IJCSE International Journal of Computer Sciences and Engineering Open Access
Research Paper Vol.-7, Issue-4, April 2019 E-ISSN: 2347-2693

Network Intrusion Detection System using Threat Intelligence and Deep Learning Approach

Kushal Jani[1*] , Punit Lalwani [2] , Deepak Upadhyay [3] and M. B. Potdar [4]

[1,3]M.E Student, GTU Cyber Security, Graduate School of Engineering & Technology
Gandhinagar 382028, Gujarat, India
[2,4]Bhaskaracharya Institute for Space Applications and Geo-Informatics, Gandhinagar 382007, India

Corresponding Author : kushaljani1990@gmail.com

DOI: https://doi.org/10.26438/ijcse/v7i4.526531 | Available online at: www.ijcseonline.org

Accepted: 18/Apr/2019, Published: 30/Apr/2019

Abstract— Network Intrusion Detection System (NIDS) is one of the best solutions against network attacks. Attackers also dynamically change tools and technologies. Powerful network security analytics is not a function of making use of simply one approach. To detect emerging threats, a network intrusion detection system should be able to use a mixture of techniques. In this research we start off evolved via collecting the proper information for complete visibility and the usage of analytical strategies along with behavioral modeling and deep learning. All that is supplemented by means of global threat intelligence that is aware about the malicious campaigns and maps the suspicious conduct to a recognized threat for extended fidelity of detection. In this research we prepare multichannel deep learning approach and incremental learning approach to enhance detection rate.

***Keywords* —** Network Intrusion Detection System, Network Security, Deep Learning, Threat Intelligence, Performance Evolution.

I. INTRODUCTION

One of the primary issues nowadays for organisation networks is safety. Many reputed organization networks and internet based offerings have been down with several attacks by the hackers. To guard the network infrastructure and internet through conversation, several strategies have been developed. The usage of firewalls, cryptography and VPN (virtual private networks) are some of them [15]. Identify intruders is a completely new phenomena to such techniques. IDS techniques can be used to acquire the facts from regarded assaults and discover if attacker tries to attack host or network. This approach can be used to reinforce the network security. To guard from numerous attacks, protection system can be set of tools [23], together with: 1) Firewalls to stop malicious traffic of network. 2) IDS to discover unauthorized activity to get into the machine or community. 3) Vulnerability evaluation equipment to locate security breaches in the network [24]. Information gathered from these tools is used to outline regulations on firewalls to thwart protection breaches from intruders.

IDS heavily use machine learning techniques now a days [7].Most of machine learning technique comes under shallow learning, they are not able to solve large data classification problems which create problem to identify network intrusion in real network traffic. Traditional Machine Learning algorithms are not that much efficient and effective. Shallow learning is not suitable for intelligent systems and high dimensional learning with large datasets.

In comparison, deep learners have ability to extract higher representations from the data set to create a lot better models. As a result, intrusion detection technology has experienced fast improvement after falling into an enormously slow duration. In this research we proposed deep learning base model [9]. Deep learning achieves excessive degree of abstractions from data via the use of a complicated structure or composition of non-linear variations. Consequently, we are able to accumulate an excessive detection rate. We train the model through the use of NSL-KDD dataset and measure the overall performance [5].

Threat intelligence referred as cyber threat intelligence (CTI), is analyzed, organized and refine information about crucial attacks that impact organization [16]. The main goal of threat intelligence is provide information to organization to understand risk and impact of common and extreme level of cyber threat, some threat intelligence also provide resistance against zero day attack, APTs (advance persistence threat) and exploits. Here threat indicator is insider threat as well as partial indication of main threat as well, the importance of threat feeds is identify kind of attacks or threats impact most in organization [10]. Threat intelligence provide depth knowledge about threat to help organization to protect itself from different type of attacks that can do most damage.

The rest of the paper is organized as follows: Segment 2 of this paper describes Literature Review. Segment 3 discusses about Deep Learning Segment 4 explain basics about Threat Intelligence. Segment 5 discusses proposed network intrusion detection system with deep learning and threat intelligence. Segment 6 discusses performance measures and experimental results of proposed model. Conclusion and future work are drawn in segment 7.

II. LITERATURE REVIEW

A survey regarding network anomaly detection methodology is given in [15]. Different Machine Learning Techniques for Intrusion Detection and its Comparative Analysis is given in [3].Adaptive Hybrid method for Network Intrusion Detection and Comparison among Machine Learning Algorithms is mentioned in [14].Authors in [1] describe Evaluation of Machine Learning Techniques [17] for Network Intrusion Detection. Network threats detection system using fuzzy logic explained in [8].Authors in [10] have explained Classification of Attack Types for Intrusion Detection Systems using a Machine Learning Algorithm. A Survey of Data Mining and Machine Learning Methods for Cyber Security Intrusion Detection explained in [6]. In [5] A Study on NSL-KDD Dataset for Intrusion Detection System Based on Classification Algorithms was evaluated. Performance Evaluation of Supervised Machine Learning Algorithms for Intrusion Detection is done in [7]. Network Intrusion Detection has different Classifiers, comparisons of them explain in this paper [2]. Deep Learning based Multi-channel intelligent attack detection for Data Security and a deep learning approach to network intrusion detection explained in [9], [13], [24].Threat intelligence and its implementation explain in [16],[20],[25].

III. DEEP LEARNING

Despite the significant advances in NIDS technology, the majority of solutions still operate using less-capable signature-based techniques, as opposed to anomaly detection techniques. Regardless of the extensive advances in NIDS generation, the majority of solutions still perform using much less-successful signature-based strategies, rather than anomaly detection strategies [3]. There are several motives for this reluctance to exchange, including the high false error rate (and associated expenses), difficulty in acquiring dependable training data durability of training facts and behavioural dynamics of the device. They're worried with three primary limitations, which make a contribution to this network safety challenge. 1) Volume of network data 2) In-depth monitoring 3) distinct protocols and the variety of data [9]. A research vicinity currently receiving tremendous interest throughout multiple domain names is that of deep learning. That is an advanced subset of machine learning, which can conquer some of the constraints of shallow learning.

Deep learning approach is enhanced version of neural network architectures, because of that deep learning referred as deep neural networks. Term deep used as number of hidden layer in neural networks. Deep learning provide facility of prepare model of complicated relationships and ideas using multiple levels of data representation [13].Following are the neural network with are part of Deep Learning.

IV. THREAT INTELLIGENCE

Threat intelligence solutions collect raw information about rising or present threat actors and threats from some of resources [20]. This data is analyzed and filtered to produce threat intelligence feeds and control reviews that incorporate data that can be used by automated security manage solutions. The primary goal of this kind of protection is to maintain corporation knowledgeable of the dangers of advanced persistent threats, zero-day threats and exploits, and how to shield towards them [16]. While carried out nicely, threat intelligence can assist to reap the following targets, ensure you stay updated with the often overwhelming volume of threats, which includes techniques, vulnerabilities, objectives and bad actors. Help you turn out to be more proactive about future cybersecurity threats [1]. Keep leaders, stakeholders and customers informed about the modern-day threats and repercussions they might have at the commercial enterprise.

A threat intelligence feed (TI feed) is an ongoing movement of information associated with potential or current threats to an organization's security [25].Examples are Alienvault, Exploitalert, Infosec, Emerging Threats IDS Rules.

V. PROPOSED NIDS WITH DEEP LEARNING AND THREAT INTELLIGENCE

The growing complexity inside the organization network has created many blind spots. These days, employees are connecting to the network from many locations and from a couple of devices. The variety of smart system having access to the network and the use of public cloud services keep growing.

To detect and respond to advanced threats, we combine three techniques

1) Behavioural Modelling
2) Deep Learning
3) Threat Intelligence

Due to the fact attackers aren't using just one technique to breach your network, proposed model employs more than one analytical strategies to detect threats early and enables ensure that the eviction is complete.

Behavioral modeling

Machine intently monitors the activity of every system at the network and is able to create a baseline of normal traffic. In addition, it also has a deep expertise of recognized anomaly traffic. It applies near 100 distinct security events or behaviours that examine diverse types of traffic, including brute force login, scanning, suspect data loss, beaconing host, suspect data hoarding, etc. Further this security events differentiate to logical alarm categories. Certain security events generate alarm on their own. So the system is capable of correlate more than one, isolated anomalous incidents and piece all of them together to determine what sort of attack might be in play, and also tie it to a selected tool and user .The incident can be analysed by the time and associated sequence of events. This is best way to identify incident cause. Physicians inspecting affected person don't examine a symptom in isolation to figure out what's wrong. They examine overall condition of patient to provide diagnosis. Similarly, system records each anomalous activity within the network and looks at it holistically to generate contextual alarms that may assist safety teams prioritize risks.

Apply Deep Learning

Methodology which is proposed in this paper applies deep learning technique to identify latest threat and malicious traffic. It merge with cloud base multistage deep learning analysis in which it checks each threat behaviour globally that present in enterprise/organization. System examine user and device behaviour to identify malware signature, CNC communication, unwanted application and data exfiltration in organization environment. There are multiple stage of processing, in which aggregation of strategies from artificial intelligence, deep learning and mathematical data enables the network to self-learn its normal traffic so it is aware of malicious transactions.

This capability is critical due to the fact that organization might also get lots of indicators day by day, and it's now not feasible for resource-strapped security groups to analyze all those indicators. With machine learning and deep learning system process large amount of data with in fraction of time, which help to identify critical incidents in real time with high accuracy and is also help to suggest action plan against the incidents.

In proposed model, to get desire accuracy we are going to implement multichannel training algorithm. In this we select best three deep learning algorithms among various algorithms (Neural Networks). We train our model with these three neural network and compare their results. Output of our proposed algorithm will be decided by voting of the results generated by neural networks. This will give high accuracy and less false positive and negative.

Threat Intelligence

One of the biggest advantage of attacker is that they can apply same attack to multiple targets, and they also successful because of the system have not latest threat definition that have only local view of threats. But what if local system have all information about malicious proxy IP, and new signature of malware that is just introduce and give alert to global threat intelligence? By doing this system would easily identify threats, save time to detect new threats and increase its detection ratio.

Effective network intrusion detection system is not rely on single technique. To detect latest advance persistent threats, system should stay ahead with solution which apply combination of techniques. This starts via gathering the proper statistics for comprehensive visibility and the use of analytical strategies including behavioural modelling and deep learning. All this is boost by Global Threat Intelligence that is aware of malicious movement and map its behaviour to recognized threats to increase detection rate. Proposed system apply every techniques that are discussed above to help organizations to identify and prevent attacks.

To enhance our model capability we will implement incremental learning approach. Proposed model takes input from threat intelligence everyday. It converts into standard CSV format then CSV file is merged with seed dataset. By doing this, model gets all updated information every day that include new threat definitions. This approach enhance our model detection capability of new upcoming threats.

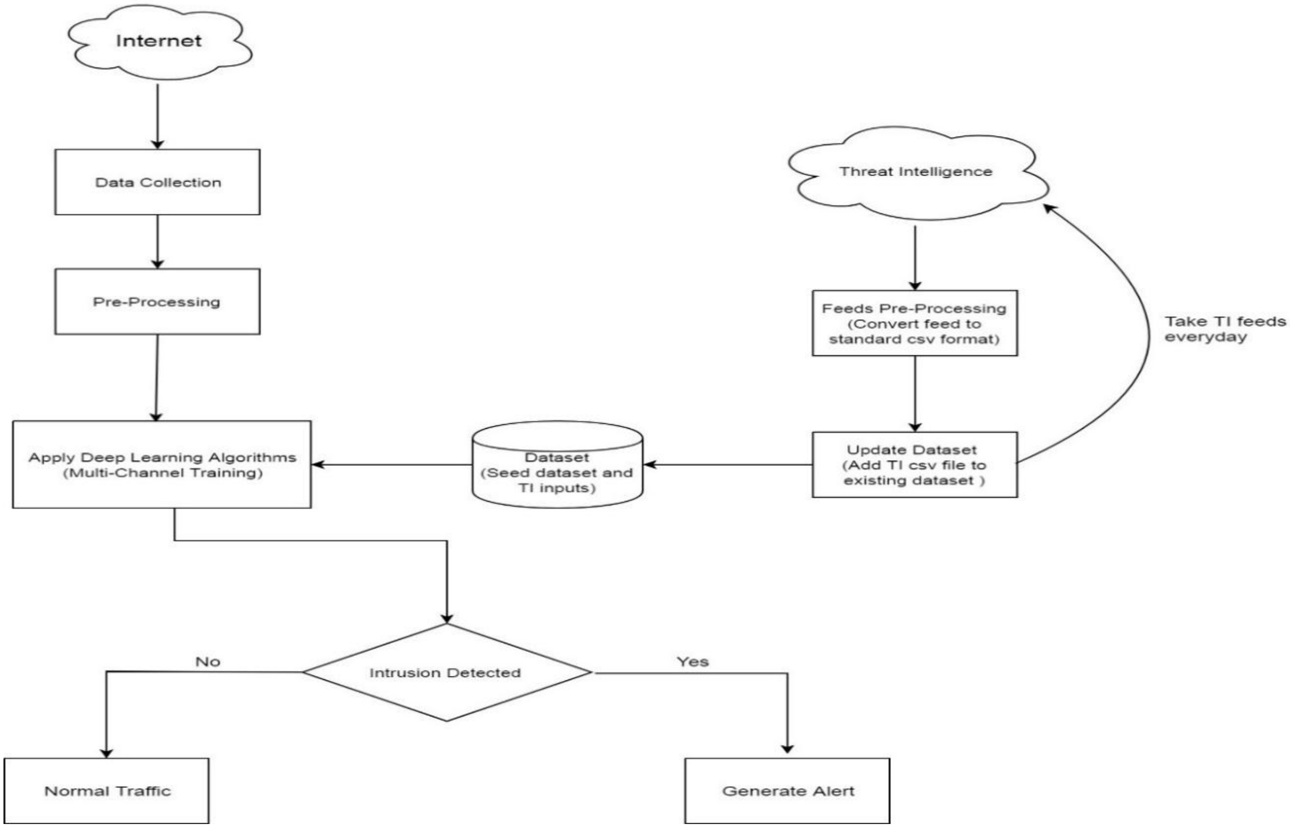
Internet
Data Collection
Pre-Processing
Apply Deep Learning Algorithms (Multi-Channel Training)
Dataset (Seed dataset and TI inputs)
Threat Intelligence
Feeds Pre-Processing (Convert feed to standard csv format)
Take TI feeds everyday
Update Dataset (Add TI csv file to existing dataset)
Intrusion Detected
No
Yes
Normal Traffic
Generate Alert

Figure 1 - Proposed Network Intrusion Detection System

VI. PERFORMANCE MEASURES AND EXPERIMENTAL RESULTS

Evaluation Metrics

Using evaluation indicator we can evaluate performance, which is important to compare performance among numerous techniques or different datasets [10]. Accuracy is main parameter to evaluate performance of Network intrusion detection system. In this research we consider three evolution parameter which is describe bellow [10].

Accuracy defines the percentage of the total quantity of accurate classifications.

Accuracy = TP + TN / TP + TN + FP + FN

Precision defines the total quantity of data appropriately predicted positive(anomaly) data over the number of instance predicted as positive(anomaly).

Precision = TP / TP + FP

Recall defines the percentage of appropriately predicted positive(anomaly) data out of the number of actual positive(anomaly)data[10]

$Recall$= TP / TP + FN

Experimental Results

It is clearly observed that the Deep Learning Algorithms achieve the highest accuracy. Now, as per proposed work we will develop different deep learning algorithms to find out which technique will give the highest accuracy , precision , recall and less response time. We develop number of neural networks namely Deep Neural Network, Deep Belief Network, Convolutional Neural Network, Restricted Boltzmann machine, Stacked Autoencoder.

To implement incremental approach as describe in proposed work, Algorithm takes input from threat intelligence (alienvault) and prepare CSV file. This CSV file will be merged with seed dataset (NSL_KDD), then updated dataset is used to train model. Model takes input from threat intelligence everyday. Following are the attributes of NSL-KDD. Below figure 6.14 shows merged file of TI feed and seed dataset.

In proposed model to get desire accuracy we are going to implement multichannel training algorithm. In this we have selected Deep Neural Network, Deep Belief Network, and Convolutional Neural Network. We train our model with these three neural network and compare their results. Output of our proposed algorithm will be decided by voting of the results generated by neural networks. This will give high accuracy and less false positive and negative.

Now, the comparison of existing five algorithm and proposed algorithm is given below.

Table 1–Comparison of existing neural networks with proposed neural network

	Precision (%)	Recall (%)	Accuracy (%)
Deep Neural Network	91.76	91.76	93.6
Deep Belief Network	92.30	91.03	93.6
Convolutional Neural Network	89.75	90.32	92.2
Restricted Boltzmann machine	90.65	71.45	84.8
Stacked Autoencoder	86.33	85.61	89.2
Proposed Algorithm	95.43	96.46	94.0

VII. CONCLUSION AND FUTURE WORK

To perceive network intrusion we introduce a methodology which use of deep learning with multichannel approach and threat intelligence with incremental model. Deep learning strategies are famous for its capability to deal with large-scale statistics in recent times and overall performance of intrusion detection. There are numerous threat intelligence resources present which provide lists or APIs for gaining updated information about latest threats. Ex - alienvault, Exploitalert, ZeuS Tracker etc. Integrating deep learning with threat intelligence we will obtain incredibly high accurate system with less false positive/negative alerts. In future work, we will evaluate performance of developed algorithm with different dataset and threat intelligence feeds.

ACKNOWLEDGMENTS

We are thankful to Shri T. P. Singh, Director, and BISAG for providing us infrastructure, motivation, and permitting to carry out this project at BISAG.

REFERENCES

[1] Almseidin, Mohammad, et al. "Evaluation of machine learning algorithms for intrusion detection system." *Intelligent Systems and Informatics (SISY), 2017 IEEE 15th International Symposium on*. IEEE, 2017.

[2] Choudhury, Sumouli, and AnirbanBhowal. "Comparative analysis of machine learning algorithms along with classifiers for network intrusion detection." *Smart technologies and management for computing, communication, controls, energy and materials (ICSTM), 2015 International conference on*. IEEE, 2015.

[3] Hamid, Yasir, M. Sugumaran, and LudovicJournaux. "Machine learning techniques for intrusion detection: a comparative analysis." *Proceedings of the International Conference on Informatics and Analytics*. ACM, 2016.

[4] Haq, Nutan Farah, et al. "Application of machine learning approaches in intrusion detection system: a survey." *IJARAI-International Journal of Advanced Research in Artificial Intelligence* 4.3 (2015): 9-18.

[5] Dhanabal, L., and S. P. Shantharajah. "A study on NSL-KDD dataset for intrusion detection system based on classification algorithms." *International Journal of Advanced Research in Computer and Communication Engineering* 4.6 (2015): 446-452.

[6] Buczak, Anna L., and ErhanGuven. "A survey of data mining and machine learning methods for cyber security intrusion detection." *IEEE Communications Surveys & Tutorials* 18.2 (2016): 1153-1176.

[7] Belavagi, Manjula C., and BalachandraMuniyal. "Performance evaluation of supervised machine learning algorithms for intrusion detection." *Procedia Computer Science* 89 (2016): 117-123.

[8] Shanmugavadivu, R., and N. Nagarajan. "Network intrusion detection system using fuzzy logic." *Indian Journal of Computer Science and Engineering (IJCSE)* 2.1 (2011): 101-111.

[9] Shone, Nathan, et al. "A deep learning approach to network intrusion detection." *IEEE Transactions on Emerging Topics in Computational Intelligence* 2.1 (2018): 41-50.

[10] Park, Kinam, Youngrok Song, and Yun-Gyung Cheong. "Classification of Attack Types for Intrusion Detection Systems Using a Machine Learning Algorithm." *2018 IEEE Fourth International Conference on Big Data Computing Service and Applications (BigDataService)*. IEEE, 2018.

[11] Papernot, Nicolas, et al. "Towards the science of security and privacy in machine learning." *arXiv preprint arXiv:1611.03814*(2016).

[12] Lee, Chie-Hong, et al. "Machine learning based network intrusion detection." *Computational Intelligence and Applications (ICCIA), 2017 2nd IEEE International Conference on*. IEEE, 2017.

[13] Jiang, Feng, et al. "Deep Learning based Multi-channel intelligent attack detection for Data Security." *IEEE Transactions on Sustainable Computing* (2018).

[14] Haque, MdEnamul, and Talal M. Alkharobi. "Adaptive hybrid model for network intrusion detection and comparison among machine learning algorithms." *International Journal of Machine Learning and Computing* 5.1 (2015): 17.

[15] Ahmed, Mohiuddin, AbdunNaser Mahmood, and Jiankun Hu. "A survey of network anomaly detection techniques." *Journal of Network and Computer Applications* 60 (2016): 19-31.

[16] Liu, Qiang, et al. "A survey on security threats and defensive techniques of machine learning: a data driven view." *IEEE access* 6 (2018): 12103-12117.

[17] https://en.wikipedia.org/wiki/Machine_learning

[18] https://en.wikipedia.org/wiki/Random_forest

[19] https://machinelearningmastery.com/a-tour-of-machine-learning-algorithms/

[20] Bromiley, Matt. "Threat intelligence: What it is, and how to use it effectively." *SANS Institute InfoSec Reading Room* (2016).

[21] https://en.wikipedia.org/wiki/Intrusion_detection_sy-stem

[22] Gaddam, Ravi Teja, and M. Nandhini. "Analysis of Various Intrusion Detection Systems with a Model for Improving Snort Performance." *Indian Journal of Science and Technology*10.20 (2017).

[23] Kumar, Sailesh. "Survey of current network intrusion detection techniques." *Washington Univ. in St. Louis* (2007).

[24] Kwon, Donghwoon, et al. "A survey of deep learning-based network anomaly detection." *Cluster Computing* (2017): 1-13.

[25] Jasper, Scott E. "US cyber threat intelligence sharing frameworks." *International Journal of Intelligence and Counter Intelligence* 30.1 (2017): 53-65.

[26] Suman Sharma, Yogesh Verma, Amit Nadda, "*Information Security: Cyber Security Challenges*", International Journal of Scientific Research in Computer Science and Engineering, Vol.7, Issue.1, pp.10-15, 2019

[27] Shailja Sharma, Sheeba Khan, "*Analysis of Cloud Security, Performance, Scalability and Availability (SPSA)*", International Journal of Scientific Research in Network Security and Communication, Vol.7, Issue.1, pp.13-15, 2019

AUTHORS PROFILE

Mr. Kushal Jani completed his bachelor degree in Computer Engineering from Ganpat University, Mehsana, Gujarat, India in the year of 2012. Now pursuing master degree in Computer Engineering from Gtu - Graduate School of Engineering and Technology.