2024 International Conference on Artificial Intelligence and Emerging Technology (Global AI Summit) | 979-8-3503-7971-6/24/$31.00 ©2024 IEEE | DOI: 10.1109/GLOBALAISUMMIT62156.2024.10947915

Machine Learning and Deep learning for Credit Card Fraud Detection: A Comparative Analysis

1st Jyoti
Computer Science dept.,
Govt. PG College for Women,
Rohtak, Haryana, India
jyotikwatra@gmail.com

2nd Komal Bhardwaj
MM Institute of Management
Maharishi Markandeshwar (Deemed to be University)
Mullana, Ambala, Haryana
komal.bj@gmail.com

3rd Garima
MM Institute of Management
Maharishi Markandeshwar (Deemed to be University)
Mullana, Ambala, Haryana
garimamsehrawat@gmail.com

4th Mukesh Kumar
MM Institute of Management
Maharishi Markandeshwar (Deemed to be University)
Mullana, Ambala, Haryana
mukeshbisnoi24@gmail.com

5th Rajit Verma
MM Institute of Management
Maharishi Markandeshwar (Deemed to be University)
Mullana, Ambala, Haryana
vermarajput007@gmail.com

6th Divyansh Kumar
Chitkara University Institute of Engineering and Technology
Chitkara University
India
gnoidaapeejay@gmail.com

***Abstract*— Since last couple of the years, credit card frauds have been inclining abruptly. These frauds can be stated as the illicit usage of card, uncommon transaction activity, or swapping of an inert card. In other words, illegal account access by a person for which the account was not anticipated, is called as fraud and the process of behavior recognition of transactions known as authentic or deceptive. Detection of these frauds is truly the procedure of transactions classification i.e. authorized class and fraud class. Numerous techniques have been put forth and put into practice to address credit card fraud detection, including proposed and implemented to treat of credit card fraud detection like, data mining, nature-inspired algorithms like evolutionary algorithms & swarm techniques, machine learning algorithms etc. Machine Learning (ML) possess outstanding role in the uncovering frauds in online transactions.**

Fraudsters are becoming increasingly smarter and accustomed so there is a need of more robust, scalable and computationally efficient prediction models like Deep Neural Networks. Machine learning includes the subfield of deep learning, which is a more comprehensive use of artificial neural networks (ANN) that use several layers of non-linear processing components for feature mining as well as transformation. Deep learning is a sort of machine learning that helps computers understand the world through a conceptual hierarchy and learn from training. Therefore, a solution to lessening losses brought on by credit card fraud is to create efficient fraud detection algorithms utilizing machine learning, and more especially, deep learning approaches. In this study the use of deep learning and machine learning techniques to combat credit card fraud, have been compared. The results show that deep learning based approach overtakes all the other ML techniques with the utmost precision and can be effectually used for fraud investigation.

Keywords— Fraud Detection, Machine Learning, Deep Learning

I. INTRODUCTION

Credit cards play a crucial role in today's economy. They are inevitable part of domestic, business and communal dealings. Although, credit cards offer several advantages when used cautiously and conscientiously yet they can cause considerable fiscal damages by fraudulent actions. As per the data available that credit card is the utmost used payment mode worldwide in 2017 in comparison to other methods such as Bank Transfer and e-wallet. Illegitimate usage of credit card or its details without the holder's awareness is termed as credit card fraud. Financial fraud is a growing concern with a very great influence in the industry. Although, we are equipped with comfort and ease due to the internet based online credit card transactions but fraud activities have also been increased at a fast rate with shocking outcomes. Thus, with this immense problem in business system, it is very serious for banks and financial institutions to develop highly refined security systems for observing false transactions and identify the frauds as rapidly as possible. Credit card companies discover fraud by identifying numerous odd transactions. Most of them are, big purchases made just following the small ones, online shopping and acquisitions that doesn't suit a cardholder's profile.

For the purpose of fraud detection, transactions are divided into two classes: valid and fraudulent. This is a binary classification problem. Moreover Machine learning (ML) practices are deployed to envisage the doubtful and genuine transactions automatically by classification models trained on normalized and anomalies data. These techniques are able to classify the transactions by learning the patterns of the data.

In recent years, ML has become much popular in image analysis, speech recognition and natural language processing. Thus, defying the fraud activities through machine learning or deep learning techniques is one of the high-flying approaches intending to bring a halt to the losses caused by illicit acts. In machine learning, Practitioners train models to extract behavioral patterns from old transactions that indicate fraud, called as features. When any card is swapped, the card turn to the model and check, if the features match fraudulent behavior, the transaction gets choked-up. Moreover, data representations are learned via deep learning algorithms, which are a subset of the larger area of ML. They extract complex high level abstractions as data representations using a tiered and multi-layer learning process. One of the objectives of this paper is to comprehend where Deep Learning stands in detecting frauds.

II. CHALLENGES

Various challenges are tackled by researchers while carrying out study on credit card transactions. Some of the major concerns accompanying the problem of fraud detection are the inaccessibility of dataset on which the researchers can work and lack of substantial computing power to sort huge number of transactions. Banks and financial bodies are not prepared to disclose their subtle customer transaction records due to confidentiality issues. According to [1], billions of such transactions are accomplished daily. Analyzing such huge volumes of transactions involves well proficient methods requiring considerable computing power.

Moreover, Fraud datasets are extremely skewed (most of the transactions are genuine, and hardly any fraudulent). In general, 98% of the transactions are authorized while only 2% of them are fraud. Another important concern is the performance metric to evaluate the classifier. Accuracy is not a suitable metric because the dataset is prominently imbalanced. Therefore, even with very low classification errors, transactions which are fraud can be misclassified as legitimate. We need to take into account false positive rate along with accuracy [2]. The cost of misclassifying deceitful transactions is greater than the cost of misclassifying the authentic ones. It is essential to work on specificity along with precision. Despite these disputes, credit card fraud detection is still demanding research topic.

III. MACHINE LEARNING

Machine learning (ML) involves algorithms to analyze data, learn from the data, and draw conversant decisions based on its understanding. In machine learning, the algorithm is equipped with more information to predict accurate outcome.

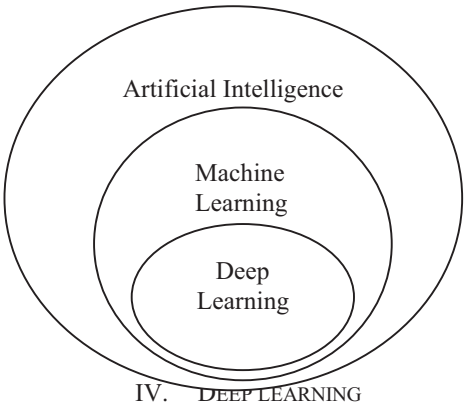


Fig. 1. Relationship between Machine Learning and Deep Learning

IV. DEEP LEARNING

Deep learning is a subdivision of machine learning. Typically, the term deep learning refers to deep neural networks or deep reinforcement learning. It constructs an "artificial neural network"—a mechanism that can absorb and make decisions on its own—through creating algorithms together which are in layer. Here deep is a technical phrase which characterizes the number of layers included in a neural network (NN). A shallow network contains only single hidden layer whereas a deep network has many. Several hidden layers assist deep manifold network to learn features in a feature hierarchy. Simpler features from each layer recombine to the subsequent layer, to build composite features. Networks with several layers propel input features over many mathematical operations and are hence more computationally intensive to train. Artificial Neural Networks (ANN) has become more powerful and complex with many deep layers and neurons. Computational gravity is one of its trait which make the deep-learning models demanding.

A deep learning model is designed to persistently examine data with a logical structure like drawing conclusions by human brain. Its design is stimulated by the natural neural structure of the human brain. The neurons at each layer make their "guesses" and most-probable calculations, and then forward that information to the subsequent level, heading towards the ultimate outcome.

Fig. 3. Shows the deep neural network with two hidden layers.

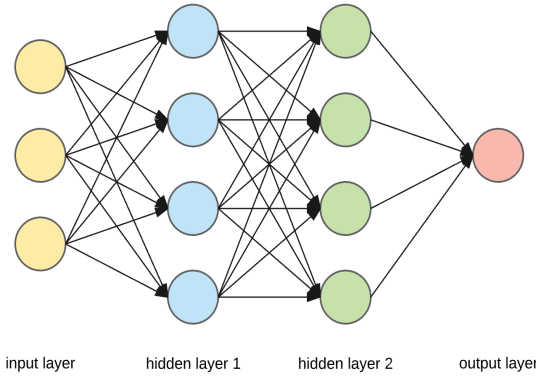


Fig. 2. Deep Neural Network

A "Deep Neural Network" (DNN) architecture's obvious feature is its hierarchical structure, which is primarily made up of an "input layer", "several hidden layers", and "one output layer". The output is computed directly along the sequent layers of DNN until input data is kept on fed. This kind of working mechanism is recognized as feed forward.

V. REVIEW OF LITERATURE

Many strategies have been expected to address the growing credit card theft. Nonetheless, there are a few recognized studies on methods for detecting frauds in credit card, may be, because of the unavailability of fraud transactions dataset for investigators[3] [4]. The best renowned techniques for fraud recognition are "logistic regression", "K-Nearest Neighbor algorithms" (KNN), "SVM", "Decision Trees", "Random Forests" and "Neural Networks".

Various ML procedures have been proposed with their usefulness for Fraud Detection. Fraud Analysis handles the supervised classification job at transaction level by categorizing the transactions as fraud or normal liable to the past record [5] [6]. A classification model is built for predicting the status for new futuristic records. There are so many model design methods in machine learning for usual two class classification. Many survey papers have been introduced in this context. These survey papers categorize, compare, and summarize almost all methodological and review articles for fraud detection.

[7] discuss how case-based reasoning was used to remove fraud from the credit approval process. Another study

include fraud detection based on SVM proposed by [8] introduced a method for uncovering fraud operations based on artificial neural networks. This problem has been examined with MLP (Multi level Perceptron), a category of "Feed Forward Artificial Neural Networks" and the "Chebyshev Function Link Artificial Neural Network" (CFANN) in [9]. The result of their study claims the dominance of MLP over Decision Tree and CFANN in fraud detection. Some effective fraud detection techniques to improve the detection efficiency have been proposed in [8][9] . It is conveyed that neural network based classifiers are best suited for huge databases despite having long training times. Machine learning technique has become foremost choice to deal with this illegitimate activity [10][11].

Nowadays, Deep Learning has yielded outstanding outcomes in applications comprising large datasets. Deep Learning algorithms are one of the propitious way with a feature upper levels of generalization with automated mining [12] [13][14].

A Deep learning package H2O to build a deep neural network was applied by [15]. A useful strategy for managing big datasets is the H2O framework. When the suggested learning model was evaluated for performance in the 2009 UCSD Data Mining Contest, it was discovered that deep learning models provided noticeably higher accuracy in identifying fraudulent transactions. [16] have also proposed deep learning centered an unsupervised learning algorithm i.e. auto-encoder (AE), which adopts back propagation by fixing the inputs equalize to outputs. Their findings confirm that "supervised learning dataset" is best fit for "archive databases".

[17] provide a thorough analysis of deep learning techniques to detect credit card fraud by using three financial datasets and compare their effectiveness with a variety of ML algorithms. The outcomes demonstrate that deep learning techniques are loftier to conventional machine learning models.

In conclusion it can be stated that "Deep learning techniques" are still hardly used at all. The investigating of these techniques is justified due to the less consideration gained by them in past studies. Expected thrust is on the research for examining existing machine learning techniques and further exploring deep learning methods in handling credit card fraud data.

VI. Fraud Detection in Credit card using Deep Learning

The problem can be stated as modeling past transactions with the knowledge of the fraud ones and then using the model to envisage whether a future transaction is fraud or not. So, the process of detecting frauds in credit cards is approached as a binary classification problem.

One way to lessen the losses brought on by fraudulent activity is to create an efficient system to detect frauds. Numerous ML models have been studied in an effort to stop and identify credit card fraud. Deep Learning is doing very well as compared to other machine learning tasks. Here, we aim to explore Deep Learning methods in detecting credit card frauds and compare them with existing machine learning techniques.

First of all, after loading the credit card datasets, preprocessing is performed on the dataset which covers normalization, elimination of redundancy, excluding missing values, converting necessary variable into factors or classes.

In this study, we have used three optimizers i.e. "Stochastic Gradient Descent" (SGD), "RMSprop" and "Adam Optimization method" for implementing deep neural network based fraud detection. However an pseudo code has been encapsulates for the proposed method.

[17] used an adaptive learning rate optimization algorithm which includes "RMSprop" and "Stochastic Gradient Descent with momentum", specifically intended for training deep neural networks. Its name ADAM is derived from "adaptive moment estimation" because Adam uses approximations of first and second moments of gradient to fine-tune the learning rate.

Pseudo Code for Deep Neural Network based Credit card Fraud Detection

//Initialization
//Create the model sequentially
model = Sequential()
// Adding the layers
model.add (Dense (units =#no. of units (tuned) , initial_kernel = 'uniform', activation_function = 'relu', input_dimension = #no. of features))
// Apending the next hidden layer
model.add (Dense (units = #no. of nodes, kernel = 'uniform', activation_function = 'relu'))
// Finally, Adding the output layer
model.add (Dense (units = 1(output node), kernel = 'uniform', activation_function = 'sigmoid'))
// Compiling the Neural Network using Different Optimization Algorithms
model.compile (optimizer = 'adam/sgd/rmsprop', loss_function = 'binary_crossentropy', metrics = ['accuracy'])
// ***Tuning the Neural Network to the Training set***
model.fit (X_train, y_train, batch_size = 16, epochs = 50)
// ***Classifier Evaluation for the unseen test data***
accuracy = model.evaluate(X_test, y_test)
// Predicting the outcomes for Test Set
y_pred = model.predict(X_test)
score = model.evaluate(X_test, y_test)

While applying deep neural networks, First of all we have created a Sequential model and added layers one after the another until it stops performing better than the previous architecture. Dense class is used for completely connected layers. Units specify the count of nodes in the layer as and activation function is inserted in place of the **activation** argument.

We have used the "Rectified Linear Unit Activation Function" (ReLU) in the leading input subsequent layers and the "Sigmoid Function" in final output layer. Classifier is run for training data over a number of epochs and each epoch is split into batches. The performance of the suggested model can be assessed using data test that hasn't been seen yet.

VII. Experimental Analysis

The objective of this proposal is to observe the realization of two advanced practices i.e. "Machine

Learning" which includes 'logistic regression', 'support vector machines and random forests' and "Deep Learning" for credit card fraud identification.

In present literature, there is no standard benchmark dataset to evaluate detection methods. In this work, two data sets have been taken from UCI Machine Learning repository. The German dataset uses a number of criteria to categorize people as either excellent or bad credit risks. It contains 20 attributes and 1000 transactions. Australian Dataset also concerns credit card fraud. It contains 14 attributes and 690 examples.

Another dataset (secondary data) is taken for experimentation from ULB Machine Learning Group. The datasets include 2013 transactions conducted by cardholders in Europe and covers "284,807 transactions" done in two days, out of which 492 are frauds transactions. The fraud transactions are only 0.172% which is highly skewed. The class distribution for all these datasets has been shown in Figure 3.

Fig. 3(a). German Dataset

Fig. 3 (b) Australian Dataset

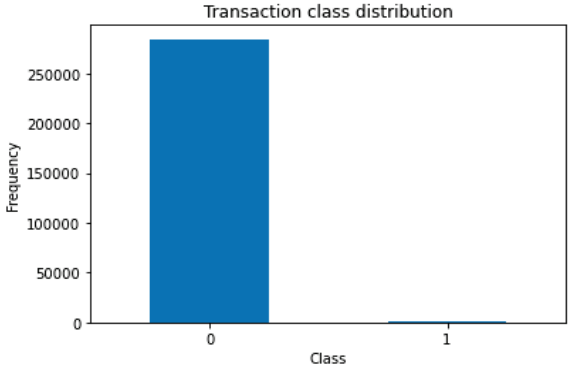


Fig. 3 (c) European card holder Dataset

Next fundamental step is feature scaling in our preprocessing channel by mapping the data in normal distribution, which makes it easier to acquire the weights of different layers of NN.

The formula of normalization can be stated by the following equation:

$$x_{std}^{(i)} = \frac{x^{(i)} - \mu_x}{\delta_x}$$

Here μ_x represents the sample mean and σ_x is the corresponding standard deviation of particular attribute.

Python programming language has been used in the implementation of proposed method. Python has become the new standard for a few years now since it is an object-oriented, interpreted, readable, high-performance programming language that is ideal for machine learning applications. It offers rich libraries and packages such as Tensor Flow & Keras.

We have used a number of "performance metrics" to report the performance of the proposed model which have been listed below:

Sensitivity or TPR $= \frac{TP}{TP+FN}$	Specificity or TNR $= \frac{TN}{TN+FP}$
False Positive Rate (FPR) $= \frac{FP}{FP+TN}$	False Negative Rate (FNR) $= \frac{FN}{FN+TP}$
Accuracy$= \frac{TP+TN}{TP+FP+TN+FN}$	Precision $= \frac{TP}{TP+FP}$
Recall=Sensitivity$= \frac{TP}{TP+FN}$	F Score $= \frac{2*Precision*Recall}{Precision+Recall}$

Here, "TP denotes the number of fraud transactions projected" as fraud correctly while "FP is the number of authorized transactions wrongly predicted as fraud". "TN indicates the number of legal transactions anticipated as legitimate" correctly while "FN is the number of legal transactions predicted as fraud".

VIII. Results

Encouragingly, all techniques exhibited acceptable skill to model fraud in the considered data. We have considered the models for SVM, Logistic regression, Decision tree, Random Forest and DNN. Performance measures such as accuracy, specificity, sensitivity and precision have been calculated and a comparison is made. We have made comparisons among various deep learning approaches and with other machine learning approaches cited in [16]. The Random forest algorithm perform better with large training data, but long execution time during training and application make it less preferable. On the other hand SVM algorithm suffers from

the class imbalance problem and entails further preprocessing to produce improved results.

We have compared the different optimizers available in keras while applying Deep Neural Networks (DNN). Table I encapsulates the results obtained by applying different optimizers in classification of all three datasets which concludes Adam Optimization be the best. The results of experiments performed on European credit card data have been shown in table II and table III compares the accuracies obtained on all the three datasets by Machine learning and deep learning methods. From the experiments the results conclude that the overall best results are obtained by DNNs with precise accuracies.

Table I. ACCURACIES OBTAINED ON ALL THREE DATASETS BY DIFFERENT OPTIMIZERS IN CONJUNCTION WITH DEEP NEURAL NETWORK (DNN).

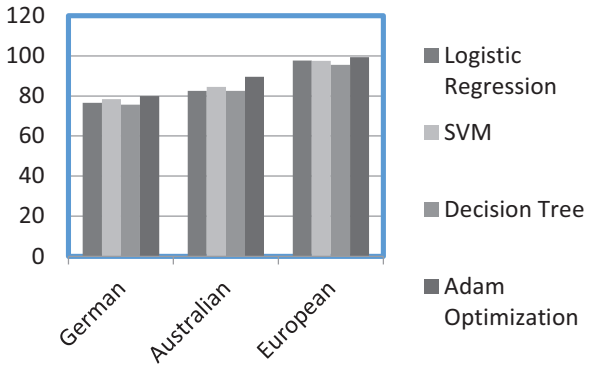
	Deep Learning		
Datasets	SGD	RMSprop	Adam
German	77.5	78.4	79.9
Australian	85.6	86.5	89.5
European Cardholder	96.7	97.8	99.4

TABLE II. MACHINE LEARNING VS. DEEP LEARNING ALGORITHMS ON EUROPEAN CREDIT CARD DATASET.

Metrics	**Classifiers**				
	Machine Learning				**Deep Learning**
	Logistic Regression	**SVM**	**Decision Tree**	**Random Forest**	**ANN (based on Adam)**
Accuracy	97.7	97.5	95.5	98.6	99.4
Sensitivity	97.5	97.3	95.5	98.4	98.2
Specificity	92.3	91.2	87.8	90.5	94.1
Precision	99.6	99.6	99.5	99.7	99.6

Table III. ACCURACIES OBTAINED ON ALL THREE DATASETS.

	Machine Learning Techniques			**Deep Learning**
Datasets	**Logistic Regression**	**SVM**	**Decision Tree**	**Adam Optimization**
German	76.5	78.4	75.6	79.9
Australian	82.6	84.5	82.5	89.5
European Cardholder	97.7	97.5	95.5	99.4



Graph 1: Accuracies obtained on all three datasets by Different Optimizers in conjunction with Deep Neural Network (DNN).

IX. CONCLUSION

As usage of credit cards has turned out to be prevalent practice these days, advance detection of fraud activities have been turned out to be much more prevailing. Building a precise and efficient fraud recognition system is one of the main jobs for the financial institutions to boost security of financial thefts in an automatic and effective approach.

ML and DL have been wondering us every day with expectation of following the trend surely in the future also. Deep learning has proved itself to be among the finest techniques in the industry for high-grade performance

One objective of this study is to ascertain the existing machine learning models that best identifies fraudulent transactions. Deep learning explores complex features inside the data to make the model learn better to envisage frauds more proficiently with less false alarms. In this project, deep neural network model is used on three datasets taken from UCI and ULB. Performance metrics of the models based on Deep Neural Networks and Machine learning have been obtained that show the DNN model along with ADAM optimization gives very less error. Other benefits of using Adam are computationally proficient, Less memory requirements, best choice for problems that are big either in terms of dataset or parameters, appropriate for cases with very noisy/sparse gradients, less requirement of tuning the Hyper-parameters. The model accurately classifies the fraudulent transactions.

By applying one or a combination of these algorithms to any financial credit card fraud detection system, fraud transactions can be prevented to a significant degree. These hybrid techniques based anti-fraud strategies can be implemented to prevent banks from suffering massive losses and lower risks.

X. REFERENCES

[1] P. K. Chan, W. Fan, A. L. Prodromidis, and S. J. Stolfo, "Distributed Data Mining in Credit Card Fraud Detection," *IEEE Intelligent Systems*, vol. 14, no. 6, pp. 67–74, Nov. 1999, doi: 10.1109/5254.809570.

[2] G. Baader and H. Krcmar, "Reducing false positives in fraud detection: Combining the red flag approach with process mining," *International Journal of Accounting Information Systems*, vol. 31, pp. 1–16, Dec. 2018, doi: 10.1016/j.accinf.2018.03.004.

[3] S. Sorournejad, Z. Zojaji, R. E. Atani, and A. H. Monadjemi, "A Survey of Credit Card Fraud Detection Techniques: Data and Technique Oriented Perspective," Nov. 2016. [Online]. Available: http://arxiv.org/abs/1611.06439.

[4] L. Delamaire, H. A. H. Abdou, and J. Pointon, "Credit card fraud and detection techniques: a review," *Banks and Bank Systems*, vol. 4, pp. 57–68, Jul. 2009. Accessed: Apr. 15, 2019. [Online].

[5] "Machine Learning Approaches for Credit Card Fraud Detection," *International Journal of Engineering & Technology*.

[6] S. Rajora et al., "A Comparative Study of Machine Learning Techniques for Credit Card Fraud Detection Based on Time Variance," in *2018 IEEE Symposium Series on Computational Intelligence (SSCI)*, Nov. 2018, pp. 1958–1963.

[7] R. Wheeler and S. Aitken, "Multiple Algorithms for Fraud Detection," *Knowledge-Based Systems*, vol. 2000, pp. 93–99, 2000.

[8] R.-C. Chen, M.-L. Chiu, Y.-L. Huang, and L.-T. Chen, "Detecting Credit Card Fraud by Using Questionnaire-Responded Transaction Model Based on Support Vector Machines," Aug. 2004, pp. 800–806, doi: 10.1007/978-3-540-28651-6_119.

[9] M. K. Mishra and R. Dash, "A Comparative Study of Chebyshev Functional Link Artificial Neural Network, Multi-layer Perceptron and Decision Tree for Credit Card Fraud Detection," in *2014 International Conference on Information Technology*, Dec. 2014, pp. 228–233, doi: 10.1109/ICIT.2014.25.

[10] A. Chouiekh and E. H. I. EL Haj, "ConvNets for Fraud Detection analysis," *Procedia Computer Science*, vol. 127, pp. 133–138, Jan. 2018, doi: 10.1016/j.procs.2018.01.107.

[11] J. O. Awoyemi, A. O. Adetunmbi, and S. A. Oluwadare, "Credit card fraud detection using machine learning techniques: A comparative analysis," in *International Conference on Computing Networking and Informatics (ICCNI)*, Oct. 2017, pp. 1–9, doi: 10.1109/ICCNI.2017.8123782.

[12] L. Frei, "Credit Card Fraud Detection Using Machine Learning Algorithm," *Data Camp Community*, 2018. [Online]. Available: https://www.datacamp.com/community/news/credit-card-fraud-detection-using-machine-learning-algorithm-8dyh3fefvrb.

[13] M. M. Najafabadi, F. Villanustre, T. M. Khoshgoftaar, N. Seliya, R. Wald, and E. Muharemagic, "Deep learning applications and challenges in big data analytics," *Journal of Big Data*, vol. 2, no. 1, p. 1, Feb. 2015, doi: 10.1186/s40537-014-0007-7.

[14] Y. Pandey, "Credit Card Fraud Detection using Deep Learning," *International Journal of Advanced Research in Computer Science*, vol. 8, no. 5, 2017.

[15] A. Candel, V. Parmar, E. LeDell, and A. Arora, *Deep learning with H2O*. H2O.ai, Inc, 2016.

[16] A. Pumsirirat and L. Yan, "Credit Card Fraud Detection using Deep Learning based on Auto-Encoder and Restricted Boltzmann Machine," *Int. J. Adv. Comput. Sci. Appl. IJACSA*, vol. 9, no. 1, Art. no. 1, pp. 55–31, 2018, doi: 10.14569/IJACSA.2018.090103.

[17] D. P. Kingma and J. Ba, "Adam: A Method for Stochastic Optimization," *ArXiv*, Dec. 2014. [Online]. Available: http://arxiv.org/abs/1412.6980.