**Available Online at www.ijcsmc.com**

**International Journal of Computer Science and Mobile Computing**

**A Monthly Journal of Computer Science and Information Technology**

**ISSN 2320–088X**
**IMPACT FACTOR: 6.199**

***IJCSMC, Vol. 9, Issue. 1, January 2020, pg.150 – 155***

# Detecting Intruders in the Web Using CNN RNN Algorithms in Deep Learning

**[1]R.Ramya; [2]M.Pearline Joy Kiruba; [2]A.Lathika; [2]P.Grupsgaya; [2]N.Deepa**
[1]Assistant Professor, Department of CSE, VSBCETC, Coimbatore, India
[2]UG Scholar, Department of CSE, VSBCETC, Coimbatore, India
[1] ramyarangasamycse@gmail.com, [2] pearlinejoykiruba84@gmail.com, [2] lathikatara@gmail.com, [2] grupsgaya@gmail.com, [2] deepanatarajan1999217@gmail.com

***Abstract- Cyber security is more important in many fields such as government, military etc., because the government, military, corporate, financial and medical organizations collect process and store unprecedented amounts of data on computers and other devices. A significant portion of that data can be sensitive information whether that be intellectual, financial data, personal information or other types of data for which unauthorized access or exposure could have negative consequences. In our approach is we can find the attack types using in deep learning methods. In this paper we develop a desktop application which identifies the attack occurred in the web application and sends a notification to the web server system.***
***Keywords- Deep learning, Neural Networks, CNN, RNN, Cyber attack***

## I. Introduction

Deep Learning relies on a multi-layered representation of the input data and can perform feature selection autonomously through a process defined representation learning. DL approaches can be further classified by differentiating between supervised and unsupervised algorithms. A large and representative set of data are required in former techniques that have been previously classified by a human expert or through other means. The latter approaches do not require a pre-labeled training dataset. Deep Neural Networks (DNN), are large neural networks organized in many layers capable of autonomous representation learning and all DL algorithms are based on DNN. Supervised DL algorithms Fully-connected Feed forward Deep Neural Networks (FNN). FNN are a variant of DNN where every neuron is connected to all the neurons in the previous layer. FNN do not make any assumption on the input data and provide a flexible and general-purpose solution for classification, at the expense of high computational costs. Convolutional Feed forward Deep Neural Networks (CNN). Each neuron receives its input only from a subset of neurons of the previous layer and CNN are a variant of DNN. This characteristic makes CNN effective at analysing spatial data, but their performance decreases when applied to non-spatial data. CNN have a lower computation cost than FNN. Recurrent Deep Neural Networks (RNN). A variant of DNN whose neurons can send their output also to previous layers; this design makes them harder to train than FNN. FNN excel as sequence generators, especially their recent variant, the long short-term memory. Unsupervised DL algorithms Deep Belief Networks (DBN). They are modeled through a composition of Restricted Boltzmann Machines (RBM), a class of neural networks with no output layer. DBN excel in the function of feature extraction so they can be used for pre-training

tasks. DBN require a training phase with unlabelled datasets. Stacked Auto encoders (SAE). They are composed by multiple Auto encoders, a class of neural networks where the number of input and output neurons is the same. SAE achieve better results on small datasets and excel in pre-training tasks similar to DBN. Convolutional neural networks (CNNs) among both cases, have shown better performances compared to other classifiers. For instance, the CNN proposed by Salamon and Bello [9] outperforms their prior approach based on unsupervised feature learning and random forest [5] on the UrbanSound8K dataset. Also, for ESC-10 and ESC-50 datasets, a 1D CNN with eight convolution layers (Sound Net) [10] outperforms random forest [6], SVM using Mel Frequency Cepstral Coefficients (MFCCs) [6], and convolutional auto encoders [10]. In addition to these CNNs, other DNN architectures such as AlexNet and GoogLeNet, which have shown remarkable performances on image classification tasks (e.g. ImageNet dataset) have also been used for environmental sound classification. Interestingly, these two CNNs trained on spectrograms have been achieving the highest recognition performance for the three aforementioned datasets as reported by Boddapati et al. [11].

This paper is organized as follows. Section II introduces general cyber attacks and describe the most important ones. In this section we also present the cyber attacks that may affect web applications. Section III presents the main cyber attacks in web applications. Section IV presents the proposed approach that aims of achieving good classification and web based cyber attacks. The conclusion is presented in the last section.

## II. Cyber Attacks

An attack is any attempt to expose, alter, modify, disable, enable, destroy, steal or gain unauthorized access to or make unauthorized use of data in computers and computer networks. A cyber attack is any type of attack which targets computer information systems, infrastructures, computer networks, or personal computer devices. A person or process that attempts to access data, functions or other restricted areas of the system without authorization, potentially with malicious intent are the attackers. Depending upon context, cyber attacks can be classified as cyber warfare or cyber terrorism. A cyber attack can be done by sovereign states, individuals, groups, society or organizations, and it may come from an anonymous source.

A cyber attack may steal, alter, or destroy a specified target by hacking into a susceptible system. Cyber attacks can range from installing spyware on a private computer to attempting to destroy the infrastructure of entire nations. Legal experts are seeking to limit the utilization of the term to incidents causing physical damage, distinguishing it from the more routine data breaches and broader hacking activities. Cyber attacks have become increasingly sophisticated and dangerous. User behavior analytics and SIEM are often wont to help prevent these attacks. A cyber attack is an assault launched by cyber criminals using one or more computers against one or multiple computers or networks. A cyber attack can maliciously disable computers, steal data, or use a breached computer as a launch point for other attacks.

Cyber warfare utilizes techniques of defending and attacking information and computer networks that inhabit cyberspace, often through a protracted cyber campaign or series of related campaigns. It denies an opponent's ability to try to an equivalent , while employing technological instruments of war to attack an opponent's critical computer systems. Cyber terrorism, on the opposite hand, is "the use of network tools to pack up critical national infrastructures (such as energy, transportation, government operations) or to coerce or intimidate a government or civilian population". That means the top results of both cyber warfare and cyber terrorism is that the same, to wreck critical infrastructures and computer systems linked together within the confines of cyberspace.

Cyber criminals-An individual or group of people who use technology to commit cybercrime with the aim or goal of stealing sensitive company information or personal data and generating profits are called as cybercriminals. In today's, they're the foremost prominent and most active sort of attacker.
Cybercriminals use computers in three wide ways to do cybercrimes-
*Select computer as their target*- Virus are spreaded, data theft, identity theft etc. are done by the cybercriminals and using that they attack the people's computer.
*Using the computer as their weapon*-Computer is used as a weapon to do conventional crime such as illegal gambling, spam, fraud, etc.
*Using the computer as their accessory*- In this, computers are used to steal data illegally. **Hacktivists**- Hacktivists are individuals or groups of hackers who perform malicious activity to market a political agenda, religion, or social ideology. According to Dan

Lohrmann, chief security officer for Security Mentor, a national security training firm that works with states said "Hacktivism may be a digital disobedience. It's hacking for a cause." Hacktivists aren't like cybercriminals who hack computer networks to steal data for the cash. They are individuals or groups of hackers who work together and see themselves as fighting injustice.

*State-sponsored Attacker*- State-sponsored attackers have particular objectives aligned with either the political, commercial or military interests of their country of origin. These sort of attackers aren't during a hurry. The government organizations have highly skilled hackers and concentrate on detecting vulnerabilities and exploiting these before the holes are patched. It is very challenging to defeat these attackers thanks to the vast resources at their disposal.

*Insider Threats*-The insider threat may be a threat to an organization's security or data that comes from within. These type of threats are usually occurred from employees or former employees, but may also arise from third parties, including contractors, temporary workers, employees or customers.

*Malicious*- The organization's data, IT infrastructure or systems are harmed potentially by an insider. The insider access those data. The ex-employees or dissatisfied employees does this type of malicious attacks. They believe that organization is not favor to them and does wrong to them in some way, so they try to take revenge on the organization. Malicious outsiders, either financial incentives or extortion may also change the insiders to become a threat.

*Accidental*- Insider employees does this type of attacks accidently. In this type of threats, any important file may be deleted accidently or inadvertently share confidential data with a business partner against company's policy or legal requirements.

*Negligent*- These are the threats during which employees attempt to avoid the policies of a corporation put in situ to guard endpoints and valuable data. For example, if the organization have strict policies for external file sharing, employees might try to share work on public cloud applications so that they can work at home.

## III. Algorithms

*I.* *Recurrent Neural Network(RNN)* -The input to the current step is the output from the previous step in this type of neural network. The inputs and outputs from previous steps are independent of each other in traditional neural network and it is fed to the next step as input. To go for next word, all input and output must be independent to each other. The previous words are to be remembered every time and it is required. The RNN solved this problem with the help of hidden layer. Hidden state is the important feature of RNN. Hidden layer always remembers information in the sequence. Thus, it exhibits temporal dynamic behaviour. Sequence of inputs of variable length are processed by RNN using their internal state unlike feed forward neural network. They are used in unsegmented, connected handwriting recognition or speech recognition.

The two broad classes of networks with a similar general structure is referred using the term "recurrent neural network" , where one is infinite impulse and the other one is infinite impulse. Temporal dynamic behavior is exhibited by both classes of network. A finite impulse recurrent network is a directed acyclic graph that can be unrolled and replaced with a strictly feedforward neural network replaces the finite impulse recurrent network which is a directed acyclic grapg, while an infinite impulse recurrent network is a directed cyclic graph that can not be unrolled.

Finite impulse and infinite impulse recurrent networks can have additional stored state, and the neural network directly controls the storage . If that incorporates time delays or has feedback, another network or graph can replace the storage. Such controlled states are referred to as gated state or gated memory, and are part of long short-term memory networks (LSTMs) and gated recurrent units. This is also called Feedback Neural Network.

*II.* *Convolution Neural Network*-The concept of Neural Network is known by the reader by assumption. Artificial Neural Networks in machine learning performs really well. Artificial Neural Networks are used in multiple applications and tasks like image, audio, words. For different purposes different types of neural networks are used. For example, for predicting the sequence of words can be predicted using Recurrent Neural Networks more precisely an LSTM, Convolution Neural Network is used for image classification. Some concepts of Neural Network must be revisited before going for CNN's classification. Three types of layers in regular neural network follows**:**

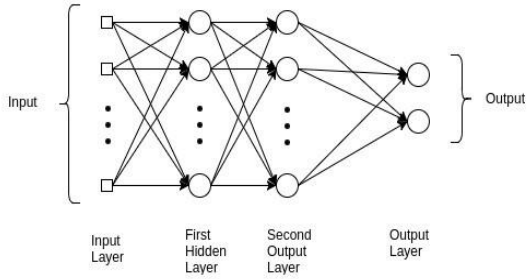
*A.* *Input Layers:* It's the layer in which we give input to our model is given in this layer. Total number of features in our data (number of pixels in case of an image) is equal to the number of neurons in the input layer.

*B.* *Hidden Layer:* The input from Input layer is then given to the hidden layer. There are many hidden layers which depends upon our model and data size. Different numbers of neurons are enrolled in each hidden layer which are generally greater than the number of features. Matrix multiplication is used to compute the output of each layer and output of the previous

layer with learnable weights of that layer and then by addition of learnable biases followed by activation function which makes the network nonlinear.

*C. Output Layer:* The output from the hidden layer is given to a logistic function. The logistic functions are similar to sigmoid or soft max. They convert the output of each class into probability score of each class.



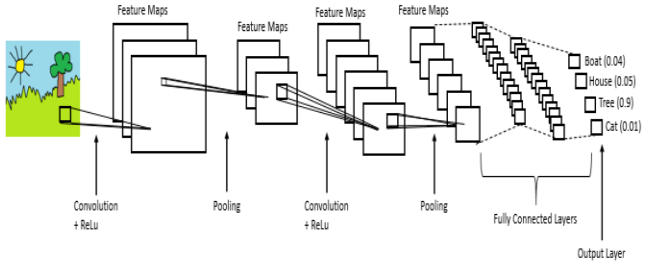

Output from each layer is obtained and the data is then given into the model and output from each layer is obtained this step is called feed forward, then an error function is used to calculate the error, some common error functions are cross entropy, square loss error etc. After that, derivatives are calculated and propagated back to the model again. This step is known as Back propagation which is basically used to minimize the loss. Bit of mathematics which is involved in the whole convolution process are discussed here.

*D. Convolution layers* consist of a set of learnable filters (patch in the above image). Every filter has small width and height and the same depth as that of input volume (3 if the input layer is image input).
For example, if we have to run convolution on an image with dimension 34x34x3. Possible size of filters can be axax3, where 'a' can be 3, 5, 7, etc but small as compared to image dimension.
During forward pass, we slide each filter across the whole input volume step by step where each step is called stride (which can have value 2 or 3 or even 4 for high dimensional images) and compute the dot product between the weights of filters and patch from input volume.
As we slide our filters we'll get a 2-D output for each filter and we'll stack them together and as a result, we'll get output volume having a depth equal to the number of filters. The network will learn all the filters.

*E. Layers used to build CovNets*
A covnets is a sequence of layers, and every layer transforms one volume to another through differentiable function.
Types of layers follows :

Let's take an example by running a covnets on of image of dimension 32 x 32 x 3.

1) *Input Layer:* The raw input of image with width 32, height 32 is holded in this layer.




2) *Convolution Layer:* The output volume is computed in this layer by computing dot product between all filters and image patch. Suppose we use total 12 filters for this layer we'll get output volume of dimension 32 x 32 x 12.

3) *Activation Function Layer:* Element wise activation function is applied to the output of convolution layer by activation function layer. Some common activation functions are RELU: max(0, x), Sigmoid: 1/(1+e^-x), Tanh, Leaky RELU, etc. The volume remains unchanged hence output volume will have dimension 32 x 32 x 12.
4) *Pool Layer:* This layer is periodically inserted in the covnets and its main function is to reduce the size of volume which makes the computation fast reduces memory and also prevents from over fitting. Two common types of pooling layers are **max pooling** and **average pooling**. If we use a max pool with 2 x 2 filters and stride 2, the resultant volume will be of dimension 16x16x12.
5) *Fully-Connected Layer:* Input from the previous layer is taken as input in this layer and computes the class scores and outputs the 1-D array of size equal to the number of classes. This layer is regular layer.

## IV. Conclusion

Deep learning approaches are increasingly employed for multiple applications and are being adopted also for cyber security, hence it is important to evaluate when and which category of algorithms can achieve adequate results. We analyse these techniques for three relevant cyber security intrusion detection. Deep learning is still at an early stage and no final conclusion can be drawn. Significant improvements may be expected, especially considering the recent and promising development of adversarial learning.

# REFERENCES

[1] A. Kurakin, I. Goodfellow, and S. Bengio, "Adversarial examples in the physical world," arXiv Prepr arXiv:1607.02533, 2016.
[2] S. Sabour, Y. Cao, F. Faghri, and D. J. Fleet, "Adversarial manipulation of deep representations," arXiv Prepr arXiv:1511.05122, 2015.
[3] C. Xie, J. Wang, Z. Zhang, Y. Zhou, L. Xie, and A. Yuille, "Adversarial examples for semantic segmentation and object detection," in IEEE Intl Conf Comp Vis, 2017, pp. 1369–1378.
[4] N. Carlini and D. Wagner, "Audio adversarial examples: Targeted attacks on speech-to-text," arXiv Prepr arXiv:1801.01944, 2018.
[5] J. Salamon and J. P. Bello, "Unsupervised feature learning for urban sound classification," in Intl Conf Acous Speech Sign Proc, 2015, pp. 171–175.
[6] K. J. Piczak, "Esc: Dataset for environmental sound classification," in 23rd ACM Intl Conf Multim, 2015, pp. 1015–1018.
[7] J. Salamon, C. Jacoby, and J. P. Bello, "A dataset and taxonomy for urban sound research," in 22st ACM Intl Conf Multim, Orlando, FL, USA, 2014.
[8] J. Salamon and J. P. Bello, "Feature learning with deep scattering for urban sound analysis," in 23rd Europ Sign Proc Conf, 2015, pp. 724– 728.
[9] ——, "Deep convolutional neural networks and data augmentation for environmental sound classification," IEEE Sign Proc Lett, vol. 24, no. 3, pp. 279–283, 2017.
[10] Y. Aytar, C. Vondrick, and A. Torralba, "Soundnet: Learning sound representations from unlabeled video," in NIPS, 2016, pp. 892–900.
[11] V. Boddapati, A. Petef, J. Rasmusson, and L. Lundberg, "Classifying environmental sounds using image recognition networks," Procedia Comp Sci, vol. 112, pp. 2048–2056, 2017.
[12] T.-W. Weng, H. Zhang, P.-Y. Chen, J. Yi, D. Su, Y. Gao, C.-J. Hsieh, and L. Daniel, "Soundnet: Learning sound representations from unlabeled video," in 6th Intl Conf Learn Repres, 2018.
[13] I. J. Goodfellow, J. Shlens, and C. Szegedy, "Explaining and harnessing adversarial examples," arXiv Prepr arXiv:1412.6572, 2014.
[14] N. Carlini and D. Wagner, "Towards evaluating the robustness of neural networks," in IEEE Symp Secur Priv, 2017, pp. 39–57.
[15] Y. Li and Y. Gal, "Dropout inference in bayesian neural networks with alpha-divergences," arXiv Prepr arXiv:1703.02914, 2017.
[16] B. Biggio, I. Corona, D. Maiorca, B. Nelson, N. Srndi ˇ c, P. Laskov, ´ G. Giacinto, and F. Roli, "Evasion attacks against machine learning at test time," in Joint Europ Conf Mach Learn Knowl Discov Datab, 2013, pp. 387–402.
[17] H. Xiao, H. Xiao, and C. Eckert, "Adversarial label flips attack on support vector machines." in ECAI, 2012, pp. 870–875.
[18] C. Xie, Z. Zhang, J. Wang, Y. Zhou, Z. Ren, and A. Yuille, "Improving transferability of adversarial examples with input diversity," arXiv Prepr arXiv:1803.06978, 2018.
[19] Y. Liu, X. Chen, C. Liu, and D. Song, "Delving into transferable adversarial examples and black-box attacks," arXiv Prepr arXiv:1611.02770, 2016.
[20] N. Papernot, P. McDaniel, and I. Goodfellow, "Transferability in machine learning: from phenomena to black-box attacks using adversarial samples," arXiv Prepr arXiv:1605.07277, 2016.
[21] N. Das, M. Shanbhogue, S.-T. Chen, L. Chen, M. E. Kounavis, and D. H. Chau, "Adagio: Interactive experimentation with adversarial attack and defense for audio," arXiv Prepr arXiv:1805.11852, 2018.
[22] M. Alzantot, B. Balaji, and M. Srivastava, "Did you hear that? adversarial examples against automatic speech recognition," arXiv Prepr arXiv:1801.00554, 2018.
[23] T. Du, S. Ji, J. Li, Q. Gu, T. Wang, and R. Beyah, "Sirenattack: Generating adversarial audio for end-to-end acoustic systems," arXiv Prepr arXiv:1901.07846, 2019.
[24] N. Roy, H. Hassanieh, and R. Roy Choudhury, "Backdoor: Making microphones hear inaudible sounds," in 15th Intl Conf Mob Sys App Serv, 2017, pp. 2–14.
[25] L. Song and P. Mittal, "Inaudible voice commands," arXiv Prepr arXiv:1708.07238, 2017.
[26] X. Ma, B. Li, Y. Wang, S. M. Erfani, S. Wijewickrema, M. E. Houle, G. Schoenebeck, D. Song, and J. Bailey, "Characterizing adversarial subspaces using local intrinsic dimensionality," arXiv Prepr arXiv:1801.02613, 2018.
[27] C. Liu, L. Feng, G. Liu, H. Wang, and S. Liu, "Bottom-up broadcast neural network for music genre classification," arXiv Prepr arXiv:1901.08928, 2019.
[28] Y. M. G. Costa, L. E. S. Oliveira, A. L. Koerich, F. Gouyon, and J. G. Martins, "Music genre classification using LBP textural features," Sign Proc, vol. 92, no. 11, pp. 2723–2737, 2012.

[29] S. Sengupta, G. Yasmin, and A. Ghosal, "Speaker recognition using occurrence pattern of speech signal," in Recen Trends Sign Image Proc. Springer, 2019, pp. 207–216.
[30] G. Yu, S. Mallat, and E. Bacry, "Audio denoising by time-frequency block thresholding," IEEE Trans Sign Proc, vol. 56, no. 5, pp. 1830– 1839, 2008.
[31] S. Mallat, A wavelet tour of signal processing: the sparse way. Academic Press, 2008.
[32] G. Yu and J.-J. Slotine, "Audio classification from time-frequency texture," arXiv Prepr arXiv:0809.4501, 2008.
[33] R. C. Gonzalez, "Digital image processing," 2016.
[34] M. Esmaeilpour, A. Mansouri, and A. Mahmoudi-Aznaveh, "A new svdbased image quality assessment," in 8th Iranian Conf Mach Vis Image Proc, 2013, pp. 370–374.
[35] M. E. Wall, A. Rechtsteiner, and L. M. Rocha, "Singular value decomposition and principal component analysis," in A practical approach to microarray data analysis. Springer, 2003, pp. 91–109.
[36] I. Goodfellow, Y. Bengio, A. Courville, and Y. Bengio, Deep learning. MIT Press Cambr, 2016, vol. 1.
[37] P. Vincent, H. Larochelle, Y. Bengio, and P.-A. Manzagol, "Extracting and composing robust features with denoising autoencoders," in 25th Intl Conf Mach Learn, 2008, pp. 1096–1103.
[38] D. G. Lowe, "Object recognition from local scale-invariant features," in 7th IEEE Intl Conf Comp Vis, vol. 2, 1999, pp. 1150–1157.
[39] H. Bay, T. Tuytelaars, and L. Van Gool, "Surf: Speeded up robust features," in Europ Conf Comp Vis, 2006, pp. 404–417
[40] D. Arthur and S. Vassilvitskii, "k-means++: The advantages of careful seeding," in 18th ACM-SIAM Symp Discrete Alg, 2007, pp. 1027–1035.
[41] A. Coates and A. Y. Ng, "Learning feature representations with kmeans," in Neural networks: Tricks of the trade. Springer, 2012, pp. 561–580.
[42] B. McFee, E. J. Humphrey, and J. P. Bello, "A software framework for musical data augmentation." in ISMIR, 2015, pp. 248–254.
[43] M. Cowling and R. Sitte, "Comparison of techniques for environmental sound recognition," Patt Recog Lett, vol. 24, no. 15, pp. 2895–2907, 2003.
[44] F. Pedregosa, G. Varoquaux, A. Gramfort, V. Michel, B. Thirion, O. Grisel, M. Blondel, P. Prettenhofer, R. Weiss, V. Dubourg et al., "Scikit-learn: Machine learning in python," J Mach Learn Research, vol. 12, pp. 2825–2830, 2011.
[45] A. Krizhevsky, I. Sutskever, and G. E. Hinton, "Imagenet classification with deep convolutional neural networks," in NIPS, 2012, pp. 1097– 1105.
[46] A. Nayebi and S. Ganguli, "Biologically inspired protection of deep networks from adversarial attacks," arXiv Prepr arXiv:1703.09202, 2017.
[47] Mohammad Esmaeilpour, Patrick Cardinal, and Alessandro Lameiras Koerich, "A Robust Approach for Securing Audio Classification Against Adversarial Attacks. VOL. X, NO. X, NOVEMBER 2019.
[48] D. Meng and H. Chen, "Magnet: a two-pronged defense against adversarial examples," in ACM SIGSAC Conf Comp and Commun Secur, 2017, pp. 135–147.