Journal of Advances in Science and Technology
Vol. 17, Issue No. 1, March-2020, ISSN 2230-9659

Review of Deep Learning Methods for Multi-Channel Intelligent Attack Detection

Mohammad Fozail Alam[1]* Dr. Priti Singla[2]

[1] PhD Student, Kalinga University, Raipur

[2] PhD Guide, Kalinga University, Raipur

Abstract – New challenges have emerged in wireless communication system since the fifth the fifth-generation networks and artificial intelligence technologies have been developed, especially when it comes to cybersecurity. In this review paper, we have a look on methods of detection for attacks that uses techniques and strength of deep learning. In particular, we first and foremost sum up central issues of organization security and attack recognition and present a few related applications utilizing profound learning structure. "Based on classification on profound learning techniques, we give unique consideration to attack identification strategies based on various types of structures, like autoencoders, neural networks, and convolutional neural networks. Subsequently, we present some benchmark datasets with depictions and contrast the exhibition of addressing approaches with show the current working condition of attack recognition techniques with profound learning structures. At long last, we sum up this paper and talk about certain ways of working on the exhibition of attack discovery under contemplations of using deep learning structures."

Keywords – Deep Learning; Cybersecurity; Artificial Intelligence, Attack, Detection

----------X----------

1. INTRODUCTION

Regardless of the wide development of data innovation, security has stayed one challenging region for networks or organizations and computers there is a rise in hacking and incursion incidents because of advancement of technologies every year. Security threat comes not only from external intruders but also from internal users in the form of misuse.

Internet has an important task in this never-ending communication, its effectiveness can reduce due to things known as intrusions. Intrusion is an commotion which harmfully concern the object the system. Intrusions is divided two categories one is host intrusions and other is network intrusions. Accessing, manipulating, modifying and destroying the information for delivering to system is host intrusion. "These include handling of system calls, change of file systems, privilege intensification, illegal logins and entrée to sensitive files and malware. which change the state of the system. Network intrusions are the intrusions that are caused due to incoming packets in the network which perform malevolent activities such as Denial of Service (DoS) attacks, or even attempt to crack into computers [1]".

The function of an intrusion detection system is to discover numerous types of malevolent routine that can give and take the safety and reliance of a computer system. This involves network attacks beside susceptible job, data driven attack on applications, host based attacks such as privilege intensification, log in which is not permitted and entrée to sensitive files, and malware. There is a huge benefit from the advancement of internet technology for which there is widespread usage of internet. So the security of network is very essential. The intention of network security is to avoid the access and change for the users who are not permitted for the same [1]. The usage of internet in various fields like military, finance make them the target of attacks which ensure threat and damage. Fundamentally, it is required to make available the efficient for attack detection which in turn preserve the network security. In addition, the attacks are progressed in various ways so the the recognition of variety of attacks is a demanding task.

Cyber security is very significant research for the influence of network now days. The application of Cyber security basically for the methods like anti-virus software, firewalls and intrusion detection systems (IDSs). As these methods save the network form different attacks. The intrusion detection system is a foremost protection method among all for the cyber security attack.

There is a choice of machine learning methods for categorization of network attacks devoid of earlier information of the distinctiveness in detail. Though, conventional machine learning methods are not capable of providing distinguishing feature descriptors for the description of detection of attack. In recent times machine learning method go a step ahead with the introduction of neural network which resembles like human brain which is called deep learning. The deep learning methods are can decipher the complex problems.

Attacks could be accepted as the challenge to avoid security policies of the system. Which in turn provide attackers trouble-free entrée to attain or adjust information, even demolishing the system. There is a need of security of wireless communication due to the network threats. The machine learning and big data plays an essential role for the network from attacks [2]. When the system is used without permission or mishandled, then this is called internet attack. Hackers do this kind of activities. The hacking can be categorized as outsiders when external people who have no rights and insiders when people from the same network use it wrongly [9].

Intrusion detection system helps in detecting and analyzing the traffic in network. Firewalls used in intrusion detection system helps in preventing malevolent attack. It worked in a way like it will not allow the data which sources some type of hazard in the system. The intrusion detection system checks the data which is requested and if there will be any kind of attack it will be cancelled.

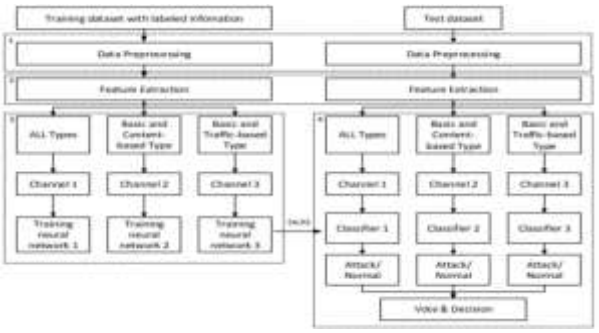

Fig. 1. Intelligent Attack detection system

For handling the threats in cyber security many proposals are discussed [3]. The attack detection is one of the effectual solutions. The attack detection observe, defy and stop the attack. In particular, attack detection accumulate the information by supervising the network which can detect illegal practice of people without human intervention.

The majority of commercial Network intrusion detection system are signature based, where a set of rules are used to determine what constitutes undesirable network traffic by monitoring patterns in that traffic. Whilst such systems are highly effective against known threats, signature based detection fails when attack vectors are unknown or known attacks are modified to get around such rule [8]".

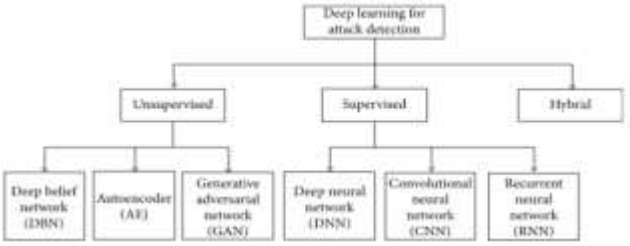

Fig. 2. Deep Learning for Attack Detection

Artificial neural network works in the principle of the way human brain works .The input given to the artificial neural network with one or more than one hidden layer. Then it is processed with weights to find out the next layer output. ANN uses "learning rule" for deciding the bias and the weights for hidden layer and output layer. ANN can handle the non-linear relationship between the dependent and independent variable. ANN can adapt the essential system model [8]. For this reason ANN is used for predicting and classifying the internet traffic .ANN can easily adapt the data with classification methods like K-nearest neighbor and decision tree.

2. LITERATURE REVIEW

Computers that are single or connected to networks are exposed to potentially damaging access by unauthorized hackers". So to get rid of it we need an effective and proper intrusion detection system. The attack detection is a classification problem.

An approach using deep learning is proposed [4] for intrusion detection system. A new approach is used for classification. For feature learning sparse auto encoder is used as it is simple and easy to implement. The network intrusion detection system is executed for different classifications. The performance of the proposed work is compared with soft max regression. And from the analysis it is found that self-taught learning is better .

To find out the intrusion attacks different machine learning techniques are used. This paper represents a survey on most of the machine learning techniques [5]. The paper defines many attack type. The paper gives a comparison of different methods from 2015 to 2018 where different data sets are used. The metric for performance comparison is accuracy here.

A review is done for intrusion detection system which uses methods of machine learning and deep learning and the applications are for internet of things [6]. As the IOT devices increased, the IOT based cyber-attacks also increased. The machine learning and deep learning methods are the proven technologies for attack detection in IOT.

An intrusion detection system by the use of recurrent neural network is proposed [7].Here the recurrent network is used to find out the patterns and features for intrusion. A principal component analysis method is used for the reduction of dimension and number of nodes of feedback network.

A method for detecting malevolent traffic is presented [8]. This is done by using artificial intelligence. The method which is proposed here is used to improve the performance of signature based detection methods. The precision is pretty much good using artificial neural network.

Neural Network is used for intrusion detection [9]. It predicts the unusual activities in the system. A training data is given to the network .Three sets of testing is done to get the stability of the network.

"A data mining method based anomaly detection is proposed [10]. It contains two major modules namely anomaly detection module and association pattern analysis. The anomaly detection module uses Local Outlier Factor (LOF) to detect anomalies and assigns a score to each data point based on the factor. A human analyst then verifies whether the data point is a real intrusion or normal behavior. Association pattern analysis is used to summarize the anomalous network connections. The major disadvantage of MINDS system is that it requires a human analyst to verify network connections."

A host-based IDS is proposed [11] for unsupervised classification. The proposed method uses an amalgamation of K-Means clustering and ID3 learning algorithms .Initially K-means is given to training data and divided into partitions for which it uses Euclidean distance. The tree is built using ID3 algorithm. The anomaly score value of the K-Means clustering algorithm and decision rules from ID3 were extracted. The ensuing anomaly score value was acquired by a new one which is an amalgamation of decision tree and K-means algorithms. The presentation of the consolidated methodology was contrasted and individual K-Means grouping, ID3 order calculation and different methodologies dependent on Markovian chains and stochastic learning automata. Improvement in precision had been seen in the joined methodology when contrasted and different methodologies.

An intrusion detection model is designed using Long Short Term Memory (LSTM) [12]. The recurrent neural network is used which is an extension of feed forward network. The performance of proposed framework is taken through KDD dataset.

A random forest classification algorithm is developed [13] for misuse detection and its output given as input to the anomaly detection system developed using weighted k-means clustering algorithm. In this approach, categorical features of the network traffic profile such as flags, services and protocol type have been encoded with binary valued features. This conversion process has been found to increase the number of features from 41 to 95 which in turn could increase the computational cost and complexity.

A parallel misuse and anomaly detection model is designed [14] using C4.5 binary decision tree technique for misuse detection and classification based association rule technique for anomaly detection. "The C4.5 decision tree separates the network traffic into normal and attack categories. Normal traffic is sent to anomaly detector while attacks are sent in parallel to a decision tree classifier for labeling the attack type". Anomaly detection has been carried out in single level and misuse with a sequence of levels to detect each type of attack at each level.

A novel contextual fuzzy intellectual guide for interruption reaction framework is designed [15]. In this framework, another cosmology is characterized dependent on the reasonable diagrams for depicting the connections between various interruption ideas and for perceiving the dubious associations. The fundamental point of fuzzy intellectual guides is to survey the adverse consequence of an interruption on the casualty framework. A hybrid intrusion detection system is explained [16]. Cluster based design is taken to reduce the energy consumption. The malevolent activities are detected by anomaly detection which uses set of signature rules for detection. Two level classification can be used for attack detection [17].

3. RESEARCH GAPS IDENTIFIED

The Internet has turned into an indispensable part in many individuals' lives. So the need to keep servers ensured, on the web and accessible has become progressively significant. In today's world all most all people uses internet in their daily life as it provides solution for everything. Due to this growing internet technologies cybercrime and cyber-attacks are major concerns. Recognizing contaminated hosts or noxious organization traffic is significant for securing client data like passwords, numbers of credit card subtleties and other classified data or for anticipation of attacks [18] – [20]. The attack detection differentiate the hostile actions from the network traffic. The detection method should easily detect any new attack in efficient manner. The conventional detection methods only detect the recognized attack but cannot handle the new attack. To conquer this issue, most of the researcher uses machine learning techniques. It works good but the accuracy is not good [21]-[24].

Deep machine learning is reasonable to display complex non-straight connections by learning numerous degrees of information portrayals that relate to various degrees of deliberation. A profound neural organization comprises of a course of many

layers of non-straight handling units for include extraction and change [25]-[28].

4. CONCLUSION

Deep machine learning consists many layers so that the design to execute info handling, that makes tremendous progress in areas of unaided learning and recognition of pattern. Roused by performing of deep machine learning techniques, we agree deep machine learning is critical for field of association security, to study the current profound learning procedures for attack recognition. We dissect ongoing strategies, characterize them as per distinctive profound learning procedures, and shows allot of agent techniques.

In the course of recent years, research on the best way to apply deep machine learning strategies on attack recognition has gained an incredible headway. Be that as it may, numerous issues actually exist. Right off the bat, it is trying to change deep machine learning techniques as ongoing classifiers for attack identification. In the majority of the past works, they just diminish include measurement for less calculation cost during period of element extraction. Also, the vast majority of the profound learning procedures are suitable for investigation of picture and example acknowledgment. In this way, how to direct the characterization of organization traffic sensibly with deep machine learning strategies will be a fascinating issue. Thirdly, with more information including the trials, the characterization results will be better [25]. In any case, a large portion of the attack identification issues are shy of adequate information. Accordingly, joining administered and solo learning might give better execution, which has been demonstrated by numerous preliminaries. Besides, with the advancement of IoT [29], mist, cloud [30], and huge information advances, how to include them to assist with further developing adequacy of attack recognition strategies utilizing profound learning stays an open and fascinating inquiry.

REFERENCES

[1]. S. Aftergood (2017). “Cybersecurity: the cold war online,” Nature, vol. 547, no. 7661, pp. 30-31.

[2]. X. Xu, C. He, Z. Xu, L. Qi, S. Wan, and M. Z. A. Bhuiyan (2019). “Joint optimization of offloading utility and privacy for edge computing enabled iot,” IEEE Internet of Things Journal, vol. 7, no. 4, pp. 2622–2629.

[3]. X. Xu, Q. Liu, X. Zhang, J. Zhang, L. Qi, and W. Dou (2019). “A blockchain - powered crowdsourcing method with privacy preservation in mobile environment,” IEEE Transactions on Computational Social Systems, vol. 6, no. 6, pp. 1407–1419.

[4]. Quamar Niyaz, Weiqing Sun, Ahmad Y Javaid, and Mansoor Alam (2015). “A Deep Learning Approach for Network Intrusion Detection System”, BICT 2015, December 03 - 05, New York City

[5]. SH Kok, Azween Abdullah, NZ Jhanjhi, Mahadevan Supramaniam (2019). “A Review of Intrusion Detection System using Machine Learning Approach”, International Journal of Engineering Research and Technology. ISSN 0974 - 3154, Volume 12, Number 1, pp. 8-15.

[6]. Javed Asharf, Nour Moustafa, Hasnat Khurshid, Essam Debie, Waqas Haider and Abdul Wahab (2019). “A Review of Intrusion Detection Systems Using Machine and Deep Learning in Internet of Things: Challenges, Solutions and Future Directions”, MDPI, Electronics, 9, 1177; doi:10.3390/electronics9071177

[7]. Jwg-sheng Xue,; Ji-zhou Sun; Xu Zhang, (2004). [IEEE 2004 International Conference on Machine Learning and Cybernetics – Shanghai, China (26 - 29 Aug. 2004)] Proceedings of 2004 International Conference on Machine Learning and Cybernetics (IEEE Cat. No.04EX826) – Recurrent network in network intrusion detection system, pp. 2676 – 2679. Doi:10.1109/icmlc.2004.1378292

[8]. Alex Shenfield, David Day, Aladdin Ayesh (2018). “Intelligent intrusion detection systems using artificial neural networks”, ICT Express, Volume 4, Issue 2, June 2018, Pages 95-99

[9]. Shun, Jimmy; Malki, Heidar A. (2008). [IEEE 2008 Fourth International Conference on Natural Computation – Jinan, Shandong, China (2008.10.18 - 2008.10.20)] 2008 Fourth International Conference on Natural Computation – Network Intrusion Detection System Using Neural Networks, pp. 242 – 246. Doi:10.1109/ICNC.2008.900

[10]. Ertoz, L., Eilertson, E., Lazarevic, A., Tan, P., Kumar, V., Srivastava, J. and Dokas, P. (2004). “MINDS - Minnesota Intrusion Detection System”, Next Generation Data Mining, MIT Press.

[11]. Yasami, Y. and Mozaffari, S.P. (2010). “A Novel Unsupervised Classification Approach for Network Anomaly Detection by K - means Clustering and ID3 Decision Tree Learning Methods”, in the Journal of

Supercomputing, Springer Netherlands, Vol. 53, No. 1, pp. 231-245.

[12]. Kim, Jihyun; Kim, Jaehyun; Thu, Huong Le Thi; Kim, Howon (2016). [IEEE 2016 International Conference on Platform Technology and Service (PlatCon) – Jeju, South Korea (2016.2.15 - 2016.2.17)] 2016 International Conference on Platform Technology and Service (PlatCon) – Long Short Term Memory Recurrent Neural Network Classifier for Intrusion Detection, pp. 1–5.

[13]. Elbasiony, RM, Sallam, EA, Eltobely, TE & Fahmy, MM (2013). 'A hybrid network intrusion detection framework based on random forests and weighted k - means', A in Shams Engineering Journal, vol. 4, no. 4, pp. 753-762

[14]. Goel, R, Sardana, A & Joshi, RC (2012). 'Parallel Misuse and Anomaly Detection Model', International Journal of Network Security, vol. 14, no. 4, pp. 211-222.

[15]. Zaghdoud, M & Al - Kahtani, MS 2013, 'Contextual fuzzy cognitive map for intrusion response system,' International Journal of Computer and Information Technology, vol. 2, no. 1, pp. 471-478

[16]. Maleh Y, Ezzati A, Qasmaoui Y, et al. A Global Hybrid Intrusion Detection System for Wireless Sensor Networks[J]. Procedia Computer Science, 2015, 52(1): pp. 1047-1052.

[17]. Panda M., Abraham A., and Patra M. R. (2010). Discriminative Multinomial Naïve Bayes for Network Intrusion Detection, in Information Assurance and Security (IAS), 2010 Sixth International Conference on 2010, pp. 5-10.

[18]. R. Vinayakumar, M. Alazab, K. P. Soman, P. Poornachandran, A. Al - Nemrat, and S. Venkatraman (2019). "Deep learning approach for intelligent intrusion detection system," IEEE Access, vol. 7, pp. 41525 – 41550.

[19]. J. Saxe and K. Berlin (2017). "Expose: a character - level convolutional neural network with embeddings for detecting malicious urls, file paths and registry keys," http://arxiv.org/abs/ 1702.08568.

[20]. R. Pascanu, J. W. Stokes, H. Sanossian, M. Marinescu, and A. Thomas (2015). "Malware classification with recurrent networks," in Proceedings of 2015 IEEE International Conference on Acoustics, Speech and Signal Processing (ICASSP), pp. 1916–1920, Queensland, Australia.

[21]. Z. Feng, C. Shuo, and W. Xiaochuan (2017). "Classification for dga - based malicious domain names with deep learning architectures," in Proceedings of 2017 Second International Conference on Applied Mathematics and Information Technology, London, UK, January 2017.

[22]. J. Woodbridge, H. S. Anderson, A. Ahuja, and D. Grant (2016). "Predicting domain generation algorithms with long short - term memory networks," 2016, http://arxiv.org/abs/ 1611.00791.

[23]. M. Z. Alom, T. M. Taha, C. Yakopcic et. al. (2018). "The history began from alexnet: a comprehensive survey on deep learning approaches," 2018 pages, CoRR abs/1803.01164.

[24]. E. Aminanto and K. Kim (2016). "Deep learning in intrusion detection system: an overview," in Proceedings of 2016 International Research Conference on Engineering and Technology (2016 IRCET), Higher Education Forum, Seoul, South Korea, January 2016.

[25]. L. Deng (2014). "A tutorial survey of architectures, algorithms, and applications for deep learning," APSIPA Transactions on Signal and Information Processing, Vol. 3.

[26]. Y. Yu, J. Long, and Z. Cai (2017). "Network intrusion detection through stacking dilated convolutional auto encoders," Security and Communication Networks, Vol., Article ID 4184196, 10 pages, 2017.

[27]. M. Yousefi - Azar, V. Varadharajan, L. Hamey, and U. Tupakula (2017). "Autoencoder - based feature learning for cyber security applications," in Proceedings of 2017 International Joint Conference on Neural Networks (IJCNN), pp. 3854 – 3861, IEEE, San Diego, CA, USA.

[28]. F. Farahnakian and J. Heikkonen (2018). "A deep auto - encoder based approach for intrusion detection system," in Proceedings of 2018 20th International Conference on Advanced Communication Technology (ICACT), pp. 178–183, IEEE, Chuncheon, South Korea.

[29]. A. Javaid, Q. Niyaz, W. Sun, and M. Alam (2016). "A deep learning approach for network intrusion detection system," in Proceedings of the 9th EAI International Conference on Bio - Inspired Information

and Communications Technologies (formerly BIONETICS), pp. 21–26, New York, NY, USA.

[30]. D. Papamartzivanos, F. Gomez Marmol, and G. Kambourakis (2019). Introducing Deep Learning Self - Adaptive Misuse Network Intrusion Detection Systems, IEEE Access, Piscataway, NJ, USA.

Corresponding Author

Mohammad Fozail Alam*

PhD Student, Kalinga University, Raipur

mdfozailalam@gmail.com