General Management MBA

# Optimierter Einsatz von Ressourcen bei der automatisierten Betrugserkennung

Masterthese zur Erlangung des akademischen Grades
**Master of Business Administration (MBA)**
an der Universität für Weiterbildung (Donau-Universität Krems)
und der Technischen Universität Wien, Continuing Education Center


eingereicht von

Dipl.-Ing. Alexander Zeiler

00926745


BetreuerIn

Hon.-Prof. Mag. (FH) Gernot Kreiger, MBA, zPM

Wien, 09.04.2020

# Eidesstattliche Erklärung

Ich, DIPL.-ING. ALEXANDER ZEILER,

erkläre hiermit,

1. dass ich meine Masterthese selbständig verfasst, andere als die angegebenen Quellen und Hilfsmittel nicht benutzt und mich auch sonst keiner unerlaubten Hilfen bedient habe,

2. dass ich meine Masterthese bisher weder im In- noch im Ausland in irgendeiner Form als Prüfungsarbeit vorgelegt habe,

3. dass ich, falls die Arbeit mein Unternehmen betrifft, meine/n ArbeitgeberIn über Titel, Form und Inhalt der Masterthese unterrichtet und sein Einverständnis eingeholt habe.

Wien, 09.04.2020

_____

Unterschrift

# Danksagung

An dieser Stelle möchte ich mich bei Herrn Univ.-Prof. Dr. Wolfgang Aussenegg und bei Frau Mag. Kastenberger für die meist reibungslose Organisation des Lehrgangs bedanken. Zudem bedanke ich mich bei Herrn Mag. Kreiger für die sehr offene und herzliche Betreuung meiner Masterarbeit.

Weiters möchte ich mich auch bei meiner Lebensgefährtin Ruth bedanken, welche mich nach so manch demoralisierendem Vorlesungstag des Lehrgangs mit einem Bier oder einem gemeinsamen Essen wieder aufgeheitert hat.

Danke auch an meine Kollegen für die tolle Hilfsbereitschaft und meinen Freunden für den nötigen Ausgleich zum MBA-Alltag. Schlussendlich möchte ich mich noch bei meiner Mutter für die teilweise Finanzierung dieses Lehrgangs bedanken.

Wien, im April 2020

# Abstract

This thesis deals with automatized, data-based fraud detection in the financial and banking sector. Machine Learning and Data Mining algorithms are widely spread in the field of the automatized detection of this kind of fraud. Generally, an algorithmic detection is followed by an assessment by professional staff. These assessments by humans cause high costs and are in practice a limited resource. Thus, companies are forced to use this human resource as systematic and optimal as possible. A general drawback of established methods remain the high rate of false positives (falsely detected frauds) by the algorithm. These false detections cause a high amount of needless assessments. Therefore, this thesis is dedicated to the question how to estimate a probability of fraud, or in other words a meaningful order of the algorithmic detections. The algorithmic detections with the highest probability of fraud are consequently the first ones being assessed. It will be shown on the example of credit card fraud that the presented method yields a significant increase of the rate of correct human assessments and in further consequence reduces costs and effort.

# Kurzzusammenfassung

Diese Arbeit thematisiert die automatisierte, datenbasierte Betrugsfallerkennung (engl. fraud detection) im Finanz- und Bankwesen. *Machine Learning* und *Data Mining* Algorithmen sind weit verbreitet in der automatisierten Erkennung von diesen Betrugsfällen. Einer positiven algorithmischen Erkennung eines Betrugsfalles folgt im Allgemeinen eine Begutachtung durch Fachpersonal. Genau diese menschlichen Überprüfungen verursachen hohe Kosten und sind in der Praxis eine begrenzte Ressource. Daher legen Unternehmen hohen Wert darauf diese möglichst systematisch und optimal einzusetzen. Eine Schwäche gängiger Methodiken sind die hohe Rate an fälschlicherweise algorithmisch erkannten Betrugsfällen, welche viele nicht notwendige menschliche Überprüfungen zur Folge haben. Daher widmet sich diese Arbeit der Frage wie für die erkannten Betrugsfälle eine Wahrscheinlichkeit, bzw. eine sinnvolle Überprüfungs-Reihenfolge geschätzt werden kann. Die wahrscheinlichsten Betrugsfälle können somit zuerst überprüft werden und die Ressource Mensch kann so optimal eingesetzt werden. Am Beispiel von Kreditkartenbetrugsfällen wird anschaulich gezeigt, dass sich durch diese Methodik die Rate an korrekten menschlichen Überprüfungen deutlich steigern lässt und somit Kosten und Aufwand eingespart werden können.

# Inhaltsverzeichnis


**1 Einleitung** **1**

1.1 Begriffsdefinitionen . . . . . 2

1.1.1 Arten von Finanzbetrugsfällen . . . . . 3

1.1.2 Risikoabschätzung vs. Betrugswahrscheinlichkeit . . . . . 4

1.1.3 Data Analytics vs. Maschinelles Lernen vs. Data Mining . . 5

1.2 Woran erkennt man Betrug? . . . . . 6

1.3 State-of-the-Art . . . . . 6

1.3.1 Kreditkartenbetrug . . . . . 7

1.3.2 Unternehmens- und Versicherungsbetrug . . . . . 9

1.4 Probleme, Hindernisse und Grenzen . . . . . 10

1.5 Zielsetzung und Motivation dieser Arbeit . . . . . 11

1.6 Gliederung der Arbeit . . . . . 12

**2 Beschreibung des Datensatzes** **14**

2.1 Umfang und Inhalt . . . . . 14

2.2 Beschreibung der Eingangsgrößen/Attribute . . . . . 15

2.3 Diskussion und Informationsgehalt des Datensatzes . . . . . 16

**3 Neuartige Methode zur Kreditkartenbetrugserkennung** **18**

3.1 Ergebnisse in der Literatur . . . . . 18

3.2 Aufbau der neuartigen Methode . . . . . 20

3.2.1 Arbeitsweise von datenbasierter Klassifikation . . . . . 20

3.2.2 Klassifikation am Beispieldatensatz . . . . . 21

3.2.3 Auswahl der Betrugsfälle nach Wahrscheinlichkeit . . . . . 24

**4 Resultate und Diskussion** **27**

4.1 Vergleich Vorhersagegenauigkeiten . . . . . 27

4.2 Diskussion der Ergebnisse . . . . . 28

**5 Zusammenfassung, Conclusion und Ausblick** **30**

5.1 Zusammenfassung . . . . . 30

5.2 Conclusion . . . . . 31

5.3 Ausblick auf zukünftige wissenschaftliche Untersuchungen . . . . . 31

**Literaturverzeichnis** **36**

# Abbildungsverzeichnis

1.1 Arten der automatisierten Betrugsfallerkennung und kombinierte Arbeitsweise eines Erkennungssystems, vgl. Nisbet, Miner und Yale (2018). . . . . 3
1.2 Einteilung und Arten von Finanzbetrugsfällen in englischen Fachtermini, vgl. West und Bhattacharya (2015). . . . . 4

2.1 Vorgehensweise zur Analyse von lernenden Modellen am Beispiel der Kreditkartenbetrugserkennung. . . . . 15

3.1 Beispiel zur Klassifikation von Leoparden und Löwen anhand von Gewicht und maximaler Laufgeschwindigkeit. . . . . 21
3.2 Klassifikation von betrügerischen Kunden mit linearer SVM auf Basis von zwei Attributen. . . . . 22
3.3 Klassifikation von betrügerischen Kunden mit RBF-SVM auf Basis von zwei Attributen. . . . . 23
3.4 Schätzung der wahrscheinlichsten Betrugsfälle (2D - lineare SVM). . 25
3.5 Schätzung der wahrscheinlichsten Betrugsfälle (2D - RBF-SVM). . . 25

# Tabellenverzeichnis

3.1 Kennzahlen zur Vorhersagegenauigkeit mit Logistischer Regression, vgl. (Yeh und Lien, 2009). . . . . 19
3.2 Vorhersagegenauigkeit gängiger Methoden auf Basis von *nur* 2 der 24 Attribute und 150 Datenpunkten aus dem Testdatensatz. . . . . 24
3.3 Vorhersagegenauigkeit der vorgestellten Methoden auf Basis von *nur* 2 der 24 Attributen und 150 Datenpunkten aus dem Testdatensatz. 26

4.1 Konfiguration systematische Untersuchung der Vorhersagegenauigkeit. 27
4.2 Vorhersagegenauigkeit der vorgestellten Methoden am vollständigen Datensatz. . . . . 28

# Executive Summary

Der Themenkomplex "Neue Technologien", auch häufig unter dem Schlagwort Digitalisierung medial präsent, führt zu sich laufend weiterentwickelnden und immer spezifischeren Arten und Methoden von Betrugsfällen im Finanz- und Bankenbereich. Sowohl der Umfang als auch die Anzahl dieser betrügerischen Ereignisse nehmen kontinuierlich zu. Aus der Perspektive der Finanzinstitutionen bieten automatisierte Vorhersagen oder zumindest die reaktive Identifikation von Betrugsfällen essenzielle, wenn auch nicht vollständig schützende Mechanismen.

Moderne datenbasierte Algorithmen stellen eine große Hilfestellung dar und können wertvolle Hinweise für Betrugsfälle liefern. Sie sind jedoch aktuell noch nicht zuverlässig genug, um auf anschließende Überprüfungen durch Fachpersonal verzichten zu können. Aufgrund der im Allgemeinen sehr niedrigen Auftrittswahrscheinlichkeit eines Betrugsfalls (unter 0.1 % der Transaktionen sind betrügerisch) neigen datenbasierte Algorithmen grundsätzlich dazu, viele nicht-betrügerische Ereignisse als betrügerisch einzustufen. Dies resultiert in einer weiteren Ressourcenbindung aufgrund zahlreicher Kontrollen durch Fachkräfte, ohne tatsächlich einen Betrugsfall zu identifizieren. Diese menschliche Ressource ist einerseits kostspielig und im Allgemeinen der limitierende Faktor für die Anzahl an Überprüfungen.

Dieses Kernproblem steht im Fokus dieser Arbeit: Es wird analysiert, anhand welcher Maßnahmen die Algorithmen zur automatisierten Betrugserkennung verbessert werden können. Das Ziel ist es, die Rate an korrekten Überprüfungen durch Fachkräfte, also Überprüfungen, die tatsächlich zu einer Entlarvung eines Betrugsfalles führen, maßgeblich zu erhöhen.

Um die Maßnahmen und Ansätze plausibel darstellen zu können, werden in dieser Arbeit folgende Fragestellungen behandelt:

- Welche datenbasierten Methoden werden in der Fachliteratur als *State-of-the-Art* angeführt? Welche Möglichkeiten stehen bei der automatisierten Betrugs-

fallerkennung zur Verfügung?

- Was ist die Idee und wie sieht die Funktionsweise gängiger Algorithmen zur automatisierten, datenbasierten Betrugserkennung aus? Diese Algorithmen werden anhand von praktischen Beispielen und unter Verzicht auf die Verwendung komplexer Formeln anschaulich beschrieben.

- Inwiefern können Algorithmen dieser Art erweitert bzw. verbessert werden, um Rate an korrekten Überprüfungen durch Fachkräfte deutlich zu steigern? Dazu wird eine neuartige Methode entwickelt und im Detail motiviert und beschrieben.

- Wie können für die algorithmisch vorhergesagten Betrugsfälle eine Art Betrugswahrscheinlichkeit geschätzt werden, um die vorhergesagten Fälle einer systematischen Auswertungsreihung zu unterziehen?

- In welchem Ausmaß ist eine Steigerung und Verbesserung der Vorhersagegenauigkeit durch den Einsatz dieser neuartigen Methoden zu verzeichnen? Dies soll anhand eines Datensatzes zu Kreditkartenbetrugsfällen erörtert werden.

Im ersten Teil der Arbeit werden relevante Begrifflichkeiten definiert und eine adäquate Einteilung von Möglichkeiten zu Betrugsfallerkennung vorgestellt. Dies soll eine gemeinsame Basis bei unterschiedlichem Vorwissen der LeserInnen schaffen.

Im nächsten Abschnitt wird die gängige Funktionsweise von Klassifikation anhand von Beispielen anschaulich dargestellt. Anhand der aktuellen Fachliteratur werden grundlegende Schwächen aufgezeigt und für die in dieser Arbeit vorgestellte Methode motiviert.

Anhand des Beispieldatensatzes folgt eine anschauliche Präsentation dieser Methode auf nachvollziehbare Weise. Die resultierende Vorhersagegenauigkeit und Zuverlässigkeit der entwickelten Methode wird einem Vergleich mit Ergebnissen aus der Literatur unterzogen. Dabei konnten folgende Ergebnisse erzielt werden:

- Die Rate an korrekten Überprüfungen konnte am Beispieldatensatz um 65 % gegenüber der in der Fachliteratur vorgeschlagenen Methode gesteigert werden. Im Detail bedeutet dies, dass statistisch gesehen anstatt von bisher 52 % durch die neuartige Methode 86 % der Überprüfungen zu einem tatsächlichen Betrugsfall führen.

- Die Rate an erkannten Betrugsfällen konnte am Beispieldatensatz ebenfalls erhöht werden.
- Die obigen Ergebnisse werden anhand eines, im Vergleich zu moderner Fachliteratur, wesentlich weniger umfangreichen Datensatz erzielt. Somit ist auch die notwendige Rechenleistung, welche in der Praxis häufig ebenfalls eine begrenzte Ressource darstellt, deutlich geringer.

Die in dieser Arbeit vorgestellte Methode ist somit insbesondere für kleinere Banken oder Kreditinstitute geeignet, welche keine allumfassenden Mengen an Daten zur Verfügung haben. Zudem stehen diese Unternehmen der Problematik mit knappen Ressourcen gegenüber: Für die Gewährleistung der geforderten - mitunter beachtlichen - Rechenleistungen besteht der Bedarf an entsprechender Hardware, welche teilweise für die modernen Ansätze benötigt wird. Durch den vergleichsweise niedrigen Rechenaufwand stellt die hier vorgestellte Methode eine vielversprechende und zukunftsweisende Alternative dar.

# 1 Einleitung

Betrug wird im *Concise Oxford Dictionary* als eine kriminelle Aktivität bezeichnet, bei welcher durch Vorspiegelung falscher Tatsachen ein ungerechtfertigter Vorteil erlangt wird. Betrug tritt in den verschiedensten Formen und Lebensbereichen auf. Im Rahmen dieser Arbeit sollen speziell Betrugsfälle im breiten Umfeld des Finanzwesen bzw. deren automatisierte Erkennung im Detail untersucht werden. Der wirtschaftliche Schaden im Zusammenhang mit Betrugsfällen im Finanzwesen, wird alleine in den USA auf bis zu $1.5 Billionen jährlich geschätzt (Gee, 2015). Die Nachfrage nach automatisierten Systemen zur Betrugserkennung ist dementsprechend hoch. Mit neuen Technologien, der Digitalisierung und wirtschaftlichen Entwicklungen steigen auch die Möglichkeiten und die Häufigkeit von finanziellem Betrug. Systeme zur Betrugserkennung erfahren daher eine ständige Entwicklung um mit diesen neuen Anforderungen schritthalten zu können.

Die automatisierte Betrugsfallerkennung (engl. *fraud detection*) ist ein Teilgebiet der Unternehmensanalytik (engl. *business analytics*). Generell kann die Erkennung von betrügerischen Ereignissen gemäß Nisbet, Miner und Yale (2018) in drei Arten unterteilt werden:

- *Expertensysteme*:
  Ein Expertensystem basiert auf einem statischen Regelwerk, dass durch Experten zusammengestellt wurde. Diese Regelwerke können beispielsweise durch Ablaufdiagramme dargestellt werden. Die Finanztransaktionen werden dann basierend auf diesem Regelwerk als Betrug oder normale Transaktion eingestuft. Die Zuverlässigkeit solcher Systeme hängt stark von der Qualität der Experten ab. Inhärent sind in diesen Regelwerken die subjektiven Empfindungen der Experten abgebildet. Frühere Systeme zur automatisierten Betrugserkennung basierten fast ausschließlich auf dieser Methode.

- *Adaptive regelbasierte Systeme*:
  Diese Systeme können als Weiterentwicklung der oben genannten Expertensysteme verstanden werden. Das Regelwerk wird basierend auf historischen Daten von Finanztransaktionen automatisiert adaptiert und optimiert. Somit spricht man von einem adaptiven Regelwerk. Verschiedene Methoden wie z. B. *Fuzzy-Logic* ermöglichen zudem das Einführen von *weichen* Entscheidungsgrenzen, also einer Weiterentwicklung der reinen entweder-oder Entscheidung.

- *Statistische datenbasierte Systeme*:
  Diese Art der Betrugserkennung sucht mithilfe von mathematischen Methoden nach statistischen Mustern (engl. *patterns*) in möglichst großen Datensätzen, welche mit Betrug in Verbindung gebracht wurden, oder welche ungewöhnlich erscheinen. Beispielsweise mit maschinellem Lernen (engl. *Machine Learning*) werden mathematische Modelle trainiert, welche diese Muster abbilden. Auf Basis solcher Modelle können dann Transaktionen in Echtzeit auf einen möglichen Betrugsfall untersucht werden.

Moderne Systeme basieren häufig auf einer Kombination aller drei vorgestellten Techniken. Abbildung 1.1 stellt die Arbeitsweise solcher kombinierter Systeme dar. Mit wachsender Rechenleistung und Datenverfügbarkeit geht die Entwicklung zunehmend in die Richtung Betrugserkennung rein auf statistischen, datenbasierten Systemen zu betreiben. Das Hauptaugenmerk dieser Arbeit richtet sich auf diese Art der automatisierten Betrugserkennung.

## 1.1 Begriffsdefinitionen und Einteilung von finanziellen Betrugsfällen

Im Umfeld der automatisierten Betrugsfallerkennung und insbesondere im Zusammenhang mit statistischen, datenbasierten Methoden gibt es eine Vielzahl von Fachtermini. Diese sind zum Teil redundant in deren Bedeutung und teilweise nur unsauber definiert (Rayner, 2016). Um dem Leser ein umfassendes Verständnis dieser Arbeit zu ermöglichen, sollen im Folgenden die wichtigsten Arten von Finanzbetrugsfällen, sowie die verknüpften Fachtermini aus der Betrugsfallerkennung definiert werden.

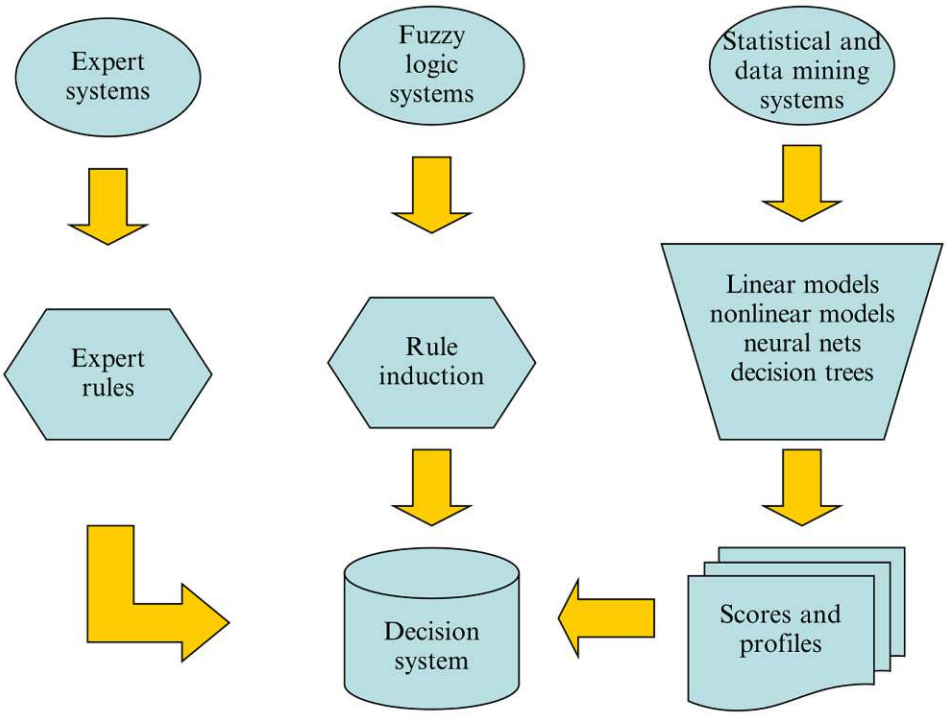


Abbildung 1.1: Arten der automatisierten Betrugsfallerkennung und kombinierte Arbeitsweise eines Erkennungssystems, vgl. Nisbet, Miner und Yale (2018).

### 1.1.1 Arten von Finanzbetrugsfällen

Gemäß West und Bhattacharya (2015) werden Finanzbetrugsfälle üblicherweise in Bankbetrug (engl. *Bank Fraud*), Unternehmensbetrug (engl. *Corporate Fraud*) und Versicherungsbetrug (engl. *Insurance Fraud*) unterteilt.

Zu den wichtigsten Unterarten des Bankbetruges zählen der Kreditkartenbetrug (engl. *Credit Card Fraud*) und die Geldwäsche (engl. *Money Laundering*). Speziell der Kreditkartenbetrug ist aufgrund der vergleichsweise hohen Häufigkeit und vor allem der großen Datenverfügbarkeit eines der wichtigsten Anwendungsgebiete von automatisierter Betrugsfallerkennung im Finanzwesen (Quah und Sriganesh, 2008). Kreditkartenbetrug basiert meistens auf Diebstahl von Kreditkartendaten beispielsweise durch *Phishing-Mails* oder durch Hackerangriffe. Zunehmend werden Kreditkartendaten auch automatisiert generiert und für Betrugsfälle genutzt. Die Prüfziffer schützt nicht ausreichend vor Betrugsfällen, da diese automatisiert aus der Kreditkartennummer generiert werden kann (Pindar u. a., 2017).

Die meist verbreitetste Variante des Unternehmensbetruges sind Betrugsfälle im Bilanzabschluss (engl. *Financial Statement Fraud*). Dokumente des Bilanzabschlusses werden in diesem Betrugsschema vorsätzlich verändert oder gefälscht um beispielsweise die Höhe der Steuerzahlungen zu verringern oder für Kreditgeber oder Investoren attraktiver zu wirken (Ravisankar u. a., 2011).

Laut Ngai u. a. (2011) ist Versicherungsbetrug dadurch gekennzeichnet, dass gewisse Ereignisse gefälscht oder absichtlich begangen werden um so zu unrecht Zahlungen von der Versicherung zu erhalten. Abbildung 1.2 soll diese Einteilung

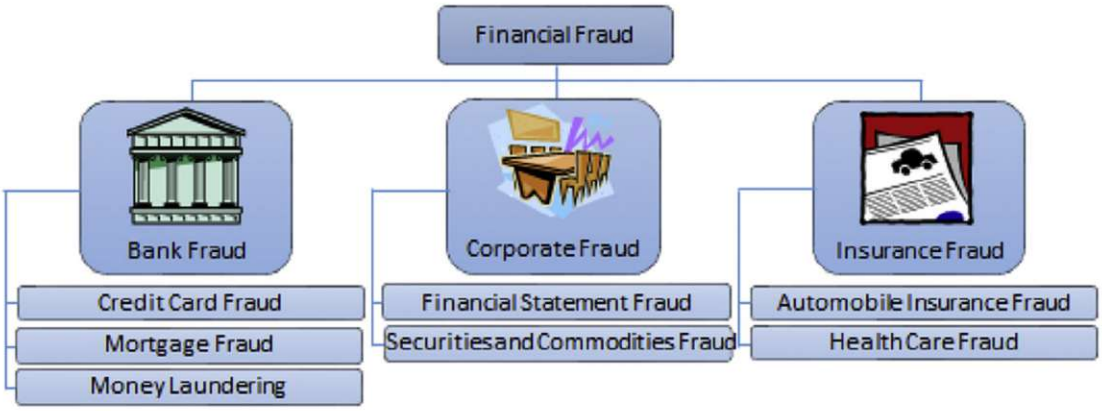


Abbildung 1.2: Einteilung und Arten von Finanzbetrugsfällen in englischen Fachtermini, vgl. West und Bhattacharya (2015).

zusammenfassend darstellen.

### 1.1.2 Risikoabschätzung vs. Betrugswahrscheinlichkeit

Quasi jede Bank und die jedes größere Unternehmen im Finanzbereich ist dem Risiko eines Finanzbetruges unmittelbar ausgesetzt. Somit muss sich auch jede dieser Institutionen Gedanken über Maßnahmen gegenüber diesem Phänomen machen. Grundlegend dafür ist eine adäquate *Risikoabschätzung*. Gee (2015) definiert das Risiko für die Institution als das Produkt der negativen Auswirkungen und der Auftrittswahrscheinlichkeit von Betrugsfällen.

$$\text{Risiko} = \text{Auswirkung x Betrugswahrscheinlichkeit}$$

Basierend auf dieser Risikoabschätzung kann systematisch entschieden werden, welcher Aufwand für präventive oder Detektionsmaßnahmen als sinnvoll erscheinen. Negative Auswirkungen und Betrugswahrscheinlichkeit müssen je separat abgeschätzt werden.

### 1.1.3 Data Analytics vs. Maschinelles Lernen vs. Data Mining

Bei den Begrifflichkeiten *Data Analytics*, Maschinelles Lernen und *Data Mining* handelt es sich laut Rayner (2016) um Überbegriffe für Methoden aus dem Bereich der mathematischen Datenverarbeitung auf Basis von statistischen und wahrscheinlichkeitstheoretischen Grundlagen. Aufgrund der Neuartigkeit dieser Überbegriffe hat sich in der Literatur auch noch keine eindeutige und saubere Abgrenzung zwischen diesen Begriffen etabliert (Rayner, 2016). *Data Analytics* ist ein Teilgebiet der künstlichen Intelligenz (engl. *Artificial Intelligence*) und kann als Sammelbegriff für alle datenbasierten Auswertungssysteme und Auswertungsmethoden verstanden werden. Somit sind Maschinelles Lernen und *Data Mining* Teilgebiete von *Data Analytics*. Unter *Data Mining* versteht man weitestgehend das automatisierte Untersuchen von großen Datensätzen auf Trends oder Querverbindungen. Maschinelles Lernen wird eher für klassische Datenverarbeitungsaufgaben wie Regression (z. B. wie wahrscheinlich ist ein Betrugsfall) oder Klassifikation (z. B. Betrugsfall ja oder nein) verwendet. Gerade der Begriff *Data Mining* wird in der Literatur oft sehr allgemein verwendet und umfasst auch oft klassische Anwendungen des maschinellen Lernens. Auch in einigen in dieser Arbeit zitierten Werken wird der Begriff *Data Mining* für klassische Anwendungen aus dem Maschinellen Lernen verwendet. Der Vollständigkeit halber soll auch der sehr gebräuchliche Begriff *Big-Data Analytics* definiert werden. Von *Big-Data* spricht man laut Dhankhar und Solanki, 2019, wenn die Datenmenge so groß ist, dass diese üblicherweise nicht mehr gleichzeitig im Arbeitsspeicher verarbeitet werden kann und weiters der Datensatz unterschiedliche Datenformate, -quellen und -flüsse beinhaltet. *Big-Data Analytics* kennzeichnet nun die Analyse bzw. die Verarbeitung solcher Datensätze.

## 1.2 Woran erkennt man Betrug?

Prinzipiell kann nur versucht werden bestimmte Warnhinweise oder Indikatoren für Betrugsfälle in den vorhandenen Daten zu erkennen. Es wird also nach Anomalien, bzw. allem was außerhalb des Normereignisses passiert oder nicht den gängigen Mustern entspricht gesucht. Beispiele für solche Anomalien sind:

- Duplizierte oder mehrfach idente Transaktionen
- Ungewöhnliche Abfolge von Transaktionen (z. B. üblicherweise Transaktionen in Österreich mit niedrigen Beträgen und plötzlich Transaktionen in Russland mit sehr hohen Beträgen)
- Inkonsistente Transaktionen
- Ungewöhnlicher zeitlicher Zusammenhang von Transaktionen (z. B. zu viele Transaktionen in kurzer Zeit)
- Ausreißer (z. B. plötzlich unverhältnismäßig hohe Transaktion)
- und viele mehr

## 1.3 State-of-the-Art

Zum sehr breiten Feld der automatisierten Betrugsfallerkennung im Finanzbereich existieren eine nicht enden wollende Anzahl von Arbeiten, Büchern und Publikationen. Diese Literaturrecherche beschränkt sich daher auf die automatisierte Betrugsfallerkennung im Finanzbereich mittels statistischer, datenbasierter Systeme, vgl. Abbildung 1.1. Auf die Angabe, bzw. den Vergleich veröffentlichter Performance-Kriterien (z. B. Quote der korrekt erkannten Betrugsfällen) wird im Folgenden bewusst verzichtet. Dies hat den Grund, dass die Performance, bzw. die Vorhersagegenauigkeit einer Methode wesentlich von der Qualität und dem Umfang des Datensatzes abhängt, die Arbeiten jedoch im Allgemeinen auf unterschiedlichsten Datensätzen basieren. Dies hat vor Allem die Ursache, dass viele der verwendeten Datensätze nicht frei zugänglich sind und somit es von Vornherein schwer möglich wäre die Performance der einzelnen Methoden zu vergleichen. Des weiteren sind

viele Methodiken speziell auf den jeweiligen Datensatz maßgeschneidert. Die Veröffentlichung von *Benchmark-Datensätzen* könnte eine gemeinsame Vergleichsbasis schaffen und so die Zuverlässigkeit verschiedenster Methoden zumindest erhöhen.

Verglichen mit regelbasierten Expertensystemen ist die automatisierte und rein datenbasierte Art der Betrugsfallerkennung eine recht junge Methode. Zhang, Patuwo und Hu (1998) stellten eine der ersten Anwendungen in diesem Bereich vor. Sie zeigten die Nützlichkeit von *Neuronalen Netzen* (NN) für die Betrugsfallerkennung im Finanzsektor anhand von verschiedenen praktischen Beispielen.

Das umfassende Werk von Gee (2015) gilt als eines der Standardwerke in diesem Bereich. Neben einer umfassenden Einteilung und Beschreibung von grundlegenden Konzepten und Methoden werden eine Vielzahl von praktischen Anwendungsbeispielen im Finanzsektor vorgestellt.

Yue u. a. (2007) sowie West und Bhattacharya (2015) präsentieren umfassende und aktuelle Literaturrecherchen zum Thema datenbasierter Detektion von Finanzbetrugsfällen und vergleichen die Performance und Vorhersagegenauigkeit verschiedener Methoden und Algorithmen anhand von verschiedenen Datensätzen.

Da sich diese Arbeit in den späteren Kapiteln speziell auf Kreditkartenbetrug konzentriert, wird im Folgenden zuerst detailliert auf den aktuellen *State-of-the-Art* in der automatisierten Erkennung von Kreditkartenbetrugsfällen eingegangen. Anschließend sollen die wichtigsten Arbeiten im Bereich der Betrugsfallerkennung im Unternehmens- und Versicherungssektor vorgestellt werden.

### 1.3.1 Kreditkartenbetrug

Die ersten Arbeiten zur automatisierten und rein datenbasierten Erkennung von Kreditkartenbetrugsfällen wurden Ende der 90er Jahre publiziert und basieren auf den damals wie auch heute im Trend liegenden Neuronalen Netzen. Aleskerov, Freisleben und Rao (1997), sowie Zhang, Patuwo und Hu (1998) präsentieren zwei Ansätze dieser Art, wobei sie Neuronale Netze auf für damalige Verhältnisse umfassende Datensätze von Kreditkartentransaktionen anwenden. Die Ergebnisse waren zu dieser Zeit jedoch noch nicht zufriedenstellend. Aus heutiger Sicht ist dies auf die zu damaliger Zeit deutlich geringere Rechenkapazität der Computersysteme zurückzuführen Die Modelle (also die Neuronalen Netze) konnten nicht in einer endlichen Zeit mit ausreichend Daten trainiert werden um eine zuverlässige Vorhersage zu

erlauben.

Die Arbeit von Bhattacharyya u. a. (2011) orientiert sich an moderneren Algorithmen. Auf Basis eines großen jedoch nicht frei verfügbaren Datensatzes von Kreditkartentransaktionen wird die Anwendung bzw. die Vorhersagegenauigkeit von gängigen Konzepten des maschinellen Lernens wie Entscheidungsbäume (engl. *Decision Trees*), Logistische Regression (LR), *Random Forrest* und *Support Vector Machines* (SVM) miteinander verglichen. Das Fazit dieser Arbeit ist, dass der Einsatz von LR und SVM die zuverlässigsten Ergebnisse erzielen. Diese beiden Methoden werden auch in der vorliegenden Arbeit eingesetzt bzw. erweitert.

Eine moderne und komplexe Methode zur Kreditkartenbetrugsfallerkennung ist die Klassifikation basierend auf sequentiellem Lernen. Das Ziel dieser Methode ist den Kontext und den sequenziellen Zusammenhang zwischen den Transaktionen, getätigt von einem Kreditkartenkonto, zu verstehen (Jurgovsky u. a., 2018). So werden übliche Transaktionshistorien von potentiell betrügerischen Transaktionshistorien unterschieden. Srivastava u. a. (2008) erzielen zufriedenstellende Ergebnisse durch Umsetzen von sequentiellem Lernen mithilfe von *Hidden Markov Models*. Das Modell wird auf Basis von nicht frei zugänglichen Datensätzen von Millionen Kreditkartentransaktionen trainiert und validiert. Jurgovsky u. a. (2018) nutzt *Recurrent Neural Nets* (RNNs) um eine Art Kurz- und Langzeitgedächtnis nachzubilden. Dadurch wird die Fähigkeit des Algorithmus, bzw. des Modells erhöht um übliche von betrügerischen Transaktionshistorien zu unterscheiden. Es wird gezeigt, dass dadurch mehr Betrugsfälle erkannt werden können als bei bisher vergleichbaren Methoden in der Literatur. Damit steht diese Aussage klar der Erkenntnis von Bhattacharyya u. a. (2011) gegenüber, dass vor allem LR und SVM zu den besten Klassifikationsergebnis im Rahmen des Kreditkartenbetrugs führen. Bei genauerer Analyse fällt auf, dass sich jedoch die Daten, welche die beiden Arbeiten zur Verfügung hatten, grundlegend unterscheiden. Die Arbeit von Jurgovsky u. a. (2018) basiert auf nicht frei zugänglichen Datensätzen von enormer Größe mit sehr detaillierten Informationen zu jeder einzeln getätigten Transaktion. Die Arbeit von Bhattacharyya u. a. (2011) hingegen basiert auf einem eher generischen Datensatz, welcher diese detaillierten Informationen nicht enthält. Dies zeigt auch, dass die Methoden auf den Datensatz abgestimmt sein müssen um die besten Ergebnisse zu erzielen.

Als Fazit kann gezogen werden, dass Methoden basierend auf sequentiellem Lernen durchaus Potential haben in naher Zukunft zu einer der gängigsten Methoden heran-

zuwachsen. Jedoch wird das Problem der Notwendigkeit für enorme Datenmengen mit einem hohen Ausmaß an Details bestehen bleiben. Somit wird diese Methode eher großen Kreditinstituten und großen Banken vorbehalten bleiben.

### 1.3.2 Unternehmens- und Versicherungsbetrug

Eine sehr umfassende und umfangreiche Arbeit zum Thema Bilanzbetrug von Unternehmen präsentieren Kirkos, Spathis und Manolopoulos (2007). Sie untersuchen die Eignung verschiedener statischer Methoden des maschinellen Lernens, sowie Neuronaler Netze auf einen großen Datensatz von Jahresabschlüssen von griechischen Unternehmen. Die Ergebnisse versprechen durchaus praktische Anwendbarkeit. In dieser Arbeit konnten besonders mit Bayes'schen Netzen gute Ergebnisse erzielt werden.

Hoogs u. a. (2007) beschreibt eine Methode zur Klassifizierung betrügerischer Unternehmen auf Basis von *Accounting and Auditing Enforcement Releases*. Sie verwenden dazu genetische Algorithmen, welche ansonsten eher in naturwissenschaftlichen Anwendungen verwendet werden. Die durchaus vielversprechenden Ergebnisse bestätigen jedoch die Eignung auch für Probleme dieser Art.

Insbesondere jüngere Arbeiten setzen bei der Betrugsfallerkennung im Bilanzbereich auf *Text Mining*. Dies beruht auf der Überlegung, dass in Bilanzberichten, bzw. Jahresabschlüssen ein Teil der Information im Text und nicht ausschließlich in den Zahlen abgebildet ist. *Text Mining* versucht nun aus textuellen Passagen Information zu extrahieren. Cecchini u. a. (2010), Spathis u. a. (2002), sowie Humpherys u. a. (2011) nutzen diese Information, kombinieren diese mit den zur Verfügung stehenden Zahlen und wenden klassische Methoden der Betrugsfallerkennung an. Beide Arbeiten zeigen, dass das Klassifikationsergebnis gegenüber klassischen Methoden verbessert werden kann. Der große Unterschied zu anderen Methoden in der Literatur ist, dass die Aufwand für die Aufbereitung der Daten durch *Text Mining* wesentlich verringert wird. Die Methode extrahiert sozusagen die notwendigen Informationen automatisiert.

Ähnlich dem Kreditkartenbetrug liefert die Anwendung von Logistischer Regression (LR) bei der Klassifikation von Versicherungsbetrugsfällen die erfolgversprechendsten Ergebnisse. Viaene u. a. (2007) sowie Pinquet, Ayuso und Guillen (2007) beweisen dies mit ihren Arbeiten, welche beide ihre auf LR basierende Me-

thode anhand eines umfassenden Datensatzes einer spanischen Autoversicherung präsentieren.

## 1.4 Probleme, Hindernisse und Grenzen

Viele der oben vorgestellten Methoden erzielen zwar gute Ergebnisse an den Beispieldatensätzen, zeigen jedoch in der Praxis deren Lücken auf (Abdulrazaq u. a., 2019). Diese Widersprüchlichkeit resultiert vor allem darin, dass die Zuverlässigkeit einer Methoden nicht immer eindeutig, bzw. genau definiert bestimmt werden kann. Manche Arbeiten wählen deren Gütekriterium sehr geschickt, um mögliche Schwächen in der Praxis zu verdecken. Ein großes Problem sind beispielsweise die hohe Anzahl an auftretenden sogenannten *False Positives*, also Transaktionen bzw. Kunden welche fälschlicherweise vom Algorithmus als Betrugsfall identifiziert werden, obwohl es sich gar nicht um ein betrügerisches Ereignis gehandelt hatte. Dies führt dazu, dass jeder vom Algorithmus erkannte Betrugsfall im Allgemeinen einer menschlichen Prüfung oder Nachforschung unterzogen werden muss. Im Normalfall stehen nicht die menschlichen Ressourcen zur Verfügung um alle vom Algorithmus vorhergesagten Betrugsfälle nachzuprüfen.

Ein weiteres Problem ist, dass insbesondere moderne Lösungen wie *Recurrent Neural Nets* etc. enorme und umfassende Datenmengen verlangen. Zudem sind im Allgemeinen Transaktionsdaten und personenbezogene, sowie demografische Daten nicht ausreichen um einen Großteil der in Abschnitt 1.3 vorgestellten Algorithmen zu trainieren. Diese basieren darauf von Datensätzen zu lernen, welche die Information enthalten, ob es sich bei den Transaktionen oder Serien von Transaktionen um betrügerische Ereignisse gehandelt hat oder nicht. Die Algorithmen lernen also von dem Datensatz (engl. *supervised learning*). Datensätze dieser Art stehen im benötigtem Umfang jedoch im Allgemeinen nur wirklich großen Banken oder Kreditinstituten zur Verfügung.

Zudem bring das Konzept der lernenden Algorithmen mit sich, dass Betrugsfälle, welche in der Vergangenheit gänzlich unbemerkt blieben auch im Datensatz fälschlicherweise als kein Betrugsfall abgebildet sind. Die Modelle werden dementsprechend falsche Tatsachen lernen. Bolton und Hand (2002) nennen dieses grundlegende Problem als eine der Hauptschwächen der automatisierten Betrugsfallerkennung.

Die Modelle können also im besten Fall nur so gut werden, wie die Datensätze auf denen diese trainiert werden.

## 1.5 Zielsetzung und Motivation dieser Arbeit

Basierend auf der obigen Literaturrecherche und Problemstellung ergibt sich für diese Arbeit folgende *Zielsetzung*:

- Entwicklung einer Methode zur automatisierten Betrugsfallerkennung, wobei die erkannten Betrugsfälle nach deren Betrugswahrscheinlichkeit gereiht werden sollen. Somit unterscheidet sich dieser Ansatz von gängigen Methoden in der Literatur, da diese großteils auf reiner Klassifikation beruhen (also Betrugsfall ja / nein).
- Der Benutzer soll eine gewisse Anzahl an verfügbaren menschlichen Überprüfungen von Betrugsfällen vorgeben können (z. B. 150 Überprüfungen, oder 3 % der Gesamttransaktionen). Die entwickelte Methode soll dann die z. B. 150 wahrscheinlichsten Betrugsfälle ausgeben.
- Die Vorteile und die Vorhersagegenauigkeit dieser Methode sollen auf Basis eines frei verfügbaren Datensatzes von Kreditkartenbetrugsfällen verifiziert werden. Die Vorhersagegenauigkeit der Methode soll mit gängigen Methoden aus der Literatur verglichen werden.
- Die Arbeitsweise von gängigen Algorithmen zur automatisierten Betrugserkennung soll anschaulich anhand von Beispielen verständlich und ohne Verwendung komplexer Formeln erklärt werden.

Durch diese Methode sollen sich folgende *Möglichkeiten und Vorteile* gegenüber gängiger Ansätze in der Literatur ergeben:

- Die Ressource Mensch wird durch den obigen Ansatz optimal eingesetzt. Eines der in der Literaturrecherche offenbarten Hauptprobleme gängiger Ansätze ist die hohe Rate an *falschen Positiven*, also fälschlicherweise erkannten Betrugsfällen. Betrugsfälle werden zwar häufig mit einer hohen Zuverlässigkeit erkannt, gemeinsam mit den vielen falschen Positiven reicht die menschliche

Ressource jedoch nicht aus um alle erkannten Betrugsfälle zu überprüfen. Durch die Reihung der vorhergesagten Betrugsfälle nach deren geschätzter Wahrscheinlichkeit soll die Rate an tatsächlich positiven Überprüfungen deutlich erhöht werden.
Beispiel: Von 1000 Transaktionen sind 100 betrügerischer Natur. Ein üblicher Algorithmus erkennt beispielsweise 80 der 100 betrügerischen Transaktionen, erkennt jedoch fälschlicherweise noch weitere 120 Transaktionen als betrügerisch. Stünden nun beispielsweise Ressourcen für 50 Überprüfungen zu Verfügung und würden diese per Zufallsprinzip aus den 200 erkannten ausgewählt, dann würde es sich nur 20 der 50 Überprüfungen tatsächlich um Betrugsfälle handeln.

- Somit soll die Rate an unnötigen menschlichen Überprüfungen minimiert werden und somit die Rate der sinnvollen, bzw. korrekten menschlichen Überprüfungen maximiert werden. Damit können Kosten und Aufwand eingespart werden.

- Die entwickelte Methode ermöglicht die Identifikation von sehr wahrscheinlichen Betrugsfällen. Daher wird die Untersuchung der kennzeichnenden Kriterien für genau diese Betragsfälle ermöglicht.

Damit ergibt sich für diese Arbeit folgende *Forschungsfrage*:

- Wie können gängige datenbasierte Methoden erweitert werden um die Ressource Mensch bei der automatisierten Betrugsfallerkennung am Beispiel des Kreditkartenbetrugs zu optimieren, bzw. zu minimieren?

## 1.6 Gliederung der Arbeit

In Kapitel 2 wird der verwendete Datensatz von Kreditkartenbetrugsfällen im Detail beschrieben. Kapitel 3 widmet sich der grundlegenden Funktionsweise von Algorithmen in der datenbasierten Kreditkartenbetrugserkennung. Weiters werden Schwächen und Verbesserungspotentiale gängiger Algorithmen aufgezeigt. In Kapitel 4 werden die erzielten Ergebnisse der entwickelten Methode zur Kreditkartenbetrugserkennung, angewandt auf den Datensatz von Kapitel 2, zusammengefasst. Es wird

die Performance und die Vorhersagegenauigkeit der Methode mit Ergebnissen aus der Literatur verglichen. Kapitel 5 gibt eine Zusammenfassung der Arbeit. Weiters werden die wichtigsten Schlüsse aus dieser Arbeit gezogen und ein Ausblick auf zukünftige Forschungsaktivitäten gegeben.

# 2 Beschreibung des Datensatzes

Die in Kapitel 3 vorgestellte Methode zur automatisierten Betrugsfallerkennung soll auf Basis eines frei verfügbaren Datensatz von Kreditkartenbetrugsfällen untersucht und validiert werden. Dazu wird in dieser Arbeit ein Datensatz von Kreditkartenbetrugsfällen in Taiwan verwendet, welcher im Rahmen der Forschungsarbeit von Yeh und Lien (2009) frei zur Verfügung gestellt wurde. Die Inhalte und der Umfang dieses Datensatzes sollen in diesem Kapitel beschrieben werden.

## 2.1 Umfang und Inhalt

Der Datensatz umfasst die Informationen von 30.000 Kunden, inklusive der Kennzeichnung ob ein Kunde einen Kreditkartenbetrug begangen hat oder nicht. Diese binäre Information (ja oder nein) jedes Kunden wird im Folgenden als *Ausgangsgröße* (*Ausgangsdaten*) bezeichnet. Von jedem Kunden stehen zudem personenbezogene Informationen und Informationen über dessen finanzielles Verhalten zur Verfügung. Diese Informationen, bzw. Daten bezeichnet man im Rahmen von lernenden Systemen als *Attribute* oder *Eingangsgrößen*. In Abschnitt 2.2 werden die einzelnen Attribute im Detail beschrieben.

Das Ziel eines statistischen, datenbasierten Systems zur Betrugsfallerkennung ist nun, rein auf Basis der Attribute/Eingangsgrößen korrekt vorherzusagen ob es sich um einen Betrugsfall handelt oder nicht. Dazu wird ein statistisches, mathematisches Modell im Vorfeld auf Basis des bekannten Zusammenhangs von Eingangs- und Ausgangsdaten trainiert. Um die Performance und Vorhersagegenauigkeit der in dieser Arbeit entwickelten Methode untersuchen zu können, wird der betrachtete Datensatz in einen *Trainingsdatensatz*, welcher die Daten von 25.000 Kunden umfasst und einen *Testdatensatz*, welcher die Daten der übrigen 5.000 Kunden umfasst, aufgeteilt. Die Eingags- und Ausgangsdaten des Trainingsdatensatz werden im Folgenden dazu verwendet das statistische Modell zu trainieren. Für die Validierung

der Methode nimmt man an, dass die Ausgangsdaten des Testdatensatzes unbekannt sind (also keine a-priori Information ob Betrug oder nicht vorliegt). Anschließend wird die Vorhersage des Modells auf Basis der Eingangsgrößen für alle Kunden im Testdatensatz getroffen. Die Vorhersagen des Modells werden dann mit den tatsächlichen Ausgangsdaten verglichen und Kennzahlen zur Performance, sowie der Vorhersagegenauigkeit berechnet. Das in Abbildung 2.1 gezeigte Blockschaltbild

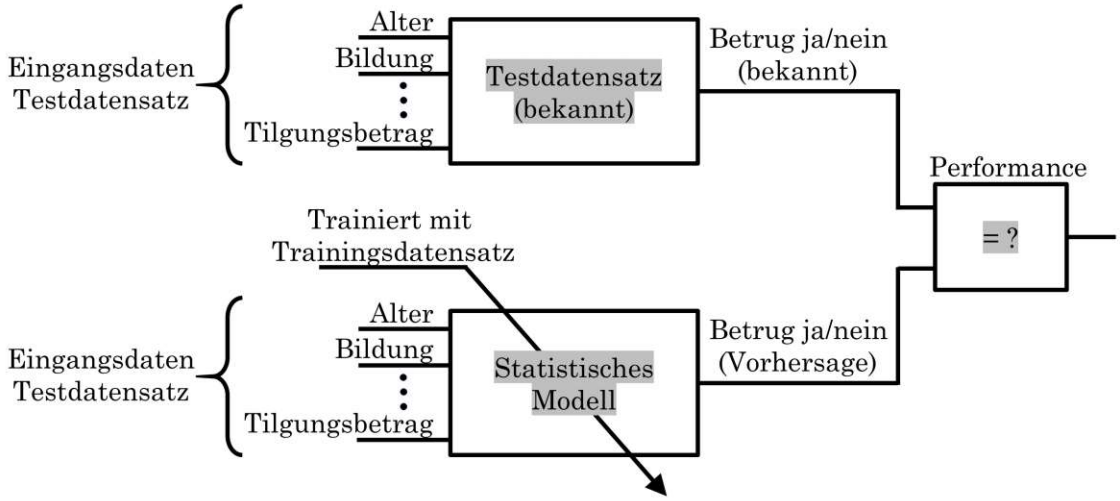


Abbildung 2.1: Vorgehensweise zur Analyse von lernenden Modellen am Beispiel der Kreditkartenbetrugserkennung.

stellt diesen Ansatz grafisch dar. Solch eine Vorgehensweise wird in der Literatur als *supervised learning validation* bezeichnet und ist eine der üblichen Methoden zur systematischen Analyse von lernenden Modellen und Systemen (Bishop, 2006).

## 2.2 Beschreibung der Eingangsgrößen/Attribute

Für jeden der 30.000 Kunden stehen je neben der binären Ausgangsgröße (Betrug ja / nein) 23 Attribute zur Verfügung:

1. Geschlecht (männlich / weiblich)
2. Bildungsstatus (Pflichtschule / Abitur / Universitätsabschluss / Andere)
3. Familienstand (verheiratet / ledig / Andere)

4. Alter

5. Kreditrahmen in Taiwan-Dollar

6.–11. Vom Kreditinstitut kalkulierte Statusvariablen auf Basis der Transaktionshistorie der jeweiligen Kunden. Die jeweiligen Attribute können die ganzzahligen Werte -1 bis 9 annehmen und sind leider nicht im Detail beschrieben.

12.–17. Betrag der monatlichen Kreditkartenabrechnungen in Taiwan-Dollar für die Monate (Sept. 2005 / Aug. 2005 / Jul. 2005 / Jun. 2005 / Mai 2005 / Apr. 2005)

18.–23. Tilgungsbetrag der monatlichen Kreditkartenabrechnung in Taiwan-Dollar für die Monate (Sept. 2005 / Aug. 2005 / Jul. 2005 / Jun. 2005 / Mai 2005 / Apr. 2005)

## 2.3 Diskussion und Informationsgehalt des Datensatzes

Grundsätzlich umfasst der betrachtete Datensatz nicht alle wünschenswerten Informationen wie z. B. Daten zu einzelnen Transaktionen, demografische Daten, oder zeitliche Information, sowie Art des betrügerischen Verhaltens. Der Datensatz ist sehr allgemein gehalten. Wie auch in der wirtschaftlichen Praxis ist die Aufgabenstellung aus den vorhandenen Daten die bestmöglichen Resultate zu erzielen. Des weiteren ist der Datensatz mit 30.000 Kunden verhältnismäßig klein. Trotzdem wurde im Rahmen dieser Arbeit dieser Datensatz ausgewählt, da bei den meisten anderen frei verfügbaren Datensätzen zu Kreditkartenbetrugsfällen alle Attribute gänzlich anonymisiert sind und somit die kennzeichnenden Kriterien für Betrugsfälle nicht hätten untersucht werden können.

Eine erste Analyse der verfügbaren Attribute legt nahe, dass auf Basis dieser nicht alle Betrugsfälle eindeutig vorhergesagt, bzw. von nicht-betrügerischen Kunden unterschieden werden können. Das spiegelt sich auch darin wieder, dass mehrere hundert Kunden mit (nahezu) identen Attributen trotzdem eine unterschiedliche Ausgangsgröße aufweisen. Es sind also per Definition nicht alle Kunden eindeutig klassifizierbar.

Das Ziel ist es nun mit statistischen Mitteln aus diesem relativ generischen Datensatz eine möglichst hohe Rate an korrekt vorhergesagten Betrugsfällen zu erzielen. Gleichermaßen soll die Rate an unnötigen menschlichen Überprüfungen möglichst gering gehalten werden (also möglichst wenige fälschlicherweise vorhergesagte Betrugsfälle). Der herangezogene Datensatz war bereits Gegenstand anderer veröffentlichter, wissenschaftlicher Untersuchungen. Diese werden im folgenden Kapitel im Detail beleuchtet und mit den in dieser Arbeit erzielten Ergebnissen und Erkenntnissen verglichen.

# 3 Neuartige Methode zur Kreditkartenbetrugserkennung

In diesem Kapitel wird eine neuartige Methode zur automatisierten Kreditkartenbetrugserkennung, welche speziell auf die Anforderung von strikt beschränkten menschlichen Überprüfungen angepasst ist, im Detail vorgestellt. Auf Basis des in Kapitel 2 vorgestellten Datensatzes sollen im ersten Teil die dazu in der Literatur veröffentlichten Vorhersageeigenschaft präsentiert und deren Schwachstellen aufgezeigt werden. Im zweiten Teil wird die Notwendigkeit der neuartigen Methode motiviert und anhand von praktischen Beispielen anschaulich beschrieben.

## 3.1 Ergebnisse in der Literatur

Yeh und Lien (2009) untersuchen die Vorhersagegenauigkeit verschiedener gängiger Methoden des maschinellen Lernens angewandt auf den Beispieldatensatz. Sie verwenden viele bereits in der Literaturrecherche hervorgehobene Algorithmen wie Logistische Regression (LR), Diskriminantenanalyse, Neuronale Netze oder Entscheidungsbäume.

Die Autoren kommen zum Schluss, dass mit Logistischer Regression die zuverlässigsten Vorhersagen erzielt werden können. Sie geben an eine *Fehlerrate* (engl. *error-rate*) von $r_e = 18\,\%$ zu erreichen. Die Fehlerrate ist definiert als

$$r_e = \frac{\text{Anzahl falsch vorhergesagt}}{\text{Anzahl Datenpunkte (Kunden)}} \cdot 100. \tag{3.1}$$

Analysiert man jedoch den Datensatz etwas genauer, dann erkennt man, dass ca. $22\,\%$ der Kunden einen Betrugsfall darstellen und die übrigen $88\,\%$ somit keinen. Würde man also einfach willkürlich vorhersagen, dass es keinen Betrugsfall gibt, würde man bereits eine Fehlerrate von $22\,\%$ erreichen. Das zeigt zum Einen, dass

die Ergebnisse aus Yeh und Lien (2009) nicht zufriedenstellend sind und zum Anderen, dass die Fehlerrate gemäß Gleichung (3.1) in diesem Fall kein sinnvolles Maß für die Beurteilung der Zuverlässigkeit darstellt. Das liegt daran, dass wir kein ausgeglichenes Verhältnis an positiven und negativen Stichproben (Betrug / kein Betrug) im Datensatz vorliegen haben (engl. *imbalanced data*). Daher sollen im Folgenden zwei weitere Kennzahlen definiert werden, welche besser geeignet sind um die Zuverlässigkeit von Vorhersagemethoden zu bewerten.

Eine wichtige Kennzahl ist die Rate an korrekt vorhergesagten Positiven (engl. *true-positives rate*), welche als

$$r_{tp} = \frac{\text{Anzahl korrekt vorhergesagten Betrugsfällen}}{\text{Anzahl an tatsächlich betrügerischen Kunden}} \cdot 100 \tag{3.2}$$

definiert ist. Diese Kennzahl gibt an wieviele (bzw. welcher Prozentsatz) der Betrugsfälle überhaupt erkannt werden. Im Folgenden soll der englische Fachterminus verwendet werden, da dieser als etabliert und üblich gilt. Eine weitere, eigens für diese Arbeit eingeführte Kennzahl ist die Rate an korrekten menschlichen Überprüfungen (engl. *rate of true controls*). Diese Kennzahl ist definiert als

$$r_{tc} = \frac{\text{Anzahl korrekt vorhergesagten Betrugsfällen}}{\text{Anzahl an vorhergesagten Betrugsfällen}} \cdot 100. \tag{3.3}$$

Diese Kennzahl sagt also aus, bei welchem Prozentsatz der fiktiv durchgeführten Überprüfungen statistisch gesehen tatsächlich betrügerische Ereignisse aufgedeckt werden würden.

Die von Yeh und Lien (2009) vorgeschlagene Methode basierend auf Logistischer Regression wurde mithilfe der numerischen Mathematiksoftware MATLAB implementiert um die oben definierten Kennzahlen zu berechnen (gemäß der in Abschnitt 2 beschriebenen Strategie mit Trainings- und Testdatensatz). Tabelle 3.1 zeigt die berechneten Kennzahlen. Es werden also überhaupt nur 48 % der Betrugs-

| Methode | $r_e$ | $r_{tp}$ | $r_{tc}$ |
|---|---|---|---|
| Logistische Regression | 18 % | 48 % | 52 % |

Tabelle 3.1: Kennzahlen zur Vorhersagegenauigkeit mit Logistischer Regression, vgl. (Yeh und Lien, 2009).

fälle erkannt ($r_{tp} = 48\,\%$), die Übrigen bleiben gänzlich unerkannt. Weiters kann schlussgefolgert werden, dass statistisch gesehen bei 100 menschlichen Überprüfungen nur tatsächlich 52 betrügerische Kunden erkannt werden ($r_{tc} = 52\,\%$), wenn man sich an die Vorhersage der in Yeh und Lien (2009) vorgeschlagenen Methode hält. Offensichtlich können diese Ergebnisse aus der Sicht einer Bank oder eines Kreditinstituts nicht zufriedenstellend sein. Daher soll im Folgenden eine neuartige Methode vorgestellt werden, welche insbesondere bei limitierten Ressourcen für menschliche Überprüfungen die Rate an korrekten menschlichen Überprüfungen $r_{tc}$ enorm steigert.

## 3.2 Aufbau der neuartigen Methode

Gemäß den Zielen definiert in Abschnitt 1.5 soll eine Methode entwickelt werden, welche die erkannten Betrugsfälle nach deren Wahrscheinlichkeit reiht. Dadurch soll bei strikt limitieren menschlichen Überprüfungen vor allem die Rate an korrekten menschlichen Überprüfungen $r_{tc}$ deutlich gesteigert werden. Die grundlegende Funktionsweise von datenbasierten Betrugserkennungsalgorithmen, sowie die Abwandlungen der neuartigen Methode sollen anschaulich beschrieben werden.

### 3.2.1 Arbeitsweise von datenbasierter Klassifikation

Wie bereits in Abschnitt 1.1.3 beschrieben, versteht man unter Klassifikation (engl. *Clustering*) die Einteilung von Objekten (in unserem Fall Datenpunkte bzw. Kunden) nach gewissen Merkmalen in bestimmte Klassen (Kiel und Rost, 2002). Im vorliegenden Fall haben wir ein binäres Klassifikationsproblem mit folglich zwei Klassen, *Betrug* und *Kein Betrug*.

Ein sehr anschaulich visualisierbarer Fall ist die binäre Klassifikation anhand von zwei Eingangsgrößen bzw. Attributen. Als Beispiel soll die Unterscheidung von Leoparden und Löwen betrachtet werden. Angenommen die Daten zu Gewicht und maximaler Laufgeschwindigkeit von je 10 Leoparden und Löwen stünden zur Verfügung. Die zwei Klassen wären somit Leopard und Löwe und die Eingangsgrößen Gewicht und maximale Laufgeschwindigkeit. Abbildung 3.1 stellt die Datenpunkte im zwei-dimensionalen Raum dar, wobei rote Punkte Leoparden und blaue Punkte Löwen kennzeichnen. Die Aufgabe eines Klassifikationsalgorithmus ist nun auf Basis

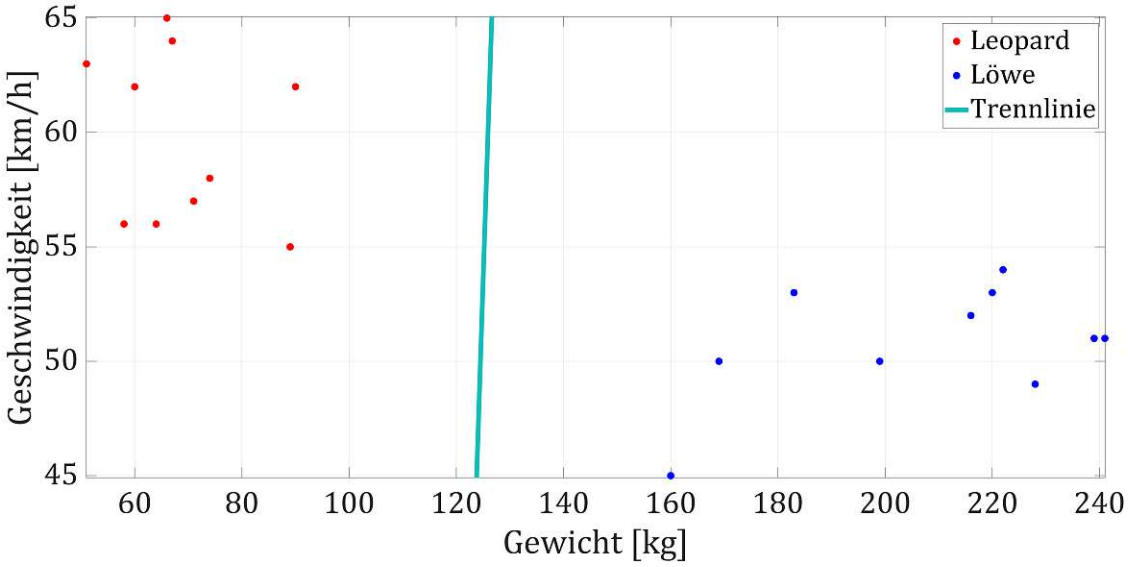


Abbildung 3.1: Beispiel zur Klassifikation von Leoparden und Löwen anhand von Gewicht und maximaler Laufgeschwindigkeit.

der vorhandenen Daten eine optimale Trennarithmetik (im 2D Fall eine Linie) der beiden Klassen zu finden. Im vorliegenden Fall erscheint die türkis dargestellte Trennlinie als sinnvoll. Auf Basis dieser Trennarithmetik können nun zukünftig Leoparden und Löwen auf Basis deren Gewicht und maximaler Laufgeschwindigkeit unterschieden bzw. in Klassen eingeteilt werden.

### 3.2.2 Klassifikation am Beispieldatensatz

Äquivalent zum obigen Beispiel sollen nun zwei Attribute aus dem in dieser Arbeit verwendeten Datensatz ausgewählt werden um die Klassifikation von Betrugsfällen zu veranschaulichen. Abbildung 3.2 stellt die vom Kreditinstitut kalkulierte Statusvariable, sowie den Kreditrahmen (vgl. Abschnitt 2.2) von 150 zufällig ausgewählten Kunden dar[1]. Es ist zu beachten, dass die Eingangsgrößen wie im Rahmen von datenbasierten Auswertungen üblich zwischen 0 und 1 normalisiert wurden. Die roten Punkte stellen betrügerische Kunden dar und blaue Kreuze die nicht betrügerischen. Offensichtlich sind die beiden Klassen auf Basis von nur zwei Attributen nicht so eindeutig zu trennen, wie im obigen Beispiel mit Leoparden und Löwen. Die Trennlinie in Abbildung 3.2 wurde mit dem *Support Vector Machine*

[1]Es werden hier nur 150 Punkte verwendet um eine übersichtliche Darstellung zu gewährleisten.

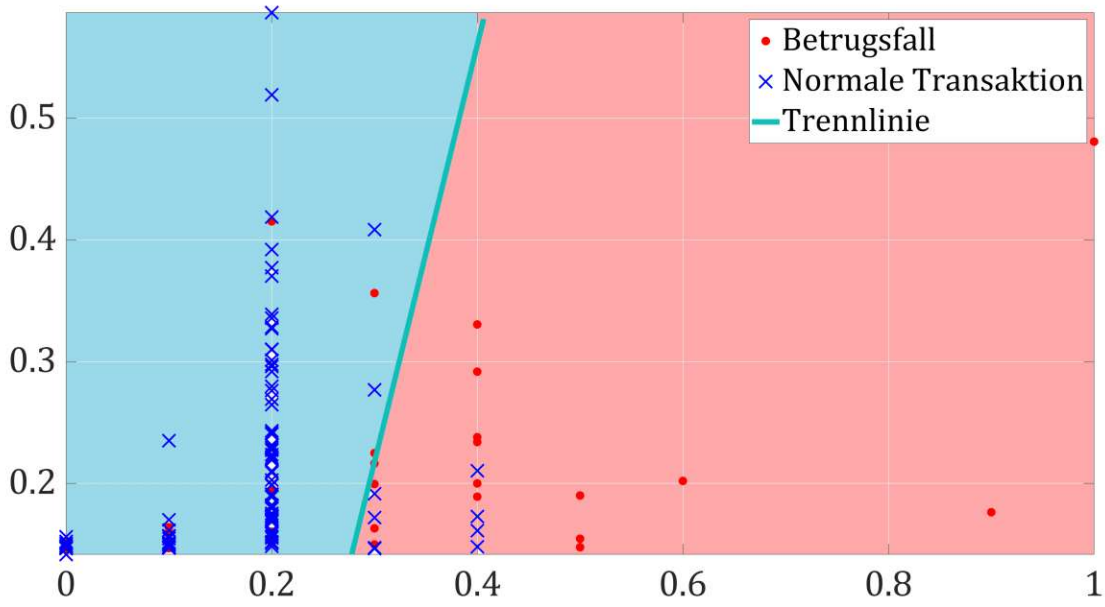


Abbildung 3.2: Klassifikation von betrügerischen Kunden mit linearer SVM auf Basis von zwei Attributen.

(SVM) Algorithmus mit linearem Kernel auf Basis der 25.000 Kundendaten aus dem Trainingsdatensatz (vgl. Abschnitt 2.1) geschätzt. Der rote Bereich kennzeichnet den Wertebereich der Eingangsgrößen für welche Kunden als betrügerisch eingestuft werden, der blaue Bereich das Gegenteil. Somit stellen in diesem Fall diese Wertebereiche für die Eingangsgrößen das statistische Modell dar. Die Trennlinie (bzw. die Wertebereiche) werden im Allgemeinen (wie auch bei der *Support Vector Machine*) durch Lösen eines mathematischen Optimierungsproblems ermittelt. Die mathematische Definition, Beschreibung und Lösung solcher Optimierungsprobleme überschreitet den Rahmen dieser Arbeit, da der Fokus auf der anschaulichen und allgemein verständlichen Darstellung liegt. Für die mathematischen Details sei auf Schölkopf und Smola (2002), Steinwart und Christmann (2008) und Cristianini und Shawe-Taylor (2004) verwiesen. Das grundlegende Konzept ist auch im Falle von mehr als zwei Attributen dasselbe. Im dreidimensionalen Fall (also unter Betrachtung von drei Attributen) stellt eine 2D-Ebene bzw. 2D-Oberfläche die Abgrenzung zwischen den Punkten im dreidimensionalen Raum dar. Im $n$-dimensionalen Fall stellt eine $(n-1)$-dimensionale Hyperfläche die Abgrenzung zwischen den Punkten im $n$-dimensionalen Raum dar.

Dass die Grenze zwischen den beiden Klassen eine Gerade (bzw. ebene Fläche im Höherdimensionalen) darstellt, bedeutet eine offensichtliche Einschränkung für die Unterscheidungsgenauigkeit. Daher soll neben der *Support Vector Machine* mit linearem Kernel die *Support Vector Machine* mit *radial-basis functions* (RBF) Kernel vorgestellt werden. Diese Abwandlung des Algorithmus erlaubt eine beliebige Form der Grenze zwischen den Klassen. Abbildung 3.3 zeigt die resultierende Trennlinie mit

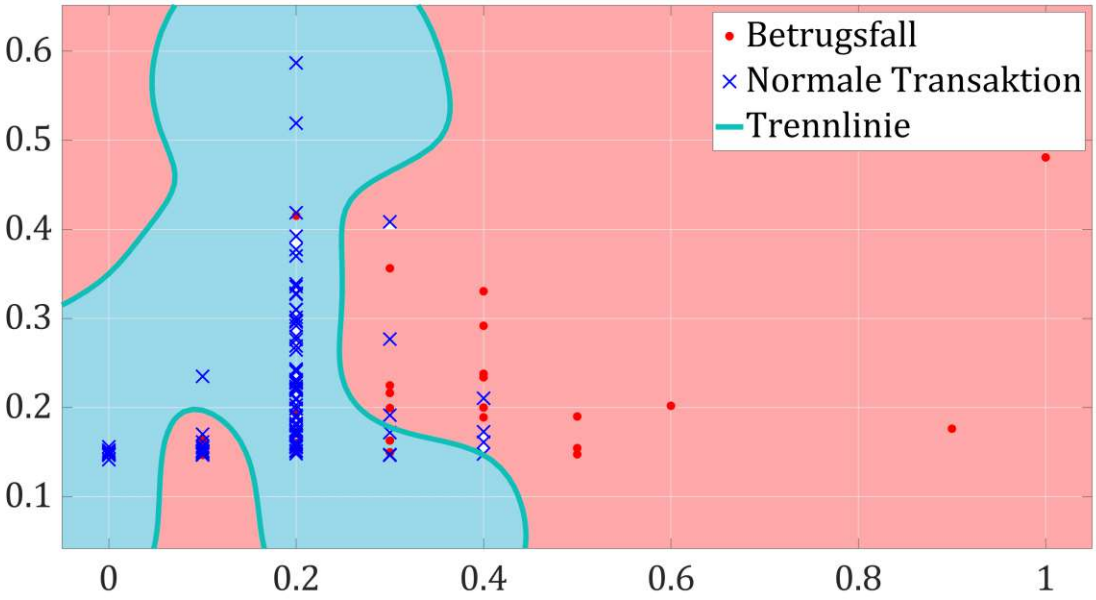


Abbildung 3.3: Klassifikation von betrügerischen Kunden mit RBF-SVM auf Basis von zwei Attributen.

dieser Methode, wobei die selben Datenpunkte wie in Abbildung 3.2 dargestellt sind. Offensichtlich hat die Grenze zwischen den beiden Formen eine weit spezifischere und komplexere Form. Auf den ersten Blick vermag die Grenze zwischen den Klassen nicht immer die augenscheinlichste oder optimalste zu sein. Es sei jedoch zu beachten, dass das Modell (und somit die Trennlinie) auf Basis der 25.000 Datenpunkte des Trainingsdatensatzes trainiert wurde. Der Vollständigkeit halber sei erwähnt, dass solch eine komplexe Grenze durch Schätzung der charakteristischen Parametern von überlagerten 2D-Gauß-Glockenkurven zustande kommt (Li u. a., 2014). Bezüglich der mathematischen Formulierungen sei wieder auf die Literatur verwiesen.

Nun stellt sich die Frage, welche Verbesserung die Verwendung der SVM bzw. deren RBF-SVM bringt. Tabelle 3.2 vergleicht die in Abschnitt 3.1 definierten Kenn-

zahlen, berechnet auf Basis der 150 dargestellten Datenpunkte. Diese zeigen, dass

| Methode | $r_{tp}$ | $r_{tc}$ |
|---|---|---|
| Logistische Regression | 44 % | 50 % |
| SupportVector Machine (linear) | 48 % | 52 % |
| SupportVector Machine (RBF) | 67 % | 52 % |

Tabelle 3.2: Vorhersagegenauigkeit gängiger Methoden auf Basis von *nur* 2 der 24 Attribute und 150 Datenpunkten aus dem Testdatensatz.

zwar gegenüber Logistischer Regression[2] geringe Verbesserungen in der Vorhersagegenauigkeit erzielt werden konnten, die Ergebnisse jedoch immer noch nicht wirklich zufriedenstellend sind. Lediglich die Rate an erkannten Betrugsfällen konnte mit der RBF-SVM spürbar erhöht werden. Die Rate an korrekten Überprüfungen konnte jedoch kaum verbessert werden. Daher soll im folgenden Abschnitt die Erweiterung eingeführt werden, welche die Betrugsfälle nach deren Wahrscheinlichkeit reiht und somit diese Rate deutlich verbessert werden soll.

### 3.2.3 Auswahl der Betrugsfälle nach Wahrscheinlichkeit

Laut Aufgabenstellung stehen Ressourcen für Überprüfungen von 3 % der Kunden zur Verfügung. Im Falle unserer in den Abbildungen 3.2 und 3.3 dargestellten 150 zufällig ausgewählten Kunden wären dies rund 5 mögliche Überprüfungen von Kunden durch Fachpersonal. Das Ziel ist es somit die 5 wahrscheinlichsten Betrugsfälle zu schätzen. Dazu wird die Annahme getroffen, dass die Datenpunkte im betrügerischen Bereich mit dem größten orthogonalen Abstand zur Trennlinie die wahrscheinlichsten Betrugsfälle darstellen. Abbildung 3.4 stellt diesen orthogonalen Abstand für einen Datenpunkt dar. Die eingekreisten Datenpunkte stellen die 5 Datenpunkte mit den größten orthogonalen Abständen und somit die 5 Kunden mit der geschätzt höchsten Wahrscheinlichkeit für einen Betrugsfall dar. Offensichtlich handelt es sich bei allen 5 vorhergesagten Datenpunkten tatsächlich um Betrugsfälle.

Abbildung 3.5 zeigt selbiges für die SVM mit RBF-Kernel. Aufgrund der unterschiedlichen Grenze werden andere Datenpunkte als betrügerisch vorhergesagt,

[2]Die Kennzahlen zur LR weichen von Tabelle 3.1 ab, da in dieser die Ergebnisse mit vollständigem Trainings- und Testdatensatz auf Basis aller Attribute darstellt.

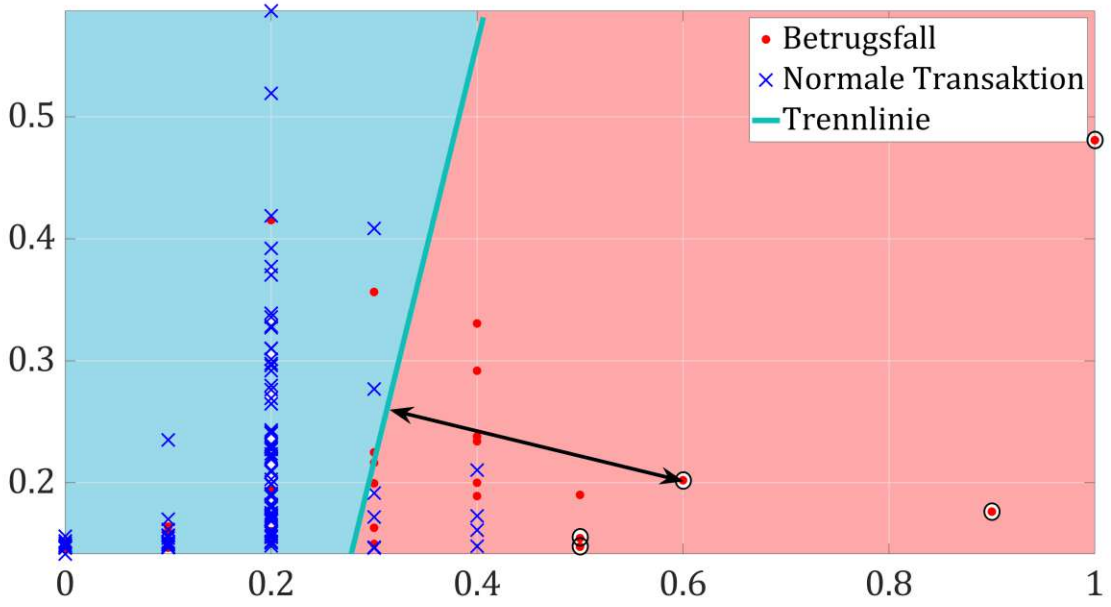


Abbildung 3.4: Schätzung der wahrscheinlichsten Betrugsfälle (2D - lineare SVM).

jedoch stellen ebenfalls alle 5 Datenpunkte in diesem Fall tatsächlich einen Betrugsfall dar. Ein Vergleich der Ergebnisse der vorgestellten Methoden inklusive

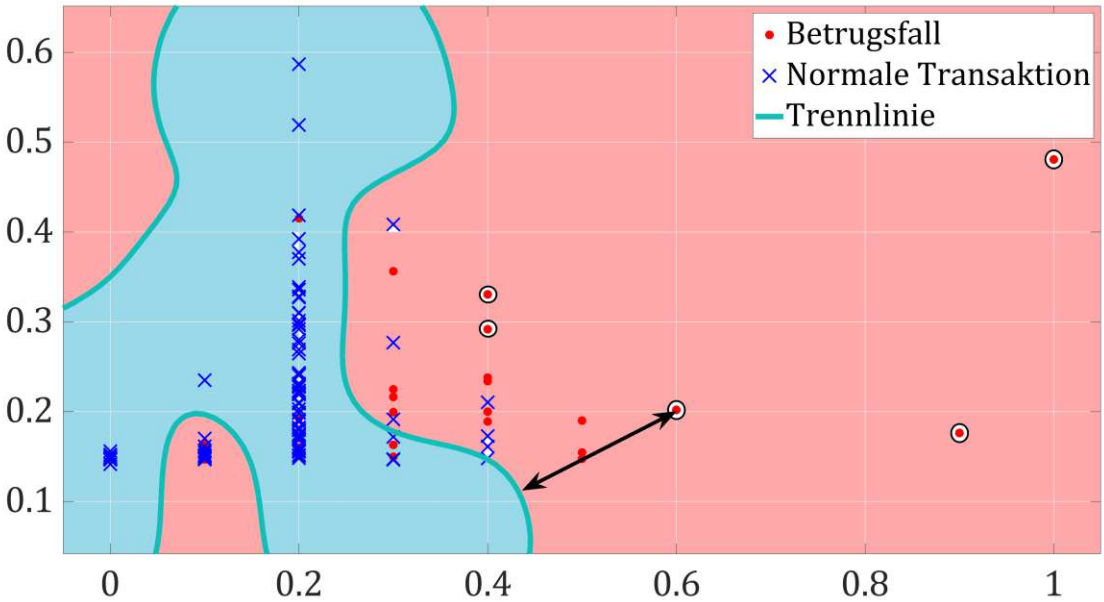


Abbildung 3.5: Schätzung der wahrscheinlichsten Betrugsfälle (2D - RBF-SVM).

Erweiterung ist in Tabelle 3.3 zusammengefasst. Die Rate an korrekten Überprü-

| Methode | $r_{tp}$ | $r_{tc}$ |
|---|---|---|
| Logistische Regression | 44 % | 50 % |
| SupportVector Machine (linear) | 48 % | 52 % |
| SupportVector Machine (RBF) | 67 % | 52 % |
| Erweiterung SupportVector Machine (linear) | 48 % | **100 %** |
| Erweiterung SupportVector Machine (RBF) | 67 % | **100 %** |

Tabelle 3.3: Vorhersagegenauigkeit der vorgestellten Methoden auf Basis von *nur* 2 der 24 Attributen und 150 Datenpunkten aus dem Testdatensatz.

fungen bezieht sich in dieser Tabelle auf 5 mögliche Überprüfungen, wobei die ersten drei Zeilen die statistisch gesehene Korrektheit einer Überprüfung angeben, wenn nach dem Zufallsprinzip 5 aus den vorhergesagten Überprüfungen ausgewählt werden. Offensichtlich liefert die Erweiterung, welche die Wahrscheinlichkeit eines Betrugsfall schätzt und diese danach reiht ausgezeichnete Ergebnisse an den 150 zufällig ausgewählten Datenpunkten. Nun stellt sich die Frage wie sich diese Methodik angewandt auf den vollständigen Datensatz (alle Attribute und Datenpunkte) auswirkt. Diese Resultate sollen im folgenden Kapitel dargestellt und diskutiert werden.

# 4 Resultate und Diskussion

Die Vorhersagegenauigkeit der in Kapitel 3 vorgestellten Methoden zur automatisierten Betrugsfallerkennung, sowie deren neuartiger Erweiterung, soll in diesem Kapitel untersucht und diskutiert werden.

## 4.1 Vergleich Vorhersagegenauigkeiten

Um die Verbesserungen bzw. Vorteile der im vorherigen Kapitel vorgestellten Methoden gegenüber Resultaten in der Literatur zu quantifizieren, sollen hier alle Methoden am vollständigen Datensatz getestet werden. Das heißt alle 30.000 Datenpunkte, sowie alle 23 Attribute werden für Training und Test berücksichtigt. Zudem wird der Datensatz gemäß Abschnitt 2.1 in Tranings- und Testdatensatz aufgespalten. Wie in der Aufgabenstellungen (vgl. Abschnitt 1.5) definiert, stehen menschliche Ressourcen für Überprüfungen von 3 % der mit der automatisierten Betrugserkennung ausgewerteten Kunden zur Verfügung. Das ergibt

$$5.000 \cdot 0,03 = 150 \tag{4.1}$$

mögliche Überprüfungen. Tabelle 4.1 fasst diese Konfiguration für die systematische

| Parameter | Anzahl |
|---|---|
| Größe Trainingsdatensatz | 25.000 |
| Größe Testdatensatz | 5.000 |
| Ressourcen menschliche Überprüfungen | 150 ($\hat{=}$3 %) |
| Berücksichtigte Attribute | 23 (alle) |

Tabelle 4.1: Konfiguration systematische Untersuchung der Vorhersagegenauigkeit.

Untersuchung der Vorhersagegenauigkeit zusammen. Die resultierenden Kennzahlen zur Vorhersagegenauigkeit der Methoden sind in Tabelle 4.2 zusammengefasst. Die

| Methode | $r_{tp}$ | $r_{tc}$ |
|---|---|---|
| Logistische Regression | 48 % | 52 % |
| SupportVector Machine (linear) | 54 % | 48 % |
| SupportVector Machine (RBF) | 59 % | 51 % |
| Erweiterung SupportVector Machine (linear) | 54 % | **80 %** |
| Erweiterung SupportVector Machine (RBF) | 59 % | **86 %** |

Tabelle 4.2: Vorhersagegenauigkeit der vorgestellten Methoden am vollständigen Datensatz.

Rate der korrekten Überprüfungen bezieht sich in dieser Tabelle auf die 150 möglichen Überprüfungen, die anderen beiden Kennzahlen beziehen sich auf all 5.000 Datenpunkte des Testdatensatzes. Diese Rate der korrekten Überprüfungen konnte durch die in dieser Arbeit vorgestellte Erweiterung deutlich auf 86 %[1] gesteigert werden. Mit Logistischer Regression würden nur 78 der 150 Überprüfungen tatsächlich zu erkannten Betrugsfällen führen. Durch die erweiterte RBF-SVM konnte diese Anzahl auf 129 gesteigert werden, was einer Steigerung um 65 % entspricht. Auch die *true-positives rate* konnte um über 10 Prozentpunkte auf 59 % gesteigert werden. Das heißt es bleiben weniger Betrugsfälle gänzlich unerkannt.

## 4.2 Diskussion der Ergebnisse

Prinzipiell wären natürlich Ergebnisse nahe der 100 % wünschenswert. Insbesondere unnötig getätigte Überprüfungen sind aufwendig und kostspielig. Bei den in Tabelle 4.2 gezeigten Ergebnisse muss man sich jedoch in Erinnerung rufen, dass es sich beim verwendeten Datensatz um einen sehr kleinen ("nur" 30.000 Datenpunkte) Datensatz mit relativ wenig Detailinformation (keine Informationen über einzelne Transaktionen, etc.) handelt, vgl. Abschnitt 2.3. Bedenkt man diesen geringen Informationsgehalt des Datensatzes ist eine Rate von 86 % an korrekten Überprüfungen

[1] Dieser Wert ist auffallend niedriger als in Tabelle 3.3. Das hat die Ursache, dass in Kapitel 3 eine deutlich kleinere (anschauliche) Stichprobe von nur 150 Kunden und somit nur 5 Überprüfungen betrachtet wurden.

daher sehr positiv hervorzuheben. Durch Erweiterung des Datensatzes durch die taiwanesische Bank könnte dieses Ergebnis noch weiter verbessert werden.

Vergleicht man die hier erzielten Ergebnisse mit der Literatur, dann erreichen nur moderne und höchst rechenaufwendige Ansätze wie sequentielles Lernen mit *Recurrent Neural Nets* oder *Artificial Immune Systems* genauere Ergebnisse. Als Beispiel soll die Arbeit von Halvaiee und Akbari (2014) genannt werden, welche Werte von über 90 % erreichen. Jedoch muss hier deutlich darauf hingewiesen werden, dass diese Arbeit auf einem Datensatz mit Millionen von Datenpunkten und hunderten Attributen basiert. Der Informationsgehalt eines solchen Datensatzes ist im Allgemeinen um ein Vielfaches höher.

Daraus kann das Fazit gezogen werden, dass sich die hier vorgestellte Erweiterung der RBF-SVM besonders für kleinere Banken oder Kreditinstitute eignet, welche keine astronomischen Mengen an Daten zur Verfügung haben. Zudem stehen solchen Unternehmen im Allgemeinen auch hardwareseitig nicht die Möglichkeiten zur Verfügung um die enorm hohen Rechenleistungen gewährleisten zu können, welche für moderne Ansätze wie von Halvaiee und Akbari (2014) benötigt werden.

# 5 Zusammenfassung, Conclusion und Ausblick

## 5.1 Zusammenfassung

Diese Arbeit beschäftigt sich mit der automatisierten Betrugsfallerkennung im Finanz- und Bankensektor. Der erste Teil widmet sich einer allgemein gehaltenen Einführung, wobei die wichtigsten Möglichkeiten zur Betrugsfallerkennung diskutiert werden. Wichtige Begrifflichkeiten im Kontext datenbasierter Vorhersagesysteme werden definiert und diskutiert. Weiters wird die Frage behandelt, anhand von welchen Merkmalen Betrugsfälle in Datensammlungen detektiert werden können. Eine umfassende Vorstellung der vorhandenen Literatur in diesem und verwandten Bereichen erläutert den *State-of-the-Art* und offenbart die Forschungslücke. Zum Ende des ersten Teils werden Ziele, Motivation, sowie die Forschungsfrage dieser Arbeit im Detail definiert.

Im zweiten Teil wird ein frei verfügbarer Datensatz von Kreditkartenbetrugsfällen vorgestellt. Dieser Datensatz wird im Rahmen dieser Arbeit verwendet um algorithmische Neuentwicklungen und deren Auswirkungen auf die Vorhersagegenauigkeit zu untersuchen.

Zu Beginn des dritten Teils wird die grundlegende Funktionsweise von Algorithmen im Bereich des Kreditkartenbetrugs anschaulich an praktischen Beispielen dargestellt. Anhand von dieser Darstellung werden generelle Schwächen von solchen Algorithmen aufgezeigt und für die hier vorgestellte Methodik motiviert. Die Idee dieser Methodik ist neben der Vorhersage ob es sich um einen Betrugsfall handelt oder nicht, die vorhergesagten Betrugsfälle nach deren Wahrscheinlichkeit zu reihen. Die Funktionsweise dieser Methodik wird anhand des Beispieldatensatzes präsentiert.

Der vierte Teil widmet sich der Diskussion der erzielten Ergebnisse. Mithilfe eines definierten Testszenarios wird die Vorhersagegenauigkeit gängiger Methoden anhand von definierten Kennzahlen mit der durch die hier entwickelte Methodik erzielten Vorhersagegenauigkeit verglichen. Es konnte gezeigt werden, dass die Vorhersagegenauigkeit und insbesondere die Rate an korrekt durchgeführten Überprüfungen von Kreditkartenbetrugsfällen maßgeblich gegenüber gängigen Methoden gesteigert werden kann.

## 5.2 Conclusion

Das grundlegende Ziel dieser Arbeit war die Ressource Mensch im Umfeld der automatisierten Betrugsfallerkennung möglichst optimal einzusetzen. Dazu ist es wesentlich, dass eine mit Kosten und Aufwand verbundene menschliche Überprüfung durch Fachpersonal zu einer möglichst hohen Wahrscheinlichkeit zu einer tatsächlichen Aufdeckung eines Betrugsfalls führt. In dieser Arbeit wurde anhand eines Datensatzes von Kreditkartenbetrugsfällen gezeigt, dass die Rate an diesen korrekten Überprüfungen um bis zu 65 % gegenüber in der Literatur üblichen Methodiken gesteigert werden kann. Zudem blieben generell weniger Betrugsfälle gänzlich unerkannt.

Es wurde gezeigt, dass insbesondere für weniger umfangreiche Datensätze mit einem dementsprechend niedrigeren Informationsgehalt das Potential für die entwickelte Methodik besonders hoch ist. Daher sind die in dieser Arbeit beschriebenen Ergebnisse besonders für kleinere Banken und Kreditinstitute, welche über keine so umfangreichen Datensammlungen verfügen, gut geeignet und könnten für diese ein hilfreiches Werkzeug für die Bekämpfung von Betrugsfällen darstellen.

## 5.3 Ausblick auf zukünftige wissenschaftliche Untersuchungen

Für zukünftige wissenschaftliche Untersuchungen und die praktische Anwendung im unternehmerischen Umfeld der hier vorgestellten Methodik wäre eine systematische Untersuchung der Vorhersagegenauigkeit eben dieser Methodik anhand von weiteren Datensätzen zu Kreditkartenbetrugsfällen von großer Bedeutung. Insbesondere

umfangreichere Datensätze, welche neben Kundendaten auch Detailinformationen zu den einzelnen von jedem Kunden getätigten Transaktionen enthalten wären von großem Interesse, da in der Praxis relevant.

# Literatur


Abdulrazaq, A.A, M.B. Abdulrazaq, I.J. Umoh und E.A. Adedokun (2019). „Fraud detection in credit card and application of VAT clustering algorithm: A review“. In: *2nd International Conference of the IEEE Nigeria Computer Chapter, NigeriaComputConf 2019*. Bd. 2.

Aleskerov, E., B. Freisleben und B. Rao (1997). „A neural network based database mining system for credit card fraud detection“. In: *Computational Intelligence for Financial Engineering (CIFE)*. IEEE: New York, S. 220–226.

Bhattacharyya, S., S. Jha, K. Tharakunnel und JC. Westland (2011). „Data mining for credit card fraud: a comparative study“. In: *Decision Support Systems* 50, S. 602–613.

Bishop, C.M. (2006). *Pattern recognition and machine learning*. Hrsg. von M. Jordan und J. Kleinberg. Springer Science+Business Media, LLC.

Bolton, R.J. und D.J. Hand (2002). „Statistical fraud detection: a review“. In: *Statistical Science* 17.3, S. 235–249.

Cecchini, M., H. Aytug, GJ. Koehler und P. Pathak (2010). „Making words work: Using financial text as a predictor of financial events“. In: *Decision Support Systems* 50, S. 164–175.

Cristianini, Nello und John Shawe-Taylor (2004). *Kernel Methods for Pattern Analysis*. Cambridge University Press, Cambridge.

Dhankhar, A. und K. Solanki (2019). „A comprehensive review of tools & techniques for big data analytics“. In: *International Journal of Emerging Trends in Engineering Research* 7.11, S. 556–562.

Gee, Sunder (2015). *Fraud and fraud detection - a data analytics approach*. John Wiley & Sons, Inc., Hoboken, New Jersey.

Halvaiee, N.S. und MK. Akbari (2014). „A novel model for credit card fraud detection using artificial immune systems“. In: *Applied Soft Computing* 24, S. 40–49.

Hoogs, B., T. Kiehl, C. Lacomb und D. Senturk (2007). „A genetic algorithm approach to detecting temporal patterns indicative of financial statement fraud“. In: *Intelligent Systems in Accounting Finance and Management* 15, S. 41–56.

Humpherys, SL., KC. Moffitt, MB. Burns, JK. Burgoon und WF. Felix (2011). „Identification of fraudulent financial statements using linguistic credibility analysis“. In: *Decision Support Systems* 50, S. 585–594.

Jurgovsky, Johannes, Michael Granitzer, Konstantin Ziegler, Sylvie Calabretto, Pierre-Edouard Portier, Liyun He-Guelton und Olivier Caelen (2018). „Sequence classification for credit-card fraud detection“. In: *Expert Systems With Applications* 100, S. 234–245.

Kiel, E. und F. Rost (2002). *Einführung in die Wissensorganisation. Grundlegende Probleme und Begriffe*. Würzburg: Ergon Verlag.

Kirkos, E., C. Spathis und Y. Manolopoulos (2007). „Data mining techniques for the detection of fraudulent financial statements“. In: *Expert Systems with Applications* 32, S. 995–1003.

Li, H., X. Li, O.M. Lucila und J. Xiaoqian (2014). „Privacy Preserving RBF Kernel Support Vector Machine“. In: *BioMed Research International* vol. 2014, 10 pages.

Ngai, E., Y. Hu, Y. Wong, Y. Chen und X. Sun (2011). „The application of data mining techniques in financial fraud detection: a classification framework and an academic review of literature“. In: *Decision Support Systems* 50, S. 559–569.

Nisbet, Robert, Gary Miner und Ken Yale (2018). „Handbook of statistical analysis and data mining applications“. In: 2. Aufl. Elsevier Inc. Kap. 15, S. 289–302.

Pindar, Z.A., S. Jamel, A. Disina, A.R. Ghali, K. Mahazer und M.M. Deris (2017). „Check digit system based on quasigroup string transformation“. In: *3rd and 4th International Engineering Research and Innovation Symposium, IRIS*. Bd. 226. 1. Malaysia.

Pinquet, J., M. Ayuso und M. Guillen (2007). „Selection bias and auditing policies for insurance claims“. In: *Journal of Risk and Insurance* 74, S. 425–440.

Quah, JT. und M. Sriganesh (2008). „Real-time credit card fraud detection using computational intelligence“. In: *Expert Systems with Applications* 35, S. 1721–1732.

Ravisankar, P., V. Ravi, G.R. Rao und I. Bose (2011). „Detection of financial statement fraud and feature selection using data mining techniques“. In: *Decision Support Systems* 50, S. 491–500.

Rayner, A. (2016). „The rise of machine learning for big data analytics“. In: *2nd International Conference on Science in Information Technology*. Bd. 2.

Schölkopf, B. und A. Smola (2002). *Learning with Kernels: Support Vector Machines, Regularization, Optimization, and Beyond (Adaptive Computation and Machine Learning)*. MIT Press, Cambridge, MA.

Spathis, C., M. Doumpos, R. Poppolis und C. Zopounidis (2002). „Detecting falsified financial statements: a comparative study using multicriteria analysis and multivariate statistical techniques“. In: *European Accounting Review* 11, S. 509–535.

Srivastava, A., A. Kundu, S. Sural und A. Majumdar (2008). „Credit card fraud detection using hidden markov model“. In: *IEEE Transactions on Dependable and Secure Computing* 5.1, S. 37–48.

Steinwart, Ingo und Andreas Christmann (2008). *Support Vector Machines*. Springer, New York.

Viaene, S., M. Ayuso, M. Guillen, D. Van Gheel und G. Dedene (2007). „Strategies for detecting fraudulent claims in the automobile insurance industry“. In: *European Journal of Operational Research* 176, S. 565–583.

West, J. und M. Bhattacharya (2015). „Intelligent financial fraud detection: A comprehensive review“. In: *Computers and Security* 57, S. 47–66.

Yeh, I-Cheng und Che-Hui Lien (2009). „The comparisons of data mining techniques for the predictive accuracy of probability of default of credit card clients“. In: *Expert Systems with Applications* 36, S. 2473–2480.

Yue, D., X. Wu, Y. Wang, Y. Li und C-H. Chu (2007). „A review of data mining-based financial fraud detection research“. In: *In WiCom 2007 - International*

*Conference on Wireless Communications, Networking and Mobile Computing, IEEE*, S. 5519–5522.

Zhang, G., E. Patuwo und B. Hu (1998). „Forecasting with artificial neural networks: the state of the art“. In: *International Journal of Forecast* 14, S. 35–62.