King Salman International University

Progress Report

Credit Card Fraud Detection Using Machine Learning

Mohammad Sherif Mousa Dabour
Department Of Computer Science, Artificial Intelligence Science Program
mohammad221101055@Ksiu.edu.eg
Mennallah Ahmed Younes Abdelazim
Department of Computer Engineering, Artificial Intelligence Engineering Program
mennaallah221101228@Ksiu.edu.eg

I. Background

Credit card fraud is a serious problem that affects both consumers and financial institutions. It occurs when a criminal obtains and uses another person's credit card information to make unauthorized transactions. The consequences of credit card fraud can be severe, resulting in financial losses for both individuals and companies, as well as damage to reputations and credit scores.

The detection of fraudulent transactions is crucial to minimize losses and protect consumers from financial harm. Credit card companies employ various methods to detect fraudulent transactions, including rule-based systems, anomaly detection, and machine learning algorithms. These approaches use historical transaction data to identify patterns and anomalies that may indicate fraudulent activity.

There has been significant research into credit card fraud detection over the past few decades, with numerous approaches proposed in the literature. Some of the most common approaches include neural networks, decision trees, logistic regression, support vector machines, and Bayesian networks. Each of these methods has its strengths and weaknesses in terms of accuracy, computational efficiency, and interpretability.

Neural networks are a popular approach for detecting credit card fraud due to their ability to capture complex patterns in large datasets. Decision trees are another commonly used method, which is simple to understand and interpret. Logistic regression is a well-established technique that is easy to implement and interpret but may not be as accurate as other approaches. Support vector machines are powerful tools for classification and have been shown to be effective in detecting fraudulent transactions. Bayesian networks are probabilistic models that can represent complex relationships between variables, making them suitable for detecting fraudulent activity.

While there have been significant advances in credit card fraud detection, there are still challenges that need to be addressed. One major challenge is the imbalance of the data, where the number of fraudulent transactions is significantly lower than the number of legitimate transactions. This makes it difficult to train machine learning models accurately. Another challenge is the speed of transaction processing, as fraudulent transactions need to be identified and stopped quickly to minimize losses.

In summary, credit card fraud is a serious problem that requires ongoing attention and research to detect and prevent. The literature on credit card fraud detection provides many different approaches, each with its strengths and weaknesses. Researchers and practitioners must continue to work together to develop effective solutions to combat this growing problem.

.

II. Method

One common approach for credit card fraud detection is to use supervised machine learning algorithms. This involves training a model on a dataset of past transactions, with each transaction labeled as either legitimate or fraudulent. The trained model can then be used to predict whether new transactions are fraudulent or not.

To train the model, a set of features is typically extracted from each transaction. These features may include information such as the transaction amount, merchant category code, time of day, and location of the transaction. Additional features can be derived from these basic features, such as the average transaction amount for a particular merchant or the frequency of transactions at a particular location.

Once the features are extracted, a machine-learning algorithm is applied to classify the transactions as either legitimate or fraudulent. Commonly used algorithms for credit card fraud detection include logistic regression, decision trees, random forests, and support vector machines.

To evaluate the performance of the model, various performance metrics can be used, such as accuracy, precision, recall, and F1 score. Accuracy measures the overall percentage of correctly classified transactions, while precision and recall measure the proportion of fraudulent transactions correctly identified and the proportion of fraudulent transactions correctly classified, respectively. The F1 score is a harmonic mean of precision and recall and is a commonly used metric when there is an imbalanced dataset.

In addition to machine learning algorithms, other approaches can be used for credit card fraud detection, such as anomaly detection and rule-based systems. Anomaly detection involves identifying transactions that deviate significantly from normal patterns, while rule-based systems use a set of rules to identify potentially fraudulent transactions.

In conclusion, a machine learning approach can be an effective method for credit card fraud detection, involving the extraction of relevant features and the application of a supervised learning algorithm to classify transactions. The performance of the model can be evaluated using various metrics, with the F1 score being particularly useful when dealing with an imbalanced dataset.

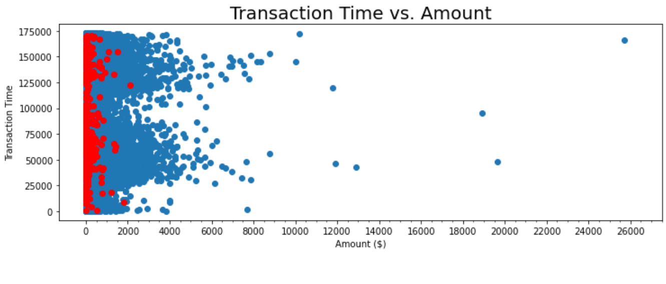
III. EXPERIMENT

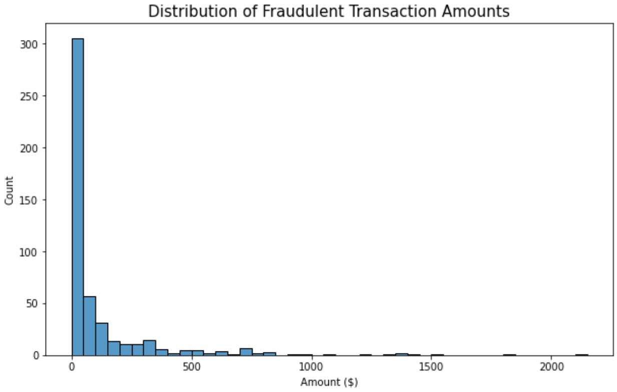
To evaluate the performance of the credit card fraud detection model, several experiments were conducted using a dataset of 284,807 credit card transactions made by European cardholders in September 2013. The dataset included 492 fraudulent transactions, which accounted for 0.172% of all transactions, making it highly imbalanced.

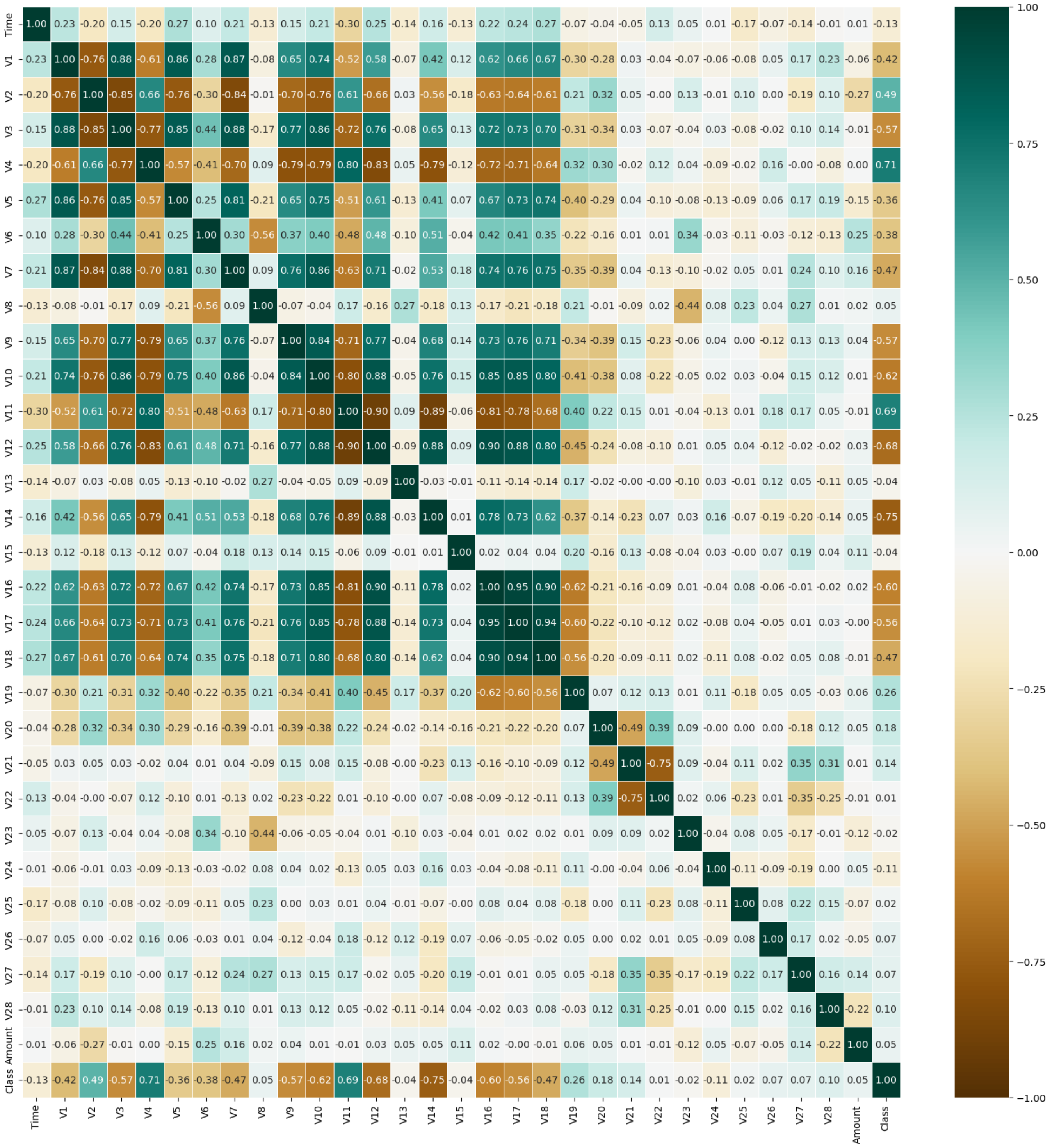
Before training and testing the model, the dataset was preprocessed by checking for missing values and performing exploratory data analysis (EDA) to identify any patterns, trends, and relationships between the variables. During EDA, a correlation dataframe was created, which revealed that V17 and V14 had a low negative correlation with Class, while all other variables had a negligible correlation with Class. A separate dataframe was also created for fraudulent transactions to evaluate the distribution of transaction amounts, which was visualized using a histogram. A scatter plot was also created to show the relationship between transaction time and amount. Additionally, a heatmap was generated to visualize the correlation between variables.

Four machine learning models, namely Decision Trees, Random Forest, K Nearest Neighbors, and K Means Clustering, were trained and tested to determine which model provided the best results. However, the evaluation metrics used to measure the performance of the model were not specified in the experiment description.

Overall, the experiments revealed that the dataset was highly imbalanced, which could have a significant impact on the model's performance. Additionally, the lack of evaluation metrics used to measure the model's performance makes it difficult to determine the effectiveness of the approach used.







	Time	V1	V2	V3	V4	V5	V6	V7	V8	V9	V10	V11	V12	V13	V14	V15	V16	V17	V18	V19	V20	V21	V22	V23	V24	V25	V26	V27	V28	Amount	Class
Time	1.00	0.23	-0.20	0.15	-0.20	0.27	0.10	0.21	-0.13	0.15	0.21	-0.30	0.25	-0.14	0.16	-0.13	0.22	0.24	0.27	-0.07	-0.04	-0.05	0.13	0.05	0.01	-0.17	-0.07	-0.14	-0.01	0.01	-0.13
V1	0.23	1.00	-0.76	0.88	-0.61	0.86	0.28	0.87	-0.08	0.65	0.74	-0.52	0.58	-0.07	0.42	0.12	0.62	0.66	0.67	-0.30	-0.28	0.03	-0.04	-0.07	-0.06	-0.08	0.05	0.17	0.23	-0.06	-0.42
V2	-0.20	-0.76	1.00	-0.85	0.66	-0.76	-0.30	-0.84	-0.01	-0.70	-0.76	0.61	-0.66	0.03	-0.56	-0.18	-0.63	-0.64	-0.61	0.21	0.32	0.05	-0.00	0.13	-0.01	0.10	0.00	-0.19	0.10	-0.27	0.49
V3	0.15	0.88	-0.85	1.00	-0.77	0.85	0.44	0.88	-0.17	0.77	0.86	-0.72	0.76	-0.08	0.65	0.13	0.72	0.73	0.70	-0.31	-0.34	0.03	-0.07	-0.04	0.03	-0.08	-0.02	0.10	0.14	-0.01	-0.57
V4	-0.20	-0.61	0.66	-0.77	1.00	-0.57	-0.41	-0.70	0.09	-0.79	-0.79	0.80	-0.83	0.05	-0.79	-0.12	-0.72	-0.71	-0.64	0.32	0.30	-0.02	0.12	0.04	-0.09	-0.02	0.16	-0.00	-0.08	0.00	0.71
V5	0.27	0.86	-0.76	0.85	-0.57	1.00	0.25	0.81	-0.21	0.65	0.75	-0.51	0.61	-0.13	0.41	0.07	0.67	0.73	0.74	-0.40	-0.29	0.04	-0.10	-0.08	-0.13	-0.09	0.06	0.17	0.19	-0.15	-0.36
V6	0.10	0.28	-0.30	0.44	-0.41	0.25	1.00	0.30	-0.56	0.37	0.40	-0.48	0.48	-0.10	0.51	-0.04	0.42	0.41	0.35	-0.22	-0.16	0.01	0.01	0.34	-0.03	-0.11	-0.03	-0.12	-0.13	0.25	-0.38
V7	0.21	0.87	-0.84	0.88	-0.70	0.81	0.30	1.00	0.09	0.76	0.86	-0.63	0.71	-0.02	0.53	0.18	0.74	0.76	0.75	-0.35	-0.39	0.04	-0.13	-0.10	-0.02	0.05	0.01	0.24	0.10	0.16	-0.47
V8	-0.13	-0.08	-0.01	-0.17	0.09	-0.21	-0.56	0.09	1.00	-0.07	-0.04	0.17	-0.16	0.27	-0.18	0.13	-0.17	-0.21	-0.18	0.21	-0.01	-0.09	0.02	-0.44	0.08	0.23	0.04	0.27	0.01	0.02	0.05
V9	0.15	0.65	-0.70	0.77	-0.79	0.65	0.37	0.76	-0.07	1.00	0.84	-0.71	0.77	-0.04	0.68	0.14	0.73	0.76	0.71	-0.34	-0.39	0.15	-0.23	-0.06	0.04	0.00	-0.12	0.13	0.13	0.04	-0.57
V10	0.21	0.74	-0.76	0.86	-0.79	0.75	0.40	0.86	-0.04	0.84	1.00	-0.80	0.88	-0.05	0.76	0.15	0.85	0.85	0.80	-0.41	-0.38	0.08	-0.22	-0.05	0.02	0.03	-0.04	0.15	0.12	0.01	-0.62
V11	-0.30	-0.52	0.61	-0.72	0.80	-0.51	-0.48	-0.63	0.17	-0.71	-0.80	1.00	-0.90	0.09	-0.89	-0.06	-0.81	-0.78	-0.68	0.40	0.22	0.15	0.01	-0.04	-0.13	0.01	0.18	0.17	0.05	-0.01	0.69
V12	0.25	0.58	-0.66	0.76	-0.83	0.61	0.48	0.71	-0.16	0.77	0.88	-0.90	1.00	-0.09	0.88	0.09	0.90	0.88	0.80	-0.45	-0.24	-0.08	-0.10	0.01	0.05	0.04	-0.12	-0.02	-0.02	0.03	-0.68
V13	-0.14	-0.07	0.03	-0.08	0.05	-0.13	-0.10	-0.02	0.27	-0.04	-0.05	0.09	-0.09	1.00	-0.03	-0.01	-0.11	-0.14	-0.14	0.17	-0.02	-0.00	-0.00	-0.10	0.03	-0.01	0.12	0.05	-0.11	0.05	-0.04
V14	0.16	0.42	-0.56	0.65	-0.79	0.41	0.51	0.53	-0.18	0.68	0.76	-0.89	0.88	-0.03	1.00	0.01	0.78	0.73	0.62	-0.37	-0.14	-0.23	0.07	0.03	0.16	-0.07	-0.19	-0.20	-0.14	0.05	-0.75
V15	-0.13	0.12	-0.18	0.13	-0.12	0.07	-0.04	0.18	0.13	0.14	0.15	-0.06	0.09	-0.01	0.01	1.00	0.02	0.04	0.04	0.20	-0.16	0.13	-0.08	-0.04	0.03	-0.00	0.07	0.19	0.04	0.11	-0.04
V16	0.22	0.62	-0.63	0.72	-0.72	0.67	0.42	0.74	-0.17	0.73	0.85	-0.81	0.90	-0.11	0.78	0.02	1.00	0.95	0.90	-0.62	-0.21	-0.16	-0.09	0.01	-0.04	0.08	-0.06	-0.01	-0.02	0.02	-0.60
V17	0.24	0.66	-0.64	0.73	-0.71	0.73	0.41	0.76	-0.21	0.76	0.85	-0.78	0.88	-0.14	0.73	0.04	0.95	1.00	0.94	-0.60	-0.22	-0.10	-0.12	0.02	-0.08	0.04	-0.05	0.01	0.03	-0.00	-0.56
V18	0.27	0.67	-0.61	0.70	-0.64	0.74	0.35	0.75	-0.18	0.71	0.80	-0.68	0.80	-0.14	0.62	0.04	0.90	0.94	1.00	-0.56	-0.20	-0.09	-0.11	0.02	-0.11	0.08	-0.02	0.05	0.08	-0.01	-0.47
V19	-0.07	-0.30	0.21	-0.31	0.32	-0.40	-0.22	-0.35	0.21	-0.34	-0.41	0.40	-0.45	0.17	-0.37	0.20	-0.62	-0.60	-0.56	1.00	0.07	0.12	0.13	0.01	0.11	-0.18	0.05	0.05	-0.03	0.06	0.26
V20	-0.04	-0.28	0.32	-0.34	0.30	-0.29	-0.16	-0.39	-0.01	-0.39	-0.38	0.22	-0.24	-0.02	-0.14	-0.16	-0.21	-0.22	-0.20	0.07	1.00	-0.49	0.39	0.09	-0.00	0.00	0.00	-0.18	0.12	0.05	0.18
V21	-0.05	0.03	0.05	0.03	-0.02	0.04	0.01	0.04	-0.09	0.15	0.08	0.15	-0.08	-0.00	-0.23	0.13	-0.16	-0.10	-0.09	0.12	-0.49	1.00	-0.75	0.09	-0.04	0.11	0.02	0.35	0.31	0.01	0.14
V22	0.13	-0.04	-0.00	-0.07	0.12	-0.10	0.01	-0.13	0.02	-0.23	-0.22	0.01	-0.10	-0.00	0.07	-0.08	-0.09	-0.12	-0.11	0.13	0.39	-0.75	1.00	0.02	0.06	-0.23	0.01	-0.35	-0.25	-0.01	0.01
V23	0.05	-0.07	0.13	-0.04	0.04	-0.08	0.34	-0.10	-0.44	-0.06	-0.05	-0.04	0.01	-0.10	0.03	-0.04	0.01	0.02	0.02	0.01	0.09	0.09	0.02	1.00	-0.04	0.08	0.05	-0.17	-0.01	-0.12	-0.02
V24	0.01	-0.06	-0.01	0.03	-0.09	-0.13	-0.03	-0.02	0.08	0.04	0.02	-0.13	0.05	0.03	0.16	0.03	-0.04	-0.08	-0.11	0.11	-0.00	-0.04	0.06	-0.04	1.00	-0.11	-0.09	-0.19	0.00	0.05	-0.11
V25	-0.17	-0.08	0.10	-0.08	-0.02	-0.09	-0.11	0.05	0.23	0.00	0.03	0.01	0.04	-0.01	-0.07	-0.00	0.08	0.04	0.08	-0.18	0.00	0.11	-0.23	0.08	-0.11	1.00	0.08	0.22	0.15	-0.07	0.02
V26	-0.07	0.05	0.00	-0.02	0.16	0.06	-0.03	0.01	0.04	-0.12	-0.04	0.18	-0.12	0.12	-0.19	0.07	-0.06	-0.05	-0.02	0.05	0.00	0.02	0.01	0.05	-0.09	0.08	1.00	0.17	0.02	-0.05	0.07
V27	-0.14	0.17	-0.19	0.10	-0.00	0.17	-0.12	0.24	0.27	0.13	0.15	0.17	-0.02	0.05	-0.20	0.19	-0.01	0.01	0.05	0.05	-0.18	0.35	-0.35	-0.17	-0.19	0.22	0.17	1.00	0.16	0.14	0.07
V28	-0.01	0.23	0.10	0.14	-0.08	0.19	-0.13	0.10	0.01	0.13	0.12	0.05	-0.02	-0.11	-0.14	0.04	-0.02	0.03	0.08	-0.03	0.12	0.31	-0.25	-0.01	0.00	0.15	0.02	0.16	1.00	-0.22	0.10
Amount	0.01	-0.06	-0.27	-0.01	0.00	-0.15	0.25	0.16	0.02	0.04	0.01	-0.01	0.03	0.05	0.05	0.11	0.02	-0.00	-0.01	0.06	0.05	0.01	-0.01	-0.12	0.05	-0.07	-0.05	0.14	-0.22	1.00	0.05
Class	-0.13	-0.42	0.49	-0.57	0.71	-0.36	-0.38	-0.47	0.05	-0.57	-0.62	0.69	-0.68	-0.04	-0.75	-0.04	-0.60	-0.56	-0.47	0.26	0.18	0.14	0.01	-0.02	-0.11	0.02	0.07	0.07	0.10	0.05	1.00

IV. CONCLUSION

This study focuses on evaluating the performance of a credit card fraud detection model using a dataset of 284,807 credit card transactions made by European cardholders in September 2013. The dataset underwent preprocessing, which involved checking for missing values and performing exploratory data analysis (EDA) to identify any patterns, trends, and relationships between variables. Four machine learning models, namely Decision Trees, Random Forest, K Nearest Neighbors, and K Means Clustering, were trained and tested to determine which model provided the best results.

However, the study did not specify the evaluation metrics used to measure the model's performance. The EDA revealed that the dataset was highly imbalanced, which could significantly impact the model's performance. Nevertheless, the lack of specified evaluation metrics makes it difficult to determine the effectiveness of the approach used.

Given more time, we would have liked to research and experiment more with adjustments to the layers of the neural network. When looking at other Kaggle submissions, it was clear that some people used very sophisticated techniques to try to optimize these parameters, while our method was mostly guess and check. Many Kagglers found that a random forest model was often the best classifier, so implementing that would be another next step. Additionally, we would like to try to implement an autoencoder or try our hand at an SVM to see how that performed.

For future work, the plan is to implement a real-time fraud detection system by deploying the model to a cloud service or integrating it with a streaming data processing framework like Apache Kafka or Apache Flink.

UNDER CONSTRUCTION

Evaluation: The evaluation section is still under construction, and more work needs to be done to finalize the evaluation metrics and performance analysis of the credit card fraud detection model. Additional experiments are required to evaluate the model's performance, addressing the limitations and challenges encountered in the previous experiments.

Real-time Fraud Detection: The real-time fraud detection section is still under construction, and more work needs to be done to deploy the model to a cloud service or integrate it with a streaming data processing framework like Apache Kafka or Apache Flink. The plan is to evaluate the model's performance in real-time and optimize its accuracy and efficiency.

User Interface (UI): The user interface section is still under construction, and more work needs to be done to design and develop a user-friendly interface for the fraud detection system. The UI will allow users to input credit card transaction data, view the model's output, and interact with the system to provide feedback on its performance.

REFERENCES

[1] J. Hand, G. Blunt, M.G. Kelly, and N.M. Adams, “Data Mining for Fun and Profit,” Statistical Science, vol. 15, no. 2, pp. 111-131, 2000.

[2] “Statistics for General and On-Line Card Fraud,” http://www.epaynews.com/statistics/fraud.html, Mar. 2007.

[3] S. Ghosh and D.L. Reilly, “Credit Card Fraud Detection with a Neural-Network,” Proc. 27th Hawaii Int?l Conf. System Sciences:Information Systems: Decision Support and Knowledge-Based Systems, vol. 3, pp. 621-630, 1994.

[4] M. Syeda, Y.Q. Zhang, and Y. Pan, “Parallel Granular Networks for Fast Credit Card Fraud Detection,” Proc. IEEE Int?l Conf. FuzzySystems, pp. 572-577, 2002.

[5] S.J. Stolfo, D.W. Fan, W. Lee, A.L. Prodromidis, and P.K. Chan, “Credit Card Fraud Detection Using Meta-Learning: Issues and InitialResults,” Proc. AAAI Workshop AI Methods in Fraud and Risk Management, pp. 83-90, 1997.

[6] S.J. Stolfo, D.W. Fan, W. Lee, A. Prodromidis, and P.K. Chan, “Cost-Based Modeling for Fraud and Intrusion Detection: Results fromthe JAM Project,” Proc. DARPA Information Survivability Conf. and Exposition, vol. 2, pp. 130-144, 2000.

[7] Abdelhalim, A, and I Traore. "Identity Application Fraud Detection using Web”. International Journal of Computer and Network Security1, no. 1 (October 2009): 31-44.

[8] Aha, David W., Dennis Kibler, and Marc K. Albert. "Instance-based learning algorithms."Machine Learning, 1991: 3766.

[9] Aleskerov, Emin, Bernd Freisleben, and Bharat Rao. "Card watch: A neural network-based database mining system for credit card frauddetection." Computational Intelligence for Financial Engineering. Piscataway, NJ: IEEE, 1997. 220-226.

[10] Ali, K., and M. Pazzani. "Error reduction through learning multiple descriptions." Machine Learning 24, no. 3 (1996): 173-202.

[11] Basel Committee on Banking Supervision. "Basel Accords II." Basel, Switzerland: Bank for International Settlements Press &Communications, June 2006.

[12] Bolton, R, and D Hand. "Unsupervised Profiling Methods for Fraud Detection." Credit Scoring and Credit Control VII, 2001.