Using ML Techniques Which Utilize Linear Algebra for Fraud Detection

IBRAHM MAHMOOD, SHAHEER ASLAM, BASIT FAISAL, ZAIN NOFAL & IBRAHIM ANSARI

[1]Faculty of computer science and engineering, Data science, GIKI

[2]2021748, 2021587, 2021126, 2021723, 2021238

ABSTRACT

With the rise of online shopping and digital financial systems, there is a greater chance of credit card theft. This study examines and implements a credit card fraud detection system that makes use of machine learning methods, including Support Vector Machines (SVM), Principal Component Analysis (PCA), and other state-of-the-art techniques.
The suggested algorithm is made to examine and categorize credit card transactions, allowing for the distinction of authentic from fraudulent activity. SVM is used as the main classification model because of its versatility in handling high-dimensional feature spaces and complex data. In order to improve computing performance and lessen the negative effects of dimensionality, Principal Component Analysis is also used to minimize the dimensionality of the input data.

Keywords

Data visualization applications, automated fraud detection, Support Vectors, Principal Component Analysis.

1. INTRODUCTION & MOTIVATION

Robust and adaptable fraud detection algorithms are becoming more and more necessary as financial transactions continue to move online.

The misuse of a profit organization's system without necessarily having immediate legal repercussions is referred to as fraud in this context. Fraud can become a major corporate issue in a competitive market if it is highly common and the preventive measures are not 100% reliable. As a component of total fraud management, fraud detection automates and minimizes the manual aspects of a screening or checking procedure. One of the most well-known industrial/government data mining applications is now in this field.

It is hard to know for sure whether an application or transaction is legitimate and what its intentions are. In light of the situation, employing mathematical algorithms to extract potential fraud evidence from the available data is the most economical course of action.

The analytical engine of these software and solutions, which originated from many research communities—particularly those in industrialized nations—is powered by artificial intelligence, auditing, distributed and parallel databases, artificial immune systems, and auditing. Expert systems, fuzzy logic, genetic algorithms, machine learning, neural networks, pattern recognition, statistics, computing, econometrics, and visualization, among other fields. Numerous specialized fraud detection software and solutions are available to safeguard companies in the credit card, e-commerce, insurance, retail, and telecommunications sectors.

Creating a sophisticated credit card fraud detection system that can accurately discriminate between authentic and fraudulent transactions is the main objective of this study. With the use of Principal Component Analysis (PCA), Support Vector Machines (SVM), and other machine learning techniques, the suggested approach seeks to improve the precision and effectiveness of fraud detection in real-time.

The rationale behind selecting SVM is its capacity to manage sophisticated data and nonlinear relationships, which makes it ideal for the complex patterns frequently seen in credit card transactions. Principal Component Analysis is also applied to overcome the difficulties presented by high-dimensional feature spaces, maximizing algorithm performance while maintaining computing economy.

We hope that this research will strengthen the security of digital financial systems, which is a continuing endeavor. This report includes data and results from other papers as well to give the stakeholders an overall idea of fraud detection and technological advancements in this domain alongside our model that we trained and tested for this issue, thus it is not only a project report but a survey of past improvements and background information of credit card fraud as well.

2. BACKGROUND

This section highlights the types of fraudsters and affected industries.

2.1 Fraudsters

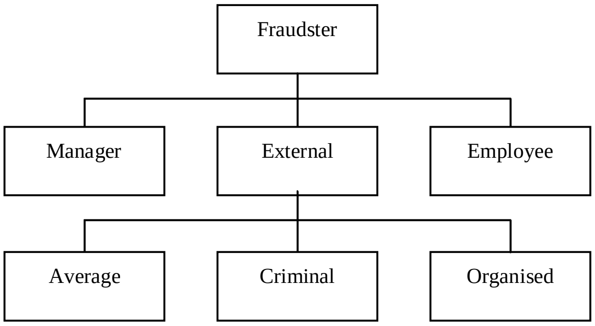

Figure 2.1: White-collar crime offenders ranked according to corporate and community levels in a hierarchical structure.

The profit-driven fraudster interacts with the impacted firm, as seen in figure 2.1. Every company has historically been vulnerable to internal fraud or corruption by both high-level and low-level management and non-management personnel. Data mining may be used as an analytical technique in addition to internal and external audits for fraud control.

The fraudster in Figure 1 may be an outside party or parties. Additionally, the fraudster may pose as a present or potential supplier (provider) or client (consumer) in order to perpetrate fraud. The typical offender, criminal offender, and organised crime offender are the three fundamental characteristics of the external fraudster. When presented with a chance, a sudden temptation, or financial difficulty, average criminals may sometimes act dishonestly.

On the other hand, individual criminals, and organized/group criminals (professional/career fraudsters) pose a greater risk to society because they frequently conceal their true identities and/or adapt their methods over time to resemble legal forms and evade detection. As a result, it's critical to take into consideration the strategic interactions, or moves and countermoves, that occur between the algorithms of a fraud detection system and the techniques used by experienced scammers. While credit and telecommunications fraud are more susceptible to professional fraudsters, internal and insurance fraud are likely to be committed by typical criminals.

Majority of external parties' identities and activities are too costly for many businesses to manually verify, especially when dealing with upto millions of them. Therefore, the most suspect ones- such as suspicion scores, rules and visual anomalies – that are identified by means of data mining output will be looked at.

Affected Business Sectors

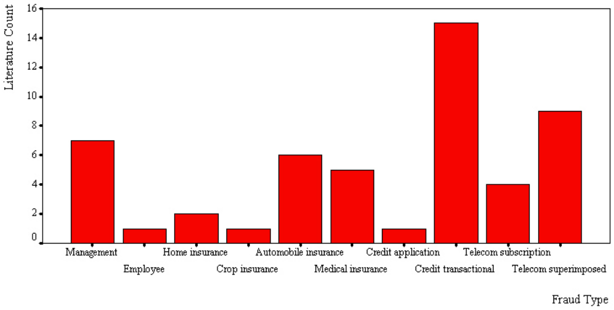

Figure 2.2: Bar graph of fraud categories derived from 51 distinct, published fraud detection studies. The author(s)'s most recent publication serves as a representation of earlier, comparable works.

The subcategories for internal, credit card, insurance, and telecommunications fraud detection are shown in detail in Figure 2.2. Determining false financial reporting by management (Lin et al., 2003; Bell and Carcello, 2000; Fanning and Cogger, 1998; Summers and Sweeney, 1998; Beneish, 1997; Green and Choi, 1997) and unusual retail transactions by staff members are the focus of internal fraud detection (Kim et al., 2003). According to Bentley (2000) and Von Altrock (1997), there are four subgroups of insurance fraud detection: home insurance; automobile insurance; crop insurance; Phua et al. (2004); Viaene et al. (2004); Brockett et al. (2002); Stefano and Gisella, 2001; Belhadji et al. (2000); Artis et al., 1999; and medical insurance. He and colleagues, 1999; Cox, 1995; Major and Riedinger, 2002; Williams, 1999). (Fan, 2004; Chen et al, 2004; Chiu and Tsai, 2004; Foster and Stine, 2004; Kim and Kim, 2002; Maes et al, 2002; Syeda et al, 2002; Bolton and Hand, 2001; Bentley et al, 2000; Brause et al, 1999; Chan et al, 1999; Aleskerov et al, 1997; Dorronsoro et al, 1997; Kokkinaki, 1997; Ghosh and Reilly, 1994) are examples of credit fraud detection. Cortes et al. (2003), Cahill et al. (2002), Moreau and Vandewalle (1997), Rosset et al. (1999), and/or wire-line and wire-less phone calls (Kim et al., 2003;) are comparable to credit fraud detection. The following studies are kept an eye on: Taniguchi et al, 1998; Cox, 1997; Ezawa and Norton, 1996; Moreau et al, 1999; Murad and Pinkas, 1999; Fawcett and Provost, 1997; Hollmen and Tresp, 1998; Burge and Shawe-Taylor, 2001.

Researchers have focused much of their effort on credit transactional fraud detection, while it has also been used haphazardly to forecast bad debts and bankruptcy (Foster and Stine, 2004; Ezawa and Norton, 1996). There is just one scholarly article for each of the following: employee/retail (Kim et al., 2003), national crop insurance (Little et al., 2002), and credit application (Wheeler and Aitken, 2000).

These detection systems' primary goal is to spot broad patterns in dubious or fraudulent transactions and applications. When it comes to application fraud, these con artists use false information to apply for insurance entitlements, as well as credit and telecommunications products and services. They also use false information to apply for identity theft, either their own or that of another else. When it comes to transactional fraud, these con artists either take over or increase the use of an already-existing, authentic credit or phone account.

Other areas exist for the identification of fraud. The blurring of lines between fraud detection systems and network intrusion detection systems is a challenge presented by e-businesses and e-commerce on the Internet. The focus of related material is on IP-based telephony services (McGibney and Hearne, 2003) and video-on-demand websites (Barse et al, 2003). Automated systems can keep an eye on online buyers and sellers (Sherman, 2002; Bhargava et al., 2003). There have also been reports of fraud detection in government agencies like customs and tax (Shao et al., 2002; Bonchi et al., 1999).

3. DATA AND MEASUREMENTS

This section discusses the dataset we used for our model.

3.1 Structured data

The purpose of this subsection is to specify the characteristics and examples that were used to train the model. This will help future research on fraud detection to either authenticate their actual data or produce fake data.

Type
Branch
Amount
nameOrig
oldbalanceOrg
newbalanceOrig
nameDest
oldbalanceDest
newbalanceDest
Unusuallogin
isFlaggedFraud
Acct type
Date of transaction
Time of day
isFraud

Figure 3.1: List of data attributes existing the dataset being used.

In general, qualities can be categorical (nominal or ordinal scales), numerical (interval or ratio scales), binary, or a combination of the three.

The dataset comprises an extensive range of variables associated with financial transactions, including crucial data for the creation of an algorithm designed to detect credit card fraud. Whereas the "type" column classifies transactions according to their type—for example, payments or transfers—the "step" column shows discrete time intervals. The "branch" column contains branch information, and the "amount" column reflects the monetary component. "nameOrig" and "nameDest" indicate the originating and destination account details, respectively, as well as the related balances before to and following transactions.

column	Non-Null Count	Dtype
Type	10122	Object
Branch	10118	Object
Amount	10122	Float64
nameOrig	10120	Object
oldbalanceOrg	10116	Float64
newbalanceOrig	10122	Float64
nameDest	10116	Object
oldbalanceDest	10121	Float64
newbalanceDest	10120	Float64
Unusuallogin	10122	Float64
isFlaggedFraud	10122	Float64
Acct type	10112	Object
Date of transaction	10115	Object
Time of day	10120	Object
isFraud	10120	Float64

Figure 3.2: Table of information about dataset features.

Figure 3.2 shows the nonempty values and data type of each value segregated by columns of the dataset.

Potential irregularities and fraud flags are highlighted by binary indicators like "unusuallogin" and "isFlaggedFraud". The kind of account in question is indicated in the "Acct type" column. The temporal context of transactions is further enhanced by the inclusion of date and time components. Finally, a critical label that indicates whether or not a transaction is fraudulent is the "isFraud" column. With the use of this extensive dataset, machine learning methods like SVM and PCA may be implemented and assessed to build a reliable system for detecting credit card fraud.

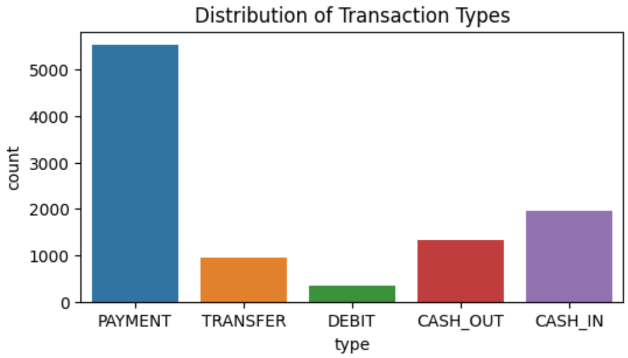

Figure 3.3: Types of transactions present in the dataset.

5 types of transactions exist in our dataset “Payment, Transfer, Debit type, Cash out & Cash in” with payment having the highest count **5000+** , followed by cash-in (close to **2000**), cash-out (**1500-1600**), transfer (close to **1000**) and lastly Debit (close to **500**). Showing the dominant day-to-day transaction type in financial institutions.

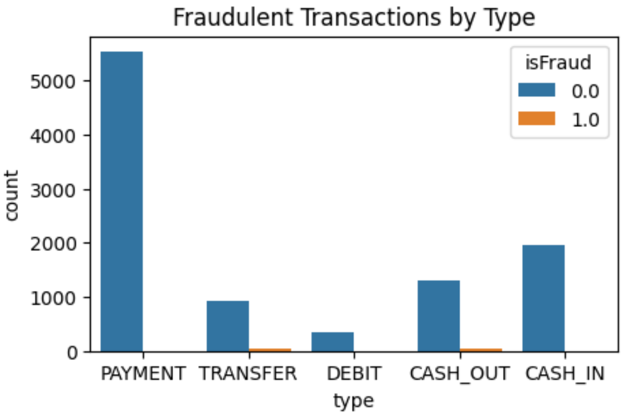

Figure 3.3: Fraud occurrence in different transactions.

As shown in the graph, out of all transaction types in the dataset we are using; transfer and cash out are the only 2 transactions out of 5 that have occurrence of fraud in them, transfer (*freq* = 33), cash out (*freq* = 33).

This means there is a 50/50 split between these 2 data types.

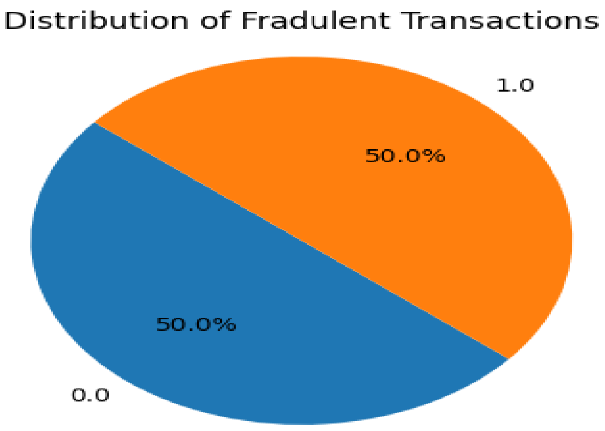

Figure 3.4: Division of fraud occurrences between transfer & cash out.

Fraudulent activities occur between 2 transaction types, Transfer & Cash out equally (for the dataset we have chosen).

Next we analyzed how the transaction amount is distributed among our dataset, which transaction amount is executed more frequently.

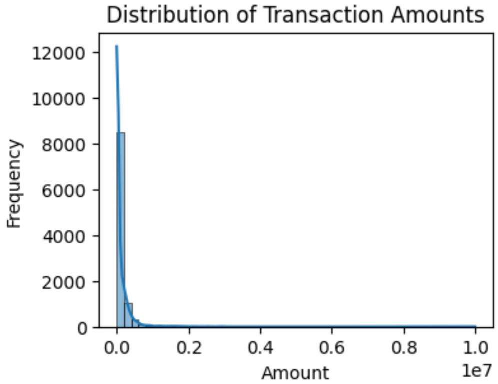

Figure 3.5: Division of fraud occurrences between transfer & cash out

The graph shows the distribution of transaction frequencies and amounts. The x-axis shows the transaction amount, while the y-axis shows the frequency of occurrence. The graph indicates that transaction amounts between $0 and $2000 are the most common, followed by $2000 and $4,000, $4,000 and $6000, and $6000 and $8000. As the transaction quantity rises, the frequency of occurrence falls.

The graph is skewed to the right, meaning there are more transactions with smaller amounts than with larger amounts. This is common for many types of transactions, such as retail purchases and online transactions.

Some possible explanations for this type of skewness for distribution of transactions amounts can be:

- People tend to make smaller purchases than large purchases.
- Many businesses have minimum purchase requirements.
- Credit card companies often have limits on the amount of money that can be charged to a card in a single transaction.

The above graph (fig-3.5) is useful in understanding the purchasing habits of the consumers and businesses and banks can use these graphs to identify potential fraudulent activities.

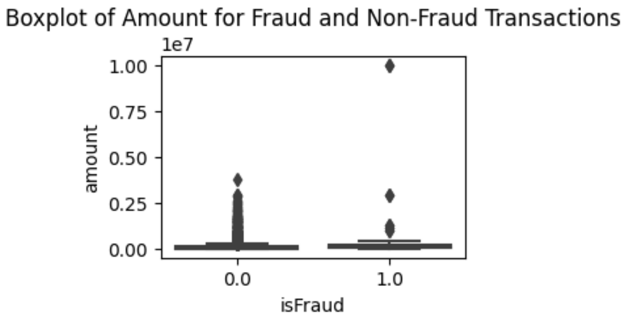

Figure 3.6: Division of fraud occurrences between transfer & cash out

This is another way we can visualize the fraudulent and non-fraudulent activities in our dataset (*Reference to figure 3.6).*

4. DATA PREPROCESSING AND MODEL TESTING

This section explains how we preprocessed our data, what features we chose and then our model training and accuracy.

4.1 Preprocessing

Our dataset was biased initially, so we had to perform sampling to make sure the model does not have any bias when predicting fraudulent activities.

IsFraud = 0	IsFraud = 1
10017	66

Figure 4.1: Structured diagram count of fraudulent transactions and non-fraudulent transactions.

According to our needs we then oversampled "IsFraud" values as it would increase the dataset and possibly train the model better.

Then we performed PCA to find principal components and what features would work better for our model. Now PCA relies heavily on linear algebra, here is a breakdown of specific linear algebra concepts used in PCA:

- Matrix operations: addition, subtraction, multiplication, transpose
- Vector operations: addition, subtraction, scaling, dot product
- Eigenvalues and eigenvectors: solving eigenvalue problems
- Covariance matrix: calculating and analyzing
- Orthogonality: ensuring the chosen eigenvectors are orthogonal (independent)

The results after applying PCA are explained via diagrams attached below.

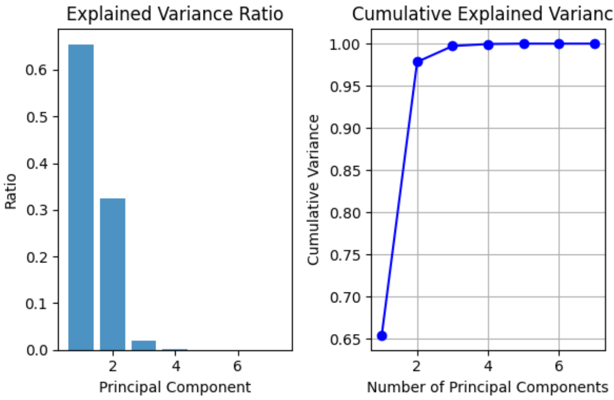

Figure 4.2: Structured diagram count of fraudulent transactions and non-fraudulent transactions.

The percentage of the overall variation in the data that each primary component accounts for is measured by the explained variance ratio. It is computed by dividing each primary component's variance by the overall variance of the information.

The total of the explained variance ratios for each primary component up to and including a particular component is known as cumulative explained variance. It calculates the percentage of the data's overall variance that can be accounted for by the first few principal components. According to the explained variance ratio graph, the first principal component, then the second, and so on, account for the majority of the variance in the data. The cumulative explained variance graph demonstrates that a significant amount of the total variation in the data is usually explained by the first few major components.

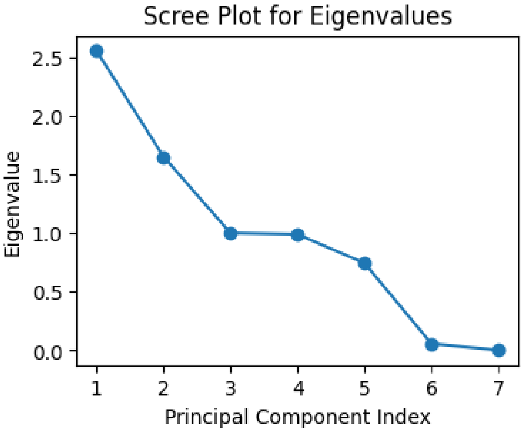

Figure 4.3: Eigenvalues of covariance matrix

The scree plot indicates that the remaining components account for very little variance in the data, but the top few primary components account for a significant amount of the total variance. This is a common finding in principal component analysis (PCA) and indicates that by projecting the data onto the top few principal components, we can reduce the dimensionality of the data without sacrificing much information.

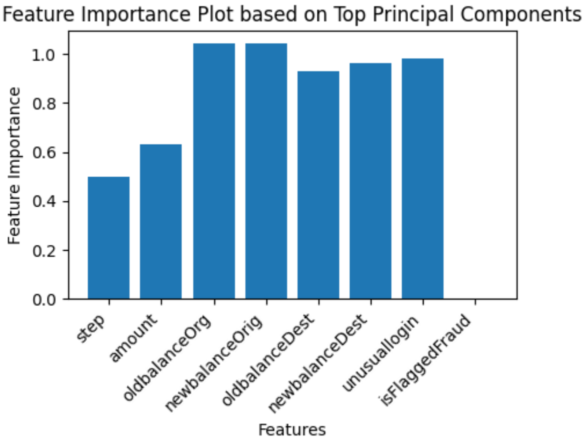

Figure 4.4: Eigenvalues of covariance matrix

The cumulative explained variance of a dataset's major components is displayed on the graph. The total of the explained variance ratios for each primary component up to and including a particular component is known as cumulative explained variance. It calculates the percentage of the data's overall variance that can be accounted for by the first few principal components.

4.2 Training ML Model

Our pipeline involves standardizing the data, using PCA to get the best attributes and then use support vector classifier to predict whether a transaction is fraudulent or not.

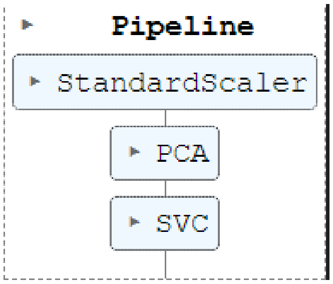

Figure 4.5: Pipeline

After training our model and all the preprocessing and finessing below are the results.

Test Accuracy	0.7263 or 72.63%
Train Accuracy	0.7293 or 72.93%
Overfit Performance Gap	0.00303 or 0.3%

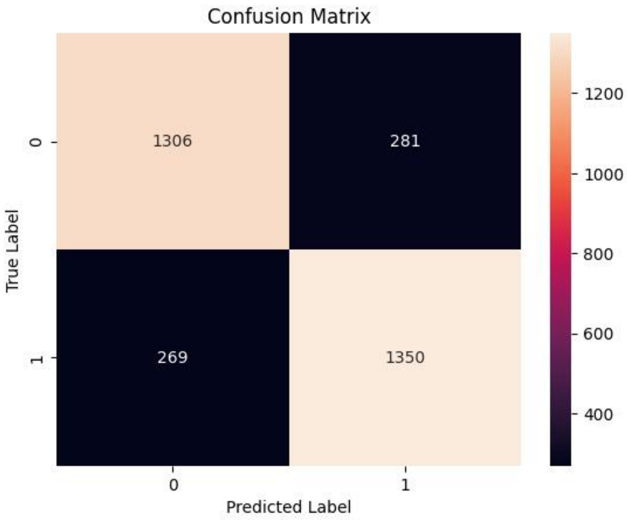

Figure 4.6 & 7: Test Results

After these results we have tested the model multitudinous times on different input and it has predicted the right values almost every time!

References

[1] Lin et al., "Determining false financial reporting by management," 2003.

[2] Bell and Carcello, "Determining false financial reporting by management," 2000.

[3] Fanning and Cogger, "Determining false financial reporting by management," 1998.

[4] Summers and Sweeney, "Determining false financial reporting by management," 1998.

[5] Beneish, "Determining false financial reporting by management," 1997.

[6] Green and Choi, "Determining false financial reporting by management," 1997.

[7] Kim et al., "Unusual retail transactions by staff members for internal fraud detection," 2003.

[8] Bentley, "Four subgroups of insurance fraud detection: home insurance; automobile insurance; crop insurance; medical insurance," 2000.

[9] Von Altrock, "Four subgroups of insurance fraud detection: home insurance; automobile insurance; crop insurance; medical insu rance," 1997.

[10] Phua et al., "Insurance fraud detection," 2004.

[11] Viaene et al., "Insurance fraud detection," 2004.

[12] Brockett et al., "Insurance fraud detection," 2002.

[13] Stefano and Gisella, "Insurance fraud detection," 2001.

[14] Belhadji et al., "Insurance fraud detection," 2000.

[15] Artis et al., "Insurance fraud detection," 1999.

[16] He and colleagues, "Insurance fraud detection," 1999.

[17] Cox, "Insurance fraud detection," 1995.

[18] Major and Riedinger, "Insurance fraud detection," 2002.

[19] Williams, "Insurance fraud detection," 1999.

[20] Fan, "Credit fraud detection," 2004.

[21] Chen et al., "Credit fraud detection," 2004.

[22] Chiu and Tsai, "Credit fraud detection," 2004.

[23] Foster and Stine, "Credit fraud detection," 2004.

[24] Kim and Kim, "Credit fraud detection," 2002.

[25] Maes et al., "Credit fraud detection," 2002.

[26] Syeda et al., "Credit fraud detection," 2002.

[27] Bolton and Hand, "Credit fraud detection," 2001.

[28] Bentley et al., "Credit fraud detection," 2000.

[29] Brause et al., "Credit fraud detection," 1999.

[30] Chan et al., "Credit fraud detection," 1999.

[31] Aleskerov et al., "Credit fraud detection," 1997.

[32] Dorronsoro et al., "Credit fraud detection," 1997.

[33] Kokkinaki, "Credit fraud detection," 1997.

[34] Ghosh and Reilly, "Credit fraud detection," 1994.

[35] Cortes et al., "Credit fraud detection," 2003.

[36] Cahill et al., "Credit fraud detection," 2002.

[37] Moreau and Vandewalle, "Credit fraud detection," 1997.

[38] Rosset et al., "Credit fraud detection," 1999.

[39] Kim et al., "Credit fraud detection comparable to wire-line and wire-less phone calls," 2003.

[40] Taniguchi et al., "Studies on wire-line and wire-less phone calls," 1998.

[41] Cox, "Studies on wire-line and wire-less phone calls," 1997.

[42] Ezawa and Norton, "Studies on wire-line and wire-less phone calls," 1996.

[43] Moreau et al., "Studies on wire-line and wire-less phone calls," 1999.

[44] Murad and Pinkas, "Studies on wire-line and wire-less phone calls," 1999.

[45] Fawcett and Provost, "Studies on wire-line and wire-less phone calls," 1997.

[46] Hollmen and Tresp, "Studies on wire-line and wire-less phone calls," 1998.

[47] Burge and Shawe-Taylor, "Studies on wire-line and wire-less phone calls," 2001.

[48] Data World, https://data.world/wayvy/synthetic-fraud-detection-dataset, 2023