by combining Sparse Auto-Encoder (SAE) and Support Vector Machine (SVM). It will reduce training and testing time considerably and effectively improves the prediction accuracy of Support Vector Machines (SVM) with regards to attacks. NSL-KDD dataset is used to compare the efficiency of the proposed approach with single SVM and that of different classification algorithms, such as naive Bayesian,random forest, multilayer perceptron etc classification algorithms in related work on binary and multiclass classification. Results are in terms of performance metrices in binary and multiclass classification.

STL is a new deep learning framework consisting of two stages. In the first stage new effective representation is achieved without using labels and hence called unsupervised feature learning. IN second stage new representation is combined with labelled data then SVM is used for classification. The performance accuracy rate of proposed approaches better than SVM alone and the training and testing time of SVM are reduced considerably due to reduced storage requirements and computing complexities.

For the KDDTrain dataset, the proposed approach achieves accuracy for two-category and five-category classification is 99.423% and 99.414%, respectively.

III. CONCLUSION:

This paper describe a literature review of ML and DL methods for network security. The paper, which has mostly focused on the last 2 years, introduces the latest applications of ML and DL in the field of intrusion detection. Unfortunately, the most effective method of intrusion detection has not yet been established. Thus, it is difficult to choose a particular method to implement an intrusion detection system over the other and there is good scope to resolve the various limitations of the existing wok.

REFERENCES

[1] S.Aftergood, "Cybersecurity:The Cold Online," vol. 547, pp. 30-31, 2017.

[2] M. A.Milenkoski, "Evaluating computer intrusion detection systems," *ACM compute,* Vols. 48 no-1, pp. 1-41, 2015.

[3] C. a. K.Acha, "Virtulization layer security challanges and intrusion detection systems," *A survey of comman pratices,* Vols. 73,no-3, pp. 1192-1234, 2017.

[4] A. E.Viegas, "Towards an energy-efficient anamoly-based intrusion detection engine for embedded systems," *IEEE Trans. Comput,* Vols. 66,no-3, pp. 163-177, 2017.

[5] Y. a. X. C. Yin, "A Deep Learning Approach for Intrusion Detectiom using Recurrent Neura;ll Network," *IEEE Access,* vol. 5, pp. 21954-21961, 2017.

[6] C. Q. W. G. Y. L. a. o. H.Zhang, "An Effective Deep Learning Based Scheme for Network Intrusion Detection," in *2018 24th International Conference on Pattern Recogination(ICPR)*, Bejing,China, 2018.

[7] A.-N. M. Santosh P, "Cloud-based Real-time Network Intrusion Detrtion using Deep Learning," in *2018 International Conference on Cyber Security and Protection of Digital Services*, Glasgow,UK, 2018.

[8] M. K. Selvakumar B, "Firefly algorithm based Feature Selection for Network Intrusion Detection," *Computers &*

Security, vol. 81, 2018.

[9] E. M.Tavallaee, A Detailed Anylasis of KDDCUP99 dataset, CISDA, 2009.

[10] C. P. Khaled Alrawashdeh, "Fast Activation Function Approach for Deep Learning Based Online Anomaly Intrusion Detection," in *2018 IEEE 4th International Conference on Big Data Security on Cloud (BigDataSecurity), IEEE International Conference on High Performance and Smart Computing, (HPSC) and IEEE International Conference on Intelligent Data and Security (IDS)*, Omaha, NE ,USA, 2018.

[11] J. H. F Farahnakiam, "Deep Auto-Encoder based Approach for Intrusion Detection," in *ICACT*, Turku,Finland.

[12] Y. A.-S. M AL-Qatf, "Deep Learning Approach Combining Sparse Autoencoder with SVM for IDS," *IEEE Access*, vol. 6, pp. 52843-52856, 2018.