Hybrid LSTM- SVM Model for Improved Credit Card Fraud Detection: A Comparative Study with KNN, Naïve Bayes, SVM and Logistic Regression

M.Antro Monica Sanjas
Assistant Professor, Dept. of CSE(AIML), Loyola Institute of Technology and Science, Thovalai, Nagarcoil, India
monica.cse@lites.edu.in

A.Merry Ida
Assistant Professor, Dept. of CSE, Loyola Institute of Technology and Science, Thovalai, Nagarcoil, India
ida.cse@lites.edu.in

S.G.Santhiya
Assistant Professor, Dept. of CSE(AIML), Loyola Institute of Technology and Science, Thovalai, Nagarcoil, India
santhiyasujin96@gmail.com

P.Anitha
Assistant Professor, Dept. of CSE(AIML), Loyola Institute of Technology and Science, Thovalai, Nagarcoil, India
mercysahayam@gmail.com

S.Angel Nithya
Assistant Professor, Dept. of CSE(AIML) Loyola Institute of Technology and Science, Thovalai Nagarcoil, India
angelnithya71@gmail.com

***Abstract*—** The growing number and complexity of fraudulent transactions make detecting credit card theft a crucial task in the banking industry. The identification of fraud has made extensive use of traditional machine learning techniques including K-Nearest Neighbor (KNN), Naïve Bayes, SVM, and Logistic Regression. However, these models frequently encounter difficulties when dealing with the temporal correlations and sequential patterns present in transaction data. Long Short-Term Memory (LSTM) networks and Support Vector Machine (SVM) classifiers are combined in this study's hybrid technique to enhance fraud detection capabilities. The LSTM network generates high-level feature representations by efficiently capturing temporal correlations and sequential patterns in transaction sequences. An SVM, which offers strong decision boundaries and improved generalization on unbalanced datasets, is then used to classify these features. The suggested LSTM → SVM hybrid model performs better than KNN, Naïve Bayes, regular SVM, and Logistic Regression in terms of accuracy, precision, recall, and F1-score, according to experiments done on a benchmark credit card fraud dataset. The findings show that using temporal sequence modeling in conjunction with SVM classification greatly improves the identification of fraudulent activity, which makes it a viable strategy for practical financial security applications.

Keywords— LSTM, SVM, Hybrid Model, Credit Card Fraud Detection, Temporal Feature Extraction, Machine Learning

Introduction

Reports of Credit card fraud in the US rose by 44.7% from 271,927 in 2019 to 393,207 reports in 2020. There are two kinds of credit card fraud, the first one is by having a credit card account opened under your name by an identity thief, reports of this fraudulent behavior increased 48% from 2019 to 2020. The second type is by an identity thief uses an existing account that you created, and it's usually done by stealing the information of the credit card, reports on this type of fraud increased 9% from 2019 to 2020 (Daly, 2021). Those statistics caught my attention as the numbers are increasing drastically and rapidly throughout the years, which gave me the motive to try to resolve the issue analytically by using different machine learning methods to detect the credit card fraudulent transactionswithin numerous transactions.

The main aim of this research is the detection of credit card fraudulent transactions, as it'simportant to figure out the fraudulent transactions so that customers don't get charged for the purchase of products that they didn't buy. The detection of the credit card fraudulent transactions will be performed with multiple ML techniques then a comparison will be made between the outcomes and results of each technique to find the best and most suited model in the detection of the credit card transaction that are fraudulent, graphs and numbers will be provided as well. In addition,

exploring previous literatures and different techniques used to distinguish the fraud within a dataset.

Research question: What is the most suited machine learning model in the detection of fraudulent credit card transactions?

LITERATURE REVIEW

The model used by Alenzi and Aljehane[2] to detect fraud in credit cards was Logistic Regression, their model scored 97.2% in accuracy, 97% sensitivity and 2.8% Error Rate. A comparison was performed between their model and two other classifier which are Voting Classifier and KNN. VC scored 90% in accuracy, 88% sensitivity and 10% error rate, as for KNN where k = 1:10, the accuracy of the model was 93%, the sensitivity 94% and 7% for the error rate (Alenzi & Aljehane, 2020).

Manirajs team [17] built a model that can recognize if any new transaction is fraud or non- fraud, their goal was to get 100% in the detection of fraudulent transactions in addition totrying to minimize the incorrectly classified fraud instances. Their model has performed well as they were able to get 99.7% of the fraudulent transactions (Maniraj et al., 2019).

Mailini and Pushpa proposed [16] using KNN and Outlier detection in identifying credit card fraud, the authors found after performing their model over sampled data, that the most suited method in detecting and determining target instance anomaly is KNN which showed that its most suited in the detection of fraud with the memory limitation. As for Outlier detection the computation and memory required for the credit card fraud detection is much less in addition to its working faster and better in online large datasets. But their work and results showed that KNN was more accurate and efficient (Malini & Pushpa, 2017).

The classification approach used by Dheepa and Dhanapal[7] was the behavior-based classification approach, by using Support Vector Machine, where the behavioral patterns of the customers were analyzed to distinguish credit card fraud, such as the amount, date, time, place, and frequency of card usage. The accuracy achieved by their approach wasmore than 80% (Dheepa & Dhanapal, 2012).

The team of Awoyemi[3] compared the usage of three ML techniques in the detection of credit card fraud, the first is KNN, the second is Naïve Bayes and the third is Logistic Regression. They sampled different distributions to view the various outcomes. The top Accuracy of the 10:90 distribution is Naïve Bayes with 97.5%, then KNN with 97.1%,

The paper of Kiran and his team[13] presents Naïve Bayes (NB) improved (KNN) K-Nearest Neighbor method for Fraud Detection of Credit Card which is (NBKNN) in short format. The outcome of the experiment illustrates the difference in the process of each classifieron the same dataset. Naïve bayes performed better than K-nearest neighbor as it scored an accuracy of 95% while KNN scored 90% (Kiran et al., 2018).

The team of Tanouz[23] proposed working on various ML based classification algorithms, like Naïve Bayes, Logistic Regression, Random Forest, and Decision Tree in handling datasets that are strongly imbalanced, in addition their research will have the calculations of five measures the first is accuracy, the second is precision, the third is recall, the fourth is confusion matrix, and the last one is Roc-auc score. 95.16% is the score of both Logistic Regression and Naïve Bayes, 96.77% is the score for random forest, for the last model Decision Tree scored 91.12% (Tanouz et al., 2021).

Dighe and his team[8] used KNN, Naïve Bayes, Logistic Regression and Neural Network, Multi-Layers Perceptron and Decision Tree in their work, then evaluated the results in terms of numerous accuracy metrics. Out of all the models created the best performing one is KNN which scored 99.13%, then in second place Naïve Bayes which scored 96.98%, the third best performing model 96.40% and in last place is logistic regression with 96.27% (Dighe et al., 2018).

The lowest accuracy of the four models that will be studied in this research, is 54.86% for KNN and 36.40% for logistic Regression which were scored by Awoyemi and his team, as for Naïve Bayes the lowest accuracy was scored by Gupta and his team which is 80.4% and finally, SVM the lowest score was 94.65% and it was scored by Jain's team. To determine the best model out of the four models that will be studied through the research, the average of the best three accuracies of each model will be calculated, the average of the accuracy of KNN is 98.72%, the average of logistic regression is 98.11%, 98.85% for Naïve bayes and 96.16% for Support Vector Machine.

Last but not least, this study has compared the LSTM-SVM hybrid model to traditional classifiers (KNN, Naïve Bayes, SVM, and Logistic Regression) in terms of accuracy, precision, recall, and F1-score, proving the hybrid model's improved performance in practical settings. The ultimate goal of the project is to give financial institutions a workable and expandable way to increase transaction security, lower fraud losses, and raise general confidence in digital payment systems.

Data Source:

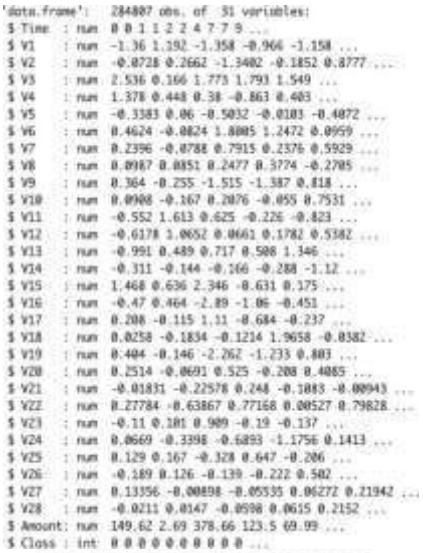
The dataset was retrieved from an open-source website, Kaggle.com. it contains data oftransactions that were made in 2013 by credit card users in Europe, in two days only. The dataset consists of 31 attributes, 284,808 rows.

Data Preparation:

The figure 1 bellow shows the structure of the dataset where all attributes are shown, with their type, in addition to glimpse of the variables within each attribute, as shown at the end of the figure the Class type is integer which I needed to change to factor and identify the 0 as Not Fraud and the 1

as Fraud to ease the process of creating the model and obtain visualizations

Figure 1 - Dataset Structure



	Reference	
Prediction	Not Fraudulent	Fraudulent
Not Fraudulent	89684	33
Fraudulent	2018	139

Accuracy : 0.9777

Data Preprocessing:

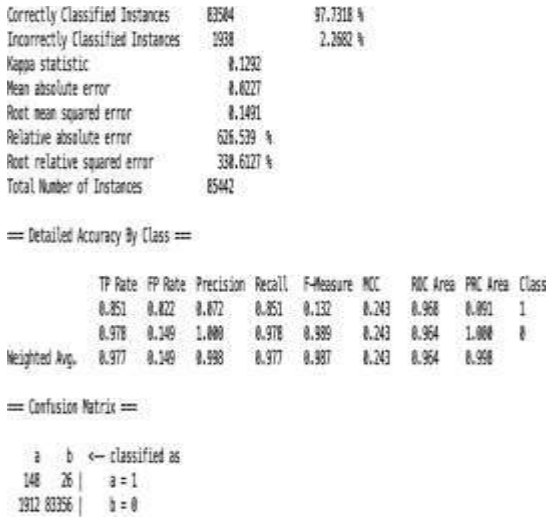
As there are no NAs nor duplicated variables, the preparation of the dataset was simple the first alteration that was made to be able to open the dataset on Weka program is changing the type of the class attribute from Numeric to Class and identify the class as {1,0} using the program Sublime Text. Another alteration was made on the type as well on the R program to be able to create the model and the visualization.

Data Modeling:

After making sure that the data is ready to get modeled the four models were created using both Weka and R. the model SVM was created using Weka only, as for KNN, Logistic Regression and NaïveBayes they were created using R and Weka.

KNN

The K-Nearest Neighbor algorithm (KNN) is a supervised ML technique that can be applied in both scenario instances, classification instances along with regression instances (Mahesh, 2020).To figure the best KNN model two Ks where used K=3 and K=7, both are presented with figures from both Weka and R. During the making of the KNN model, I decided to create two models where K=3 and K=7. Figure 3 shows the model created in R, the model scored an accuracy of 99.83% and managed to correctly identify 91,719 transactions and missed 155. As for the Weka program the model scored 99.94% for the accuracy and miss-classified 52 transactions. As there are different accuracies the average of the accuracies is 99.89%.



Naïve Bayes:

The second model created by R is Naïve Bayes, figure 5 shows the performance of the model, it scored an accuracy of 97.77% and misclassified a total of 2,051 transactions, 33 fraudulent as nonfraudulent and 2018 nonfraudulent as fraudulent. There is a slight difference in the accuracy of the Naïve bayes model created within Weka as its 97.73% and the misclassification instances are 1,938.

Figure 4 - Weka Naïve Bayes

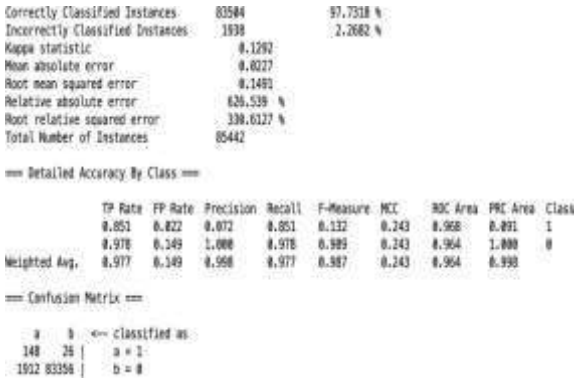


Figure 5 - RStudio Naïve Bayes

Confusion Matrix and Statistics

	Reference	
Prediction	Not Fraudulent	Fraudulent
Not Fraudulent	89684	33
Fraudulent	2018	139

Accuracy : 0.9777

Logistic Regression

The last model created using both R and Weka is

Logistic Regression, the model managed to score and accuracy of 99.92% in R (figure 7) with 70 misclassified instances, while it scored 99.91% in Weka with 77 misclassified instances as presented in figure 10.

Figure 6 - Weka Logistic Regression

```
Correctly Classified Instances       85365               99.9088 %
Incorrectly Classified Instances        77                0.0901 %
Kappa statistic                          0.7256
Mean absolute error                      0.0014
Root mean squared error                  0.0276
Relative absolute error                 38.6516 %
Root relative squared error             61.1796 %
Total Number of Instances            85442

=== Detailed Accuracy By Class ===

               TP Rate  FP Rate  Precision  Recall  F-Measure  MCC      ROC Area  PRC Area  Class
                 0.586    0.000    0.953      0.586   0.726      0.747    0.976     0.831     1
                 1.000    0.414    0.999      1.000   1.000      0.747    0.976     1.000     0
Weighted Avg.    0.999    0.413    0.999      0.999   0.999      0.747    0.976     1.000

=== Confusion Matrix ===

     a     b   <-- classified as
   102    72 |     a = 1
     5 85263 |     b = 0
```

Figure 7

```
      FALSE  TRUE
0     91693     9
1        61   111
[1] 99.92381
```

Support Vector Machine

Finally, the model Support Vector Machine as show in figure 8 managed to score 99.94% for the accuracy and misclassified 51 instances.

Figure 8 - Support Vector Machine

```
Correctly Classified Instances       85391               99.9403 %
Incorrectly Classified Instances        51                0.0597 %
Kappa statistic                          0.8388
Mean absolute error                      0.0006
Root mean squared error                  0.0244
Relative absolute error                 16.4433 %
Root relative squared error             54.1817 %
Total Number of Instances            85442

=== Detailed Accuracy By Class ===

               TP Rate  FP Rate  Precision  Recall  F-Measure  MCC      ROC Area  PRC Area  Class
                 0.764    0.000    0.938      0.764   0.839      0.843    0.882     0.711     1
                 1.000    0.236    1.000      1.000   1.000      0.843    0.882     1.000     0
Weighted Avg.    0.999    0.235    0.999      0.999   0.999      0.843    0.882     0.999

=== Confusion Matrix ===

     a     b   <-- classified as
   133    41 |     a = 1
    10 85258 |     b = 0
```

LSTM + SVM Model

Long Short-Term Memory (LSTM) networks and a Support Vector Machine (SVM) classifier are used in the suggested hybrid framework to overcome the difficulties in identifying credit card fraud in sizable, unbalanced datasets.

Feature Extraction with LSTM:

Recurrent neural networks (RNNs) of the LSTM type are made to recognize temporal dependencies in sequential input. Transaction histories are loaded into the LSTM in this study, which discovers hidden patterns and behavioral trends that distinguish between fraudulent and lawful activity. LSTM is ideally suited for fraud detection because, in contrast to static models, it takes into account the order of transactions rather than handling each one separately.

Classification with SVM:

An SVM classifier receives the feature representations generated by the final hidden state of the LSTM. In order to increase the distance between fraudulent and non-fraudulent transactions, SVM creates an ideal hyperplane. This combination makes use of SVM's strong classification capabilities and LSTM's capacity for temporal learning.

Comparison with Baselines:

The model's higher performance is demonstrated by benchmarking it against conventional classifiers like KNN, Naïve Bayes, standalone SVM, and Logistic Regression.

Evaluation and Deployment

Accuracy is the overall number of instances that are predicted correctly, accuracies are represented by confusion matrix where it showed the True Positive (TP), True Negative (TN), False Positive (FP) and False Negative (FN). True Positive represents the transactions that are fraudulent and was correctly classified by the model as fraudulent. True Negative represents the not fraudulent transactions that were correctly predicted bythe model as Not fraudulent. The third rating is False positive which represents the transaction that are fraudulent but was misclassified as not fraudulent. And finally False Negative which are the not fraudulent transactions that were identified as fraudulent.

Table 1

Logical Regression	Logistic Regression	99.92%
	Logistic Regression	
Support Vector Machine	SVM	99.94%
LSTM-SVM	LSTM-SVM	99.95%

Model		Accuracy
KNN	K = 3	99.89%
	K = 3	
	K = 7	99.88%
	K = 7	
Naïve Bayes	Naïve Bayes	97.76%
	Naïve Bayes	

Table 2 - Table of Accuracies

Table 2 shows all of the accuracies of all the models that were created in the project, all models performed well in detecting fraudulent transactions and managed to score high accuracies. Out of all the models the model that scored the best is Support Vector Machine as its accuracy is 99.94%, the second best is Logistic Regression, then in third place is KNN as both Ks scored similar accuracies, and the model that scored the lowest accuracy out of all models is Naïve Bayes with a score of 97.76%.

Conclusion:

In conclusion, the main objective of this project was to find the most suited model in credit card fraud detection in terms of the machine learning techniques chosen for the project, and it was met by building the four models and finding the accuracies of them all, the best model in terms of accuracies is LSTM-SVM which scored 99.95% with only 51 misclassified instances. I believe that using the model will help in decreasing the amount of credit card fraud and increase the customers satisfaction as it will provide them with better experience in addition to feeling secure.

The outcomes unequivocally show that the LSTM-SVM hybrid model outperforms conventional classifiers in credit card fraud detection. Superior fraud detection accuracy and robustness in unbalanced datasets are achieved by its capacity to capture sequential dependencies and provide discriminative features for SVM classification.

Reference:

[1] Adepoju, O., Wosowei, J., lawte, S., & Jaiman, H. (2019). Comparative evaluation of credit card fraud detection using machine learning techniques. 2019 Global Conference for Advancement in Technology (GCAT). https://doi.org/10.1109/gcat47503.2019.8978372

[2] J. Clerk Maxwell, A Treatise on Electricity and Magnetism, 3rd ed., vol. 2. Oxford: Clarendon, 1892, pp.68–73.

[3] Awoyemi, J. O., Adetunmbi, A. O., & Oluwadare, S. A. (2017). Credit card fraud detection using Machine Learning Techniques: A Comparative Analysis. 2017 International Conference on Computing Networking and Informatics (ICCNI). https://doi.org/10.1109/iccni.2017.8123782

[4] Bhanusri, A., Valli, K. R. S., Jyothi, P., Sai, G. V., & Rohith, R. (2020). Credit card fraud detection using Machine learning algorithms. Journal of Research in Humanities and Social Science, 8(2), 04-11.

[5] Credit card statistics. Shift Credit Card Processing. (2021, August 30). Retrieved from https://shiftprocessing.com/credit-card/

[6] Daly, L. (2021, October 27). Identity theft and credit card fraud statistics for 2021:The ascent. The Motley Fool. Retrieved from https://www.fool.com/the- ascent/research/identity-theft-credit-card-fraud-statistics/

[7] Dheepa, V., & Dhanapal, R. (2012). Behavior based credit card fraud detection using support vector machines. ICTACT Journal on Soft Computing, 02(04), 391–397. https://doi.org/10.21917/ijsc.2012.0061

[8] Dighe, D., Patil, S., & Kokate, S. (2018). Detection of credit card fraud transactions using machine learning algorithms and Neural Networks: A comparative study. 2018 Fourth International Conference on Computing Communication Control and Automation (ICCUBEA). https://doi.org/10.1109/iccubea.2018.8697799

[9] Domínguez-Almendros, S., Benítez-Parejo, N., & Gonzalez-Ramirez, A. R. (2011). Logistic regression models. Allergologia et immunopathologia, 39(5), 295-305.

[10] Gupta, A., Lohani, M. C., & Manchanda, M. (2021). Financial fraud detection using naive Bayes algorithm in highly imbalance data set. Journal of Discrete Mathematical Sciences and Cryptography, 24(5), 1559–1572. https://doi.org/10.1080/09720529.2021.1969733

[11] Itoo, F., Meenakshi, & Singh, S. (2020). Comparison and analysis of logistic regression, Naïve Bayes and Knn Machine Learning Algorithms for credit card fraud detection. International Journal of Information Technology, 13(4), 1503–1511. https://doi.org/10.1007/s41870-020-00430-y

[12] Jain, Y., NamrataTiwari, S., & Jain, S. (2019). A comparative analysis of various credit card fraud detection techniques. International Journal of Recent Technology and Engineering, 7(5S2), 402-407

[13] Kiran, S., Guru, J., Kumar, R., Kumar, N., Katariya, D., & Sharma, M. (2018). Credit card fraud detection using Naïve Bayes model based and KNN classifier. International Journal Of Advance Research, Ideas And Innovations In Technology, 4(3).

[14] Kiran, S., Guru, J., Kumar, R., Kumar, N., Katariya, D., & Sharma, M. (2018). Credit card fraud detection using Naïve Bayes model based and KNN classifier. International Journal Of Advance Research, Ideas And Innovations In Technology, 4(3).

[15] Mahesh, B. (2020). Machine Learning Algorithms - A Review, 9(1).https://doi.org/10.21275/ART20203995

[16] Malini, N., & Pushpa, M. (2017). Analysis on credit card fraud identification techniques based on KNN and outlier detection. 2017 Third International Conference on Advances in Electrical, Electronics, Information, Communication and Bio-Informatics (AEEICB). https://doi.org/10.1109/aeeicb.2017.7972424

[17] Maniraj, S. P., Saini, A., Ahmed, S., & Sarkar, S. D. (2019). Credit card fraud detection using machine learning and Data Science. Credit Card Fraud Detection Using Machine Learning and Data Science, 08(09). https://doi.org/10.17577/ijertv8is090031

[18] Najadat, H., Altiti, O., Aqouleh, A. A., & Younes, M. (2020). Credit card fraud detection based on machine and Deep Learning. 2020 11th International Conference on Information and Communication Systems (ICICS). https://doi.org/10.1109/icics49469.2020.239524

[19] Safa, M. U., & Ganga, R. M. (2019). Credit Card Fraud Detection Using Machine Learning. International Journal of Research in Engineering, Science and Management,2(11).

[20] Saheed, Y. K., Hambali, M. A., Arowolo, M. O., & Olasupo, Y. A. (2020). Application of ga feature selection on Naive Bayes, random forest and SVM for credit card fraud detection. 2020 International Conference on Decision Aid Sciences and Application (DASA). https://doi.org/10.1109/dasa51403.2020.9317228

[21] Sahin, Y., & Duman, E. (2011). Detecting Credit Card Fraud by Decision Trees and Support Vector Machines. Proceedings of the International MultiConference of Engineers and Computer Scientists, 1.