Credit-card Fraud Detection System using Neural Networks

Salwa Al Balawi
Faculty of Computers and Information Technology,
University of Tabuk, Saudi Arabia
salwa7805@gmail.com

Njood Aljohani
Faculty of Computers and Information Technology,
University of Tabuk, Saudi Arabia
noaljohani@ut.edu.sa

Abstract: *Recently, with the development of online transactions, the credit-card transactions begun to be the most prevalent online payment methods. Credit-card fraud refers to the use fake Credit-Cards to purchase goods without paying. With the fast research and development in the area of information technology and data mining methods including the neural networks and decision trees, to advanced machine learning and deep learning methods, researchers have proposed a wide range of antifraud systems. Mainly, the Machine Learning (ML) and Deep Learning (DL) methods are employed to perform the fraud detection task. This paper aims to explore the existing credit-card fraud detection methods, and categorize them into two main categories. In addition, we investigated the deployment of neural network models with credit-card fraud detection problem, since we employed the Artificial Neural Network (ANN) and Convolutional Neural Network (CNN). ANN and CNN models are implemented and assessed using a credit-card dataset. The main contribution of this paper focuses on increasing the fraud-detection classification accuracy through developing an efficient deep neural network model.*

Keywords: *Credit-card, fraud detection, machine learning, deep learning, neural networks, classifications.*

Received December 3, 2020; accepted August 31, 2021
https://doi.org/10.34028/iajit/20/2/10

1. Introduction

Today, there are more diverse selection of credit cards in the world than ever before. According to recent statistics from Federal Reserve, more than half of the entire payments each year are made through credit cards. In 2017, 40.8 billion credit-card transactions were made worth $3.6 trillion, which is approximately 10% more than the previous year. Moreover, the increasing evolution of e-commerce that increases the online payments, and hence fraud detection has become a critical issue for banks [13, 19].

Mainly, the purpose of credit-card fraud may be to obtain goods or services, or to process a payment to another account, which is owned by a criminal. Credit-card fraud is a problem, which affects the whole consumer credit industry. Credit-card fraud involves using a credit-card that has been revoked, stolen, reported lost, or cancelled to obtain anything of value. In addition, the using of credit-card number without owning the actual card is also another type of credit-card fraud. Moreover, stealing a person's identity to receive his/her credit card is another form of credit-card fraud [2]. There are several credit card fraud techniques, including:

- Card-present fraud which includes stealing the credit-card physically. However, this fraud is not so common nowadays.
- Coping of a credit card details in some way.
- Vendors may charge the customers extra amount of money than agreed.

The increasing of infiltration rate of electronic transactions payments has led researchers to design and implement new methods to detect and identify the credit-card frauds in credit-card transactions. Machine Learning (ML) on the other hand, is a combination of several algorithms and statistical models in order to allow the computer to perform tasks with no need for coding. Neural Network (NN) and Deep Learning (DL) are the hottest topics nowadays; they used to detect the fraud. The idea is development model would be learning from the "training phase" [20]. However, with larger datasets, it is significant to select the appropriate set of features, which has significant effect on the output. The work aims to investigate the existing credit-card fraud detection methods, and to develop a credit-card fraud detection model. The main contribution of this paper lies on the following aspects:

- Research the recent development of current credit-card fraud detection systems.
- Classify and discuss the existing credit-card fraud detection systems.
- Design and implement an efficient credit-card fraud detection model, which is able to detect the frauds for credit-card transactions using NN.
- Assess the efficiency for the implemented credit-card fraud detection models using real dataset transactions.

The rest of this paper is organized as follows: Section two discusses the recent development in credit-card

fraud detection models. In section three, the experiment setup is discussed in details, whereas in Section four, the results obtained from real experiments are presented and analysed. Section five discusses the results of the ANN and CNN models, and finally, Section six, concludes the work presented in this paper and presents future works.

2. Related Works

The credit-card fraud detection issue is one of the most discovered domains of fraud detection, and it depends on automatic analysis of documented transactions to detect fraudulent actions [6]. Lucas [4], introduced an exhaustive comparison of a large number of algorithms and modelling techniques on two real datasets, where authors focused on testing three different supervised algorithms: NN, Random Forests (RF), and Support Vector Machine (SVM). They revealed that RF method clearly outperforms its competitors and accuracy is improved by increasing the training size.

According to [17], 49 different supervised learning techniques are reviewed, where authors conclude that decision trees, NN, SVM, and logistic regression are employed more than others. Maes *et al*. [15], applied two ML techniques, Artificial Neural Networks (ANN) and Bayesian Belief Networks (BBN), and study the impact of those techniques on real world financial data. The main idea is correctly classify a transaction that it has never ever seen before as fraudulent or not. Pillai *et al*. [18], the authors aimed to offer a guidance on how to pick the finest model to achieve the optimal results with the minimal cost, using an efficiency of Multi-Layer Perception (MLP). The results show the highest precision 96%. The benefit of auto-encoder method is the generality virtues, and has the ability to work with huge datasets. Because of the large number of behaviours of customers in the banking transactions, the extracting of the appropriate features to detect the fraudulent is a very complex task. Therefore, employing deep auto-encoder is a beneficial idea to solve out the aforementioned issue [11].

Unsupervised fraud detection system by auto-encoder-based clustering used to detect the fraud transactions in unsupervised manner. The results from applying k-means clustering appear that accuracy of 98.7% was achieved [24]. Shenvi *et al*. [22], proposed a credit-card fraud detection system using DL neural networks. Author reveals that even if the NN is trained over a huge number of iterations, it is not accurate enough to classify the transactions data as fraudulent or non-fraudulent because of the skewness of the dataset. On the other hand, author proposed two sampling mechanisms named:

1. The under-sampling, through reducing the number of non-fraudulent observations.
2. The over-sampling, where the fraudulent class observations are duplicated. The obtained results showed that these two methods increase the accuracy of the prediction process.

Feature mining used to extend the features of credit-card transaction with time dimension to categorize the distinct payment habits for legal users and criminals, the other methods was Capsule Network (CapsNet) employed to further pick other deep features base on the extended features. CapsNet is a powerful feature extraction model, which further increases the efficiency of the fraud detection model. Although the CapsNet offers the best performance, but it still has a number of limitations, as with large time consumption [23]. Chen *et al*. [5], combined the sparse autoencoder (SAF) and discriminator of Generative Adversarial Networks (GAN) to perceive whether a certain transaction is fraud or not. The experimental results show that the combined solution offers a significant increment in the detection accuracy.

The recent developed systems offer reasonable credit-card fraud detection accuracy; however, the fraud detection accuracy must be high. Therefore, in this paper, we focus on developing an accurate credit-card fraud detection system using deep neural networks.

In this article used the ANN and Convolutional Neural Network (CNN) with and without pooling, in order to detect fraud [9, 10]. CNN is better to convert the data to picture and train the CNN to detect the fraud. From the previous, this article introduce the best accuracy reach to more than 99%. In all the previous this search on the high accuracy.

3. Methodology

The credit-card fraud detection problem involves modelling past credit-card transactions with the previous knowledge of existing transactions that turned out to be fraud. This section covers the experimental setup including the development environment, the selected credit-card dataset, and experimental setup.

3.1. Development Environment

For evaluation purposes, several experiments have been conducted in order to validate the developed models' efficiency. This section discusses the development environment, that includes the followings:

1. Colab or Colaboratory: is a cloud and supports free GPU. Moreover, Colab supports many popular ML libraries such as Tensorflow and Keras. We apply our experiments on Colab environment.
2. TensorFlow: is an open-source library for numerical computations and large-scale ML. We used TensorFlow library to execute the experiments.
3. Keras: is a neural network library running on the

top of Tensorflow. Keras was designed to offer fast experimentation and help the user to apply NN in easy methods. We used the Keras library command to achieve experiments.

3.2. Dataset

After considering an extensive search on the available Credit-card datasets, a few credit-card transaction datasets are available online. This is because, Credit-card transactions contain sensitive information which must be kept secure and unrevealed. In this Section, he selected credit-card dataset is discussed and analysed.

The Credit-card Fraud Detection dataset at Kaggle consists of credit-card transactions made in September 2013 by the European cardholders for two days [4]. The selected credit-card dataset has been adopted in many research works [1, 8, 12], and this indicates the importance of the selected dataset. Table 1, shows general statistics about the credit-card dataset.

The selected credit-card dataset consists of 248,807 transaction records where very few transactions are actually fraudulent (0.1727%) 492 fraud transactions; this means that this dataset is highly unbalanced. The dataset contains numerical input variables, which are the results of Principal Component Analysis (PCA) transformation. This dataset does not deliver the original features and clarifications about the data.

Features V1, V2, V3, V28 are the principal component values acquired with PCA. However, there is no metadata about the original featured provided, therefore pre-analysis or feature study could not be accomplished. On the other hand, the Time and Amount features are not transformed data, and the dataset does not contain any missing data. Since all features presented in the credit-card dataset are anonymous, Time and Amount features will be analysed.

Table 1. Credit-card dataset general statistics.

Parameter name	Total #
Total number of transactions	284,807
Total number of columns	31
Total number of features	28
Total number of labels	1
Total number of normal transactions	284,315
Total number of fraudulent transactions	492
% of fraudulent transactions	00.1727%
% of normal transactions	99.8273%

There are three non-transformed values: Time, Amount, and Class. The 'Time' attribute includes the seconds passed between any transaction and the 1st transaction in the dataset. On the other hand, the feature 'Amount' is the total amount for each transaction.

Moreover, feature 'Class' is the type of transaction value; it is '0' for normal transaction and '1' for fraud transaction. Figure 1, presents the heat map for the credit-card attributes in the credit-card dataset, where there is a high correlation between the Time and V3, Amount and V2, and Amount and V4. In addition, the correlation matrix shows that none of the V1 to V28 components have any correlation to each other. Moreover, the Class attribute has no correlation with Amount and Time attributes, whereas in various cases, the Class attribute has positive and negative correlations with some V attributes.

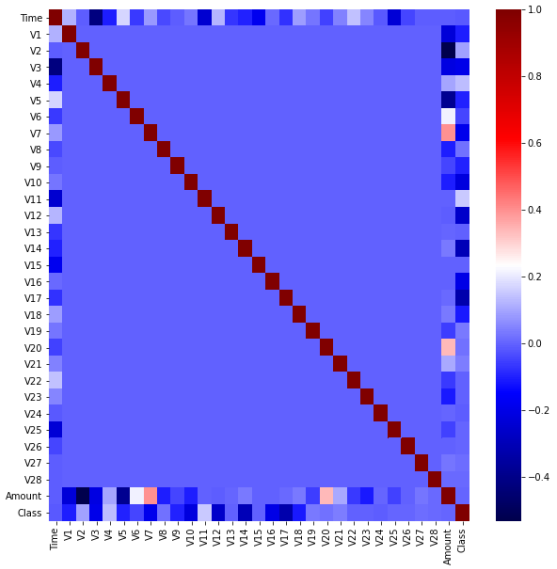

Figure 1. The heat map for the credit-card dataset.

3.3. Neural Network Models

In this section, the neural network models are discussed in details: ANN, and CNN. The defined models are then used to identify whether a new transaction is normal or fraudulent ones. The main aim of the implemented prediction models is to detect maximum possible ratio of the fraudulent transactions while reducing the number of incorrect fraud classifications. Figure 2, presents the developed ANN model for fraud-detection in credit-card transactions. The designed ANN model is based on Sequential model, which is appropriate for a plain stack of layers.

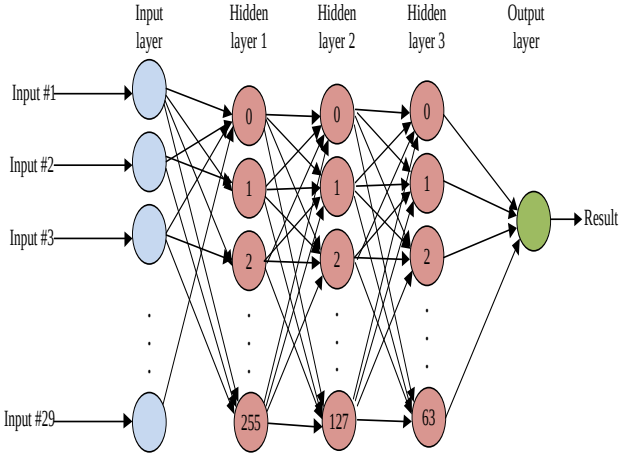

Figure 2. The credit-card of the ANN model.

Convolutional networks are neural networks that employ convolution in place of general matrix multiplication in at least one of the CNN layers. As

with normal neural network model, the CNN contains an input and output layers, in addition to multiple hidden layers. However, in the CNN, the hidden layers consist of a series of convolutional layers that convolve with a multiplication. In this paper, a one-dimensional CNN model is adopted for credit-card fraud detection. The CNN architecture is presented in Figure 3. On the other hand, in this paper we study the performance of the Pooling layer with the one-dimensional CNN model, therefore, another CNN model for credit-card fraud detection without the employment of pooling layer. Figure 4, shows the CNN model without pooling layer.

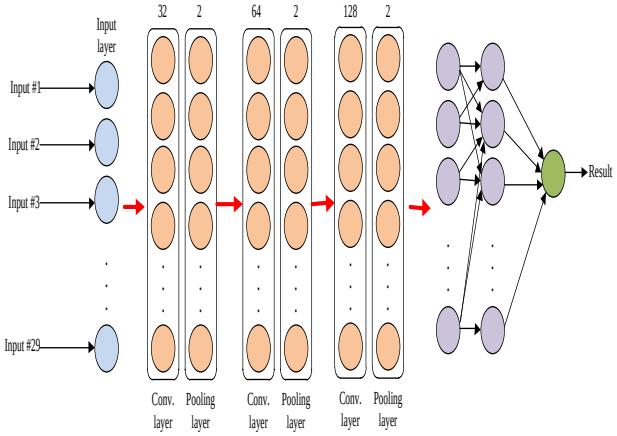

Figure 3. The credit-card of the CNN model with pooling layer.

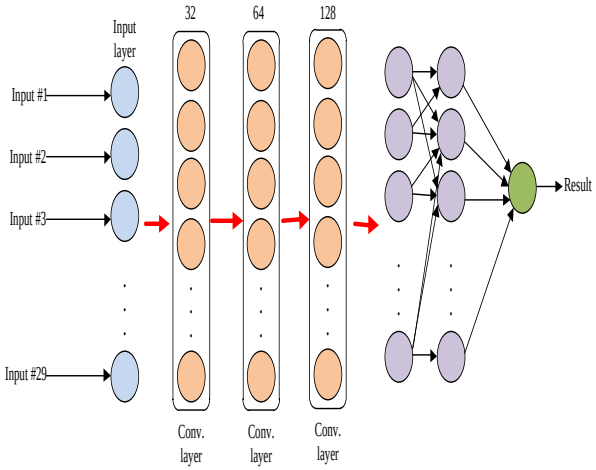

Figure 4. The credit-card of the CNN model wihtout pooling layer.

4. Results

This section discusses the real experiments, which have been conducted in order to validate the developed credit-card fraud detection system. For both models (ANN and CNN), the training dataset consists of samples of data used to fit the ANN and CNN models, where the NN model sees and learns from the training dataset. On the other hand, the validation dataset is used to evaluate the NN model and tune the model hyper-parameters. The validation dataset helps during the development phase of the NN model. Finally, the testing dataset, offers the gold standard used to assess the NN model, and it is used once the NN model is completely trained. Table 2, presents general statistics for the credit-card dataset, where it consists of number of train, validation, and testing records.

Table 2. Statistics of the credit-card dataset.

Parameter name	Normal	Fraud
Training records	159,207	284
Validation records	39,812	61
Testing records	85,296	147
Transaction records	284,315	492

4.1. Results of Training Phase

During the training of a NN model, each state of the NN model at each step can be evaluated. It can be evaluated on the training dataset in order to give a clue of how well the NN model is learning. The presented NN model is evaluated using the validation dataset, which is not a part of the training dataset, because evaluation on the validation dataset informs how well the NN model is generalizing. Figure 5, shows the training loss of the ANN model for the training and validation datasets, where the validation loss is lower than the training loss. On the other hand, Figure 6, shows the training loss for CNN model with pooling layer for the training and validation datasets, where the validation loss is almost less than the training loss, and Figure 7, presents the training loss for the CNN model without pooling layer. From the previous, the training loss for the CNN is slightly better than the ANN model. On the other hand, the training loss for the CNN without pooling layer is much better than the CNN with the Pooling layer.

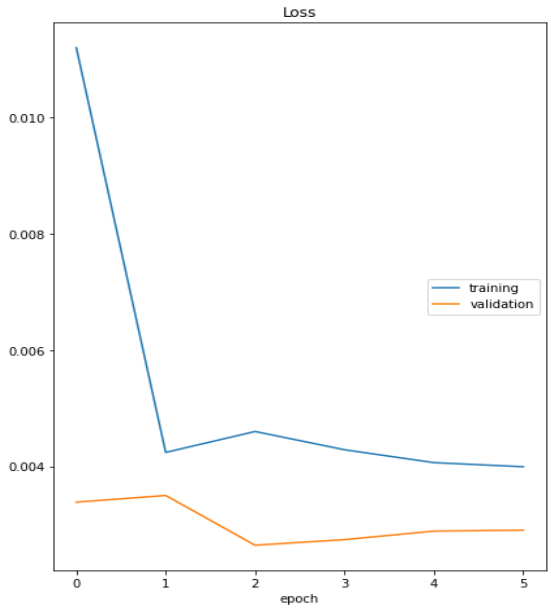

Figure 5. The training loss graph for the ANN model.

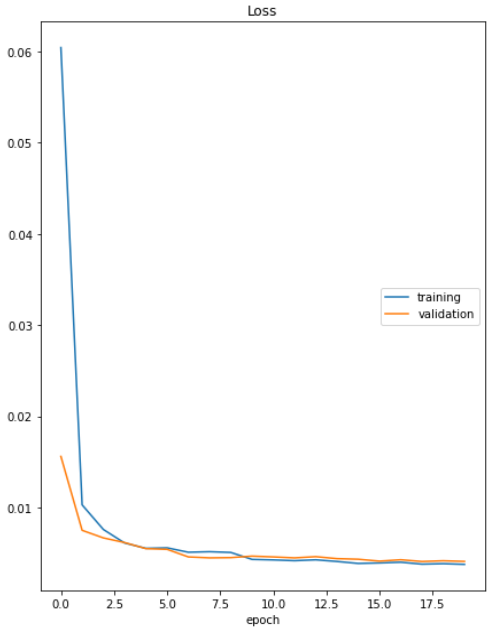

Figure 6. The training loss graph for the CNN model with Pooling layer.

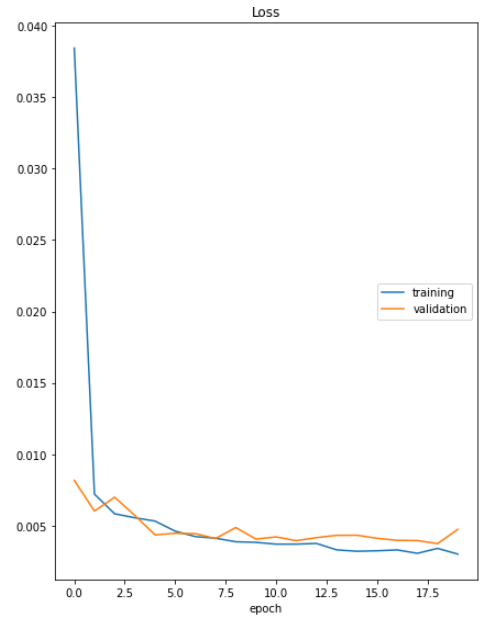

Figure 7. The training loss graph for the CNN model without Pooling layer.

The training accuracy for both the training dataset and validation dataset is also studied. Whenever the training process is conducted, accuracy and loss could be variating with different cases.

Usually, with every epoch increasing, loss should be going down while accuracy should be going up. Figures 8, 9, and 10, show the training accuracy of the training and validation sets for the ANN, CNN with pooling layer, and CNN without pooling layer, respectively. As presented, the training accuracy has increased with every epoch, and this means that the ANN and CNN models are learning and working fine.

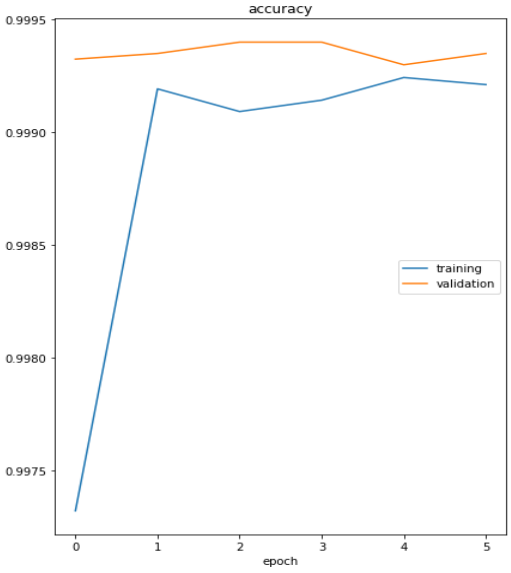

Figure 8. The training accuracy graph for the ANN model.

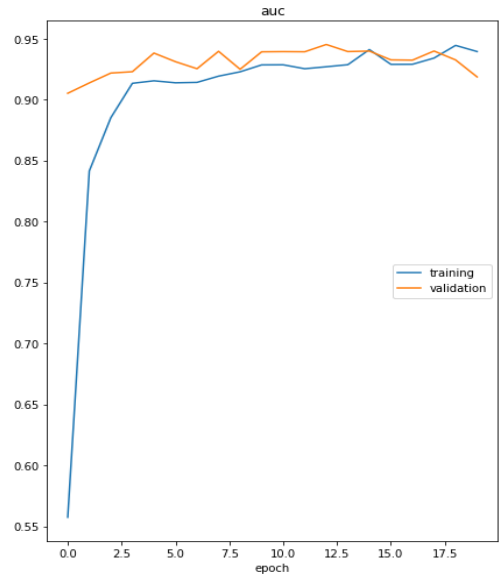

Figure 9. The training accuracy graph for the CNN model with Pooling layer.

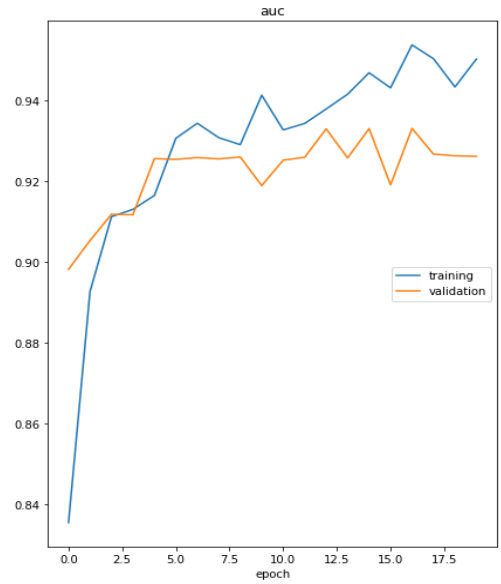

Figure 10. The training accuracy graph for the CNN model without Pooling layer.

4.2. Results of Classifications

This section discusses the classification results for the three models: ANN, CNN with Pooling layer and CNN without Pooling layer. After considering several experiments, Table 3, shows the classification report for the ANN classification, which determines the quality of predictions. In ANN model, the False Negative Rate (FNR) is almost 23%, this is because the selected credit-card dataset is unbalanced, where the fraud transaction rate is very low. On the other hand, the False Positive Rate (FPR) is a quite low with 0.018%, since the normal transaction records are high in total. On the other hand, Table 4, shows the classification report for the CNN model, and Table 5, presents the CNN without pooling layer classification report. As presented below, CNN without pooling layer achieves better results in classifying the fraud transactions than the CNN with pooling layer. Both models (CNN with Pooling layer and CNN without pooling layer) offer high precision in classifying the normal transactions. In overall, the CNN without Pooling layer offers better results than the CNN with Pooling layer and the ANN models.

Table 3. ANN classification report for the testing dataset.

Class	Precision	recall	F1-score	support
0	1.00	1.00	1.00	85296
1	0.96	0.53	0.68	147
Accuracy			1.00	85443
Macro average	0.98	0.77	0.84	85443
Weighted average	1.00	1.00	1.00	85443

Table 4. CNN with pooling layer classification report.

Class	Precision	recall	F1-score	support
0	1.00	1.00	1.00	85,307
1	0.74	0.87	0.80	136
Accuracy			1.00	85,443
Macro average	0.87	0.93	0.90	85,443
Weighted average	1.00	1.00	1.00	85,443

Table 5. CNN without pooling layer classification report.

Class	Precision	recall	F1-score	support
0	1.00	1.00	1.00	85,307
1	0.83	0.84	0.84	136
Accuracy			1.00	85,443
Macro average	0.92	0.92	0.92	85,443
Weighted average	1.00	1.00	1.00	85,443

5. Discussion

In this paper, two main NN algorithms (ANN and CNN) have been employed, implemented, and experimentally tested for credit-card fraud detection applications. ANN model is able of learning any nonlinear function, and has the capacity to learn weights that map any input value to any output value. Moreover, activation function plays a significant rule to adapt nonlinear functions, and helps the network to learn any complex relationship between the input and output values.

On the other hand, the CNN model is one of the most popular models employed nowadays. CNN model is a class of deep neural networks, which is most commonly used to analyse visual imagery. CNN learns the filters in an autonomous way without mentioning it explicitly, where these filters help in extracting the correct and relevant features from the input dataset. CNN uses various multilayer perceptions and includes one or more convolutional layers, which can be either completely connected or pooled. In CNN, the convolutional layers are very effective in learning low-level features and hence increase the efficiency of choosing the correct features from the credit-card dataset. The main advantage of convolutional layers is to create a feature maps without human supervision.

In CNN model, the Pooling layer usually applied after the convolutional layer in order to minimize the spatial size of the input array, hence, pooling layer aims to minimize the number of training parameters, and therefore governing the overfitting. In this paper, two different CNN models have been experimented, as follows: CNN model with pooling layer, and CNN model without pooling layer, in order investigate the effect of pooling layer on the credit-card fraud detection problem. As presented in section 4, employing Pooling layers with CNN does not usually enhance the efficiency of the credit-card fraud detection model. Hence, the Pooling is loss and does not reserve all the spatial information well by dropping spatial resolution. In addition, Max Pooling selects discrete maximum values of the input array of features, which is not truly the maximum. As presented earlier in section 4, the CNN model achieves low FNR (13%) whereas the ANN achieves almost (46%), and therefore CNN model is more secure credit-card fraud detection model, since rarely the CNN model predicts a fraud transaction as a normal transaction. On the other hand, the CNN with pooling layer offers the best True Positive Rate (TPR) with (86.76%), the CNN without pooling layer (83.82%), and the ANN model (77.23%). This result better than using other algorithm such as [3, 14].

The loss and metric values are also studied for each experimented model. Table 6, presents the loss and metrics values for the ANN, CNN with pooling layer, and the CNN without pooling layer. As presented, the CNN model without pooling layer achieves the best results in terms of loss and metrics values.

Table 6. Loss and metrics for the ANN and CNN models.

Parameter name	Normal	Fraud
NN model	0.00392	0.94986
CNN model with Pooling Layer	0.00301	0.95855
CNN model without Pooling Layer	0.00244	0.96991

The F1-score is also evaluated for the three models. F1-score is the weighted average of precision and recall, where both the false positives and false

negatives are taken into account. F1-score is considered as more useful than accuracy when evaluating any classification model, and especially when the dataset is unbalanced. Accuracy is more useful when the false positives and false negatives are almost equal (balanced dataset), however, with the selected dataset the F1-score is more significant to assess the employed ANN models. As presented in Table 7, the CNN model without pooling layer achieves the best F1-score, whereas the CNN model with pooling layer comes in the second place, because using pooling leads to reduce the visibility, and the worse F1-score was with the NN model.

Table 7. Evaluating of F1-score for the three classifiers.

Parameter name	F1-score
ANN model	71.01%
CNN model with Pooling Layer	81.38%
CNN model without Pooling Layer	83.72%

According to [2, 16], experimental results offers the best accuracy result (99.47%). The proposed system achieves (99.64%) accuracy better than [21]. In [7], proposed a Credit-Card fraud detection model using ANN and Back propagation, the experimental results show high accuracy (99.76%) compared to the existing models. However, the implemented CNN model in this work achieves higher accuracy (99.81%), and this indicates the significance of the developed CNN model.

As a result, the developed deep neural network model achieves efficient classification accuracy, and offers an improvement in the classification accuracy over the existing credit-card fraud detection systems.

6. Conclusions and Future Work

This paper aims to investigate the existing credit-card fraud detection methods, and to design and implement a credit-card fraud detection method using NN models. The recent credit-card fraud detection systems are categorized, presented, analysed, and discussed. In addition, two different NN models have been experimentally tested, where the performance for each model has been assessed through analysing several parameters. The effect of pooling layer in CNN models is also studied, analysed, and experimentally tested. As a result, the developed deep neural network model offers efficient classification accuracy. For future work, we aim to consider balanced credit-card dataset in order to assess the performance of the developed ANN and CNN model. In addition, we aim to implement machine learning models to assess the precision and accuracy for these models, and compare the obtained results with the deep neural network models.

References

[1] Bahnsen A., Aouada D., Stojanovic A., and Ottersten B., "Feature Engineering Strategies for Credit Card Fraud Detection," *Expert Systems with Applications*, vol. 51, pp. 134-142, 2016.

[2] Bhattacharyya S., Jha S., Tharakunnel K., and Westland J., "Data Mining for Credit Card Fraud: A Comparative Study," *Decision Support Systems*, vol. 50, no. 3, p. 602-613, 2011.

[3] Buonaguidi B., Mira A., Bucheli H., and Vitanis V., "Bayesian Quickest Detection of Credit Card Fraud," *Bayesian Analysis*, vol. 17, no.1, pp. 1-30, 2021.

[4] Cardholders E., "Credit-card Fraud Detection Dataset [cited; Available from:https://www.kaggle.com/mlg-ulb/creditcardfraud, Last Visited, 2021.

[5] Chen J., Shen Y., and Ali R., "Credit Card Fraud Detection Using Sparse Autoencoder and Generative Adversarial Network," *in Proceedings of IEEE 9th Annual Information Technology, Electronics and Mobile Communication Conference*, Vancouver, 2018.

[6] Dal Pozzolo A., Caelen O., Le Borgne Y., Waterschoot S., and Bontempi G., "Learned Lessons in Credit Card Fraud Detection from A Practitioner Perspective," *Expert Systems with applications*, vol. 41, no.10, pp. 4915-4928, 2014.

[7] Dubey S., Mundhe K., and Kadam A., "Credit Card Fraud Detection using Artificial Neural Network and BackPropagation," *in Proceedings of 4th International Conference on Intelligent Computing and Control Systems*, Madurai, 2020.

[8] Fiore U., De Santis A., Perla F., Zanetti P., and Palmieri, F., "Using Generative Adversarial Networks for Improving Classification Effectiveness in Credit Card Fraud Detection," *Information Sciences*, vol. 479, pp. 448-455, 2019.

[9] Gholamalinezhad H. and Khosravi H., "Pooling Methods in Deep Neural Networks, a Review," *arXiv preprint arXiv:2009.07485*, 2020.

[10] Hussain F., Abbas S., Husnain M., Fayyaz U., Shahzad F., and Shah G., "IoT DoS and DDoS Attack Detection using ResNet," *in Proceedings of IEEE 23rd International Multitopic Conference*, Bahawalpur, 2020.

[11] Kazemi Z. and Zarrabi H., "Using Deep Networks for Fraud Detection in The Credit Card Transactions," *in Proceedings of IEEE 4th International Conference on Knowledge-Based Engineering and Innovation*, Tehran, 2017.

[12] Lakshmi S. and Kavilla S., "Machine Learning for Credit Card Fraud Detection System," *International Journal of Applied Engineering Research*, vol. 13, no. 24, pp. 16819-16824, 2018.

[13] Lebichot B., Le Borgne Y., He-Guelton L., Oblé F., and Bontempi G., "Deep-Learning Domain Adaptation Techniques for Credit Cards Fraud

Detection," *in Proceedings of INNS Big Data and Deep Learning Conference*, Genova, 2019.

[14] Lucas Y., "Credit Card Fraud Detection Using Machine Learning With Integration of Contextual Knowledge, Thesis Université de Lyon; Universität Passau (Deutscheland), 2019.

[15] Maes S., Tuyls K., Vanschoenwinkel B., and Manderick B., "Credit card fraud Detection Using Bayesian and Neural Networks, *in Proceedings of the 1st International Naiso Congress on Neuro Fuzzy Technologies*, Havana, 2002.

[16] Mubarek A. and Adalı E., "Multilayer Perceptron Neural Network Technique for Fraud Detection," *in Proceedings of International Conference on Computer Science and Engineering*, Antalya, 2017.

[17] Ngai E., Hu Y., Wong Y., Chen Y., and Sun X., "The Application of Data Mining Techniques in Financial Fraud Detection: A Classification Framework and an Academic Review of Literature," *Decision Support Systems*, vol. 50, no. 3, p. 559-569, 2011.

[18] Pillai T., Hashem I., Brohi S., Kaur S., and Marjani M., "Credit Card Fraud Detection Using Deep Learning Technique," *in Proceedings of 4th International Conference on Advances in Computing, Communication and Automation*, Subang Jaya, 2018.

[19] Pokkuluri K., Nedunuri S., and Devi U., "Crop Disease Prediction with Convolution Neural Network (CNN) Augmented with Cellular Automata," *The International Arab Journal of Information Technology*, vol. 19, no. 5, pp. 765-773, 2022.

[20] Raghavan P. and El Gayar N., "Fraud Detection Using Machine Learning And Deep Learning," *in Proceedings of International Conference on Computational Intelligence and Knowledge Economy*, Dubai, 2019.

[21] Sahin Y. and Duman E., "Detecting Credit Card Fraud by ANN and Logistic Regression," *in Proceedings of International Symposium on Innovations in Intelligent Systems and Applications*, Istanbul, 2011.

[22] Shenvi P., Samant N., Kumar S., Kulkarni V., "Credit Card Fraud Detection Using Deep Learning," *in Proceedings of IEEE 5th International Conference for Convergence in Technology*, Bombay, 2019.

[23] Wang S., Liu G., Li Z., Xuan S., Yan C., and Jiang C., "Credit Card Fraud Detection Using Capsule Network," *in Proceedings of IEEE International Conference on Systems, Man, and Cybernetics*, Miyazaki, 2018.

[24] Zamini M. and Montazer G., "Credit Card Fraud Detection Using Autoencoder Based Clustering," *in Proceedings of 9th International Symposium on Telecommunications*, Tehran, 2018.

Salwa Al Balawi, I have a Bachelor's degree in Computer Science from the University of Tabuk, Saudi Arabia, in 2015, and I obtained a master's degree in information security from the University of Tabuk, Saudi Arabia, in 2020. I worked as a lecturer at Unaizah College in Qassim in the Department of Cybersecurity from 2021 to in 2022, my research interests include machine learning, deep learning, and information steganography.

Njood Aljohani, I obtained a Ph.D. in artificial intelligence and I am currently working as an associate professor at the Faculty of Computer at the University of Tabuk. And I am currently working as a dean of the Faculty of Computer at the University of Tabuk