Hindusthan International Journal of Multidisciplinary Research (HIJOMR)
Volume 1 Issue 1, September 2024, pp.7-13

NEURAL NETWORK APPROACHES IN INTERNET OF THINGS

D.Mythili

Assistant Professor, Department of Computer Technology,
Hindusthan College of Arts & Science (Autonomous)
Coimbatore, India.
dmythilijayam@gmail.com

ABSTRACT

Security is the most challenging part of developing internet and network applications. The expertise of neural network - Deep Learning could be used to act on the weaknesses in the system, attacks, and incursions such as viruses, spamming, hacking, and attacks happening in the virtual environment to secure the data of a company. Machine learning, one of the subfields of artificial intelligence, is the source of deep learning. Deep learning provides better predictive value, more sophistication, and improves prediction over time. We can leverage all this data volume for training our machine learning algorithms. This paper reviews some IoT security challenges that deep learning solves.

Keywords: *Deep Learning, Encoding, Decoding, Neural Networks, Internet of Things Security.*

1. INTRODUCTION

Security in IoT is a generic term that applies to all measures, policies, instruments, and guidelines instituted in unison to counter unauthorized access to computing power, communications, applications, and data. This has existing cyber defense measures at the application, network, host, and data levels. Nowadays, there are intrusion prevention and identification systems, network firewalls, software for antivirus protection, and among many other solutions, working in isolation to prevent attacks and detect problems in security. As the number of systems connected to the Internet increases, so does the risk of incursion, along with the number of attacks. It is intended for readers who want to begin investigating deep learning for IoT security.

The rest of this paper is structured as follows: Section 2 provides an overview of Deep Learning in IoT Security. Section 3 provides a breakdown of several Deep Learning techniques applied in network security, and Section 4 finishes the article with a brief summary of the major points and additional concluding notes.

Deep learning is absolutely a much more recent activity, with its first computer implementation dating back to 2006 [1].In its simplest form, deep learning is a set of machine learning algorithms that aim to learn at multiple levels; each of them associated with a distinct degree of abstraction. The levels distinguish high-level concepts from weaker ones, and the same lower concepts also contribute to the definition of several higher-level perceptions [2]. The first few layers of the deep network handle feature extraction. There are three Deep Learning architectures: blended, supervised, and unsupervised. A Deep neural networks are networks that can learn new skills on its own. The same can be said for any

other algorithm in machine learning. Two recent advances in technology make it possible for the average person to build a DL model with relative ease. First, increasingly, access to GPUs is becoming ubiquitous; these provide much faster computation. The second benefit of a Deep Learning model's layers is that they can be trained apart from one another [3]. This implies that a massive model having millions of parameters can be optimized using far fewer resources in short, more manageable pieces.

This is what is depicted by Figure 1: Monitoring IoT devices that could provide a witty defense against novel or zero-day attackers. Technologies that are effective in data analysis to learn "regular" or "unusual" behavior about how IoT devices and their components interact with one another are machine learning and deep learning. The input data from each element of the IoT system can be gathered and analyzed in search of common trends or patterns of interaction that can help in spotting malignant behavior very early. To be successful and safe systems, IoT systems must move from just secure device-to-device connectivity towards integrating security-driven intelligence that is based on deep learning or machine learning technologies.

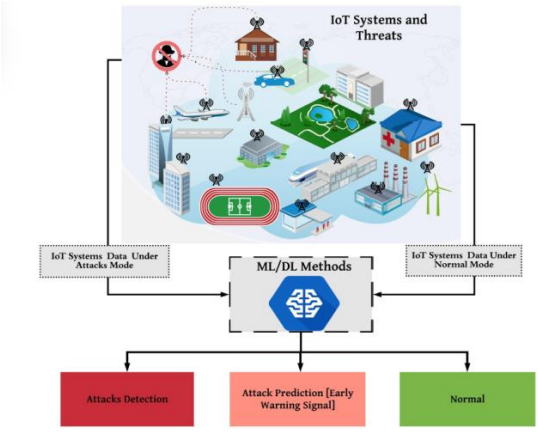


Figure1 : Deep Learning in IoT Industry

2. RELATED WORKS

Huseyin Ahmetoglu and ResulDas [4] addressed machine learning methods' approaches to identifying attacks. The segmentation, aggregation, analysis, and network flow features of threats linked to intrusion detection system were investigated. Techniques for analysing malware behaviours and Mobile malware detection were summarised by Naser Mahmood, Mohammad Jabed, and Morshed Chowdhury [5]. It combines several machine learning and deep learning algorithms for detecting behavior-based viruses. YadigarImamverdiyev and FarganaAbdullayeva [6] evaluated the datasets used to evaluate the performance of cyberattack detection systems proposed by researchers. For cyber security intrusion detection, the datasets used, and comparison research, a statistical analysis of articles published on cybersecurity with the use of DL over the years is performed. It specifically reviews intrusion detection systems based on deep learning methodologies. Because the dataset is important in intrusion detection, we describe 35 well-known cyber datasets and categorise them into seven categories: network traffic-based dataset, electrical

network-based dataset, internet traffic-based dataset, virtual private network-based dataset, android apps-based dataset, IoT traffic-based dataset, and internet-connected devices-based dataset. MuderAlmianilia and Abu ghazleh et al [7] provided a fully automated intrusion detection solution for Fog security from cyber-attacks. Multi-layered recurrent neural networks, which are intended to be used for Fog computing security close to end users and IoT devices, are used in the proposed model. Deep learning with cybersecurity is mostly discussed by Priyanka Dixit and Sanjay Silakari [8].Bhavuk Sharma [9] discussed the deep learning issues, challenges in Cyber security in broad manner. It explains how to face the issues raised when the malicious intervention occurred in IoT.

3. DEEP LEARNING METHODS USED IN IOT SECURITY

3.1 Deep Autoencoders

That means that some unsupervised neural network, an autoencoder, takes a vector as input and tries to make the output as similar to the original vector as possible. Taking the input, changing its dimensionality, and reconstructing the input allows making a higher or lower multidimensional representation of data. This will create a very flexible sort of neural network because it is trained using unsupervised learning of the compressed data encoding. Moreover, they can be pre-trained one layer at a time, which reduces the computing power needed for training a useful model. When the hidden levels have less dimensions than the input and output layers, the network is used for data encoding. As illustrated in Figure 2, by training an autoencoder to reconstruct the input from a noisy version of the input.However, as shown in Figure 2, an autoencoder could be created in order to be more robust and decrease noise [10]. It turned out that such an approach is more resistant and generalizable than the traditional auto-encoder approach.

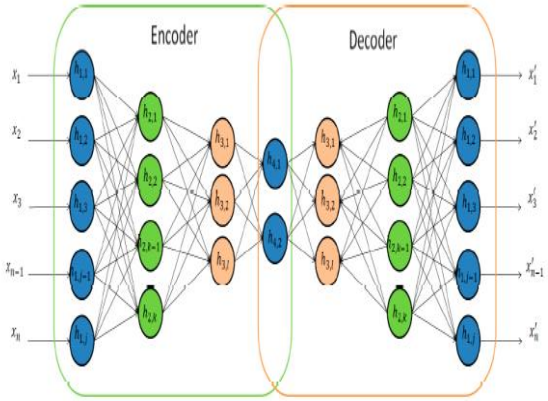


Figure 2: Autoencoder

3.2 Restricted Boltzmann Machines

DBNs are based on RBMs (Restricted Boltzmann Machines), themselves two-layer, bipartite, undirected graphical models – data can flow in both directions, rather than just one [11]. Like auto-encoders RBMs are taught unsupervisedly, one layer at a time. The top layer will be referred to as the input layer, and the lower layer as the hidden layer. There is

complete connectivity between all nodes in the input layer and all other nodes in the hidden. There are no intra-layer connections—that is, no connection between nodes in the same layer.

Usually, binary components could only exist in the input and hidden layers. Taking most of the math from statistical mechanics, the network is trained to minimize "energy," a function that measures the model's compatibility. Actually, the training of the model was aimed at finding the functions that would minimize the energy of the system—and thus the hidden state.

3.3 Recurrent Neural Network

A recurrent neural network is a neural network that, besides the usual function with fixed-length data inputs limited only to normal neural networks, is capable of dealing with variable-length input sequences. This is run by the RNN one at a time through the use of the output from the hidden unit as an additional input for the next element. Therefore, RNNs can not only deal with speech and language problems but also time series problems. Because the gradients can easily explode or vanish, RNNs are usually harder to train [12]. RNNs have been shown to be quite effective for time-series prediction applications relating to language translation, image captioning, speech recognition, and word prediction in phrases [13–16].

3.4 Convolutional Neural Networks

One of the types of neural networks working with input stored in arrays is a Convolutional Neural Network (CNN). Then, a simple example for the input will be a 2D array of pixels that portray a color or grayscale image. More often than not, CNNs are implemented for processing audio spectrograms and 2D picture arrays. Another quite common use for them is videos and volumetric images in 3D. Although less frequent, their use with one-dimensional (1D) arrays (signals) is increasing. CNNs are applied regardless of dimensionality anywhere there is temporal or spatial ordering. A CNN includes three different types of layers as building blocks of its architecture, as seen in Figure 3: the convolution layers, the pooling layers, and the classification layer.

The real core of any CNN is its convolutional layers. Here, the weighted convolution kernel, otherwise known as the receptive field, views the original input one small window at a time. This basically applies these filters across the whole input to create what is called a feature map and then passes it through a non-linearity, most frequently a ReLU. These convolutional kernels, named so for the mathematical convolution process, allow accounting for close physical or temporal relationships within the data by using the same kernel all over an image. This assists in memory conservation.

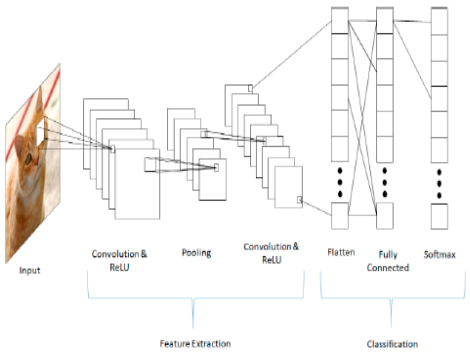
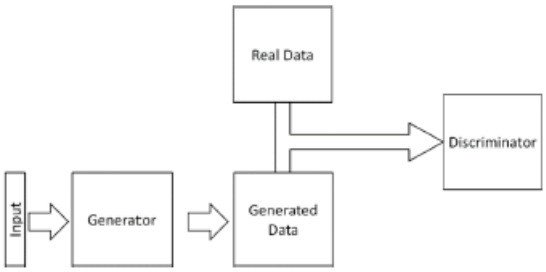


Figure 3*:* Convolutional Neural Network

3.5 Generative Adversarial Networks

Basically, GANs involve setting up a game between two neural networks in a zero-sum scenario. This design of a neural network applies to unsupervised machine learning. As designed by Goodfellow et al., one network is a generator and the other is a discriminator. It takes in input data and produces output data, generating output that is identical to the source data on attributes. The discriminator tries to find distinctions between real input and fake generated input to make an authentic-fraudulent decision. Then, after training, a generator can generate new data that isn't far from other data.



Since their inception, GANs have had numerous applications, most of them image-related. This includes optical flow estimation, caption generation, and image enhancement. There is even an open-sourced pre-trained GAN for image generation available on Facebook, under the name of DCGAN, or deep convolution generative adversarial network.

4. CONCLUSION

With the increasing pace of cyber network attacks, which seems to be getting ahead in comparison with the ability of cyber defenders to generate and deploy new signatures that identify emerging threats, there is a good opportunity for detecting new malware variants and zero-day attacks using deep learning techniques based on neural networks in cyber security apps.In this survey article, we focus on the application of deep learning techniques against various types of cyber security vulnerabilities that target data, networks, host systems, and application software. We have also presented a detailed review of the Deep Learning techniques used earlier to identify such forms of online threats.

Current techniques treat these different types of assaults separately. Future research should investigate how malignant behaviors propagate through an attack lifecycle

REFERENCES

[1] WickramasingheC.S., Marino, D.L. Amarasinghe, K. Manic M , “Generalization of Deep Learning forCyber-Physical System Security: A Survey”, In Proceedings of the IECON 2018-44th Annual Conference ofthe IEEE Industrial Electronics Society,Washington, DC, USA, 21–23 October 2018; pp. 745–751.

[2] Deng L, Yu D, “Deep learning: Methods and applications. Found. Trends Signal Process.”, 2014, 7, 197–387.

[3] Hinton G, OsinderoS,Teh Y.W “A fast learning algorithm for deep belief nets”, Neural Comput. 2006, 18,1527–1554.

[4] HuseyinAhmetoglu , ResulDas “A comprehensive review on detection of cyber-attacks: Data sets, methods, challenges, and future research directions”, Internet of Things , Volume 20, November 2022, 100615.

[5] Pascal, Maniriho, Abdun NaserMahmood,, Mohammad Jabed , MorshedChowdhury, "A study on malicious software behaviour analysis and detection techniques: Taxonomy, current trends and challenges ", Future Generation Computer Systems", Volume 130, May 2022, Pages 1-18.

[6] YadigarImamverdiyev, FarganaAbdullayeva , " Deep Learning in Cybersecurity: Challenges and Approaches",International Journal of Cyber Warfare and Terrorism (IJCWT) 10(2):82-105 , Volume 50, February 2020, 102419.

[7] MuderAlmiani,AliaAbuGhazlehAmerAl-RahayfehSaleh, AtiewiAbdulRazaque "Deep recurrent neural network for IoT intrusion detection system", Simulation Modelling Practice and Theory , Volume 101, May 2020, 102031.

[8] PriyankaDixit, SanjaySilakari , "Deep Learning Algorithms for Cybersecurity Applications: A Technological and Status Review",Computer Science Review , Volume 39, February 2021, 100317.

[9] Bhavuk Sharma, Dr Ramchandra Mangrulkar"Deep Learning Applications In Cyber Security: A Comprehensive Review, Challenges And Prospects" , International Journal of Engineering Applied Sciences and Technology, 2019 , Vol. 4, Issue 8, ISSN No. 2455-2143, Pages 148-159 , December 2019.

[10] Vincent P, Larochelle H , Lajoie I ,Bengio, Y, Manzagol P.A. "Stacked denoising autoencoders: Learning useful representations in a deep network with a local denoising criterion", J. Mach. Learn. Res. 2010, 11, 3371–3408.

[11] Jarrett, K ,Kavukcuoglu K ,LeCunY " What is the best multi-stage architecture for object recognition" , In Proceedings of the 2009 IEEE 12th International Conference on Computer Vision, Kyoto, Japan, 29 September–2 October 2009; pp. 2146–2153.

[12] BengioY , Simard P ,Frascon iP "Learning long - term dependencies with gradient descent is difficult ", . IEEETrans. Neural Netw. 1994, 5, 157–166.

[13] SutskeverI ,Vinyals O , Le Q.V. "Sequence to sequence learning with neural networks in Advances in Neural Information Processing Systems"; MIT Press: Cambridge, MA, USA, 2014; pp. 3104–3112.

[14] Cho K , van Merriënboer B, Gulcehre C ,Bahdanau D ,BougaresF,SchwenkH,Bengio Y "Learningphrase representations using RNN encoder-decoder for statistical machine translation", 2014,1406.1078.

[15] BahdanauD , Cho K ,BengioY "Neural machine translation by jointly learning to align and translate", 2014, arXiv:1409.0473.

[16] GravesA ,MohamedA.R , Hinton G , " Speech recognition with deep recurrent neural networks ", In Proceedings of the 2013 IEEE International Conference Acoustics, Speech and Signal Processing (ICASSP),Vancouver, BC, Canada, 26–31 May 2013; pp. 6645–6649.

[17] LeCunY ,Boser B.E , Denker J.S , Henderson D , Howard R.E. , HubbardW.E ,Jackel, L.D. " Handwrittendigit recognition with a back-propagation network ", In Advances in Neural Information Processing Systems; MITPress: Cambridge, MA, USA, 1990; pp. 396–404.

[18] LeCunY ,Bottou L ,Bengi Y, Haffner P "Gradient-based learning applied to document recognition " ,Proc. IEEE 1998, 86, 2278–2324.

[19] GoodfellowI ,Pouget-AbadieJ , Mirza M , XuB ,Warde-Farley D ,Ozair S, CourvilleA,Bengio, Y "Generative adversarial nets. In Advances in Neural Information Processing Systems; MIT Press: Cambridge ", MA, USA, 2014; pp. 2672–2680.

[20] LedigC Theis, L HuszárF , Caballero J, CunninghamA , AcostaA, AitkenA,Tejan A,Totz J, Wang Z et al. "Photo-realistic single image super-resolution using a generative adversarial network " arXiv2016, arXiv:1609.04802.
[21] Reed S A kata Z ,Y and X ,LogeswaranL , Schiele B, Lee H. " Generative adversarial text to image synthesis " arXiv 2016, arXiv:1605.05396.
[22] Dosovitskiy A , Fischer P, IlgE ,HausserP, Hazirbas C ,Golkov V, van der Smagt P , CremersD, Brox TFlownet "Learning optical flow with convolutional networks ", In Proceedings of the 2015 IEEEInternational Conference on Computer Vision (ICCV), Santiago, Chile, 7–13 December 2015; pp. 2758–2766.
[23] Radford A , Metz L ,Chintala S " Unsupervised representation learning with deep convolutional generativeadversarial networks", arXiv 2015, arXiv:1511.06434.

AUTHOR PROFILE:

Mrs.Mythili D is Assistant Professor of the Department of Computer Technology with 15+ years of experience in Hindusthan College of Arts & Science. She has published papers in various Journals and Conferences. She holds the patent on IoT. Apart from Teaching, she trained IT Professionals with recent technologies. She serves as Reviewer in IEEE Conference. Her spheres of interest are centered on Big Data Analytics, Wireless Sensor Networks, Data Visualization. She is passionate about exploring new paradigms of Teaching as well as Learning. She has received the Best Faculty Awards.