2021 International Conference on Computational Performance Evaluation (ComPE),
North-Eastern Hill University, Shillong, Meghalaya, India. Dec 1–3, 2021

2021 International Conference on Computational Performance Evaluation (ComPE) | 978-1-6654-3656-4/21/$31.00 ©2021 IEEE | DOI: 10.1109/ComPE53109.2021.9751909

Deep Learning Techniques for Anomaly based Intrusion Detection System: A Survey

Yogendra Kumar
Department of CSE
NIT Hamirpur
Hamirpur, H.P., India
yogendra@nith.ac.in

Lokesh Chouhan
Department of CSE
NIT Hamirpur
Hamirpur, H.P., India
lokeshchouhan@gmail.com

Basant Subba
Department of CSE
NIT Hamirpur
Hamirpur, H.P., India
basantsubba@nith.ac.in

***Abstract*—Information security has become one of the significant concerns with the advancement of technology and digital assistance. An Intrusion Detection System(IDS) plays a substantial role in guarding the systems from security threats. However, existing IDS frameworks have faced challenges such as high false alarm rate, low detection rate, raw and huge dataset handling, etc. The Deep Learning techniques has grown as a reliable methodology to address such issues. This paper presents a taxonomy of anomaly based IDS frameworks. It also includes a detailed analysis of Deep Learning algorithms used in IDS frameworks and their comparison based on different characteristics. In addition, this study indicates critical challenges of the anomaly based IDS frameworks followed by possible future directions to improve their performances.**

***Index Terms*—Neural Network, Deep Learning, Intrusion Detection System, Anomaly based IDS framework.**

I. Introduction

Information Security has become one of the major components of industries, businesses and personal lives as dependency on Information Technology increase with the rapid growth of technology. As per CISCO[1] annual internet report 2018, Mobile devices will be used by more than 70% of the global population and around 29.3 billion network devices will be connected through IP addresses by 2023. Information Security ensures data availability, integrity, and confidentiality from different attacks using various strategies and techniques. There are some methods such as authentication [1], cryptography [2], firewalls [3] etc., developed in the literature to protect end-users from various security threats. These methods are known as a first-line defence, which is quite effective in detecting some specific intrusions. However, the first line of defence is associated with various limitations, especially in detecting unforeseen attacks. In line with this, a technique introduced in the literature, namely Intrusion Detection System(IDS) [4] is a notable research accomplishment that strengthens information security by addressing the issues of the first line of defence. IDS can detect and mitigate ongoing intrusions or security threats [5], [6] in a network or an individual system. The operations of the IDS are to analyze and monitoring the network traffic activities, detecting vulnerable parts in a system, and integrity analysis of sensitive data. IDS detection methodologies are divided into two major categories (i) Signature based IDS (SIDS) [7] and (ii) Anomaly based IDS(AIDS) [8]. SIDS is also known as misused detection; it compares the predefined attack patterns or signatures against captured events or data. SIDS is effective to classify known attacks but inadequate to distinguish unseen attacks [9]. AIDS learns the behaviour of system activities or network communication based on the available parameters and pinpoint any malicious activity if it perceives a notable deviation from the normal behaviour [10]. The most prominent benefit of anomaly based detection over signature based detection is its potential to identify unknown attacks [11]. However, the shortcoming associated with AIDS is that it is computationally extensive compare to SIDS.

[1]https://www.cisco.com/c/en/us/solutions/collateral/executive-perspectives/annual-internet-report/white-paper-c11-741490.html

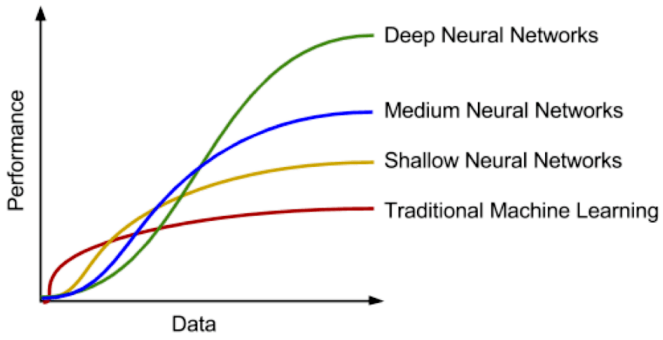

Fig. 1: Performance of various Machine Learning algorithms [12]

Machine Learning(ML) [13], [14] is a superset of Deep Learning which is used to develop the Anomaly based IDS frameworks. Many conventional ML techniques are used to effectively train security frameworks that assist an administrator in taking the corresponding course of actions to prevent and mitigate intrusions. In general, most of the conventional ML algorithms are ineffective in solving extensive and high-dimensional data classification problems, which leads to limited detection rates and accuracy. On the other hand, DL has strong capabilities to extract relevant information from a relatively huge dataset to build an enhanced IDS framework. The performance comparison of different ML algorithms is depicted in figure 1.

978-1-6654-3656-4/21/$31.00 ©2021 IEEE

The Deep Learning techniques are gaining popularity among security researchers as it is conducive to addressing various information security related issues [15]. In summary, information security has three significant challenges to address: (i) The rapid growth in unstructured data volume of network traffic (iii) The accuracy and efficiency of the intrusion detection model with in-depth surveillance (iii) Handling diversity in attacking techniques and data protocols [16]. The DL based IDS frameworks can deal with all these challenges and overcome the related issues effectively. Taking it into account, this paper provides a detailed analysis of various Deep Learning techniques used in the Anomaly based IDS framework.

This study provides in-depth assessments of DL techniques pertaining to anomaly based IDS, which is convenient for readers to become aware and discover research ideas in this domain. Diverse datasets have distinct traits and attributes that make them fit for different DL algorithms. Therefore, this study also presents the characteristics of IDS datasets along with the suitable DL approaches. Lastly, it highlights the significant existing challenges and future possibilities in the domain of anomaly based IDS.

The rest of the paper has been structured in the following ways. Section II provides an overview of DL algorithms along with a generic structure and the comparative analyses. Further, the usability of different DL techniques in the Anomaly based IDS framework and classification procedure are explained in section III. The subsequent section IV discusses the research challenges in Deep Learning based IDS frameworks followed by critical future directions. Finally, the study is concluded in section V.

II. Deep Learning Approaches Pertaining to IDS

Deep Learning is a subfield of ML concerned with methodologies evolved from information and cognitive theories. It mimics the functioning and organization of the human brain, endeavouring to imitate the process of human learning using Artificial Neural Networks(ANN). McCulloch and Pitts [17] introduced ANN by presenting a study of a mathematical model inspired by biological neurons in 1943. In 1986, Carnegie Mellon and Geoffrey E. Hinton introduced backpropagation for enhancing word prediction and shape classification. Further, Geoffrey E. Hinton [18] coined the term Deep Learning by describing the many-layered restricted Boltzmann machines network training model as “Deep” in 2006.

A. Generic Structure of Deep Learning

An Artificial Neural Network(ANN) is a computative prototype that emulates biological neurons. It includes one layer for input the dataset, multiple hidden layers for computation and one layer for producing the results. The ANN comprises just one hidden layer, is known as the shallow neural network. The early research on ANN was concentrated on the shallow neural network with back-propagation learning [19]. The shallow neural network is inadequate to solve the higher-level concepts and requires feature extraction to be performed separately.

Deep Leaning is much more persuasive than Shallow Neural Networks as it has more processing capability and is capable of solving higher-level concepts because of multiple hidden layers. Feature extraction is a part of many DL algorithms. DL approaches hold no sole structure for each application [20], but a general model as shown in figure 2. It can be observe from the figure, the first hidden layers h_1 receives the inputs ($x_1, x_2, ..., x_n$) from in input layer. The first hidden layer feeds the input to its next layer. Finally, the outermost layer, known as the output layer, produces the result ($y_1, y_2, y_3, , y_n$) based on the last hidden layer’s h_n input values [5]. The DL approach uses various non-linear mathematical activation functions. Some of the essential functions are the rectified linear(ReLu) unit, hyperbolic tangent function, sigmoid function, softmax, etc.

Deep Learning has several advantages over conventional ML in terms of data volume, feature engineering, learning capacity, accuracy, etc. DL based classifiers are able to learn the model directly from the raw dataset like text, image, etc.

B. Types of Deep Leaning approach

Deep Learning is categorized broadly into two categories, namely supervised and unsupervised learning. The algorithms apply to labelled datasets for training the DL based model are known as supervised learning algorithms. In contrast, unlabeled datasets are used for training the unsupervised learning based DL algorithms. Various types of DL approaches based on both categories are given as following.

1) Deep Neural Network(DNN): DNN is a basic approach of DL that contains more than one hidden layer. A general structure of DNN is shown in figure 2. It uses a feedforward learning approach to train the model, and each layer is able to learn features at various levels of abstraction. Potluri et al. [21] implemented an IDS using DNN and analyze the relevance of the input dataset. In the study, the NSL-KDD dataset used for performance evaluation and observed a considerable classification accuracy. Similarly, an IDS framework using DNN was proposed by Farhana et al. [22] and evaluated on the CICIDS-2017 dataset.

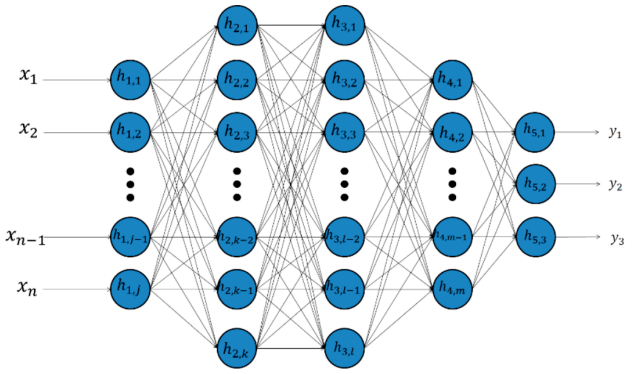

Fig. 2: Generic structure of deep neural network [5]

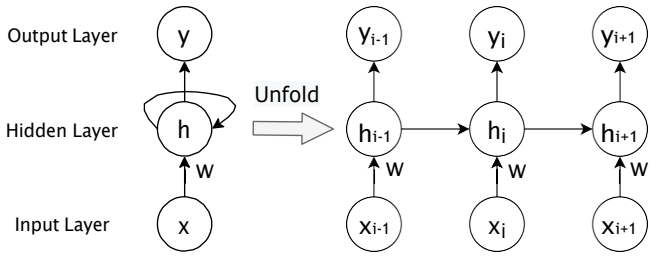

Fig. 3: Generic structure of RNN

2) Recurrent Neural Network(RNN): It is one of the popular networks which utilizes feedback connections in the hidden layers to enhance the learning speed. It receives feedback from nodes of preceding layers as well as from the node itself, as shown in figure 3. In addition, it maintains a small memory to store the state of its output which makes the training more manageable and reduces the probability of error. RNN is primarily applied for analyzing and classifying sequential data. Anyanwu et al. [23] introduced a framework using RNN for detecting intrusion in the communication network. Another IDS framework using RNN was proposed in [24] to detect the Denial of Service(DoS) attack.

3) Convolutional Neural Network (CNN): CNN diminishes the size of the input vector using various methods like pooling and filtering without losing the critical features, which are essential for significant classification. It is prevalent in the field of image processing [25]. The generic structure of CNN is depicted in figure 4. Potluri et al. [26] introduced an approach for the classification of malicious activities using CNN. The performance of the framework was evaluated on UNSW-NB 15 and NSL-KDD datasets. Similarly, Tran et al. [27] proposed CNN based HIDS to detect the malicious activities using the traces system calls; the feasibility and accuracy of the study were evaluated on datasets ADFA-LD and NGIDS-DS.

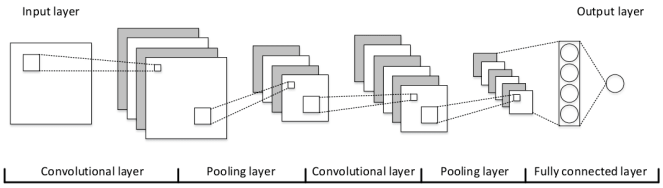

Fig. 4: Generic structure of CNN [28]

4) Deep Brief Network (DBN): It is required two stages as the supervised and unsupervised mode for training the complete model. Supervised learning is needed as preprocessing and unsupervised learning to tune the parameters. It contains hidden as well as visible layers as shown in figure 5. Zhao et al. [29] introduced a DBN based IDS framework to identify the intrusive network traffic. A detailed survey on DBN based security frameworks is provided in [30].

5) Autoencoder: It is an unsupervised DL algorithm and applies the encoder and the decoder to train the classifier. The encoder is utilized for encoding the raw data into a low-

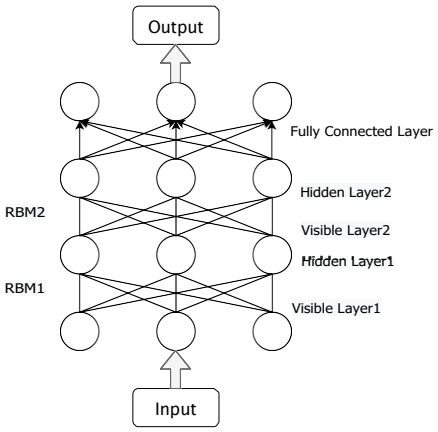

Fig. 5: Generic structure of DBN

dimensional representation. The decoder is used for reconstructing the input data as shown in figure 6. Farahnakian et al. [31] introduced a deep autoencoder based approach for identifying intrusive activities in a network. Likewise, Niyaz et al. [32] presented a network-based anomaly IDS using the autoencoder and softmax regression.

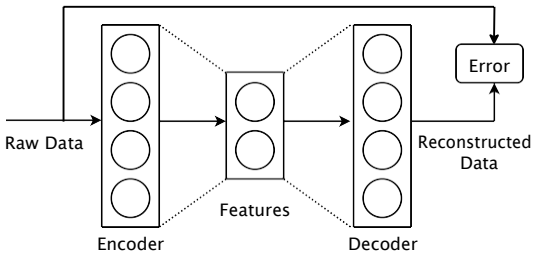

Fig. 6: Generic structure of Auto-encoder

6) Restricted Boltzmann Machine (RBM): It composes using some hidden and visible layers. The nodes in this approach are fully connected except the same layer. Figure 7 shows the structure of RBM. It is based on a stochastic graph model and follows the joint probability distribution over all layers [33]. Zhang presented a comprehensive view, detailed analyses, and future perspectives in [34].

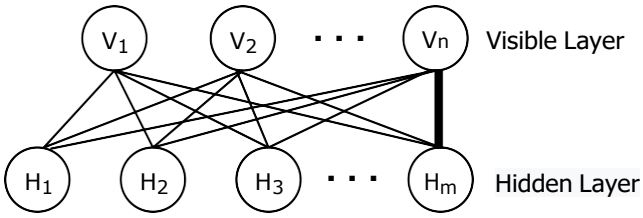

Fig. 7: Generic structure of RBM

7) Generative Adversarial Network (GAN): This DL approach is essential when the available training data is not evenly distributed. GAN is composed based on two modules (i)Generative, for generating the synthetic data and (ii)Discriminator, for separating actual data from synthetic

data. It is capable of training the model based on normal data only. Additionally, it is beneficial to apply in the area where insufficient or imbalanced training data is available. Salem et al. [35] introduced a host-based IDS using GAN with considerable classification accuracy. Similarly, Yan et al. [36] implemented a GAN based IDS to protect the network from Denial of Service attacks.

C. Comparative analyses of various DL approaches

There is a diversity in the DL approaches. As discussed earlier, the DL approaches are categorized into supervised and unsupervised as per the availability and nature of training data(labeled and unlabeled data) [28]. DL algorithms accept only suitable input data such as raw data or feature vectors as per their functions and requirements. The analyses and comparison of different DL algorithms their learning approaches, functions, suitable data types, and some recent studies are given in table I.

III. Anomaly based IDS using Deep Learning

A. Intrusion Detection System

An intrusion is to compromise or bypass the fundamental security policy components such as confidentiality, integrity, and availability of services or personal data. A secure system has to support security policies that provide data confidentiality to protect the information from unauthorized users. It requires integrity to furnish reliability and surety to deliver the original data to the end-user without alteration. It necessitates availability that can assure accessibility of the resources or information when needed. An Intrusion Detection System(IDS) plays a crucial role in such scenarios. IDS is used to analyze network traffic or system activities to detect malicious activities, system irregularities, vulnerability exploits and violations of the security policies mentioned above. An IDS is expected to do the following three tasks once the intrusion is identified. (i) Notify the respective authorities by triggering an alert [38] (ii) log the details of the detected anomaly [39] (iii) Perform a corrective task to mitigate the intrusion [9]. The hierarchy of IDS frameworks is depicted in figure 8.

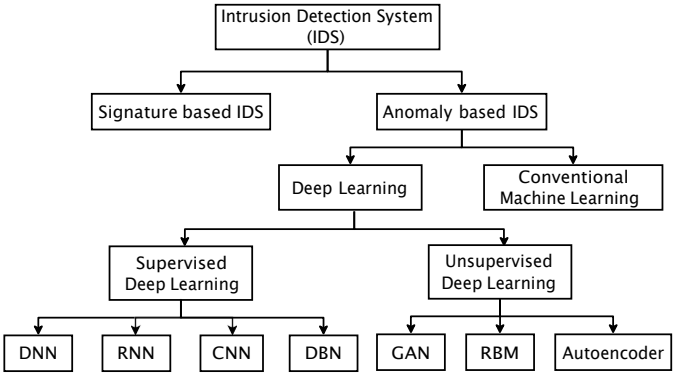

Fig. 8: Hierarchy of IDS frameworks.

B. Anomaly based IDS framework development using Deep Learning

Anomaly based IDS frameworks are applicable to identify the malicious and benign activity in the system. In line with this, a suitable dataset is a fundamental element to developing any Deep Leaning based IDS framework. Every field has various techniques, procedures, parameters, and forms of collecting the raw data as per their requirement. Likewise, the Anomaly based IDS frameworks include network traffic information, log files details, communication protocol or transaction time, etc. Therefore, data acquisition is the first and foremost step in the development of an Anomaly based IDS framework.

After data acquisition, the dataset is clean by nominal to numerical conversion, handling missing values and etc., to make it compatible with deep learning algorithms. Further, the unrelated and unimportant features are eliminated using data reduction techniques to decrease the data noise and training time and improve model accuracy. Three major strategies are used for feature reduction [40] (i) Data Reduction [41] (ii) Clustering [42] and (iii) Sampling [43].

Subsequently, the dataset is divided into the training and testing sub-datasets in an appropriate ratio. The training dataset is utilized for training the DL model. A small segment of training data, known as validation data, is also separated for tuning the model's parameters. The testing dataset is required for analyzing the overall accuracy of the trained model. After this preprocessing, a DL Algorithm is applied to the training dataset to build an IDS framework. If the results are not satisfactory, the model is retrained with a new set of hyperparameters. This process is repeated until the model is able to achieve satisfactory results. The model is finally evaluated on the Test(unseen) dataset to analyze its overall efficacy. The complete procedure of Anomaly based IDS framework development using Deep Learning is given in figure 9.

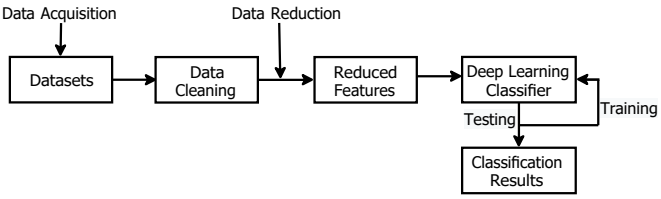

Fig. 9: Development of Anomaly based IDS framework development using Deep Learning

C. IDS Dataset

Performance evaluation is necessary for validating any IDS framework, and a dataset has a significant role in the performance evaluation. Due to the privacy issues, some datasets used in a commercial product are not available publicly [44]. However, few standard IDS datasets [30], such as NSL-KDD, DARPA-98, KDD-99, ADFA-LD/WD, etc., use widely as benchmarks datasets are available publicly. The

TABLE I: COMPARATIVE ANALYSES OF VARIOUS DEEP LEARNING APPROACHES.

Classifier	Learning Type	Suitable Data Types	Functions	References
Deep Neural Network	Supervised	Feature vectors	Feature extraction; Classification	[21]
Recurrent Neural Network	Supervised	Raw data; Feature vectors; Sequence data	Feature extraction; Classification	[23]
Convolutional Neural Network	Supervised	Raw data; Feature vectors; Matrices	Feature extraction; Classification	[26]
Deep Brief Network	Supervised	Feature vectors	Feature extraction; Classification	[37]
Autoencoder	Unsupervised	Raw data; Feature vectors	Feature extraction; Feature reduction; Denoising	[31]
Generative Adversarial Network	Unsupervised	Raw data; Feature vectors	Data augmentation; Adversarial training	[36]
Restricted Boltzmann Machine	Unsupervised	Feature vectors	Feature extraction; Feature reduction; Denoising	[34]

existing datasets assist the research community in analyzing and presenting a comparative study of the IDS frameworks. Some standard datasets use for Anomaly based IDS framework evaluation are provided in Table II.

TABLE II: COMPARISON OF DIFFERENT DATASETS (✔=True, ✘=False)

Dataset	Label data	Realistic Traffic	Full packet captured	Year
KDDCUP-99	✔	✔	✔	1999
DARPA-98	✔	✔	✔	1998
NSL-KDD	✔	✔	✔	2009
ISCX-2012	✔	✔	✔	2012
CICIDS-2017	✔	✔	✔	2017
ADFA-LD	✔	✔	✔	2014
Bot-IoT	✔	✔	✔	2018
ADFA-WD	✔	✔	✔	2014
CAIDA	✘	✔	✘	2007

IV. Research challenges and future directions

1) False alarm rate: Although the DL approaches have assisted in minimizing false alarm rates to a significant extent, there is still a space and requirement to lower the false alarm generation.

2) Real time response: A real-time response enhances the security level of a system. Thus, developing the IDS framework is required to provide a quicker, active, more accurate, and automatic response.

3) Data collection and measurement: Data is one of the essential supports of any research. However, there exists a lot of difficulties in collecting and making available quality data to researchers. DL is capable of noise excreting, feature reduction and processing big data. But still, there is a possibility to improve the data collection, processing, and managing methodologies.

4) Risk assessment: Good risk analysis and assessment of various aspects, perspectives, and constraints of any system, always leads to better results. IDS frameworks need more reliable methodologies and tools for optimal risk assessment to help in selecting appropriate algorithms and technology to enhance their performance.

5) Hardware failure: There is always a possibility of hardware failure. But the defence system should ensure continuous operation during such situations also.

Future Directions:

Intruders are evolving with distinct approaches to launch the attacks with the growth and easy access to the latest technology. An anomaly based IDS frameworks using DL methodologies provide the capabilities to effectively protects the system from various malicious activities. Additionally, most of the existing IDS frameworks have focused on improving accuracy. However, there is still a space to enhance the overall performance in future IDS frameworks design. Some of the future directions to improve the Anomaly based IDS frameworks are given as follows.

- Some well-known existing challenges such as raw and massive datasets can be handled using the appropriate deep learning technique [45].
- The false alarm rate of an IDS framework can be minimize using ensemble based deep learning approaches. Ensemble based learning [46] lessens the likelihood of producing incorrect results because it does not rely on the output of a single model but instead obtains the findings by integrating multiple models.
- Hardware failure can be targeted by adding early detection [47], auto fault repairability, bypassing or compensating the damaged components in IDS frameworks with a better risk assessment.

V. Conclusion

This paper has rendered a detailed analysis of Anomaly based IDS frameworks using Deep Learning techniques along with their significant requirements. Several Deep Learning algorithms and their comparison based on different characteristics are thoroughly analyzed. The classification of IDS and its general development procedure using the Deep Learning technique has been presented to give an insight into information security. Additionally, a variety of IDS datasets have been reviewed and critiqued based on different parameters to provide an overview of publicly available datasets. Finally, this paper has also ascertained the major limitations and viable future directions to improve the Anomaly based IDS frameworks.

References

[1] Y. Zhang, C. Xu, H. Li, K. Yang, N. Cheng, and X. S. Shen, "Protect: efficient password-based threshold single-sign-on authentication for mobile users against perpetual leakage," *IEEE Transactions on Mobile Computing*, 2020.

[2] E. Thambiraja, G. Ramesh, and D. R. Umarani, "A survey on various most common encryption techniques," *International journal of advanced research in computer science and software engineering*, vol. 2, no. 7, 2012.

[3] A. Hanamsagar, N. Jane, B. Borate, A. Wasvand, and S. Darade, "Firewall anomaly management: a survey," *International Journal of Computer Applications*, vol. 105, no. 18, 2014.

[4] S. Axelsson, "Intrusion detection systems: A survey and taxonomy," Technical report, Tech. Rep., 2000.

[5] D. S. Berman, A. L. Buczak, J. S. Chavis, and C. L. Corbett, "A survey of deep learning methods for cyber security," *Information*, vol. 10, no. 4, p. 122, 2019.

[6] C. Yin, Y. Zhu, J. Fei, and X. He, "A deep learning approach for intrusion detection using recurrent neural networks," *IEEE Access*, vol. 5, pp. 21 954–21 961, 2017.

[7] V. Kumar and O. P. Sangwan, "Signature based intrusion detection system using snort," *International Journal of Computer Applications & Information Technology*, vol. 1, no. 3, pp. 35–41, 2012.

[8] V. Jyothsna, V. R. Prasad, and K. M. Prasad, "A review of anomaly based intrusion detection systems," *International Journal of Computer Applications*, vol. 28, no. 7, pp. 26–35, 2011.

[9] H.-J. Liao, C.-H. R. Lin, Y.-C. Lin, and K.-Y. Tung, "Intrusion detection system: A comprehensive review," *Journal of Network and Computer Applications*, vol. 36, no. 1, pp. 16–24, 2013.

[10] S. Aljawarneh, M. Aldwairi, and M. B. Yassein, "Anomaly-based intrusion detection system through feature selection analysis and building hybrid efficient model," *Journal of Computational Science*, vol. 25, pp. 152–160, 2018.

[11] M. Gyanchandani, J. Rana, and R. Yadav, "Taxonomy of anomaly based intrusion detection system: a review," *International Journal of Scientific and Research Publications*, vol. 2, no. 12, pp. 1–13, 2012.

[12] B. Alejandro, "Correa," *Building ai applications using deep learning, URL: https://blog.easysol.net/wp-content/uploads/2017/06/image1.png*, 2016.

[13] S. K. Wagh, V. K. Pachghare, and S. R. Kolhe, "Survey on intrusion detection system using machine learning techniques," *International Journal of Computer Applications*, vol. 78, no. 16, 2013.

[14] Y. Kumar and B. Subba, "A lightweight machine learning based security framework for detecting phishing attacks," in *2021 International Conference on COMmunication Systems NETworkS (COMSNETS)*, 2021, pp. 184–188.

[15] R. Chalapathy and S. Chawla, "Deep learning for anomaly detection: A survey," *arXiv preprint arXiv:1901.03407*, 2019.

[16] N. Shone, T. N. Ngoc, V. D. Phai, and Q. Shi, "A deep learning approach to network intrusion detection," *IEEE Transactions on Emerging Topics in Computational Intelligence*, vol. 2, no. 1, pp. 41–50, 2018.

[17] W. S. McCulloch and W. Pitts, "A logical calculus of the ideas immanent in nervous activity," *The bulletin of mathematical biophysics*, vol. 5, no. 4, pp. 115–133, 1943.

[18] G. E. Hinton, S. Osindero, and Y.-W. Teh, "A fast learning algorithm for deep belief nets," *Neural computation*, vol. 18, no. 7, pp. 1527–1554, 2006.

[19] D. E. Rumelhart, G. E. Hinton, and R. J. Williams, "Learning representations by back-propagating errors," *nature*, vol. 323, no. 6088, pp. 533–536, 1986.

[20] W. G. Hatcher and W. Yu, "A survey of deep learning: Platforms, applications and emerging research trends," *IEEE Access*, vol. 6, pp. 24 411–24 432, 2018.

[21] S. Potluri and C. Diedrich, "Accelerated deep neural networks for enhanced intrusion detection system," in *2016 IEEE 21st international conference on emerging technologies and factory automation (ETFA)*. IEEE, 2016, pp. 1–8.

[22] K. Farhana, M. Rahman, M. Ahmed *et al.*, "An intrusion detection system for packet and flow based networks using deep neural network approach." *International Journal of Electrical & Computer Engineering (2088-8708)*, vol. 10, no. 5, 2020.

[23] L. O. Anyanwu, J. Keengwe, and G. A. Arome, "Scalable intrusion detection with recurrent neural networks," in *2010 Seventh International Conference on Information Technology: New Generations*, 2010, pp. 919–923.

[24] R. SaiSindhuTheja and G. K. Shyam, "An efficient metaheuristic algorithm based feature selection and recurrent neural network for dos attack detection in cloud computing environment," *Applied Soft Computing*, vol. 100, p. 106997, 2021.

[25] T. Agrawal and P. Choudhary, "Focuscovid: automated covid-19 detection using deep learning with chest x-ray images," *Evolving Systems*, pp. 1–15, 2021.

[26] S. Potluri, S. Ahmed, and C. Diedrich, "Convolutional neural networks for multi-class intrusion detection system," in *International Conference on Mining Intelligence and Knowledge Exploration*. Springer, 2018, pp. 225–238.

[27] N. N. Tran, R. Sarker, and J. Hu, "An approach for host-based intrusion detection system design using convolutional neural network," in *International Conference on Mobile Networks and Management*. Springer, 2017, pp. 116–126.

[28] H. Liu and B. Lang, "Machine learning and deep learning methods for intrusion detection systems: A survey," *Applied Sciences*, vol. 9, no. 20, p. 4396, 2019.

[29] G. Zhao, C. Zhang, and L. Zheng, "Intrusion detection using deep belief network and probabilistic neural network," in *2017 IEEE International Conference on Computational Science and Engineering (CSE) and IEEE International Conference on Embedded and Ubiquitous Computing (EUC)*, vol. 1, 2017, pp. 639–642.

[30] I. Sohn, "Deep belief network based intrusion detection techniques: A survey," *Expert Systems with Applications*, p. 114170, 2020.

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

[32] A. Javaid, Q. Niyaz, W. Sun, and M. Alam, "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)*, 2016, pp. 21–26.

[33] C. L. P. Chen, C. Zhang, L. Chen, and M. Gan, "Fuzzy restricted boltzmann machine for the enhancement of deep learning," *IEEE Transactions on Fuzzy Systems*, vol. 23, no. 6, pp. 2163–2173, 2015.

[34] N. Zhang, S. Ding, J. Zhang, and Y. Xue, "An overview on restricted boltzmann machines," *Neurocomputing*, vol. 275, pp. 1186–1199, 2018.

[35] M. Salem, S. Taheri, and J. S. Yuan, "Anomaly generation using generative adversarial networks in host-based intrusion detection," in *2018 9th IEEE Annual Ubiquitous Computing, Electronics Mobile Communication Conference (UEMCON)*, 2018, pp. 683–687.

[36] Q. Yan, M. Wang, W. Huang, X. Luo, and F. R. Yu, "Automatically synthesizing dos attack traces using generative adversarial networks," *International Journal of Machine Learning and Cybernetics*, vol. 10, no. 12, pp. 3387–3396, 2019.

[37] G. E. Hinton and R. R. Salakhutdinov, "Reducing the dimensionality of data with neural networks," *science*, vol. 313, no. 5786, pp. 504–507, 2006.

[38] I. Butun, S. D. Morgera, and R. Sankar, "A survey of intrusion detection systems in wireless sensor networks," *IEEE communications surveys & tutorials*, vol. 16, no. 1, pp. 266–282, 2013.

[39] B. Subba and P. Gupta, "A tfidfvectorizer and singular value decomposition based host intrusion detection system framework for detecting anomalous system processes," *Computers & Security*, vol. 100, p. 102084, 2021.

[40] D. Kshirsagar and S. Kumar, "An efficient feature reduction method for the detection of dos attack," *ICT Express*, 2021.

[41] S. S. Panwar and Y. Raiwani, "Data reduction techniques to anayze nsl-kdd dataset," *Int. J. Comput. Eng. Technol*, vol. 5, no. 10, pp. 21–31, 2014.

[42] A. K. Jain, "Data clustering: 50 years beyond k-means," *Pattern recognition letters*, vol. 31, no. 8, pp. 651–666, 2010.

[43] G. H. John and P. Langley, "Static versus dynamic sampling for data mining." in *KDD*, vol. 96, 1996, pp. 367–370.

[44] A. Khraisat, I. Gondal, P. Vamplew, and J. Kamruzzaman, "Survey of intrusion detection systems: techniques, datasets and challenges," *Cybersecurity*, vol. 2, no. 1, p. 20, 2019.

[45] Y. Wang, Y. Jiang, and J. Lan, "Fcnn: An efficient intrusion detection method based on raw network traffic," *Security and Communication Networks*, vol. 2021, 2021.

[46] S. Krishnaveni, S. Sivamohan, S. Sridhar, and S. Prabakaran, "Efficient feature selection and classification through ensemble method for network intrusion detection on cloud computing," *Cluster Computing*, pp. 1–19, 2021.

[47] A. Balakir, A. Yang, and E. Rosenbaum, "An interpretable predictive model for early detection of hardware failure," in *2020 IEEE International Reliability Physics Symposium (IRPS)*, 2020, pp. 1–5.