TEST Engineering & Management

May – June 2020
ISSN: 0193-4120 Page No. 205 - 216

A Review on Deep Learning Approaches to Real Time Network Intrusion Detection System

[1]Teena K.B, [2]Dr. Smitha M. Rao,
[1]Presidency University, Mail: teenakb1@gmail.com
[2]Presidency University, Mail: smitharao@presidencyuniversity.in

Article Info
Volume 83
Page Number: 205 - 216
Publication Issue:
May - June 2020

Abstract:
Organizations are adapting the network security technologies to protect their data and infrastructure in the wake of rapid increase in modern sophisticated cyber-attacks. IDS is one such system used by organization to differentiate between abnormal and normal behavior and identify the system attacks. But intrusion analysis of large data such as audit or log files with present IDS solution is not optimal since these IDS generate high False-Positive rate and Time to identify attack is also more. In recent times we have seen Machine learning being used to aid IDS to improve its performance. Machine learning based IDS identify sophisticated attack with better accuracy, reduce the False-Positive rate and in a timely manner. In this paper we will be looking at the different phases of an cyber-attack, and we will look at different Machine Learning algorithm such as Cluster-Based Approach, machine-Learning Based Approach, Optimization Algorithm based approach, artificial neural network based approach, deep learning based approach, model based approach, hybrid mock-up based approach. Here we will have a brief discussion on working of this algorithm, their shortcoming and their false positive accuracy rate with respect to each other.

Keywords— *Intrusion Detection, Classifier, Machine Learning, Deep Learning, Artificial Neural Network*

Article History
Article Received*: 11August 2019*
Revised*: 18November 2019*
Accepted*: 23January 2020*
Publication*:07May2020*

I. INTRODUCTION

As per the survey result of Internet World Stats Conducted in 2018 [1], a majority of the population who use internet are above 18 years age for various purposes ranging from research, Information, entertainment, infotainment etc. The introduction of Internet of Things in recent years also increased usage of internet [2]. Thus there is a tremendous growth of internet users in the last decade in every possible domain. It is projected by Cisco that within 2021 the network device may uprise above 27.1 billion worldwide [3]. Because of the a tremendous growth of internet users, machines on a network generate terabytes of data every day and within a enterprises, one terabyte of data is easily generated daily.10 to 100 billions of events are generated in a day in large enterprises. Security-relevant data such as software application events, people's action events and network events make up to a size of terabytes which are regularly collected by the enterprises for forensic analysis. As the enterprise enable more event logging, employ more people, install multiple devices and softwares the data becomes huge. But, such huge data with variety of information becomes unmanageable. Conventional analytical tool that exists does not perform well with huge data and results in identification of more false positives. The problem becomes worse when the enterprise moves to cloud architecture.

Integrating security events from heterogeneous sources (such as firewalls, IDS and host log files) for better situational awareness is another major challenge. Slammer Worm is one of the well

May – June 2020
ISSN: 0193-4120 Page No. 205 - 216

executed network mass destruction and information takeover malware, where a Denial of Service attack (DoS) Bug was injected over Microsoft SQL server which disabled the database server by overload it. This bug is considered to be "one of the fastest computer worms in history" [4]. The infection rate of Slammer was more than 75000 computer system around the world within a period of 10 minutes. The vulnerability was not stopped in database access; it extended network outrage in cancellation of air flights, ATM failures etc. Another Distributed Denial of Service (DDos) based attack witnessed in 2016 [5] was Botnet attack, which exploited vulnerabilities among the IoT devices leading to unplanned downtimes in applications.

Intrusion in generally is explained as an act of intruding the resource availability [9].One solitary answer for dealing with these types of network attacks is by introducing a strong Intrusion detection System [6]. The detection of the network attack or computer attack using IDS is done by investigating the previous data records from the network process flow [7, 8]. IDS mainly focus on the sighting of illegal or malicious assaults on a computer system. IDS is generalized into two categories based on their behavioral model on assault detection as misuse detector and anomaly detector. Misuse detector symbolizes the detecting potential of known attack [10, 11]. Anomaly detector signifies the nature of irregularity over the user profile depending on the data and similarity measure. The utmost intention of the IDS is not only restricted to attack detection but also take some automatic remedial action over the network environment such as data logging, connection failure, system shutdown, ending process flow etc [12].). But differentiating anomalous network activity from normal network traffic is difficult and tedious. A human analyst must search through vast amounts of data to find anomalous sequences of network connections and the large data volume hampers ability to perform data mining experiments to gain necessary insights.Large-scale analytics for long-term for analyzing various network logs, events for detecting intrusion using conventional technologies do not serve well because of the following reasons,

- Keeping a backup of large amount of data is not feasible , thus data related to event logs will be deleted after fixed time period.
- Conventional technologies will not perform well when complex analytics on huge data having unstructured data and also noise.

The intention of this paper is to discuss the state-of-the-art methods for detecting intrusion and to stumble on a technique which can be well adopted for any Intrusion Detection System. The various existing research on IDS using various approaches are discussed, such as Clustering based approach, Machine learning based approach, Optimization algorithm based approach, Artificial neural network based approach, Deep learning based approach, Model based approach and Hybrid mock-up based approach.

II. Intrusion in Real Time Networks

This section provides an introduction about the intrusion in network and intrusion detection system. The behaviour of any system/unit which deviates from its normal course and results in some unexpected act is referred as intrusion. There are four stages in intrusion. They are [13]:

- **Probing stage:** Attack done over by exploiting the potential vulnerability of the target computer in any software or configuration means. One such type of intrusion is password cracking.
- **Exploitation Stage:** Stage with added advantage of probing stage. The exploited resource is used by the attacker to access any resources of the host as the administration privileges are obtained by the attackers by probing.
- **Mark Stage:** Stage which marks the information theft, resource mishandling or the attacker's goal is called the mark stage[14]. In most cases, they will plant a virus or spyware for further attacks increasing the accessibility.

May – June 2020
ISSN: 0193-4120 Page No. 205 - 216

- **Masquerding Stage:** Attack trace removal stage is called the masquerading stage [14]. Information revealing the truth about the attack will be removed by the intruder in this stage.

The three widely adopted network attacks are [15],

1) Denial of Service (DoS):

Request mishandling or denial is the general purpose of DoS types of attacks. DoS results in system crash which prevents the system functioning. As mentioned in [15], different types of DoS attacks are abuse legitimate features, Dismantle the stack of the machine packet reconstruction by malformed packets thereby tending a confused TCP/IP stack, or Make use of the distant listening host on to the same network.

2) User to Root (U2R):

These types of attacks are most common among the intruders who try to get the administration privilege of any operating system and software. As noted in [15], buffer overflow tendency crop up when a firmware tries to duplicate the data into the static buffer. The reason for the overflow is because of inappropriate condition consent over the existing data fitness function. This is considered as an effective intruding option in U2R type of attacks.

3) Remote to Local (R2L):

R2L behaviour has some similarity to U2R type of attack classes. Instead of the admin privilege intrusion, these attacks attempts to attain the local access across network host. The easy option for R2L is misconfiguration in security policies or with the help of any social engineering flow.

Intrusion detection in any form of networks such as wireless, mobile ad hoc, sensor networks etc is the focal point in recent years. The IDS attracts these network because of distributive nature and infrastructure [16,17] and also because of widespread vulnerability.

III. Intrusion in Real Time Networks

This section discusses the existing intrusion detection approaches available over the potential intrusion in the real time computer networks. Figure 1 depicts the taxonomy of the intrusion detection approaches considered in this literature. They are Clustering based approach, Optimization based approach, artificial neural network based approach, model based approach, hybrid mock-based approach, deep learning based approach and finally machine learning approach. The utmost intent of this literature is to find the best optimal choice of algorithm for IDS on any types of networks.

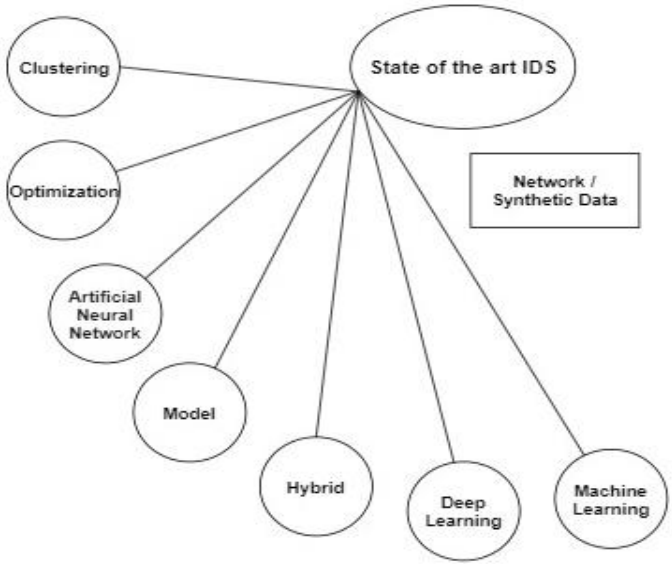

Figure ERROR! SWITCH ARGUMENT NOT SPECIFIED.**: Taxonomy of Intrusion Detection Approaches**

A. Clustering Based Approach

Clustering is one among the unsupervised learning algorithm. Some of the common benefits of the clustering based approach on IDS are i) Non compulsory data extraction or natural pattern streaming, ii) No need of impractical data labelling. The clustering based approaches overlayed on unsupervised learning algorithm are commonly found over existing anomaly detection system, which is reviewed in this section.

The clustering based approach centred on k-means, k-medoid, etc are listed out with and without labelled data [18-20] in this section. A revised

May – June 2020
ISSN: 0193-4120 Page No. 205 - 216

clustering based approach was presented in most the research papers published in 2018-2019. The cluster generation using end to end delay threshold values has been used in conjunction with anomaly search the research [18]. The detailed report on classification based IDS, Statistical IDS, clustering based IDS were disclosed. Additive information about the importance of the evaluation criteria and datasets were also revealed [18]. Authors based their research on intrusion attack such as Denial of service, User to Root, Remote to User on network data. They addressed the problems on types of anomalies, network mapping, etc.

K-medoid clustering algorithm based approach was used in the research for the detection of wireless sensor networks (WSN) anomalies such as blackhole and misdirection attacks [19]. They also granted a customizable option for further kind of anomaly detection. This was considered as one of the stable anomaly detection principles for wireless sensor networks based on clustering algorithm. Pure clustering algorithm, an under-sampling hierarchical model finds large pure cluster among the generated test and train set. The framework is found to be semi-supervised because of the divergence in the under sampling method over the dataset using k-mean algorithm. The problematic class imbalance in intrusion detection is tried to resolve in this research work using the pure clustering algorithm [20].

B. Model Based Approach

Model based approaches are the explicit state based classification approach. This type of approach assumes "successive observations are independent and that the probability of being in a given state at time t only depends on the state at time t-1" [21]. Model based approaches using Hidden Markov Model (HMM), behavioural model etc are reviewed in this section [22-25].

Behavioural model based on IP metrics is a key component for the success of IDS. In [22], researchers address a behaviour detection model of Internet hosting. The IP metric abstraction method is used to assess the traffic behaviour in this system. The suggestion has also streamed a behavioural habit analysis centred on abnormal behaviour detection. Clustering based characteristics construction algorithm is used for the anomaly detection. Distributed Denial of Service attack detection model is proposed as the accurate model depending on model based approach [23]. Some of the attributes which is given higher priority in this research are high attack detection accuracy and alleviation reaction. This model approach is ranked as the first attack detection framework with respect to security and programmable network. They tend to create a behaviour analysis model workflow as a part of anomaly detection. The solution for the detection of anomaly in network slice by a cooperative scheme has been implemented in the IDS [24] where Transfer learning approach for IDS is adopted. The HMM model is used in finding the intrusion by network map movement observation. Experimentation is performed over physical nodes with four different states. Hidden Markov Model incorporation on the transfer learning concept increased the cooperative anomaly detection possibility. The tolerance over the speed of transfer learning, better detection accuracy is achieved. In [25], authors present DNS-ADVP, a DNS Anomaly Detection Visual Platform, which gives a good visualization depicting the DNS traffic using a one-class classifier for detection of network traffic anomaly. The is implementation done by the feature vector selection considering the DNS behavior characteristic. Classification method, K-NN, is used because of dynamic nature of DNS traffic and the model continuously updated the normal behavior.

C. Optimization Algorithm Based Approach

In this section, the different types of the optimization algorithm based approaches are discussed. One of the significant challenge that has received much attention on anomaly detection for imbalanced data and is found increasing in recent years. Optimization algorithm is a class of nature

May – June 2020
ISSN: 0193-4120 Page No. 205 - 216

inspired algorithms which are used to attain real time classification problems.

In [26], a hybrid approach, ImGWO is presented as aid for IDS using optimization algorithm . A combined approach with machine learning for feature extraction and classification was the intent of this research. Grey Wolf optimization (GWO) algorithm was chosen for feature extraction as it is considered to be flexible for optimal results. Further, deep learning principle from CNN was utilized for the anomaly classification. In addition to the proposed combined model, efforts were also made to improve the basic characteristics of the GWO.

In advanced to the above GWO based approach, Text Based Intrusion detection system for cloud data security using modified artificial neural network (MANN) [27]. Authors have used the Neural network principle hybridizing with optimization algorithm for better intrusion detection results. Particle swarm optimization algorithm was chosen because of its flexibility over down sampling. Structuring details about the inner layer of ANN have been assumed precisely.

D. Artificial Neural Network Based Approach

In this section, a brief view on artificial neural network approach based IDS is deliberated. Artificial Neural Network (ANN) is best among other supervised learning algorithm because of its desirable properties such as self-learning capability of complex pattern, generalization of known patterns [28] etc. Most of the recent research papers on IDS are found to be using ANN approach because of its simplicity.

A multi-layer approach for IDS was proposed by Jiajun Lin et al in [29]. A network approach based on GoogleNetNP with multiple layers was utilized by the authors. The usage of the multiple layers on CNN yielded in reduction of false rate over the anomaly attack detection. Random Forest Classifier was also used over the output of the first layers to help in minimal trial over the existing data. In the same year 2019, Yong Zhang et al presented an approach named parallel cross convolutional neural network (PCCN) [30]. Authors have clearly provided a network intrusion detection system model for imbalance multi-class level. This work was the first of kind to use parallel neural network covering issues related multi class imbalance. Prior mismatch on CNN layers over existing system was overcome here by making use of the flow features from two layered CNN for IDS.

A relative approach using improved convolution neural network (ICNN) for outlier detection is presented in [31]. Wireless Network Traffic attack detection system via an improved version of convolution neural network has been addressed. Prior importance on data characterization was also achieved by optimal feature selection algorithm. Aggregation over the second layer convolution neural network gained better accuracy.

E. Deep Learning Based Approach

Instance Based Learning (IBL) techniques are employed by many researchers in intrusion detection and event correlation/fault management. This is because of the flexibility of deep learning approach compared to most of the expert systems, particularly for dynamic networks. The nominal drawbacks of expert systems listed out in the literature [32,33] are:

• Most of the expert system utilizes unbearable time for the execution and it is found difficult in perception of rule based knowledge extraction from data.

• Modification and calibration of the rule base seems tricky.

• Cannot detect slight variations of know attacks because of many specific rules.

Problems are solved based on previously solved instances/cases by Instance Based Learning techniques and, thus, does not require rule based amalgamation for the conclusion which is necessary in expert systems. Updating of the knowledge base of instances/cases is done automatically and the system will learn from its own experience during operation.

May – June 2020
ISSN: 0193-4120 Page No. 205 - 216

In [34], the problem related to ANN is presented. Deep learning Network is considered to be prime factor for intrusion detection by the authors. The principle of better feature abstraction results in better accuracy was utilized because of the poor modelling of the traditional learning methods. The better understanding on structuring the hidden layer of the DNN has been found effective. In [35], the use of deep and machine learning approaches have been reviewed on approach presented handling imbalance data. Techniques such as DNN, Random Forest, Voting, Stack classifiers etc are deliberated with explanation over CIDDS dataset. Mainly significant problem due to class imbalance distribution is highlighted.

Singular value decomposition (SVD) adaption for the IDS is the foremost intent of the approach presented by Jun et al [36] for high order data. Big data redundancy over small time data was successfully achieved in this method. Authors provided a pathway for the reduction in big data sampling optimal features which helps in IDS for any anomaly detection techniques. The comparison result over the existing methodologies also validated the performance. An Intrusion Detection System for Optical Network is offered by Boajia et al for data outlier monitoring [37]. The system models have the ability to learn it synchronously called as self-learn. The deep learning network architecture hybridizing supervised and unsupervised machine learning algorithms are combined. Their evaluation seems to provide less than 1% false positive on most of the network attack detection system. Authors call it self - taught because of the feature segregation.

F. Hybrid mock-up Based Approach

Deep learning approach is not as efficient as expert systems in performing event correlation [38]. The memory obligation of deep learning methods are high in bondage to store a large number of cases. Hybrid approaches are the clever approaches which are the amalgamation of classifiers so as to devise the result in IDS in perfect manner.

A cumulative approach for the detecting network attacks such as User to Root and Remote to Local on network data is addressed by Hamed et al as methodology in [39]. The problems in the dimensionality reduction and computational speed in the intrusion detection is answered in a method using two layer phenomena. The combined approach comprises of naïve bayes classifier, and k-nearest neighbour hybridized altogether. An outlier detector with the tagline “no prior knowledge of features” is the target of the author and named as compression analytics [40]. They utilized compression algorithms for the classification of anomaly as well as the detection of anomaly. They opted out one solution known as slice compression thereby characterizing the local behaviour of the network.

A proactive anomaly detector before failure is the slogan of network anomaly detection proposed by Shi Jin et al named CP(change point)-anomaly detector [41]. They employed a change point based outlier detector over the collected dataset with time as the base. The clustering algorithm is later implanted over the changepoint windows for the anomaly detection. The principle application of this research started from the real time dataset collection from a router. The false alarm rate of this research[41] founds to be too less over the traditional outlier detection approaches.

G. Machine Learning Based Approach

A range of machine learning algorithms have been benchmarked by many researchers, and it’s found that different classes of intrusions are better detected by different techniques. This is because of due to differences in methods. Creating classifier ensembles of different techniques has been shown to perform better than the individual classifiers. Although some researchers experience the instability of DTs as a drawback on data insensitiveness on training percentage [42], others exploit this as a beneficial trait to construct successful ensembles of DTs (classifier combination). The overall error rate

May – June 2020
ISSN: 0193-4120 Page No. 205 - 216

is significantly lower for all machine-learning methods compared with the other techniques.

A combined machine learning approach for the intrusion detection on network data was deliberated in [43]. Primary aspect of attack classification and feature mapping over the network dataset are discussed in this method. The limitations in most of the existing deep learning algorithm were also depicted with their solution in regard to feature set by them. Five Team advance using conventional machine learning methods such as K-nearest neighbor, Support Vector machine, Naïve Bayes, Random Forest and Decision tree classifier for intrusion detection have been conversed against the proposed Fully Connected Neural Network (FCNN), Convolutional Neural Network (CNN) and Long Short Term Memory (LSTM) methods by Jonghoon et al in [44]. Adaptive learning is proved for the machine learning models in their study.

An approach for the Distributed Network Intrusion Detection System is presented by Ying et al in [45] for vehicular adhoc network. The challenges on DDOS network attack of big data on VANET is considered by the authors. Apache spark is used by the authors for computing advantage in data pre-processing. The attack classification is done using Random Forest classifier. Upon considering IDS, equal importance was given for the data collection module. Most of the micro-batch processing on network data was performed as micro services using spark. A multi-framework design utilizing meta classifier approach combining random forest classifier and bagging model have been proposed in a method as a solution for nominal ensemble learner based IDS [46]. Accurate assumption is made on the feature selection interconnecting multi-feature selection paradigm. One class support vector based machine learning streaming is used as the crucial tool for the anomaly detection by Xuedan et al in [47]. More resemblance on conventional SVM was replaced with a random approximate function in this method. The performance evaluation on synthetic and real datasets is done which improved the quality of IDS. The authors in [48] tried to imitate the flow of engineering concept with the machine learning algorithms for the detection of DDos attacks. They maintained a proportional approach for the anomaly detection procedure over k-means, svm classifier etc. The results from this study concluded in the fact that steps inclined on the feature extraction will increase the DDoS detection speed. The dimensionality of the dataset was taken in account for measuring the credibility of the system.

IV. Approach Evaluation

The evaluation of the existing approaches considered in this paper is discussed in this section. Table 1 depicts the evaluation tabulation listing the cumulative accuracy and false alarm rate of the different approaches used for IDS techniques.

Table 1: Evaluation of Existing Approaches

SNo	Approaches	Cumulative Accuracy	Cumulative False Alarm Rate
1	Clustering	<90%	9%
2	Model	<89%	9%
3	Optimization	<93%	5%
4	Hybrid mock-up	>90%	9%
5	Artificial Neural Network	<93%	7%
6	Deep Learning	<95%	7%
7	Machine Learning	>99%	2%

V. Shortcomings

In this section, the shortcomings of the approaches considered in this literature on IDS are discussed [27-48]. Substantial support over network level attack was given more priority on most of the intrusion detection techniques using clustering approach. Moreover, manipulation detection on the behaviour of the network seems difficult in this kind of clustering based approach because of the multi class probability function. Augmented data reality for IDS was left unreciprocated. Empirical relation

May – June 2020
ISSN: 0193-4120 Page No. 205 - 216

for the clustering transformation in regards to the choice of the hyper parameter is left open. Retraining issue related to cyber security application was also left myriad in most of the reviewed literature in section III.A.

In model based approaches, the limitation for the abnormality behaviour on single network is found high. Most of the research left the scope for the detection in multiple networks. Evaluation on synthetic datasets resulted in middling. Inherent complexity on combining optimization algorithm and deep learning was also considered tedious. Effort for reducing the computational power and memory was not preserved in ANN approach. Timing for the anomaly detection was found to be pricey. Feature extraction for the CNN was not found that much effective.

Fuzzy situation over the dimension reduction of dataset is left unexplored in most of the hybrid approaches which resulted in ineffective accuracy. Performance evaluation of deep learning approach doesn't conclude in the reproducibility of the learning algorithms in intrusion detection. Moreover, low frequency attacks are untouched on the working scenario. Loss function on optimal feature selection algorithm resulted in fuzzy situation over feature selection.

When comes to machine learning approaches, the class balancer issues in Random Forest classifier were not discussed. Furthermore, down sampling problems were also left. Strong supports for security attacks were deliberated indulging other types of network attacks. The performance excellence was left open for other machine learning techniques to get acquainted.

Even though machine learning was addressed neatly for IDS its possibility for threat prediction on multiple networks were not addressed. Problems related to data labelling for training was unnoticed. Feature extraction processing was not found compatible for synthetically generated datasets. The deployment was only successful on processed dataset. In most possible IDS, attacks associated with the traffic flow were not estimated. Only concern was given for DDoS attack among different attack categories.

Large scale evaluation was performed mostly on the synthetic datasets. Multi class and Imbalance problem related issues are left void. The speed of anomaly detection depends on the swiftness of the training data and the learning process.. The delays for feature selection also have considerable impact on the AUC(area under curve) of the results. Performance over the normalized data was not achieved in most of the literatures. Security over information breach in data reduction was upheld as the future work in most of the literatures, which serves a negative impact for the usage. Solving course of action for multi-class problem was not resolved in most of the literatures. Result concerned on theoretical accuracy, specificity, and precision metric were given more priority.

VI. Evolving Machine Learning

In this section, the evolving machine learning approach with better evaluation is discussed with its importance over IDS. The main motivation for machine learning combination is stated by [49]

Three specific reasons why machine learning based IDS classifier combinations can be beneficial:

1. Numerical Theory based workout: Most of the prediction algorithms relies on the training data to model the detection space with the help of one classifier, the same can be amplified to a better level by the combined knowledge of an ensemble of classifiers may reach more accurate predictions.
2. Algorithm workout: Most of the prediction algorithms can befall in optimal problem and it may be divisively exclusive to find the global optimum. Instead, local search algorithms of machine learning can be employed to form different starting points by combining local optima.
3. Representational: the optimal classifier may not be found, because the technique is incapable of

May – June 2020
ISSN: 0193-4120 Page No. 205 - 216

finding the fitness function for true problem of the anomaly detection.

VII. Conclusion

IDS are system unit which helps in finding the intrusion that exploits the application vulnerability and detecting network level attacks. The evaluation of any type of IDS can be performed using accuracy, and false positive rate. This literature attempted to perform a cumulative survey of different types of approaches and algorithms available on existing IDS. Many relational factors such as feature selection, imbalance problem, multi class probability are left open in most of the existing approaches. Machine learning approaches give the impression to be helpful for analysing any network traffic, virus signatures, behaviours, profiles, incidents etc. The conclusion on selection of machine learning algorithm confined considering dataset selection, accuracy, and false positive rate. One big challenge in existing machine learning approaches is feasibility in handling huge data. In future, attempts can be made on machine learning based IDS approaches incorporating tensorflow, apache spark etc for better processing and evaluation.

References

1. (2019) Internet World Stats World Internet Users Statistics website [Online] https://www.internetworldstats.com/stats.htm
2. (2019) A. Popular Internet of Things Forecast of 50 Billion Devices. [Online] https://spectrum.ieee.org/tech-talk/telecom/internet/popular-internet-of-things-forecast-of-50-billion-devices-by-2020-is-outdated
3. (2017) Cisco Cisco Visual Networking Index: Forecast and Trends. [Online] https://www.cisco.com/c/en/us/solutions/collateral/service-provider/visual-networking-index-vni/white-paper-c11-741490.html
4. D. Moore, V. Paxson, S. Savage, C. Shannon, S. Staniford and N., Weaver, "Inside the Slammer Worm", IEEE Security and Privacy, Vol. 1, pp. 33–39, 2003.
5. (2019) What We Know About Friday's Massive East Coast Internet Outage [Online] https://www.wired.com/2016/10/internet-outage-ddos-dns-dyn/
6. Anderson, J. P., "*Computer security threat monitoring and surveillance*," Technical Report, Fort Washington, PA, USA, 1980.
7. Endorf. C, Schultz, E., & Mellander, J., "*Intrusion detection and prevention*", California: McGraw-Hill, 2004.
8. Heady R., Luger G., Maccabe A., and Servilla M., "*The architecture of a Network level intrusion detection system*", Technical Report, CS90-20, Dept. of Computer Science, University of New Mexico, Albuquerque, NM 87131,1990.
9. Denning D. "*An Intrusion-Detection Model*," IEEE Transactions on Software Engineering, Vol. SE-13, No. 2, pp.222-232, 1987.
10. Kumar S., Spafford E. H. "*An Application of Pattern Matching in Intrusion Detection*," Technical Report CSD-TR-94-013. Purdue University, 1994.
11. Ryan J., Lin M-J., Miikkulainen R, "*Intrusion Detection with Neural Networks*," Advances in Neural Information Processing Systems, Vol. 10, and Cambridge, MA: MIT Press, 1998.
12. Terran lane, Carla E. Brodley, "*Temporal Sequence Learning and Data Reduction for anomaly Detection*," Vol. 2, No. 3, pp. 295-331,August 1999.
13. M. Asaka, A. Taguchi and S. Goto, *"The Implementation of IDA: An Intrusion Detection Agent System.",* In Proceedings of the 11th Annual FIRST Conference on Computer Security Incident Handling and Response (FIRST'99), 1999.
14. C. Kruegel, F. Valeur and G. Vigna, "*Intrusion Detection and Correlation"*, ser. Advances in Information Security. US:Springer-Verlag , Vol. 14, 2005.

May – June 2020
ISSN: 0193-4120 Page No. 205 - 216

15. K. Kendall, "A Database of Computer Attacks for the Evaluation of Intrusion Detection Systems" Master's thesis, Massachusetts Institute of Technology, 1999.
16. Y. Zhang and W. Lee, "Intrusion detection in wireless ad-hoc networks," in *MobiCom '00: Proceedings of the 6th annual international conference on Mobile computing and networking*, New York, NY, USA, pp. 275–283, 2000.
17. S. Zhicai, J. Zhenzhou and H. Mingzeng, "A Novel Distributed Intrusion Detection Model Based on Mobile Agent," in *Proceedings of the International Conference on Information Security*, Shanghai, China, 2004.
18. Mohiuddin Ahmed, Abdun Naser Mahmood, Jiankun Hu, "A survey of network anomaly detection techniques", *Journal of Network and Computer Applications*, Vol. 60, pp. 19-31, 2016.
19. Bilal Ahmad, Wang Jian, Zain Anwar Ali, Sania Tanvir, M. Sadiq Ali Khan, "Hybrid Anomaly Detection by Using Clustering for Wireless Sensor Network", *Wireless Personal Communications*, Vol. 106, pp. 1841–1853, Jun 2019.
20. Haipeng Yao, Danyang Fu, Peiying Zhang, Maozhen Li, Yunjie Liu, "MSML: A Novel Multi-level Semi-supervised Machine Learning Framework for Intrusion Detection System", *IEEE Internet of Things Journal*, Vol . 6 , 2019.
21. K. Lee, J. Kim, K.H. Kwon, Y. Han and S. Kim, "DDoS attack detection method using cluster analysis", in *Expert Systems with Applications*, Vol . 34, pp 1659–1665, 2008.
22. Xiaodong Zang, Jian Gong, Siyi Huang, Xiaoyan Hu and Yun Yang, "IP backbone traffic behavior characteristic spectrum composing and role mining", *CCF Transactions on Networking*, Vol. 2, pp. 153–171, 2019.
23. Prabhakar Krishnan, Subhasri Duttagupta, Krishnashree Achuthan, "SDNFV Based Threat Monitoring and Security Framework for Multi-Access Edge Computing Infrastructure", *Mobile Networks and Applications*, Vol . 24, pp 1896–1923, 2019.
24. Weili Wang, Qianbin Chen, Xiaoqiang He, Lun Tang, "Cooperative Anomaly Detection with Transfer Learning based Hidden Markov Model in Virtualized Network Slicing", *IEEE Communications Letters*,Vol. 23, Sept 2019.
25. Luis A. Trejo, Victor Ferman, Miguel Angel Medina-Perez, Fernando Miguel Arredondo Giacinti, Raul Monroy, Jose E. Ramirez-Marquez, "DNS-ADVP: A Machine Learning Anomaly Detection and Visual Platform to Protect Top-Level Domain Name Servers Against DDoS Attacks", *IEEE Access* , Vol. 7, pp. 116358 - 116369, 2019.
26. Sahil Garg, Kuljeet Kaur, Neeraj Kumar, Georges Kaddoum, Albert Y. Zomaya, Rajiv Ranjan, "A Hybrid Deep Learning-Based Model for Anomaly Detection in Cloud Datacenter Networks", *IEEE Transactions on Network and Service Management*, Vol. 16, pp. 924-935, Sept 2019.
27. J. Anitha Ruth, H. Sirmathi, A. Meenakshi, "Secure data storage and intrusion detection in the cloud using MANN and dual encryption through various attacks", *IET Information Security*, Vol. 13, pp. 321-329, 2019.
28. S. Haykin, "*Neural Networks: A Comprehensive Foundation*", 2nd edition, Prentice Hall PTR Upper Saddle River, NJ, USA, 1998.
29. X Zhang, J Chen, Y Zhou, L Han, J Lin , "A Multiple-Layer Representation Learning Model for Network-Based Attack Detection", *IEEE Access* , Vol. 7, pp. 91992 - 92008, 2019.
30. Yong Zhang, Xu Chen, Da Guo, Mei Song, Yinglei Teng, Xiaojuan Wang, "PCCN: Parallel Cross Convolutional Neural Network for Abnormal Network Traffic Flows Detection in Multi-Class Imbalanced Network Traffic Flows", *IEEE Access* , Vol. 7, pp. 119904 - 119916, 2019.

May – June 2020
ISSN: 0193-4120 Page No. 205 - 216

31. H Yang, F Wang, "Wireless Network Intrusion Detection Based on Improved Convolutional Neural Network", *IEEE Access* , Vol. 7, pp. 64366 - 64374, 2019.
32. M. Esmaili, B. Balachandran, R. Safavi-Naini and J. Pieprzyk, "Case-Based Reasoning for Intrusion Detection", in *ACSAC '96: Proceedings of the 12th Annual Computer Security Applications Conference*, p. 214, Washington, DC, USA, 1996.
33. G. Jakobson, J. Buford and L. Lewis. "Towards and Architecture for Reasoning About Complex EventBased Dynamic Systems", in *Proceedings of the 3rd International Workshop on Distributed Event Based Systems*, 2004.
34. Y Jia, M Wang, Y Wang, "Network intrusion detection algorithm based on deep neural network", *IET Information Security*, vol 13, pp. 48 – 53, 2019.
35. Razan Abdulhammed, Miad Faezipour, Abdelshakour Abuzneid, Arafat AbuMallouh, "Deep and Machine Learning Approaches for Anomaly-Based Intrusion Detection of Imbalanced Network Traffic", *IEEE Sensors Letters*, Vol 3, Jan. 2019.
36. Jun Feng, Laurence T. Yang, Guohui Dai, Wei Wang, Deqing Zou , "A Secure High-Order Lanczos-Based Orthogonal Tensor SVD for Big Data Reduction in Cloud Environment", *IEEE Transactions on Big Data*, Vol. 5, pp. 355-367, Sept. 2019.
37. Xiaoliang Chen, Baojia Li, Roberto Proietti, Zuqing Zhu, S. J. Ben Yoo, "Self-Taught Anomaly Detection With Hybrid Unsupervised/Supervised Machine Learning in Optical Networks", *Journal of Lightwave Technology*, Vol 37, pp. 1742 - 1749, 2019.
38. A. Hanemann. "A Hybrid Rule-Based/Case-Based Reasoning Approach for Service Fault Diagnosis", in *Proceedings of the 2006 International Symposium on Frontiers in Networking with Applications*, Vienna, Austria, 2006.
39. Hamed Haddad Pajouh, Reza Javidan, Raouf Khayami, Ali Dehghantanha, Kim-Kwang Raymond Choo, "A Two-Layer Dimension Reduction and Two-Tier Classification Model for Anomaly-Based Intrusion Detection in IoT Backbone Networks", *IEEE Transactions on Emerging Topics in Computing*, Vol 7 , pp. 314-323 , 2019.
40. C Ting, R Field, A Fisher, T Bauer, "Compression Analytics for Classification and Anomaly Detection Within Network Communication", *IEEE Transactions on Information Forensics and Security*, Vol 14 , pp. 1366-1376, May 2019.
41. Shi Jin, Zhaobo Zhang, Krishnendu Chakrabarty, Xinli Gu, "Changepoint-Based Anomaly Detection for Prognostic Diagnosis in a Core Router System", *IEEE Transactions on Computer-Aided Design of Integrated Circuits and Systems*, Vol 38, pp. 1331-1344, 2019.
42. S. Peddabachigari, A. Abraham, C. Grosan and J. Thomas, "Modeling Intrusion Detection Systems Using Hybrid Intelligent Systems", *Journal of Network and Computer Applications*, Vol. 30, pp.114–132, 2007.
43. Preeti Mishra, Vijay Varadharajan, Uday Tupakula, Emmanuel S. Pilli, "A Detailed Investigation and Analysis of Using Machine Learning Techniques for Intrusion Detection", *IEEE Communications Surveys &Tutorials*, Vol 21 , pp. 686-728, 2019.
44. J Lee, J Kim, I Kim, K Han, "Cyber Threat Detection Based on Artificial Neural Networks Using Event Profiles", *IEEE Access*, Vol 7, pp. 165607-165626, 2019.
45. Ying Gao, Hongrui Wu, Binjie Song, Yaqia Jin, Xiongwen Luo, Xing Zeng, "A Distributed Network Intrusion Detection System for Distributed Denial of Service Attacks in Vehicular Ad Hoc Network", *IEEE Access*, Vol. 7, pp. 154560 - 154571, 2019.
46. BA Tama, M Comuzzi, KH Rhee, "TSE-IDS: A Two-Stage Classifier Ensemble for Intelligent

May – June 2020
ISSN: 0193-4120 Page No. 205 - 216

Anomaly-Based Intrusion Detection System", *IEEE Access*, Vol. 7, pp. 94497 - 94507, 2019.

47. X Miao, Y Liu, H Zhao, C Li, "Distributed Online One-Class Support Vector Machine for Anomaly Detection Over Networks", *IEEE Transactions on Cybernetics*, Vol 49, pp. 1475-1488, 2019.
48. M Aamir, SMA Zaidi, "DDoS attack detection with feature engineering and machine learning: the framework and performance evaluation", *International Journal of Information Security*, Vol. 18, pp. 761–785, 2019.
49. L.I. Kuncheva and C.J. Whitaker, "Measures of Diversity in Classifier Ensembles and Their Relationship with the Ensemble Accuracy", *Machine Learning*, Vol. 51, pp. 181–207, 2003.