International Journal on Advances in Engineering Technology and Science
Volume: 5, Issue: 1, 2024, e-ISSN: 2455-3131
DOI: 10.5281/zenodo.10779137

A Review of Deep Learning Mechanisms for Intrusion Detection and Prevention in Network and IOT based Environments

Nikhil Chaurasia[1], Neeraj Sharma[2]

[1]Assistant Professor, Sanjeev Agrawal Global Educational University, Bhopal
[2]Research Scholar, University Institute of Technology, RGPV, Bhopal

[1]nikhilsub97@gmail.com, [2]neerajsharmans12@gmail.com

***Abstract*– As the Infrastructure is growing, we found a tremendous growth in Digitization, every enterprise is focusing on premise Data center or on the Rented Cloud, so to meet security prospective from Intrusion is one of the major concerns. A New terminology is being used as CSP's (cyber-physical systems) instead of Datacenter and with the Evolvement of Deep Learning (DL) Concepts and its efficiency DL procedures finds a great scope to remove all the vulnerabilities by priory identifying Risks and then afterwards by prevention from any king of malware impacts .In our survey we basically focusing the Application of Deep Learning (DL) Procedures to Build a secure systems by implementing strong Neural Networks (NN) by providing suitable Training with the malicious Data sets and then afterwards to develop a good prevention capabilities, Deep learning is the subset of machine Learning (ML) and also in the previous scenarios ML techniques proves to be very much stable due to their self-Learning and enhancing Capacity in terms of Weighted Attributes they are used in Spam detection,DoS Attacks, probe Attacks, Host based Attacks, Network based Attacks etc. In our survey paper we will enlist multiple DL Learning Procedures as per the Attack Types.**

***Keywords:* cyber-physical systems (CSP's), Deep Learning (DL), Machine Learning (ML), Neural Networks.**

I. INTRODUCTION

Technology is continuously evolving and peoples are constantly using it on the large scale, creating a lot of problem for security related context and everything is digital and might be hacked, so it has to be prevented for unauthorized gain and access. As online world Increase everyone is doing purchasing and selling online by using credit cards or debit cards due to which Information will pass through multiple end points and will have the probability to be get breached and to be trapped by some faulty personnel which will be used further ward for the fault Intensions, cybercrime have been increased to the very high scale in the present scenario's As our study in [2] among all the cyber security Attacks DDos have been used up to the extent of about 40% approx. among all. These Attacks are dangerous for both the organization related information or individual information of any personnel, while on the other side to prevent for cyber security loss, Intelligent cyber prevention (ICP) [1] [3] system contains multiple layers of security containing authentications at Server Level, Network level, desktop or system level security, Antivirus level also.

Any organization will Implement security in multiple layers, and the accessible data have to be passed one by one from all the levels without any breach and if there is any probability the Intelligent cyber prevention system will prevent the data to be get passed from it, To understand the breach Intelligent cyber prevention (ICP) system will check the multiple Attributes such as network parameters, traffic Attributes, IP Addresses attributes, probes detection, Data Packet Level authentication, pattern etc. Also, the organizational or Individual data both have the threats. Firewall, anti-virus software, data loss prevention (DLP) systems and intrusion detection systems are used to prevent cyberattacks, Data leakage, Hacking, phishing Attacks, Ransomware attacks etc. Artificial Intelligence (AI) has come up with the great capabilities in the field of cyber security first by detection of any of the vulnerability and then after by prevention from multiple type of cyber security attacks. Deep Learning (DL) algorithms [4]. and Artificial Neural Networks(ANN's) will be trained on high dimensional data received from previous stats of fraudulent detection to predict whether there is any possibility of data or Information breach and (if any) the system will automatically stops all the data or information flows without going through any losses .In the current study we will discuss about Intrusion Detection systems Implemented through Deep Learning algorithms (DL), also about the parameters on which DL procedures works and how they will prevent the Cyber Intelligent systems(CIS) to be get security breached .

The following is the organization of the study, second part will be emphasized, on AI based IDS (Intrusion Detection and prevention systems, later on third part will give a comparative view about multiple secured architectures used in Deep Learning, while the fourth chapter will tell us about the Datasets used in various DL architecture studies. fifth chapter, gives a detail and examine about various studies done in the literature work in the AI field for building secured systems. In the last chapter, general evaluations and suggestions for future work are presented.

II. INTRUSION DETECTION SYSTEM

Intrusion detection systems find its position after the firewall and antivirus software and it is completely responsible to generate alarm by identifying some abnormal behaviour to system Administrator, It (IDS) is an application which prevent the overall system from any unauthorized access .In the present scenario Intrusion detection systems will capture all events and traffic for any activity over the local and remote hosts and in case of any breach if the captured Events and Logs properly studied we will find out the deep cause of breach. And this will help us to make our system more stable for the next time if the same thing will be happened. The Anomaly and signature based attacks will be identified on priority i.e. in case of signature based our system will have database entries for matching purpose and if it find the known events same as that were occurred in some previous cases it will quickly abort the Information transfer that will prevent the breach, while on the other side in case of anomaly detection the IDS will capture all abnormal events and can detect the unknown attacks as well after recognizing abnormal events but there is the possibility to get more False positives(FP) in case of anomaly based IDS.

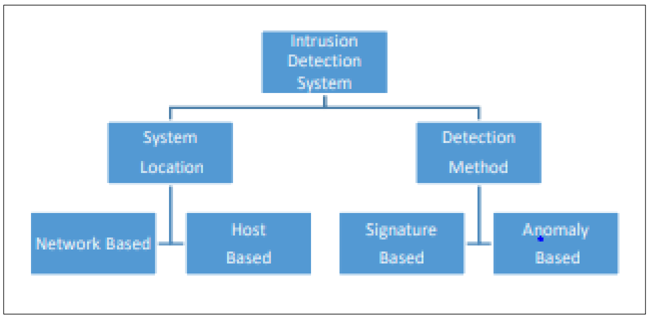

Figure 1.1

The above diagram will show us more details about the type of intrusion detection systems on the basis of network based or host based also whether the approach used is Signature based or anomaly based, to build a future secured system it is very important to increase the strength of IDS through the application of multiple ML techniques.

III. MULTIPLE DEEP LEARNING TECHNIQUES

Deep learning (DL) is the subset of machine learning (ML), while Artificial intelligence (AI) is the superset of ML. In deep learning we are focusing to increase the learning capability of the Artificial Neural Network (ANN) by providing training data sets to the network, there are multiple category of neural networks available to Implement a deep learning procedure some of the common examples are CPN, BPN, ADALINE, MADALINE etc. Restricted Boltzmann Machine (RBM) are also used for deep learning purpose for Natural language processing and Voice and Image pattern recognition.

A. Convolutional Neural Networks

Convolution Neural Networks are the basic Implementation model used for Machine Learning (ML) it is the Network of Neurons connected with each other through weighted factors and contains many Layers with in i.e. Input layer, Hidden Layers, Output Layers as per the complexity and requirement the Network may contains many Hidden layers also the training data set is very Big for these networks and they are much complicated in comparison to simple Neural Networks.

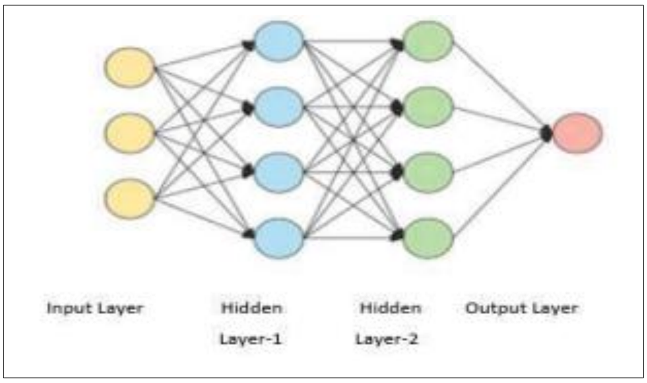

Figure 1.2

B. Recurrent Neural Networks

We will not find any connection between input and output streams in traditional Neural Networks, but is very much required to mix the previous output with the new input for better predictions. At every step the previous output will be combined with the new input. RNN found the major Application in the field of Image recognition.

C. Long short-term memory Network

It will come under the category of RNN. LSTM is the refinement of RNN and will be used in the field of language processing and word processing. This Network will retain the important parameters and threshold for the long term period.

D. Deep Belief Network

These networks will contain multiple layers inside and will be very much feasible for complex scenarios. These Networks are of very dense nature also Human Intervention is not allowed in them and the Training time is also large.

E. Restricted Boltzmann Machine

This is the two-layer network It find its application in language and word processing; they are not very much dense Network as others. It will be used in numerous models for enhancing Intrusion Detection System Capabilities

IV. DATASETS AND METRIC CLASSIFICATION

To train a network For Deep Learning is one of the critical tasks, otherwise it will not detect and predict anything, but to gather good Training data for Deep learning network is very Important task, the overall data sets should be prepared in such a way that it has data for both the scenarios for Normal traffic cases and also for Abnormal Traffic cases, also the flowing network traffic contains information in Data packets i.e. having Ip Addresses, encoding techniques used etc. The following are the examples of some frequently used datasets available UNB ISCX 2012, UNSW-NB15, NSL-KDD and KDD CUP 99.

S.No	Result of Binary Classification	Description
1	True Positive (TP)	It can be simply defined as the count of Non-Malicious Samples and correct Data packets samples, authorized (Valid) applications classified as Good and Normal, i.e. identified by our ML Model
2	True Negative (TN)	It can be defined as the count of Malicious attempts samples or hackers attempts as Bad or Abnormal by our ML model
3	False Positive (FP)	It can be simply defined as count of malicious Data samples or negative samples that has been marked as Good or Normal by our model.
4	False Negative (FN)	It can be simply defined as the count of Non-Malicious Samples and correct Data packets samples, authorized (Valid) applications classified as Bad and Abnormal, i.e.by our ML Model

Table 1.1

Metrics To be used for Evaluation criteria in Multiple datasets for ML model will be done through classification [18] the basic metric calculations has been given to calculate Efficiency and Accuracy of ML model, afterwards by using these matrix other parameters such as space complexity, time complexity, reliability etc. of the ML model will be calculated. Consider the below simple Table 1.1 for the terminology we are going to be used that is basically called a confusion matrix or error matrix. Now consider the below Table to calculate multiple metrics using the Above four Binary classifiers.

S. No	Metric Name	Calculation	Description
1	Positive Predictive Value / Precision (PRV)	PRV = TP/(TP+FP)	It is the ratio of positive samples correctly classified, positive data, and applications to the total overall positive sample.
2	True Negative Rate (TNR)	TNR = TN/(TN+FP)	It can be Defined as the ratio of total correctly classified malicious sample to the total number of malicious samples.
3	True Positive Rate (TPR)	TPR = TP/(TP+FN)	It is the percentage correctly classified samples to the Total positive samples
4	Accuracy (A)	A = (TP+TN) / (TN+FP+FN+ TP)	It is the percentage of truly classified ones to the overall prediction
5	False Positive Rate (FPR)	FPR = FP/(FP+TN)	It is the ratio of malicious samples classified incorrect to the total number of malicious samples
6	False Negative Rate (FNR)	FNR = FN/(FN+TP)	It is the percentage of positive sample classified Incorrectly to the total number of positive samples
7	False Discovery Rate (FDR)	FDR = FP/(FP+TP)	It is the ratio of malicious sample classified incorrectly to the total Malicious samples
8	False Omission Rate (FOR)	FOR = FN/(FN+TN)	It is the percentage of Incorrectly classified positive sample to the total positive classified samples

Table 1.2

The Above parameters and classifiers are very Important to measure the efficiency of overall system and for better prediction, The ANN were trained over these data and will respond to Malicious data once it will identify and stop any Intrusion Inside the system by un authorized personal.

V. RELATED WORKS / LITERATURE REVIEW

Many Research studies are available for Deep Learning in the literature H.A. Najada [5] proposed a Research on deep learning using data set i.e. UNB ISCX IDS 2012, The Deep Learning Network used contains about 200 nodes for each of the layer and there were about 4- hidden layers were Implemented for the network, The Intrusion Detection System Implemented is Anomaly-based, also RELU is used as an activation function.

Research made by S. Parampottupadam [6] has provided the system to detect real time Intrusion in cloud-based systems, they have used NSLKDD dataset to carry out the research. Although the efficiency is good, they have calculated the Results in terms of binary classification and Multiple classification

Research made by A. Diro [7], is priory done for IOT based Infrastructure where a Distributed Intrusion Detection system is being established and accuracy is being captured in terms of Binary and Multiple classifiers, while NSL-KDD (UBMK'19) is being used as a Data set in It.

Research made by A. Shengield [8] uses a shellcode-based intrusion detection systems the Snort and Squil Data sets are used in it and Deep learning used a Multilayer perceptron-based network architecture with 2 hidden layers in ANN.

While the D. Aksu [9] developed a deep learning architecture to identify port-scanning attacks and compared the results with the machine learning algorithm of the support vector machine (SVM). CIC IDS 2017 dataset was used and there were 7 hidden layers in deep learning architecture. Activation function was RELU, It will detect the breach if found though port number login patterns.

In the Research made by H. Liu [10], payload classification-based IDS (Intrusion detection System) is used, RELU is being used as the Activation function for Training Purpose, The networks used for Implementation are CNN and LSTM

Research made by Yu Liu [11] Implemented deep learning for IDS using Traditional Networks

Research made by F. Feng [12] primary focuses on Adhoc Networks from the prospective of intrusion Detection, also It detected and afterwards prevented Cross Site Scripting (XSS), SQL, DoS Attacks, it founds its applications in the networks (self-organizing) for Military purpose CNN and LSTM network-based architecture will be used in it.

C. Yin [13] used the NSL-KDD dataset in this study and created the structure of the RNN-based intrusion detection system. In this study, binary and multiple classification was done. The test results for the number of hidden nodes and selection of learning rate of RNN were shared.

T.A. Tang [14] created an intrusion detection system with flow-based deep learning approach for software-defined networks. 3 hidden-layer deep belief network architecture

F. Khan [15], in his study, used UNSW-NB15 and KDD CUP 99 datasets, author priory focuses on the Traditional intrusion detection systems, this study has worked by implementing neural Networks for Leaning purpose.

Research made by A. Dawoud [16] defined a software-defined based security solution prominently for IOT systems where dataset used is KDD CUP 99 proposed system which was a security solution based on software-defined networks for IoT systems.

Research made by M. Hawawreh [17], uses a standard Deep Feed Forward Neural Network (DFNN) for intrusion detection or Industry based, below table will provide the comparative view of various techniques.

SN	Paper Reference No.	Area Focussed on	Used Datasets
1	H. A. Najada [5]	Anomaly-based IDS	UNB ISCX IDS 2012
2	S. Parampottupadam [6]	Real-time IDS for cloud system	NSL-KDD, 41 features
3	A. Diro [7]	Distributed IDS for IoT system	NSL-KDD, 41 features
4	A. Shengield [8]	Shell code-based IDS	Snort and Sguil alert data
5	D. Aksu [9]	Port Scanning Detection	CIC IDS 2017
6	H. Liu [10]	Payload Classification	CNTC-2017 WebShell, Darpa 1998, KDD99, CSIC 2000 http header
7	Yu Liu [11]	Traditional network IDS	NSL-KDD, 41 features
8	F. Feng [12]	IDS for ad-hoc networks	KDD CUP 99 Dos attack, Waf logs for XSS and SQL attack
9	C. Yin [13]	IDS for traditional networks	NSL-KDD, 41 features

10	T. A. Tang [14]	IDS for SDN	NSL-KDD, 6 features
11	F. Khan [15]	IDS for traditional networks	KDDCUP 99, UNSW-NB15
12	A. Dawoud [16]	SDN based IDS for IoT	KDDCUP 99
13	M. Hawawreh [17]	IDS for Industrial IoT	NSL-KDD, UNSWNB15
14	Saini, N, Bhat [20]	APT assaults	NSL-KDD, UNSWNB15
15	Vanin P [19]	DoS at the transport and application layers	NS-3 simulation datasets with the Forecasting and Chaos approach

Table 1.3

VI. CONCLUSION

In the mentioned study we have given brief description about the Intrusion detection systems, also we have discussed about multiple Deep Learning Models and Multiple Algorithms available in it. In our study we majorly discussed about Anomaly based Intrusion detection systems, also a detailed Note about various available data sets has been given with their characteristics and how they will be Helpful for training purpose, also we have compared multiple woks proposed by different authors in the respected area. The overall Intrusion detection system should be capable To identify any unusual and unseen pattern which is Abnormal and IDS should quickly Inform the system Administrator about the breach Attempt.

REFERENCES

[1] R.Raj, I. Lee, and J. Stankovic, “Cyber-Physical Systems : The Next Computing Revolution,” pp. 731–736, 2010.

[2] DDos (Distributed Denial of Service)C. A. C. Report, ‘Cisco Annual Cybersecurity Report’, Cisco, 2018.

[3] A. C. Alvaro, “Challenges for Securing Cyber Physical Systems.”

[4] Y. Bengio, P. Lamblin, D. Popovici, and H. Larochelle, “Greedy layer-wise training of deep networks,” in Proceedings of the 19th International Conference on Neural Information Processing Systems, ser. NIPS’06. Cambridge, MA, USA: MIT Press, 2006, pp. 153–160. [Online]. Available: http://dl.acm.org/citation.cfm?id=2976456.2976476.

[5] H. Al Najada, ‘Cyber Intrusion Prediction and Taxonomy System Using Deep Learning And Distributed Big Data Processing’, IEEE, pp. 631-638, 2018.

[6] S. Parampottupadam, ‘Cloud-based Real-time Network Intrusion Detection Using Deep Learning’.

[7] A. Diro, ‘Distributed attack detection scheme using deep learning approach for Internet of Things’, Future Generation Computer Systems, pp. 761-768, 2017.

[8] A. Shenfielda, ‘Intelligent intrusion detection systems using artificial neural networks’, ICT Express 4, pp. 95-99, 2018.

[9] D. AKSU, ‘Detecting Port Scan Attempts with Comparative Analysis of Deep Learning and Support Vector Machine Algorithms’, IEEE, pp. 77-80, 2018.

[10] H. Liu, ‘CNN and RNN based payload classification methods for attack’, Knowledge-Based Systems, pp. 332-341, 2019.

[11] Y. Liu, ‘Intrusion detection based on IDBM’, IEEE, pp. 173-178, 2016.

[12] F. Feng, ‘Anomaly detection in ad-hoc networks based on deep learning model: A plug and play device’, Ad Hoc Networks, pp. 82-89, 2019.

[13] C. Yin, ‘A Deep Learning Approach for Intrusion Detection Using Recurrent Neural Networks’, IEEE Access, cilt 5, pp. 21954-21962, 2017.

[14] T. Tang, ‘Deep Learning Approach for Network Intrusion Detection in Software Defined Networking’, IEEE, pp. 1-7, 2016.

[15] F. Khan, ‘A Novel Two-Stage Deep Learning Model for Efficient Network Intrusion Detection’, IEEE Access, cilt 7, pp. 30373-30385, 2019.

[16] A. Dawoud, ‘Deep learning and software-defined networks: Towards secure IoT architecture’, Internet of Things, pp. 82-89, 2018.

[17] M AL-Hawawreh, ‘Identification of malicious activities in industrial internet of things based on deep learning models’, Journal of Information Security and Applications, pp. 1-11, 2018.

[18] X. Deng, Q. Liu, Y. Deng, and S. Mahadevan, "An improved method to construct basic probability assignment based on the confusion matrix for classification problem," Information Sciences, vol. 340, pp. 250-261, 2016.

[19] Vanin P, Newe T, Dhirani LL, O’Connell E, O’Shea D, Lee B, Rao M. A Study of Network Intrusion Detection Systems Using Artificial Intelligence/Machine Learning. Applied Sciences. 2022; 12(22):11752. https://doi.org/10.3390/app122211752.

[20] Saini, N, Bhat Kasaragod, V, Prakasha, K, Das, AK. A hybrid ensemble machine learning model for detecting APT attacks based on network behavior anomaly detection. Concurrency Computat Pract Exper. 2023;e7865. doi: 10.1002/cpe.7865