VIT®

Vellore Institute of Technology

(Deemed to be University under section 3 of UGC Act, 1956)

School of Information Technology and Engineering

Digital Assignment-II, SEPTEMBER 2020

B.Tech., Fall-2020-2021

NAME	PRIYAL BHARDWAJ
REG. NO.	18BIT0272
COURSE CODE	ITE2011
COURSE NAME	MACHINE LEARNING
SLOT	E2+TE2
FACULTY	Prof. DURAI RAJ VINCENT P.M.

DEEP LEARNING BASED APPROACHES

(All papers taken from IEEE)

Journal 1: A Survey of Deep Learning: Platforms, Applications and Emerging Research Trends
Authors: William Grant Hatcher, Wei Yu
Date: April 2018
Link: https://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=8351898

In this paper, the ever-increasing domination of Deep Learning techniques has been surveyed and discussed. Amazon, Apple, Microsoft, Google etc. and other big companies are rapidly becoming invested in this field to supply hardware and software advancements in the industry. Deep learning is the application of a multi-neuron, multi-layer neural networks to perform learning, encoding and many other tasks. In place of complex hard-coded programs that used to be developed for a sole inflexible task, a single deep learning architecture can be applied to all types of data, be they visual, audio, numerical, text, or some combination. Not all algorithms under machine learning can be classified under deep learning as well. For example, singular algorithms, including statistical mechanisms like Bayesian algorithms, function approximation such as linear and logistic regression, or decision trees, while powerful, are limited in their application and ability to learn massively complex data representations. Deep learning has developed from cognitive and information theories, trying to replicate the learning process of human neural networks and create complex interconnected neural network structures. It has major applications in Recognition systems, text analysis, healthcare, cyber security etc. Some emerging areas of applications are network management, secure deep learning etc. These applications have been discussed in detail in this paper.

Journal 2: Deep Learning Approach for Intelligent Intrusion Detection System
Authors: R. Vinayakumar, Mamoun Alazab, K.P. Soman, Prabaharan Poornachandran, Ameer Al-Nemrat, Sitalakshmi Venkatraman
Date: January 2019
Link: https://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=8681044

In this paper, deep learning approaches to intrusion detection system are discussed. Intrusion Detection System (IDS) are systems that detect any suspicious activity and issues and alerts the concerned person if something discovered. it's a software application that scans a network or a system for harmful activity or policy breaching. Deep learning is an advancement in machine learning and it significantly improves the classification accuracy on highly-structured and large-scale database in less time as well. NIDS and HIDS datasets to check the performance of deep learning and machine learning algorithms. Deep learning uses multiple non-linear layers transformation to perform representation learning, and it's powerful capabilities of information abstraction. Patient dataset was used for training and association between drug dose and patient gene was observed. Deep neural networks are used as a more advanced model of the classic feedforward neural network with each hidden layer employing a non-linear activation function, rectified linear measure because it helps to scale back the state of vanishing

and error gradient issue. For future work it absolutely was proposed that a module will be added to observe DNS within the network that's being tested for any intrusion.

Journal 3: Deep Learning for Natural Language Parsing
Authors: Sardar Jaf, Calum Calder
Date: August 2019
Link: https://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=8827454

In this paper, it's discussed how deep learning techniques can tackle the issues faced by linguistic communication Processing algorithms. a number of the issues are in speech recognition, text-based data processing, and text or speech generation. Parse trees are used as a part of many language processing applications. during this paper, a multi-lingual dependency parser was implemented. Using advanced deep learning techniques, the parser architecture tackles common issues with parsing like long-distance head attachment, while using 'architecture engineering' to adapt to every target language so as to scale back the feature engineering often required for parsing tasks. RNN architectures like LSTM and bidirectional LSTM (BiLSTM) are employed in occasions where the educational problem is sequential, e.g. you have got a video and you wish to understand what it is that everything is about otherwise you want an agent to read a line of document for you which ones is a picture of text and isn't in text format. Parsing, classifier, arc labelling, multi-lingual parser, transfer learning, model optimization and training are implemented and experimented on within the paper. The proposed architecture demonstrated very promising results when parsing languages with very limited resources.

Journal 4: A Survey on the New Generation of Deep Learning in Image Processing
Authors: Licheng Jiao, Jin Zhao
Date: November 2019
Link: https://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=8917633

In this paper, applications of deep learning within the field of image processing are surveyed and discussed. Image processing may be a widely used technique in medical images, nature image and remote sensing image. In pattern recognition and machine learning, the commonly used image processing includes image generation, compression and encoding, image deblurring, super-resolution, image segmentation, classification and visual perception, change detection, image annotation, and image retrieval, etc. Deep learning is usually used as classifiers or feature extractors for various tasks in image processing. Firstly, they surveyed CNN model due to its weight sharing property. Weight sharing dramatically reduces the amount of free parameters learned, thus to lower the memory requirements for running the network and allowing the training of more extensive, more powerful networks. Then complex valued CNN (CV-CNN) was surveyed. it had been observed through experiments that the classification error might be further reduced by this method. Next, they surveyed super resolution CNN (SRCNN) because it can directly learn end-to-end mapping between low-resolution image and high-resolution image. Other models that were surveyed were Resnet, Mask R-CNN, FCN etc. it had been concluded that deep learning thrives with large neural

networks and huge datasets. One key ingredient for achievement of deep learning in image classification is that the use of convolutional architectures. This paper reflects a really comprehensive survey regarding deep learning techniques in image processing and would be very helpful if someone plans to try and do a project associated with this.

Journal 5: Differential Privacy Preservation in Deep Learning: Challenges, Opportunities and Solutions
Authors: Jingwen Zhao, Yunfang Chen, Wei Zhang
Date: April 2019
Link: https://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=8683991

In this paper, how deep learning addresses and solves privacy issues cybersecurity attacks. The deep learning model is presented by the authors in respect to three aspects, membership inference, training data extraction and model extracting. Datasets from many big companies like Microsoft, Google, Amazon were used and that they contained some sensitive information. The privacy threats in deep learning models may be classified in keeping with training phase and prediction phase. Empirical risk minimization (ERM) and doubtless approximately correct (PAC) are required for these styles of deep private learning algorithms. ERM converts the educational into convex minimization problem and PAC estimates the link between accuracy of the model and number of learning samples it's an urgent have to develop a universal privacy protection framework with more generalization. it absolutely was concluded that differential privacy must be developed to match multiple iterations of high-dimensional data in deep learning for privacy protection.

****