ISSN-2394-5125 VOL 7, ISSUE 6, 2020

CYBER SECURITY METHODS FOR DETECTING NETWORK INTRUSIONS USING DEEP LEARNING

Dr. N.D. Jambhekar[1]*

[1]*Department of Computer Science, G.S. Gawande Mahavidyalaya Umarkhed, Dist. Yavatmal
jambhekarnd@gmail.com

***Corresponding Author:** Dr. N.D. Jambhekar
*Department of Computer Science, G.S. Gawande Mahavidyalaya Umarkhed, Dist. Yavatmal
jambhekarnd@gmail.com

Abstract: A modern Intrusion Detection System (IDS) is an essential component of any cutting-edge information and communication technology (ICT) architecture because of the growing concern for online security and the complexity and unpredictability of cyberattacks. Integration of Deep Neural Networks (DNNs) into Intrusion Detection Systems (IDS) for increased security measures is driven by the requirement to understand the nature of these assaults, which is why their relevance grows. With a learning rate of 0.1 and 1000 epochs of execution on the 'KDD Cup-99' dataset for training and benchmarking, this article uses DNNs to anticipate assaults on Network Intrusion Detection Systems (N-IDS). Additionally, the dataset was trained using a variety of DNNs with layers ranging from 1 to 5, in order to conduct comparative analysis and determine the effectiveness. Based on the results of this study, a deep neural network (DNN) with three layers outperforms existing deep learning models and standard machine learning techniques.

Key Words: Intrusion detection, deep neural networks, machine learning, deep learning, DARPA dataset

Introduction

Every company in the contemporary world has been driven to embrace the integration of information and communication technology (ICT) as a result of the rapid speed of technical breakthroughs. As a result establishing a setting in which every activity is directed via that system, which makes the organisation vulnerable to attack in the event that the security of the information and communication technology system is compromised. As a result, this necessitates the implementation of multilayered detection and protection strategies that are not only capable of coping with assaults on the system that are really innovative but also have the ability to independently adjust to the new data.

A number of different technologies, including anomaly detection and intrusion detection systems (IDSs), may be used to protect information and communications technology (ICT) systems against vulnerabilities. Among the shortcomings of anomaly-detection systems is the fact that it is difficult to formulate rules for these systems. Each procedure that is being analysed has to be created, put into action, and tested to ensure that it is accurate. There is another potential hazard associated with anomaly detection, which is that potentially dangerous behaviour that is consistent with the typical pattern of use is not identified. Because of this, it is very necessary to have an identification system that is capable of adjusting to the new threats that have been introduced recently, and that can be taught and deployed by making use of datasets that have an irregular distribution.

A variety of cybersecurity-based technologies known as intrusion detection systems (IDSs) were first created with the purpose of identifying vulnerabilities and exploits that were directed against a target host. IDS is only used for the purpose of identifying potential dangers. As a result, it is situated outside of the band on the infrastructure of the network and is not included in the actual communication transit that occurs between the sender and the recipient of the data. Instead, the solutions will often make use of TAP or SPAN ports to analyse the copy of the inline traffic stream. They will then attempt to forecast the assault based on an algorithm that has been taught in the past, which will make the requirement for human participation very insignificant.

Within the realm of cyber security, machine learning algorithms have shown to be of critical importance. There has been an increase in the reliability of applying deep learning networks for Artificial Intelligence (AI) and unsupervised challenges. This is particularly due to the incredible performance and potential of deep learning networks in recent days in various problems from a wide variety of fields that were considered unsolvable in the past. In essence, deep learning is nothing more than a subfield of machine learning that attempts to simulate the operations of the human brain, which is where the term "artificial neural network" comes from.

When it comes to tackling high-level issues, deep learning is a notion that involves the formation of hierarchical representations that are complicated and entail the production of basic building pieces.

RELATED WORK

Ever from the beginning of computer architectures, there has been research on the use of identification in network security. These days, it is normal practice to use machine learning strategies and solutions to holistic intrusion detection systems.

The available training data, on the other hand, is restricted and is mostly used for benchmarking purposes. The DARPA dataset [1] is often considered to be among the most extensive datasets that are available to the general public. After being cleaned up, the data from the dump that was provided by the DARPAIDE valuation network in 1998 was used for the KDDCupcontest that took place in 1999 at the 5th International Conference on Knowledge-edge Discovery and Data Mining. The task at hand was to organise the records of the connections that have previously been preprocessed into either traffic that is considered to be normal or one of the following kinds of attacks: "DoS," "Probing," "R2L," and "U2R."

Preprocessing the data from the KDDCup-'99 competition was accomplished with the help of the MADAMID framework [2]. The entries that employed decision tree variants and showed only modest changes in performance were the ones that took the top three spots [3,4,5]. Following the evaluation of all seventeen of the competition's first entries, it was discovered that they all performed well [6]. The bulk of the findings that were published were evaluated and trained using just a 10% training set, and they observed the feature reduction on the datasets that were used for the KDDCup-'99 study [7 8, 9]. Only a small number of researchers made use of self-constructed datasets, which were taken from the 10% KDDCup-'99' training set [10, 11,12].

There are a number of fascinating publications that are published as a result of the utilisation of a variety of training and test datasets. These articles compare the results in an unintentional manner. Genetic algorithms and decision trees were used in a work [13] for the purpose of automatically generating rules for an intelligent system with the intention of improving the capabilities of an existing intrusion detection system (IDS). It was argued by [14] and [15] that this integrated use of neural networks in IDS would be beneficial. In [16], an application of recurrent neural networks (RNNs) was presented, and in [17], a comparison was made between the performance of neural network topologies for statistical anomaly detection and datasets from four distinct situations.

Despite the fact that the datasets of KDDCup-'99' contain a number of problems [18], [19] contends that they are still an efficient benchmarking dataset that is accessible to the public and can be used to evaluate various intrusion detection systems.

The capacity of machine learning-based systems to combat continually developing complex and varied threats in order to achieve an acceptable false positive rate of identification while maintaining a fair computing cost is the primary rationale for the widespread use of these approaches. According to [36], the PNrule approach, which is developed from P-rules and N-rules, was used in the early phases of the process in order to determine whether or not the class existed.

The improvement of the detection rate in the other sorts of assaults, with the exception of the U2R category, is one of the reasons why this has positive implications.

The term "Convolutional Neural Network" (CNN) refers to a network that is an evolution of the standard Feed Forward Networks (FFN) in the plane of drawing inspiration from biological aspects. When CNN was first developed, it was used for the purpose of image processing. This was accomplished by the utilisation of conventional 2D layers, pooling 2D layers, and entirely linked layers. The research conducted by [37] investigated the uses of CNN for intrusion detection systems (IDS) using the KDDCup dataset from 1999 and compared the findings with those of several other cutting-edge algorithms. After careful consideration, they have arrived with the general opinion that CNN is better than the other approaches. The applicability of the Long-Short-Term Memory (LSTM) classifier was investigated in [38], which used the same dataset. According to what has been said, the utility of LSTM in relation to intrusion detection systems may be shown by its ability to look into the past and link the consecutive records of connections.

The primary objective of this research is to make advantage of the unexpected unpredictability that may occur during an incoming cyberattack. This randomness is not apparent by the naked sight of a human being, but it can be filtered by the addition of an artificial intelligence layer to the network. It is also possible to learn to quickly anticipate an incoming assault by training the neural network with the current data on cyber attacks. This allows one to either notify the system or execute a pre-programmed reaction, both of which have the potential to prevent the attack from continuing. As a consequence of this, it is possible to avoid costly data breaches and aftershock collateral damage that might amount to millions of dollars simply by adding an additional layer to the security system. A more current dataset must be utilised for retraining before the algorithm is deployed in the field. This is necessary in order to improve the real-time resilience of the system. The benchmarking dataset that was used for training the networks has been used. The purpose of this article is to provide an introduction to the fundamentals of artificial neural networks within the context of the rapidly developing topic of cybersecurity.

Deep Neural Network(DNN)

Deep neural networks are layered in an increasing hierarchy of complexity as well as abstraction, in contrast to the linear nature of typical machine learning methods. Every layer is applicable.This algorithm performs a nonlinear transformation on its input and generates a statistical model as an output based on what it has learned. A straightforward explanation would be that the input layer is the one that receives the input layer and then passes it on to the first hidden layer. These hidden layers do computations and analysis on the information that we provide. In the process of developing neural networks, one of the issues that occurs is determining the hidden layers' count and the count of the neurons for each layer. An activation function is present in every neuron and is used to standardize the output of the neuron. The "Deep" in deep learning refers to the presence of multiple hidden layers. The output layer returns the output data. Until the output has reached an acceptable level of accuracy, epochs are recontinued. Cybersecurity is a critical concern in today's interconnected world, with network intrusions posing significant threats to both individuals and organizations. Traditional intrusion detection systems (IDS) often struggle to keep pace with the evolving nature of cyber threats, prompting the exploration of more advanced techniques. Deep learning, a subset of machine learning, has emerged as a promising approach for enhancing the effectiveness of intrusion detection by leveraging its ability to automatically learn and adapt from large volumes of data.

The purpose of this research paper is to investigate the application of deep learning methods for detecting network intrusions and to evaluate their effectiveness compared to traditional approaches. This paper will provide an overview of deep learning techniques relevant to cybersecurity, discuss their advantages and limitations, and present experimental results demonstrating their performance in detecting various types of network intrusions.

Shortcomings of the KDDCup-’99 dataset

ReLu has shown to be more effective, and it provides a comprehensive report. However, the sin-thetic data set that was supplied, which included KDDCup-'98' and KDDCup-'99, does have a number of significant inadequacies.

The primary criticism levelled against them was that they missed the opportunity to evaluate their data set by simulating a real-world profile. However, despite all of these critiques, the dataset KDD Cup-'99 has been used by Byman researchers as an efficient dataset for benchmarking the IDS algorithms throughout the course of the years. [27] has provided a deep examination of the contents, found the non-uniformity, and replicated the artefacts in simulated network trafficdata. This is in contrast to the criticisms that have been levelled against the production of the dataset.

The reasons why machine learning classifiers have limited skill in recognising assaults that correspond to the content categories R2L and U2R in KDDCup-'99' data sets have been explored by [28]. Also included in this discussion are the reasons why these attacks are difficult to recognise. They came to the conclusion that it is not feasible to get a detection rate that is satisfactory by using traditional machine learning techniques. In addition, it is said that it is possible to get a high detection rate in the majority of instances by creating data sets that have been refined and enhanced via the procedure of integrating the train set with the test set. Nevertheless, a substantial method has not been presented in this article.

There was a lot of criticism directed to the DARPA/KDDCup-'88 since it did not test the typical intrusion detection system. For the purpose of eliminating this, [29] used the Snort ID system on DARPA/ KDDCup- '98'tcpdumptraces information. As a consequence of the system's poor performance, the accuracy was low, and the false positive rates were unacceptable. Despite the fact that it was unsuccessful in identifying dos and probing category, it performed much better than the detection of R2L and U2R overall.

The KDDCup-'99 season of the most extensively used publicly accessible benchmarking datasets is trustworthy for research linked to IDS assessment and other security-related activities [31], notwithstanding the severe critiques that have been levelled against it [30]. A refined version of the dataset, which was given the moniker NSL-KDD, was offered by [31] in an attempt to address the fundamental issues that were present with the KDDCup-'99' collection. The redundant connection records of the full train and test data were eliminated as a result of this action. Furthermore, the inaccurate records were removed from the samples that were being tested. Through the use of these procedures, the classifier is prevented from exhibiting a bias towards records that occur more often. Although this was refined, it was not successful in resolving the concerns that were noted by [32, 33]. As a result, a new dataset that was given the name UNSW-NB15 was proposed.

In today's digitally interconnected world, cybersecurity has become a paramount concern due to the escalating frequency and sophistication of cyber threats. Network intrusions, in particular, pose significant risks to individuals, organizations, and critical infrastructure, leading to data breaches, financial losses, and reputational damage. Traditional methods of detecting and mitigating network intrusions often rely on rule-based approaches and signature-based detection systems, which may struggle to keep pace with the rapidly evolving landscape of cyber threats.

Deep learning, a subset of machine learning techniques inspired by the structure and function of the human brain, has emerged as a promising approach for enhancing cybersecurity measures. Deep learning models, such as artificial neural networks, are capable of automatically learning complex patterns and relationships from large volumes of data, enabling them to detect subtle anomalies and intrusions that may evade traditional detection methods. By leveraging the power of deep learning, cybersecurity practitioners can develop more adaptive and resilient defense mechanisms to safeguard against cyber threats.

The objective of this research paper is to explore the application of deep learning methods for detecting network intrusions and to evaluate their effectiveness compared to traditional approaches. Specifically, we aim to investigate how deep learning techniques can be applied to analyze network traffic data and identify malicious activities, such as unauthorized access attempts, malware infections, and denial-of-service attacks. By harnessing the capabilities of deep learning, we seek to enhance the accuracy, efficiency, and scalability of intrusion detection systems, thereby bolstering the overall cybersecurity posture of individuals and organizations.

Conclusion

The study has provided a thorough summary of the benefits of DNs in intrusion detection systems. We have taken into consideration some traditional ML algorithms for the sake of comparison and when pitted against DNN's output. The research mainly employed the publicly available KDDCup-'99 dataset as its benchmarking tool, which provided unambiguous documentation of the DNN's superiority over the other techniques tested. This study considers DNNs with varying counts of hidden layers for algorithmic refinement and finds that a DNN with three layers is the most effective and accurate.The use of an out-of-date benchmarking dataset to train the neurons is a problem with this approach, as mentioned many times in this study. Luckily, it may be defeated by using a new dataset that captures the essence of current attack techniques. This should be done before deploying the artificial intelligence layer to the existing network infrastructures. This will ensure that the algorithm is adaptable in the real world.Although deep learning approaches show promise for cyber security problems, this paper's empirical findings suggest that they may not be the best choice.

References

1. R. Lippmann, J. Haines, D. Fried, J. Korba and K. Das. “The 1999 DARPA off-line intrusion detection evaluation”. Computer networks, vol. 34, no. 4, pp. 579– 595, 2000. DOI http://dx.doi.org/10.1016/S1389- 1286(00)00139–0.
2. W. Lee and S. Stolfo. “A framework for constructing features and models for intrusion detection systems”. ACM transactions on information and system security, vol. 3, no. 4, pp. 227–261, 2000. DOI http://dx.doi. Org/10.1145/382912.382914.
3. B. Pfahringer. “Winning the KDD99 classification cup: Bagged boosting”. SIGKDD explorations newsletter, vol. 1, pp. 65–66, 2000. DOI http://dx.doi.org/10. 1145/846183.846200.
4. M. Vladimir, V. Alexei and S. Ivan. “The MP13 approach to the KDD’99 classifier learning contest”. SIGKDD explorations newsletter, vol. 1, pp. 76– 77, 2000. DOI http://dx.doi.org/10.1145/846183. 846202.
5. R. Agarwal and M. Joshi. “PNrule: A new framework for learning classier models in data mining”. Tech. Rep. 00–015, Department of Computer Science, University of Minnesota, 2000.
6. C. Elkan. “Results of the KDD’99 classifier learning”. SIGKDD explorations newsletter, vol. 1, pp. 63– 64, 2000. DOI http://dx.doi.org/10.1145/846183. 846199.
7. S. Sung, A.H. Mukkamala. “Identifying important features for intrusion detection using support vector machines and neural networks”. In Proceedings of the symposium on applications and the Internet (SAINT), pp. 209–216. IEEE Computer Society, 2003. DOI http: //dx.doi.org/10.1109/saint.2003.1183050.
8. H. Kayacik, A. Zincir-Heywood and M. Heywood. “Selecting features for intrusion detection: A feature relevance analysis on KDD 99 intrusion detection datasets”. In Proceedings of the third annual conference on privacy, security and trust (PST). 2005.
9. C. Lee, S. Shin and J. Chung. “Network intrusion detection through genetic feature selection”. In Seventh ACIS international conference on software engineering, artificial intelligence, networking, and parallel/distributed computing (SNPD), pp. 109–114. IEEE Computer Society, 2006
10. S. Chavan, K. Shah, N. Dave, S. Mukherjee, A. Abraham and S. Sanyal. “Adaptive neuro-fuzzy intrusion detection systems”. In Proceedings of the International Conference on Information Technology: Coding and Computing (ITCC), vol. 1, pp. 70–74. IEEE Computer Society, 2004. DOI http://dx.doi.org/ 10.1109/itcc.2004.1286428.
11. S. Chebrolu, A. Abraham and J. Thomas. “Feature deduction and ensemble design of intrusion detection systems”. Computers \& security, vol. 24, no. 4, pp. 295– 307, 2005. DOI http://dx.doi.org/10.1016/j. Cose.2004.09.008.
12. Y. Chen, A. Abraham and J. Yang. “Feature selection and intrusion detection using hybrid flexible neural tree”. In Advances in Neural Networks (ISNN), vol. 3498 of Lecture notes in computer science, pp. 439– 444. Springer Berlin / Heidelberg, 2005. DOI http://dx.doi.org/10.1007/11427469_71.
13. C. Sinclair, L. Pierce and S. Matzner. “An application of machine learning to network intrusion detection”. In Proceedings of the 15th annual Computer Security Applications Conference (ACSAC), pp. 371–377. IEEE Computer Society, 1999. DOI http://dx.doi.org/ 10.1109/csac.1999.816048.
14. H. Debar, M. Becker and D. Siboni. “A neural network component for an intrusion detection system”. In Proceedings of the IEEE Computer Society Symposium on research in security and privacy, pp. 240–250. IEEE Computer Society, 1992. DOI http://dx.doi.org/ 10.1109/risp.1992.213257.
15. J. Cannady. “Artificial neural networks for misuse detection”. In Proceedings of the 1998 National Information Systems Security Conference (NISSC), pp. 443–456. Citeseer, 1998.
16. H. Debar and B. Dorizzi. “An application of a recurrent network to an intrusion detection system”. In an International joint conference on neural networks, 1992. IJCNN., vol. 2, pp. 478 –483 vol.2. jun 1992. DOI http://dx.doi.org/10.1109/ijcnn. 1992.226942.
17. Z. Zhang, J. Lee, C. Manikopoulos, J. Jorgenson and J. Ucles. “Neural networks in statistical anomaly intrusion detection”. Neural network world, vol. 11, no. 3, pp. 305–316, 2001.
18. J. McHugh. “Testing intrusion detection systems: A critique of the 1998 and 1999 DARPA intrusion detection system evaluations as performed by Lincoln Laboratory”. ACM transactions on information and system security, vol. 3, no. 4, pp. 262–294, 2000. DOI http://dx.doi.org/10.1145/382912.382923.

19. M. Tavallaee, E. Bagheri, W. Lu and A. A. Ghorbani. “A detailed analysis of the KDD CUP 99 data set”. In IEEE symposium on computational intelligence for security and defence applications, Cisda, pp. 1–6. IEEE, Jul. 2009. DOI http://dx.doi.org/10.1109/cisda. 2009.5356528.
20. X. Glorot, A. Bordes, and Y. Bengio, “Deep sparse rectifier neural networks,” in Proceedings of the Fourteenth International Conference on Artificial Intelligence and Statistics, 2011, pp. 315–323.
21. Bengio, Y., Simard, P. and Frasconi, P., 1994. Learning long-term dependencies with gradient descent is difficult. IEEE Transactions on Neural Networks, 5(2), pp.157–166.
22. Maas, A.L., Hannun, A.Y. and Ng, A.Y., 2013, June. Rectifier nonlinearities improve neural network acoustic models. In Proc. icml (Vol. 30, №1, p. 3).
23. F. Chollet, “Keras (2015),” URL http://keras. Io, 2017.
24. M. Abadi, P. Barham, J. Chen, Z. Chen, A. Davis, J. Dean, M. Devin, S. Ghemawat, G. Irving, M. Isard et al., “Tensorflow: A system for large-scale machine learning.” in OSDI, vol. 16, 2016, pp. 265–283.
25. Stolfo, S., Fan, W. and Lee, W., KDD-CUP-99 Task Description. 1999–10–28)[2009–05–08]. http://KDD. ics. uci. edu/databases/kddcup99/task, html.
26. J. McHugh. “Testing intrusion detection systems: A critique of the 1998 and 1999 DARPA intrusion detection system evaluations as performed by Lincoln Laboratory”. ACM transactions on information and system security, vol. 3, no. 4, pp. 262–294, 2000. DOI http://dx.doi.org/10.1145/382912.382923.
27. M. Mahoney and P. Chan. “An analysis of the 1999 DARPA/Lincoln Laboratory evaluation data for network anomaly detection”. In Recent advances in intrusion detection, vol. 2820 of Lecture notes in computer science, pp. 220–237. Springer Berlin / Heidelberg, 2003.
28. Sabhnani, Maheshkumar, and Gursel Serpen. “Why machine learning algorithms fail in misuse detection on KDD intrusion detection data set.” Intelligent Data Analysis 8, no. 4 (2004): 403–415.
29. S. Brugger and J. Chow. “An assessment of the DARPA IDS evaluation dataset using snort”. Tech. Rep. CSE2007–1, Department of Computer Science, University of California, Davis (UCDAVIS), 2005.
30. J. McHugh. “Testing intrusion detection systems: A critique of the 1998 and 1999 DARPA intrusion detection system evaluations as performed by Lincoln Laboratory”. ACM transactions on information and system security, vol. 3, no. 4, pp. 262–294, 2000. DOI http://dx.doi.org/10.1145/382912.382923.
31. Tavallaee, Mahbod, Ebrahim Bagheri, Wei Lu, and Ali-A. Ghorbani. “A detailed analysis of the KDD CUP 99 data set.” In Proceedings of the Second IEEE Symposium on Computational Intelligence for Security and Defence Applications 2009. 2009.
32. Moustafa, Nour, and Jill Slay. “The evaluation of Network Anomaly Detection Systems: Statistical analysis of the U[8] H. Kayacik, A. Zincir-Heywood and M. Heywood. “Selecting features for intrusion detection: A feature relevance analysis on KDD 99 intrusion detection datasets”. In Proceedings of the third annual conference on privacy, security and trust (PST). 2005.
33. Moustafa, Nour, and Jill Slay. “UNSW-NB15: a comprehensive data set for network intrusion detection systems (UNSW-NB15 network data).”Military Communications and Information Systems Conference (MilCIS), 2015. IEEE, 2015.
34. KDD Cup 1999. Available on: http://kdd.ics.uci.edu/database[8] H. Kayacik, A. ZincirHeywood and M. Heywood. “Selecting features for intrusion detection: A feature relevance analysis on KDD 99 intrusion detection datasets”. In Proceedings of the third annual conference on privacy, security and trust (PST). 2005.
35. McDowell, M. (2013). Understanding Denial-of-Service Attacks US-CERT. United States Computer Emergency Readiness Team.
36. [36] R. Agarwal and M. V. Joshi, “Pnrule: A new framework for learning classifier models in data mining (a case study in network intrusion detection),” in Proceedings of the 2001 SIAM International Conference on Data Mining. SIAM, 2001, pp. 1–17.
37. Vinayakumar, R., Soman, K. P., \& Poornachandran, P. (2017, September). Applying convolutional neural network for network intrusion detection. In Advances in Computing, Communications and Informatics (ICACCI), 2017 International Conference on (pp. 1222–1228). IEEE.
38. Staudemeyer, R. C. (2015). Applying long short-term memory recurrent neural networks to intrusion detection. South African Computer Journal, 56(1), 136– 154.
39. Sommer, R. and Paxson, V., 2010, May. Outside the closed world: On using machine learning for network intrusion detection. In Security and Privacy (SP), 2010 IEEE Symposium on (pp. 305–316). IEEE.
40. Vinayakumar, R., Soman, K. P., \& Poornachandran, P. (2018). Evaluating deep learning approaches to characterize and classify malicious URLs. Journal of Intelligent \& Fuzzy Systems, 34(3), 1333–1343.
41. Vinayakumar, R., Soman, K. P., \& Poornachandran, P. (2018). Detecting malicious domain names using deep learning approaches at scale. Journal of Intelligent \& Fuzzy Systems, 34(3), 1355–1367.
42. Vinayakumar, R., Soman, K. P., Poornachandran, P., \& Sachin Kumar, S. (2018). Evaluating deep learning approaches to characterize and classify the DGAs at scale. Journal of Intelligent \& Fuzzy Systems, 34(3), 1265–1276.

43. Vinayakumar, R., Poornachandran, P., \& Soman, K. P. (2018). Scalable Framework for Cyber Threat Situational Awareness Based on Domain Name Systems Data Analysis. In Big Data in Engineering Applications (pp. 113–142). Springer, Singapore.