Deep Learning Methods for Anomaly Detection

Rajeev Subedi[1, a)] **Anil Kumar** [2, b)] **Narendra Kumar** [3, c)]

Author Affiliations
[1, 2, 3] *School of Computing, DIT University Dehradun, Uttarakhand, India*
Author Emails
[a)] *Corresponding author: 1000014411@dit.edu.in*
[b)]*dahiyaanil@yahoo.com*

[c)]*narendra298@gmail.com*

Abstract.

The invention and upgrading of systems and instruments that collect data at each point are narrowing the world. As a result, data is growing at an exponential rate. We are unable to process such a vast volume of information in a timely manner. The data comprises numbers that change over time, as well as other factors and functions that cause it to fluctuate suddenly. Anomaly is a term used to describe an abrupt change in data from its standard. The purpose of this survey is to present the deep learning approaches and the deep learning architectures with which we can detect anomalies. The review also presents the summarized view of the various approaches, techniques, datasets used to detect the anomalies in the studies done over the years. The prime goal of this paper is to summarize the various deep learning approach, architecture, and datasets with which we can detect anomalies.

Keywords. Anomaly, Outliers, Neural network, Deep learning, Auto encoder.

1. INTRODUCTION

The Anomalies are rapid changes in data from normal deviation into clusters. Anomaly detection is the process of analysing the data provided by machines or sets of machines to find abnormalities. Anomaly detection has recently had a big influence in areas including hospital monitoring systems, security, banking, IoT and sensor networks, marketing, and natural disasters. As a consequence, anomaly detection has been a popular research topic for decades, owing to its intrinsic complexity and tumultuous nature[1]. While traditional techniques of identifying anomalies have existed for a long time, deep learning emerged to outwit numerous learning tasks by learning complicated data using neural networks, which are computer representations of brain neurons. Many research methodologies are employed to build the most effective model that can identify irregularities with a reduced signal to noise ratio. The goal of such a model is to detect as many outlier clusters as possible while reducing risk. The necessity for new models that can evaluate enormous datasets was essential since previous approaches could not handle such quantities to create outliers. Traditional approaches failed to optimise time-series, picture, and sequential data due to their complicated structures[2]. Whereas a standard model relies on human feature selection

from a dataset, a model using deep learning outlier detection may learn graded discriminative features[2].

2. DIFFERENT DEEP LEARNING APPROACHES FOR ANOMALY DETECTION

2.1. Supervised anomaly detection

Separating training and test datasets is essential for supervised anomaly detection. Despite better efficiency and outcomes, semi-supervised and unsupervised techniques of anomaly detection were more reliable due to greater unlabeled training samples in the created dataset [2][3].

2.2. Unsupervised Anomaly Detection

Unsupervised deep learning anomalydetection builds and trains a model using an unclassified and uncategorized dataset[1]. A model evaluates unscaled datasets and predicts hidden patterns. It is explained in the study publication [2] that an unsupervised anomaly detection system is able to learn from the data and find anomalies by separating normal from abnormal data points.

2.3. Semi-Supervised Anomaly Detection

It is using both scaled and unscaled datasets to train a model is called hybrid learning[4][5].The scaled to unscaled data ratio is decreasing, indicating that less scaled data is used for training and more unscaled data is used for better outcomes [6].

3. DIFFERENT ARCHITECTURES IN DEEP LEARNING FOR ANOMALY DETECTION

3.1. Multi-layer Perceptron neural network

Multilayer perceptron (MLP) is a multiple layered feed-forward neural network[7], [8].

These activation functions[9] are represented as

$$y(v_i) = \tanh(v_i) \quad (3.1)$$

$$y(v_i) = (1 + e^{-vi})^{-1} \quad (3.2)$$

Here, back-propagation, popular supervised learning technique is used for training the dataset[9].

The multilayer perceptron neural network as given:

Let us consider d_j as the targeted value and y_j as the output value calculated by the perceptron algorithm. Now the error in one neuron is generated by:

$$e_j(n) = d_j(n) - y_j(n) \quad (3.3)$$

with which our error function is calculated by:

$$\varepsilon(n) = \frac{1}{2} \Sigma e_j^2(n) \quad (3.4)$$

Now apply the gradient descent, the value while updating the weights in each cycle is calculated by:

$$\Delta w_{ij}(n) = -\eta (d\varepsilon / dv_j) y_i(n) \quad (3.5)$$

3.2. Convolution Neural Network(CNN)

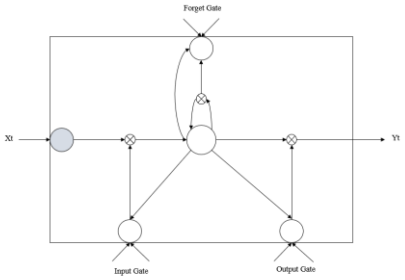
CNN prioritises the local dependencies in the input data gathered earlier in the process. Many engineers, academicians built CNN models using image datasets. A variety of methodologies and datasets have been used by other researchers to create the model [10]-[11].

3.3. Recurrent Neural Network

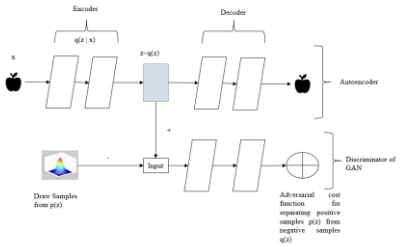
It is a type of advanced deep learning that operates by sending the hidden layer output back to the input layer, resulting in the prediction of that layer's output [14]. Unlike other neural networks, RNNs have an internal memory that allows them to perform the same function for each input.

3.4. Long Short-Term Memory

In Researchers developed the LSTM as a sophisticated RNN in the late 1990s and early 2000s[10]. The vanishing gradient issue in RNN happens when back-propagation is used to train a model [17]. LSTM is an efficient solution. Advanced recurrent neural network architecture that uses previously stored data to analyse and forecast abnormalities [15].



(a) LSTM network architecture[14]



(b) An architecture of adversarial autoencoder[19]

Figure 3.1 An architecture of LSTM Network and adversarial autoencoder

3.5 Adversarial Auto Encoder

Adversarial Autoencoder (AAE) is a promising strategy in deep learning to identify anomalies that may transform an autoencoder model into a generative adversarial network with the primary goal of minimising AE reconstruction error and mapping a prior to the hidden code vector[13].

3.6 Restricted Boltzmann Machine

It is a stochastic neural network controlled by energy principles and distinguished by variables such as entropy, energy, and temperature[16]. With applications ranging from feature extraction to filtering to pre-training neural networks to picture reconstruction [33-42], networks are increasingly becoming unsupervised learning machines. RBM is an

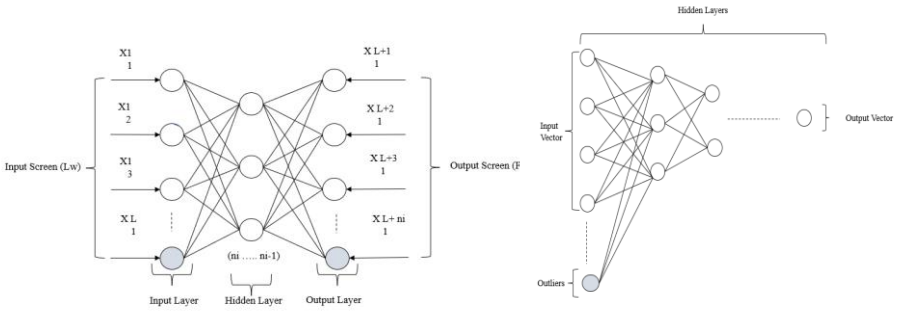
unsupervised learning technique with two layers: input and hidden. Because there is no output layer, the propagation entails returning the reconstruction to the input layer[15].

3.7 Generative Adversarial Networks

In order to simulate the large variety of distribution of complicated and multi-dimensional data, we need more sophisticated approaches, such as generative adversarial networks (GANs)[16],[17]. The primary flaw of GANs is that they are unstable to train and provide absurd outputs.

3.8 Deep Belief Networks

Deep Belief networks (DBNs)[18] are generative model for neural network that stack RBMs layer by layer and carry out the learning process.



(a) Multilayer perceptron network architecture[7] **(b)**Deep belief network architecture

Figure 3.3 Multilayer perceptron and Deep belief network architecture[21].

Above architecture of DBN shows us the combine structure of simple and hierarchical connected RBMs [19].

3.9 Autoencoder

The key objective of an autoencoder is to learn in an unsupervised manner interpretation of the dataset which can later be used to solve several real-life applications[20].Also, several variations of regularization techniques for autoencoders were studied in various case studies which includes Sparse Autoencoders[21]–[23],Denoising Autoencoders[24], [25] and Contractive Autoencoders[26].

3.10 Deep Neural Networks

Moreover, with these features DNNs is widely used for anomaly detection methods surpassing the effectiveness and accuracies of MLP, CNN, RNN, LSTM, RBM and LSTM and are being used as black boxes in a model with their dense non-linear structure[27], [28].

4. COMPARISON RESULTS

Supervised, semi-supervised and unsupervised approaches were presented in the paper reviewed throughout the research, but most importantly unsupervised learning approach is most desired for anomaly detection.Couple of more anomaly detection architecture based on LSTM[29], LSTM-SVM[30], CNN-LSTM[11], LSTM-RNN[32] and Stacked

LSTM[31] were observed where we could see various decision function and some methods are extremely good where maximum ratio of anomalies was detected whereas some were average.This research was conducted by making model to detect anomalies from normal patters using deep Auto-encoder and restricted Boltzmann machine which uses backpropagation by setting equal inputs, outputs and generate the results based on MSE, RMSE and AUC.Last but not the least, we observed Deep Auto-encoder (DAE) architecture [33]which elaborates the need of hybrid semi-supervised anomaly detection model which could minimize the complexity observed in dimensionality in high dimensional space for high-dimensional data.

5. CONCLUSION

This paper presents the Deep learning anomaly detection approach and methods along with the literature survey based on the approach, detection technique, architecture, datasets used, and result obtained. The prime goal of this paper was to summarize the various deep learning approach, architecture, and datasets with which we can detect anomalies. Another aspect of this research was to find the application areas within deep learning for which we can opt anomaly detection technique. Anomaly detection using deep learning technique is the major area of research and this paper could be useful for researchers in the field.

6. REFERENCES

1. G. Pang, C. Shen, L. Cao, and A. van den Hengel, ACM Computing Surveys 54, (2021).
2. R. Chalapathy and S. Chawla, (2019).
3. N. Görnitz NICOGOERNITZ, K. Rieck KONRADRIECK, and U. Brefeld, Toward Supervised Anomaly Detection Marius Kloft (2013).
4. B.R. Kiran, D.M. Thomas, and R. Parakkal, Journal of Imaging 4, (2018).
5. E. Min, J. Long, Q. Liu, J. Cui, Z. Cai, and J. Ma, in Lecture Notes in Computer Science (Including Subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics) (Springer Verlag, 2018), pp. 322–334.
6. P. Perera and V.M. Patel, IEEE Transactions on Image Processing 28, 5450 (2019).
7. G. Raman MR, N. Somu, and A.P. Mathur, International Journal of Critical Infrastructure Protection 31, (2020).
8. R. Collobert and S. Bengio, Links between Perceptrons, MLPs and SVMs (2004).
9. 9 T. Teoh, P. Ng, G. Chiew, E.J. Franco, and de Y. Goh, Anomaly Detection in Cyber Security Attacks on Networks Using MLP Deep Learning (n.d.).
10. A. Krizhevsky, I. Sutskever, and G.E. Hinton, Communications of the ACM 60, 84 (2017).
11. Y. Heryadi and H.L.H.S. Warnars, in 2017 IEEE International Conference on Cybernetics and Computational Intelligence, CyberneticsCOM 2017 - Proceedings (Institute of Electrical and Electronics Engineers Inc., 2018), pp. 84–89.
12. A. Dimokranitou, G. Tsechpenakis, J. Yu Zheng, and M. Tuceryan, STATEMENT OF THESIS APPROVAL (2017).
13. G.H. de Rosa, M. Roder, D.F.S. Santos, and K.A.P. Costa, International Journal of Information Technology (Singapore) 13, 49 (2021).
14. A. Pumsirirat and L. Yan, Credit Card Fraud Detection Using Deep Learning Based on Auto-Encoder and Restricted Boltzmann Machine (2018).

15. I.J. Goodfellow, J. Pouget-Abadie, M. Mirza, B. Xu, D. Warde-Farley, S. Ozair, A. Courville, and Y. Bengio, (2014).
16. A. Radford, L. Metz, and S. Chintala, (2015).
17. M.K. Sharma, D. Sheet, and P.K. Biswas, in ACM International Conference Proceeding Series (Association for Computing Machinery, 2016).
18. I. Kakanakova and S. Stoyanov, in ACM International Conference Proceeding Series (Association for Computing Machinery, 2017), pp. 73–79.
19. D. Bank, N. Koenigstein, and R. Giryes, (2020).
20. P. Malhotra, L. Vig, N. Gugulothu, and G. Shroff, Sparse Neural Networks for Anomaly Detection in High-Dimensional Time Series (2018).
21. M.R. Shahid, G. Blanc, Z. Zhang, and H. Debar, (2019).
22. J. Sun, X. Wang, N. Xiong, and J. Shao, IEEE Access 6, 33353 (2018).
23. J. Chen, J. Li, W. Chen, Y. Wang, and T. Jiang, Renewable Energy 147, 1469 (2020).
24. M.G. Narasimhan and S. Sowmya Kamath, Multimedia Tools and Applications 77, 13173 (2018).
25. S.F. Lokman, A.T. Othman, S. Musa, and M.H. Abu Bakar, in Advanced Structured Materials (Springer Verlag, 2019), pp. 195–205.
26. K. Amarasinghe, K. Kenney, and M. Manic, in Proceedings - 2018 11th International Conference on Human System Interaction, HSI 2018 (Institute of Electrical and Electronics Engineers Inc., 2018), pp. 311–317.
27. W. Samek, T. Wiegand, and K.-R. Müller, (2017).
28. G. Kim, H. Yi, J. Lee, Y. Paek, and S. Yoon, (2016).
29. T. Ergen and S.S. Kozat, IEEE Transactions on Neural Networks and Learning Systems 31, 3127 (2020).
30. P. Baldi, Autoencoders, Unsupervised Learning, and Deep Architectures (2012).
31. T.K. Dang, R. Wagner, J. Küng, N. Thoai, M. Takizawa, and E. Neuhold, editors , Future Data and Security Engineering (Springer International Publishing, Cham, 2016).
32. H. Song, Z. Jiang, A. Men, and B. Yang, Computational Intelligence and Neuroscience 2017, (2017).
33. N. Kumar, H. Shukla and R. Tripathi, International Journal Of Intelligent Engineering And Systems 10, (2017).
34. H. Shukla, N. Kumar and R. Tripathi, International Journal Of Computer Applications 95, (2014).
35. N. Kumar, A. Dahiya, K. Kumar and S. Tanwar, 2021 9Th International Conference On Reliability, Infocom Technologies And Optimization (Trends And Future Directions) (ICRITO) (2021).
36. K. Kumar, N. Kumar and R. Shah, International Journal Of Intelligent Networks 1, (2020).
37. N. Kumar, H. Shukla and R. Tripathi, International Journal Of Intelligent Engineering And Systems 10, (2017).
38. A. Sharma, N. Kumar, International Journal of Science and Research (IJSR) 3,(2014)
39. N. Kumar, H. Shukla, A. Tiwari and A. Dahiya, SSRN Electronic Journal (2019).
40. N. Kumar, H. Shukla and R. Tripathi, International Journal Of Intelligent Engineering And Systems 10, (2017).
41. N. Kumar, K. Kumar and A. Kumar, Sersc.Org (2020).
42. K. Kumar, R. Singh, P. Ranjan and N. Kumar, Algorithms For Intelligent Systems ((2021).

Biographies

Er. Rajeev Subedi received his bachelor's degree (B.Tech) in Computer Science & Engineering from Chandigarh University in 2019 and currently perusing M.Tech in Computer Science & Engineering from DIT University respectively. He is also working as an IT consultant in multiple schools and colleges in Nepalgunj, Nepal. His research areas include machine learning, deep learning, and cloud computing.

Dr. Anil Kumar is now employed at DIT University as a Professor of CSE,Head-Data Science Research Group and Accreditation Coordinator . Prof. Anil Kumar received his M.Tech. from the Delhi College of Engineering and his Ph.D. from the Manipal Group. He has over 24 years of teaching and working experience. He is an IEEE Senior Member and served on the Executive Committee of the IEEE Computer Society India Council in 2015 and 2016. His research interests include cryptography, image processing algorithms, artificial intelligence, neural systems, signal and system analysis, and genetic algorithms.

Dr. Narendra Kumar completed his M.Tech(Computer Science) from BIT Mesra Ranchi, and Ph.D.(Computer Science) from D.D.U Gorakhpur University. Narendra Kumar has more than 14 years' rich experience in Computer Science & Engineering field. He is working at DIT University as an Assistant Professor for the last 14 years, His research area includes image processing, Optimizations techniques and the internet of things and deep learning. Narendra is Editor of two books including publication like CRC Press, Taylor & Francis Group and Springer publication. He has published numerous research papers in international journals and conferences including Springer, IEEE, and Elsevier.