IJCSE International Journal of Computer Sciences and Engineering Open Access
Survey Paper Vol-6, Special Issue-4, May 2018 E-ISSN: 2347-2693

# Recent Advances in Deep Learning Techniques

**M.Sornam[1*], E. Panneer Selvam[2]**

[1,2]Department of Computer Science, University of Madras, Chennai, India

[*]*Corresponding Author: madasamy.sornam@gmail.com, Tel.: +91-044-25399628*

**Available online at: www.ijcseonline.org**

***Abstract*—** Deep Learning is currently being used for a variety of different applications. It has drawn increasing research interest because of the capability of overcoming the drawback of traditional algorithms. Some of the important applications are pattern recognition, computer vision, speech recognition, natural language processing, handwriting recognition, face recognition, IoT and medical. There are several researches has been done in the area of deep learning from the last decade of the nineteenth century and still many more to come. This paper gives survey on deep learning and some of the recent research that has been done in the area of deep learning.

***Keywords*—**Machine Learning, Deep learning, Fog Computing, Genetic Algorithm, Pattern Recognition.

## I. INTRODUCTION

Machine Learning is a subset of Artificial Intelligence which uses algorithms to parse and learn from data and then apply what has been learned to make informed decisions. Deep Learning is a subset of Machine Learning that uses layered structure of algorithms called artificial neural network. Its design is inspired from the biological neural network that human brain uses [1].

Deep Learning uses layers of algorithms to process data. Information is passed through each layer, with the output of the previous layer providing input for the next layer. The first layer in a network is called the input layer, while the last layer is called output layer. All the layers between these two are referred to as hidden layers. Each layer consists of set of neurons also called as units. Feature extraction is important aspect of deep learning. It uses an algorithm to automatically construct meaningful "features" of data for the purpose of training, learning, and decision making.

The history of Deep Learning can be traced back to 1943, when Walter Pitts and Warren McCulloch created a computer model based on the neural networks of the human brain. They used a combination of algorithms and mathematics they called "threshold logic" to mimic the thought process to compute any arithmetic or logical function. Their work is often acknowledged as the origin of the neural network field. Since that time, Deep Learning has evolved steadily.Henry J. Kelley has given credit for developing the basics of a continuous Back Propagation Model in 1960. In 1962, a simpler version based only on the chain rule was developed by Stuart Dreyfus. The concept of back propagation used in neural network is to adjust the weight of neurons by calculating the gradient of the loss function. This technique is also called backward propagation of errors, because the error is calculated at the output and distributed back through the network layers. In addition, optimization algorithms are used with back propagation to reduce the training period.

The earliest efforts in developing Deep Learning algorithms came from Alexey GrigoryevichIvakhnenko and Valentin Grigor′evich Lapa in 1965. They used models with polynomial activation functions that were then analyzed statistically. From each layer, the best statistically chosen features were then forwarded on to the next layer (a slow, manual process). Since 1970's there has been a significant evolution in all the aspect of neural network design such as different architecture, activation functions and optimization learning algorithms.

The rest of the paper is organized as follows. Section II describes a review on deep learning. Summary of neural network model used is given in section III. Section IV gives proposed work. Conclusion is given in Section V.

## II. LITERATURE REVIEW

Weibo et al. [1], survey describe the deep neural architecture and their applications. This paper describes the neural architecture of Restricted Boltzman Machine (RBM), Deep Belief Network (DBN), Auto Encoder (AE) and Deep Convolution Neural Network (DCNN) and important deep learning applications were discussed such as speech recognition, computer vision and pattern recognition, Natural Language Processing (NLP), handwriting recognition, face detection or behavior recognition and image classification. This paper concluded with the discussion of future research area in deep learning such as design of deep model to learn from less training data, use of optimization algorithm to

 

adjust the network parameter, implementation of deep learning algorithms on mobile device and application of deep neural network in nonlinear networked control systems. Vrizlynn L.L. Thing [2], described IEEE 802.11 wireless network anomaly detection and attack classification using deep learning approach. In this experiment Stacked Auto-Encoder (SAE) is used with four different activation functions to measure the better performance of the model over the given problem, such as Rectified Linear Unit (ReLU), Leaky Rectified Linear Unit (LReLU), Parametric Rectified Linear Unit (PReLU) and Sigmoid with J48 classifier for four different classes such as normal, injection, flooding and impersonation. The experiment result shows that the overall accuracy of SAE model with PReLU activation function gives the best result of 98.66%. However, there is a significant drop in flooding attack classification accuracy which is just 57.47%. Another example of anomaly detection is the intruder detection using deep learning and association rule mining [3]. This paper consists of two important stages such as detection stage and analysis stage. In detection stage Recurrent Neural Network (RNN) is used. To overcome the problem of scalability of network model fly generation procedure model has been used. Association Rule Mining is used to classify the recognized pattern. In intruder analysis stage intruder distribution is displayed in the world in a world map. Using pie and line charts, it would show the growth of the intruder attacks and then it would predict the future intruder operations that can occur along with the location.This paper concludes with the future work of trying with different deep network model for measuring the accuracy and evaluates the effectiveness of the recurrent network with large dataset.

Chuanlong et al. [4], utilize a deep learning approach for intrusion detection using recurrent neural network on the$KDDTrain^{+}$(training set), $KDDTest^{+}$ and $KDDTest^{-21}$ datasets (testing set), which has different normal records and four different types of attack records namely Dos, Proble, R2L and U2R. In data preprocessing stage nonnumeric features in the NSL-KDD dataset is converted into numeric format because the input value of RNN-IDS should be numeric matrix. The activation function sigmoid and classification function softmax are used. To measure the accuracy, detection rate and false positive rate were introduced. Table 1 shows the detection rate and false positive rate of the different attack types.The experiment have been conducted in two different way, one is RNN-IDS model for binary classification with two classes as normal, anomaly and RNN-IDS model for multiclass classification, such as Normal, DoS, R2L, U2R and Probe.

The comparison of both binary and multiclass classification with traditional classification methods, such as J48, naïve bayesian, and random forest, the performance is obtaining a higher accuracy and detection rate under the multiclass classification. This paper concludes with the future work of reducing the training time using GPU acceleration and Bidirectional RNNs algorithm in the field of intrusion detection.Nancy Patel et al. [5], proposed an implementation of pattern matching algorithm to defend SQLIA. Two different types of experiments were conducted, such as using software and neural network. Initially, the input query is checked whether the query is injected or not by SQLMAP tool and AIIDA-SQL technique but this technique suffers with the time constraint because it take 15-20 minutes to evaluate one query. In the second phase Multi-Layer neural network is used which has 4 inputs, 5 hidden units and 3 outputs such as infected, not infected and cannot determine. After checking the infected query, pattern matching algorithm is applied to check the query with the static pattern list. However, there is a class of cannot determine as third output which may sometime give inaccurate result.

Table1. Results of evaluation metrics for five-category class [4].

| Intrusion Type | FPR(%) | DR(%) |
|---|---|---|
| DoS | 2.06 | 83.49 |
| R2L | 0.80 | 24.69 |
| U2R | 0.07 | 11.50 |
| Probe | 2.16 | 83.40 |

Youbiao et al. [6], described a system has to detect real time False Data Injection (FDI) attacks in smart grid with the algorithm of Sequential Quadratic Programming optimization model to characterize the behavior of one type of FDI attack that compromises the limited number of state measurements of the power system for electricity theft. The proposed model employs conditional Deep Belief Network (CDBN) to efficiently capture the high dimensional temporal behavior features of unobservable FDI attack that bypass the State Vector Estimator (SVE). The experiment is conducted on IEEE 118-bus test system as well as IEEE 300-bus test system to evaluate the scalability of the system. This paper concluded with the future work of analyzing the minimum number of the sensing units required to detect practical behaviors of the FDI attacks.

Hongmei et al. [7], demonstrated a semantic attribute deep learning with Linguistic Attribute Hierarchy (LAH), embedded with Linguistic Decision Tree (LDT) for spam detection. The study is performed on SMS message database from UCI machine learning repository. According to the examination of LAHs for different decompositions were examined in terms of sensitivity, specificity, accuracy and ROC curve. The result shows that LAH embedded with LDTs, provides a transparent approach in analyzing feature impact on spam detection and also efficiently reduce the dimensionality problem in spam detection. Automatic knowledge based decomposition of features and the optimization of linguistic attribute hierarchies is considered as a future work. Another example of deep learning

 

contribution in security is distributed attack detection scheme using deep learning in Internet of Things [8]. In the recommended system fog nodes are responsible for training model and hosting attack detection system at the edge of fog network. The system uses deep model with four different activation functions, such as Tanh, Rectified Linear, Maxout and Softmax with Stochastic Gradient Descent (SGD) optimization technique for weight update. The result shows that deep model provide better result than traditional shallow model in finding cyber-attacks over IoT.

Table 2. Accuracy of deep model (DM)and shallow model (SM) [8]

| | 2-class | | | 4-class | | |
|---|---|---|---|---|---|---|
| Model Type | Accuracy (%) | DR (%) | FAR (%) | Accuracy (%) | DR (%) | FAR (%) |
| DM | 99.20 | 99.27 | 0.85 | 98.27 | 96.5 | 2.57 |
| SM | 95.22 | 97.50 | 6.57 | 96.75 | 93.66 | 4.97 |

Comparison of proposed deep model with the traditional machine learning algorithm is considered as the work extension. Dayieng Liu et al. [9], proposed a neural words encoding model to encrypt and decrypt words using Deep Belief Network (DBN). The training set contains vocabulary of American National Corpus which includes approximate 60,000 different English words. The learning procedure of the model is divided into two stages: pre-training with unlabelled samples and fine-tuning the whole deep network with labeled samples.In pre-training stage, each pair of layers grouped together to reconstruct the input layer to output layer. The last hidden layer is the code layer. In fine tuning stage, the goal is to reconstruct word set and make the output of code layer as binary.

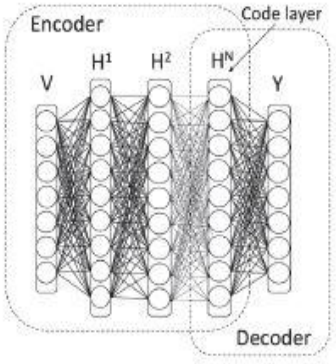


Fig. 1. Architecture of neural words encoding model [9]

The entire network is refined using back propagation via Steepest Gradient Descent (SGD). After fine tuning, for any word of word set which is input, the output of code layer is its encoding.

Table 3. Performance of Models [9]

| Model | Code layer binary output | R |
|---|---|---|
| Neural words encoding model | Yes | 99.04% |
| RBM 60-128 | Yes | 85.46% |
| RBM 60-256 | Yes | 89.16% |
| Auto-encoder 120-128-120 | Yes | 89.75% |
| Auto-encoder 120-256-120 | Yes | 90.12% |
| DBNs 60-256-128-64-128-256-60 | Yes | 99.87% |

The experiment conducted with different model shows thatproposed neural word encoding model produce best result of 99.04%. Xiaoguang et al. [10], proposed convolution neural network for automatic facial recognition. In that paper, faces are detected in the preprocessing stage and cropped using OpenCV library. Then, the facial expressions features are extracted using convolution neural network.In this model Stochastic Gradient Descent (SGD) is used for training and the model was tested on the database from the extend cohn-kanaded database (CK+) with one or seven expression categories: angry, disgust, neutral, sad, fear, surprise and happy. Investigate the model with bigger database in order to increase the robustness of facial expression recognition in different environments and adding age identification function as well as improving the recognition accuracy is added as the future work of this experiment.

Zijing et al. [11], describes an EEG-based biometric identification with deep learning using Convolution Neural Network (CNN). In this experiment, task1 examined the performance of identifying 100 subjects using XB driving data with the accuracy of 97% to distinguish 100 subjects. In task2, subjects were identified under non-specific stimulation scenario such as car left/right perturbation to correction, speed, control and so on but in this case accuracy was dropped down from 97% to 90%. This experiment suggested that EEG-based biometric identification should include less diversity of events in order to get better accuracy.

Daniele Ravi et al. [12], described a deep learning approach to on-node sensor data analytics for mobile or wearable devices by combining features learned from inertial sensor data together with complementary information from a set of shallow features to enable accurate and real-time activity classification. An example of deep learning for motor imagery classification can be found in [13]. This study involved systematic experiments on publicly available benchmark dataset and it showed that frequency domain input to DBN can lead to much improved performance than the raw time series data as comparison with the state-of-art methods. M Sornam et al. [14], proposed Deep convolutional neural network for handwritten tamil character recognition using principal component analysis. The model contains nine layer which includes two convolutional layer, two maxpooling layer, three fully connected layer and one input and one output layer. The experiment shows that handwritten tamil character recognition using PCA provide better accuracy and future work involved recognizing words in an image using GPU.

 

Table 4. Performance Measures [14]

| Metrices | Without PCA(%) | With PCA(%) |
|---|---|---|
| Accuracy | 85.05 | 88.96 |
| Precision | 85 | 89 |
| Recall | 85 | 89 |
| F1 score | 85 | 89 |

Genetic algorithm is used to optimize neural network architecture [15]. In this experiment, multi-objective mathematical model is used to determine the optimal number of hidden layers, the number of neurons in each layer and good values of weights with GA and back propagation in feed-forward neural network. Another example of optimization of neural network architecture is the learning rate optimization using GA combined with back propagation [16]. The experiment showed that LOG-BP learning process can be optimized by locality-controlled parallel search and genetic mutations. Future work involved comparison of LOG-BP with other learning methods and optimum distributions of the initial values.

**III.TABLE 5: SUMMARY OF VARIOUS NEURAL NETWORK IMPLEMENTED**

| Reference Number | Author | Year | Network Model |
|---|---|---|---|
| [2] | Vrizlynn L.L. Thing | 2017 | Stacked Auto Encoder with ReLu, LReLu, PReLu and sigmoid |
| [3] | Asantha et al. | 2016 | Used Recurrent Neural Network for anomaly detection. |
| [5] | Nency et al. | 2015 | Implemented multi perceptron to identify infected query |
| [6] | Youbiao et al. | 2017 | Conditional Deep Belief Network is used for False Data Injection |
| [9] | Dayieng et al. | 2016 | Implemented Deep Belief Network to encrypt and decrypt words |
| [10] | Xiaoguang et al. | 2017 | Implemented Convolutional Neural Network for facial expression recognition |

## IV. PROPOSED WORK

This paper discussed various research work of deep learning in different domains. In [11], CNN is successfully applied for EEG based biometric identification this give us an interest to propose the utilization of deep learning to discover features of EEG signals in speech for silent communication.

## V. CONCLUSIONS

Deep learning gives the significance performance improvements in many application domains. This paper mainly reviewed some of the latest research of deep learning in security and other domain with its limitation, future work and also optimization of neural network is discussed.

## REFERENCES


[1] Weibo Liu, Zidong Wang, Xiaohui Liu, Nianyin Zeng, Yurong Liu, Fuad E. Alsaadi, "A survey of deep neural network architecture and their applications," Neurocomputing, vol. 234, pp. 11-26, 2017.

[2] Vrizlynn L.L. Thing, "IEEE 802.11 Network Anomaly Detection: A Deep Learning Approach," *IEEE Wireless Communication and Networking Conference*, pp. 1-6, 2017.

[3] AsanthaThilina, Shakthi Atanayake, SacithSamarakoon, DahamiNawodya, LakmalRupasinghe, NadithPathirage, TharinduEdirisinghe, KesavanKrishnadeva, "Intruder Detection using Deep Learning and Association Rule Mining," *IEEE Conference on Computer and Information Technology*, pp. 615-620, 2016.

[4] Chuanlong Yin, Yuefei Zhu, Jinlong Fei, Xinzheng He, "A Deep Learning Approach for Intrusion Detection using Recurrent Neural Networks," *IEEE Access*, vol.5, pp. 21954-21961, 2017.

[5] Nency Patel, Narendra Sekokar, "Implementation of pattern matching algorithm to defend SQLIA," *Procedia Computer Science*, vol.45, pp. 453-459, 2015

[6] Youbiao He, Gihan J, Mendis, Jin Wei, "Real-Time Detection of False Data Injection Attacks in Smart Grid: A Deep Learning-Based Intelligent Mechanism," *IEEE Transaction on Smart Grid*, vol. 8, no. 5, pp. 2505-2516, 2017.

[7] Hongmei He, Tim Watson, Carsten Maple, JornMehnen, Ashutosh Tiwari, "A New Semantic Deep Learning with a Linguistic Attribute Hierarchy for Spam Detection," *International Joint Conference on Neural Networks*, pp. 3862-3869, 2017.

[8] A.ADiro, N. Chilamkurti, "Distributed Attack Detection Scheme using Deep Learning Approach for Internet of Things," *Future Generation Computer Systems* DOI=http"//dx.doi.org/10.1016/j.future.2017.08.043

[9] Dayieng Liu, JianchengLv, Xiaofeng Qi and Jiangshhu Wei, "A Neural Words Encoding Model," *International Joint Conference on Neural Network*, pp. 532-536, 2016.

[10] Xiaoguang Chen, Xuan Yang, Maosen Wang, Jiaancheng Zou, "Convolutional Neural Network for Automatic Facial Expression Recognition," *International Conference on Applied System Innovation*, pp. 814-817, 2017.

[11] Zijing Mao, Wan Xiang Yao, Yufei Huang, "EEG-based biometric identification with deep learning," *International IEEE/EMBS Conference on Neural Engineering*, pp. 609-612, 2017.

[12] Daniele Ravi, Charence Wong, Benny Lo, Guang-Zhong Yang, "A Deep Learning Approach to on-Node Sensor Data Analytics for Mobile or Wearable Devices," IEEE Journal of Biomedical and Health Informatics, vol. 21, no.1, pp. 56-64, 2017.


 

[13] Na Lu, Tengei Li, Xiaodong Ren, Hongyu Miao, "A Deep Learning Scheme or Motor Imagery Classification based on Restricted Boltzman Machines," *Transaction on Neural Systems and Rehabilitation Engineering*, vol. 25, no. 6, pp. 566-576, 2017.

[14] M. Sornam, C. Vishnu Priya, "Deep Convolutional Neural Network for Handwritten Tamil Character Recognition using Principal Component Analysis," *International Conference on Next Generation Computing Technologies*, *University of Petroleum and Energy Studies*, Dehradun, Oct 30th and 31st 2017, pp. 102-112.

[15] Mohammed Amine JanatiIdrissi, Hassan Ramchoun, Youssef Ghanou, "Genetic Algorithm for Neural Network Architecture Optimization," *International Conference on Logistics Operation Management*, pp.1-4, 2017.

[16] YausiKanada, "Optimizing Neural Network Learning Rate by Using a Genetic Algorithm with Per-epoch Mutations," International Joint Conference on Neural Networks, pp. 1472-1479, 2016.

## Authors Profile

*Dr M. Sornam*received her MSc in Mathematics from the University of Madras in the year 1987, Master's Degree in Computer Applications from the University of Madras in the year 1991 and received her Ph.D in the year 2013 from University of Madras. Since 1991–1996, she worked as a Lecturer in Computer Science at Anna Adarsh College, Chennai. Later, from 1996 to 2000 she worked as a Lecturer in Computer Science at T.S. Narayanasami College of Arts and Science, Chennai. Since 2001, she has been working in the Department of Computer Science, University of Madras. At present, she is working as an Associate Professor in Computer Science at the University of Madras. Her area of interest includes artificial intelligence, artificial neural networks, image processing, data mining, pattern recognition and applications

E. Panneer Selvam received Masters degree in computer applications from Jaya Engineering College in the year 2016. Since Apr 2012 to Sep 2014 worked as Jr.Hr.Executive in Datamark Prodapt India BPO Pvt Ltd at Chennai. Since Oct 2016 to Sep 2017 worked as a software developer in Skalable Technologies. Currently pursuing M.Phil in computer science at University of Madras, Chennai. His area of interest includes Artificial Intelligence, BCI and security in computing.

 