3-5-2015

Netzwerkanalysen für die Betrugserkennung im Online-Handel

Timm Marschall

David Morawitzky

Marco Reutter

Raphaele Schwartz

Henning Baars

Netzwerkanalysen für die Betrugserkennung im Online-Handel

Timm Marschall[1], David Morawitzky[1], Marco Reutter[1], Raphaele Schwartz[1] und Henning Baars[1]

[1] Universität Stuttgart, Stuttgart, Deutschland
Timm1991@gmx.net, David.Morawitzky@t-online.de,
Marco.Reutter@outlook.com, RaphaeleSchwartz@googlemail.com,
Baars@wi.uni-stuttgart.de

Abstract. Der Online-Handel muss einer zunehmenden Frequenz und Komplexität an Betrugsversuchen begegnen. Eine besondere Herausforderung ist es dabei, Betrugsmuster zu erkennen, bei denen unterschiedliche virtuelle Identitäten zum Einsatz kommen. Der vorliegende Beitrag zeigt auf, dass und wie mit Netzwerkanalysen Gruppen verdächtiger Identitäten aufgedeckt werden können. Hierfür wurde in Kooperation mit der arvato Financial Solutions, dem Design-Science-Ansatz folgend, eine prototypische Lösung entwickelt und erprobt, die Algorithmen zur Identifikation und Bewertung von Ähnlichkeiten zwischen virtuellen Identitäten mithilfe einer Graphdatenbank umsetzt und mit einem Werkzeug zur visuellen Netzwerkanalyse interaktiv aufbereitet. Des Weiteren wird demonstriert, welche Relevanz massiv parallele Big-Data-Infrastrukturen in diesem Zusammenhang haben. Die Ergebnisse legen nahe, dass Netzwerkanalysen herkömmliche Ansätze aus dem Fraud-Detection-Umfeld ergänzen und für die Identifikation von Betrugsmustern genutzt werden können, die mit herkömmlichen Verfahren nur bedingt erkennbar sind.

Keywords: Netzwerkanalysen, Graphdatenbanken, Fraud Detection, Big Data, visual analytics

1 Problemstellung und Motivation

Im Kontext der IT-basierten Entscheidungsunterstützung ist die Betrugserkennung, engl. Fraud Detection, eine seit langem viel beachtete Anwendungsdomäne, für die im Laufe der Zeit bereits eine größere Zahl an Verfahren entwickelt wurde [1]. Diese sind vor allem für Online-Händler relevant, da Betrugserkennung im Umfeld des eCommerce immer mehr an Bedeutung gewinnt. Einer der Gründe ist, dass die Möglichkeit zur Nutzung einer virtuellen Identität das Erschleichen von Leistungen erleichtert. Hinter einer solchen virtuellen Identität können sich dabei einer oder mehrere Betrüger verbergen, die versuchen, durch falsche Angaben Ware zu erhalten, für die nicht gezahlt wird [2][3]. Im Folgenden wird diskutiert, wie neuartige Kombinationen von Ansätzen der Netzwerkanalyse auf Basis von Graphdatenbanken, Netzwerkvisualisierungstools und Big-Data-Infrastrukturen helfen können, Betrüger

12th International Conference on Wirtschaftsinformatik,
March 4-6 2015, Osnabrück, Germany

Marschall, T.; Morawitzky, D.; Reutter, M.; Schwartz, R.; Baars, H. (2015): Netzwerkanalysen für die Betrugserkennung im Online-Handel, in: Thomas. O.; Teuteberg, F. (Hrsg.): Proceedings der 12. Internationalen Tagung Wirtschaftsinformatik (WI 2015), Osnabrück, S. 1859-1873

schneller zu identifizieren und somit mögliche Verluste zu vermeiden. Eine besondere Herausforderung, der hierbei begegnet wird, ist, dies ausschließlich mit Daten zu erreichen, die unmittelbar bei einer Bestellung anfallen. Dies ist in Fällen erforderlich, in denen aus Datenschutzgründen keine externen Daten zur Anreicherung hinzugezogen werden dürfen.

Ziele des Beitrags sind, die entsprechenden Ansätze zur Betrugserkennung im Online-Handel zu explorieren sowie ein entsprechendes Lösungsdesign zu entwickeln und zu erproben. Hierfür wurde dem Design-Science-Research-Paradigma folgend eine Lösung entwickelt, die auf den Anforderungen und Daten von arvato Financial Solutions beruht und die mit diesem hinsichtlich ihrer Ergebnisgüte und ihrer Relevanz evaluiert wurde.

Der Gang der Argumentation ist wie folgt: Zunächst wird das Thema begrifflich eingeordnet und in Bezug zum Stand der Forschung gesetzt. Im Anschluss wird die angewandte Methodik erläutert, um dann die Ergebnisse der Arbeit, d.h. das entwickelte Verfahren, den Prototypen inkl. der vorgeschlagenen Architektur und die Evaluationsergebnisse vorzustellen. Der Beitrag schließt mit einer Diskussion des Forschungs- und des Praxisbeitrags sowie von Grenzen und verbleibendem Forschungsbedarf.

2 Grundlagen und Stand der Forschung

2.1 Big Data im Kontext der Business Intelligence

Konform mit [4][5] wurde die betrachtete Lösung im gegebenen Forschungsvorhaben als Teil eines Business-Intelligence-Ansatzes konzipiert. Unter Business Intelligence (BI) werden im Folgenden integrierte Ansätze der betrieblichen IT-basierten Management- und Entscheidungsunterstützung verstanden, wobei speziell dem Integrationsaspekt besondere Bedeutung zukommt [6]. Entsprechend war es eine Randbedingung des Vorhabens, die hier diskutierten analytischen Komponenten zur Netzwerkanalyse und -visualisierung wie auch die genutzten Big-Data-Infrastrukturen in vorhandene BI-Landschaften einzubetten.

Der Begriff Big Data wird in der Literatur unterschiedlich abgegrenzt. Den verschiedenen Ansätzen gemeinsam ist die Hervorhebung von Anforderungen an den Umfang (*Volume*), die Datenbereitstellungs- und Verarbeitungsgeschwindigkeit (*Velocity*) sowie den Umgang mit Formatvielfalt (*Variety*), die dazu führen, dass Lösungen nicht mehr adäquat mit etablierten (i.d.R. relationalen) Ansätzen zur Datenverarbeitung umgesetzt werden können (3V). In dieser Arbeit kommen alle drei Vs zum Tragen: Die Menge der zu berücksichtigenden Daten, die Near-Time-Anforderungen in der Betrugserkennung sowie die netzwerkorientierte Datenhaltung [7]. Hierfür wird auf sog. NoSQL-Ansätze zurückgegriffen. Der Begriff „NoSQL“ wurde 2009 von Eric Evans geprägt. Das Kürzel wird mittlerweile üblicherweise mit „Not Only SQL“ aufgelöst. NoSQL-Datenbanken verfolgen einen Ansatz, bei dem auf ein fixiertes Relationenschema verzichtet wird, um eine hohe horizontale Skalierbarkeit sicherzustellen, d.h. die Möglichkeit zum Einsatz massiv-paralleler Infrastrukturen. Zu beachten ist jedoch das CAP-Theorem [8] von Eric Brewer. Die Abkürzung „CAP” steht

für Consistency, Availability and Tolerance to network Partitions. Das Theorem besagt, dass es nicht möglich ist, gleichzeitig alle drei Eigenschaften zu erfüllen. Für die BI bedeutet dies eine wesentliche Restriktion, da *Konsistenz* ein essenzielles Designziel der in BI-Architekturen zentralen Data Warehouses (DWHs) ist. Dies deutet darauf hin, dass NoSQL-Datenhaltungen in der BI eher einen komplementären Charakter haben – eine Einschätzung, die auch in der Literatur geteilt wird [9].
Graphdatenbanken werden dem NoSQL-Ansatz zugeordnet und speichern Daten nicht in relationalen Tabellen, sondern in Knoten und Kanten, wodurch Datenstrukturen, die auf Verbindungen zueinander basieren – wie Hypertext oder geographische Informationen – besonders effizient abgebildet werden können[10]. Dabei enthalten Knoten die Daten eines Objekts und Kanten die Beziehungen zwischen diesen Objekten. Entsprechend können Algorithmen der Graphentheorie angewandt werden, dazu zählen insbes. Tiefen- und Breitensuche.

2.2 Betrugserkennung

Es kann zwischen Betrugsprävention und Betrugserkennung unterschieden werden. Zur *Betrugsprävention* zählen Mechanismen wie Passwörter oder Wasserzeichen, die ein Betrugsvorhaben erschweren sollen. Da jedoch keines dieser Verfahren perfekt ist, wird auch eine nachgelagerte *Betrugserkennung* benötigt. Als Betrugserkennung bzw. Fraud Detection wird das Vorgehen bezeichnet, durch das eine „widerrechtliche oder kriminelle Täuschung, die zu persönlichem oder finanziellem Gewinn führt“ [11], erkannt und registriert wird. Betrugserkennung spielt in drei Feldern eine besonders ausgeprägte Rolle: Kreditkartenbetrug, Sicherheit von Computernetzwerken und in der Telekommunikationsbranche. Jedes dieser Felder erfordert bestimmte Methoden, um einen Betrug mit höchstmöglicher Wahrscheinlichkeit zu entdecken. Eine hierfür genutzte Methode ist der Einsatz von neuralen Netzwerken, die mit Hilfe von historischen Daten trainiert werden, um Anomalien zu entdecken [12]. Ein zweiter verbreiteter Ansatz ist der Gebrauch eines regelbasierten Systems. Der entscheidende Nachteil ist jedoch, dass für jeden möglichen Fall von Betrug eine Regel vorliegen muss. Dies ist in einem dynamischen Umfeld sehr schwer umzusetzen. Die hier entwickelte Methode ist für den Bereich des *Online-Handels mit physischen Gütern* optimiert und verbindet den Einsatz von historischen Daten mit Regelstrukturen. In diesem Umfeld liegt der Fokus darauf, externe Betrüger zu identifizieren, die kriminell und z.T. auch organisiert handeln [13].

Aktuell werden im Bereich des Online-Handels häufig Scoring-Verfahren genutzt, um bekannte Identitäten mit einer Risikobewertung zu versehen [14]. An Grenzen stoßen diese Verfahren, wenn eine Identität aufgrund von leicht veränderten Merkmalen nicht eindeutig zugeordnet werden kann und ein Scoring somit nicht auf den vollständigen Datenbestand zu einer Identität zurückgreifen kann. Ein System, das Netzwerkanalysen nutzt, um Transaktionen mit ähnlichen Merkmalen miteinander in Beziehung zu setzen, ist im Gegensatz dazu in der Lage, deutlich mehr auffällige Transaktionen zu markieren. Die Idee, für die Betrugserkennung Netzwerkanalysen zu nutzen, ist bekannt [15] und wird bereits in verwandten Szenarien, wie z.B. dem Erkennen von auffälligen Nutzern in Online-Auktionshäusern eingesetzt [16]. Im Ge-

gensatz zu dem hier vorgestellten Ansatz liegt der Fokus bei [16] auf plattformbasierten Transaktionen und der Manipulation des dort integrierten Reputationssytems. Grundlage sind dort allerdings Netzwerke, die sich aus *Interaktionsbeziehungen* zwischen Nutzern ergeben, wie sie im gegebenen Fall nicht vorliegen. Hier werden vielmehr Netzwerke aus Transaktionen anhand von deren wechselseitigen *Ähnlichkeiten* gebildet.

Nach unserem Erkenntnisstand (resultierend aus Literaturrecherche, Befragung von Experten beim Händlerbund und einer Web-Recherche zu bestehenden Praxislösungen) gibt es bis jetzt keinen vergleichbaren netzwerkbasierten Ansatz.

2.3 Netzwerkanalysen

Netzwerkanalysen befassen sich mit der Struktur der Beziehungen zwischen Individuen in einem Netzwerk [17]. Das Hauptziel der Netzwerkanalysen ist das Aufspüren und die Interpretation von Beziehungen zwischen Individuen [18]. Im Gegensatz zu sozialen Netzwerkanalysen in der Soziologie, bei denen die dem Netzwerk zugrunde liegenden Daten oft durch eine direkte Befragung von Individuen gewonnen [19][20], durch die Analyse von sozialen Netzwerken im Web [21][22] oder mithilfe von Sensoren [23] erhoben werden, darf im Kontext der hier betrachteten Betrugserkennung ausschließlich auf Daten zurückgegriffen werden, die typischerweise bei einer Bestellung angegeben werden. Eine Anreicherung aus externen Datenquellen und aus sozialen Netzwerken ist aus Datenschutzgründen auf jeden Fall zu vermeiden. Von besonderem Interesse bei der Untersuchung des gebildeten Netzwerkes sind *Gruppen* von Transaktionen unterschiedlicher virtueller Akteure, die aufgrund ihrer wechselseitigen Ähnlichkeit aus einem Gesamtnetzwerk hervorstechen.

3 Methodik und Vorgehen

Das Forschungsvorhaben folgte dem Paradigma der Design Research. Das erstellte Artefakt [24] ist ein Systemkonzept für die Betrugsidentifikation mit Netzwerkanalysen. Dieses umfasst ein Verfahren zur Netzwerkbildung und -bewertung, ein Architekturkonzept sowie Empfehlungen für die Nutzung massiv-paralleler Infrastrukturen. Hierbei wurde darauf geachtet, den Anforderungen an Design-Science-Projekte zu genügen, wie sie etwa Gregor et al. [24] formulieren: Als „Blaupause“ für Vorhaben mit einer ähnlichen Ausrichtung war das Projekt auf *Generalisierung* ausgelegt, wobei allgemeine Schlussfolgerungen zu Methodik, Architektur und Aufbau einer solchen Lösung im Mittelpunkt stehen (*principles of form and function*). Die mit dem Artefakt verfolgte Zielsetzung (*purpose*) ist eine Identifikation von Betrugsversuchen, die auf der Nutzung virtueller, zu Verschleierungszwecken angelegten Identitäten basieren. Im Mittelpunkt des Forschungsprojektes stand die *Instanziierung* auf der Grundlage eines lauffähigen Prototyps, der zur iterativen Entwicklung und Evaluation herangezogen wurde. Die Zusammenarbeit mit arvato Financial Solutions durch eine zyklische Rückkopplung von Zwischenergebnissen und die Nutzung von realen Testdaten haben die *Relevanz* der Ergebnisse sichergestellt. Der Ansatz hat dabei auf dem Stand der Forschung zur Betrugserkennung aufgesetzt (*justificatory knowledge*). Zur

Evaluation wurden am Projektende identifizierte Fälle von Betrugskandidaten mit Analysten von arvato Financial Solutions auf ihre Güte hin überprüft. Genauso wurden reale Betrugsfälle in den Prototypen eingespeist, um zu prüfen, ob diese erkannt worden wären.

Da es sich bei der Methode zur Betrugserkennung um einen Spezialfall der Datenmustererkennung handelt, wurde darauf geachtet, dass eine Abbildung auf das Vorgehensmodell Crisp-DM möglich ist. Die dort definierten Schritte wurden im Forschungsprojekt wie folgt konkretisiert:

1. *Geschäftsverständnis* (Ziele und Anforderungen): Ziel des Projekts war die Entwicklung eines Prototyps für Netzwerkanalysen in Bezug auf Betrugsmustererkennung.
2. *Datenverständnis*: Die Sichtung der von arvato Financial Solutions bereitgestellten Daten.
3. *Datenvorbereitung:* Filterung und Bereinigung der Daten, um diese im System verarbeiten zu können.
4. *Modellierung:* Erarbeitung von Modellen und Methoden. Die Methodenentwicklung war eine der Kernaktivitäten des Forschungsprojektes.
5. *Evaluation:* Die Methoden und ihre Ergebnisse wurden wiederholt zusammen mit arvato Financial Solutions überprüft.
6. *Bereitstellung:* Die Projektergebnisse wurden in eine handhabbare Form überführt.

Das Projekt hatte eine Laufzeit von sechs Monaten und war Bestandteil der Abschlussarbeit von vier Studierenden der Wirtschaftsinformatik. Das Unternehmen arvato Financial Solutions ist ein globaler Anbieter von Finanzdienstleistungen und bietet flexible Komplettlösungen für wertorientiertes Management von Kundenbeziehungen und Zahlungsflüssen. Das Projekt bezieht sich dabei besonders auf Dienstleistungen in den Kontexten Auskunftei und Betrugserkennung. Hierfür kann arvato Financial Solutions auf die Daten seiner Kunden, d.h. der Online-Händler, zurückgreifen. Konkret wurde das Projekt in zwei Phasen realisiert, wobei die erste die Schritte eins und zwei des Crisp-DM-Modells adressiert hat und die zweite die Schritte drei bis fünf:

Die **erste Phase** begann mit diversen Recherchen rund um das Thema Online-Betrug. Dabei wurde gezielt nach dem Vorgehen von Betrügern und gegen Betrüger im Online-Handel gesucht. Das Vorgehen von Betrügern lässt sich zum einen aus Artikeln und Foren-Diskussionen von betroffenen Händlern erschließen, zum anderen durch Anleitungen zum Betrügen, die aber gezielt im Deep Web, in unserem Fall mit Hilfe des Tor Netzwerks, gesucht wurden. Wie sich Online-Händler vor Betrügern schützen können und wie der Stand der Technik dahingehend ist, wurde aus entsprechenden, an Shop-Betreiber adressierten Artikeln abgeleitet. Zusätzlich wurden Informationen bei arvato Financial Solutions erhoben. Dies geschah während eines Workshops Mitte April 2014, bei dem vier führende Mitarbeiter aus den Bereichen „Business Intelligence Services“, „DWH and BI Solutions“ und „Datenbankentwicklung“ beteiligt waren. Durch das so erworbene Wissen, den Workshop und mehrere Telefonkonferenzen wurde die Zielsetzung gemeinsam mit arvato Financial Solutions konkretisiert.

In der **zweiten Phase** wurden zunächst die netzwerkbasierten Methoden entwickelt und in einem Prototypen umgesetzt. Hierbei wurde auf einen Datenauszug von arvato Financial Solutions mit 4,5 Millionen Einträgen zurückgegriffen. Dabei wurde so vorgegangen, dass Methoden entwickelt oder verfeinert, von uns auf richtige Implementierung überprüft, am Testdatensatz umgesetzt und anschließend evaluiert wurden. Dieser Schritt wurde als iterativer Prozess umgesetzt, der so lange durchgeführt wurde, bis die Ergebnisse eine angemessene Qualität besaßen. Dies beinhaltete insbes. eine Kalibrierung der Datenbereinigung sowie der Methoden zur Gruppenbildung und -bewertung, sodass einerseits relevante Betrugsversuche gekennzeichnet werden, andererseits die Menge der gekennzeichneten Gruppen möglichst klein und so die Ergebnisse handhabbar bleiben. Während zwei Vor-Ort-Terminen im Juni und September 2014 sowie mehreren Telefonkonferenzen mit zwei weiteren Experten aus dem Bereich „Risk and Fraud Management" wurden die Methoden und Ergebnisse gemeinsam mit arvato Financial Solutions evaluiert und angepasst.

4 Ergebnisse

4.1 Betrugsmuster im Online-Handel

Die Recherche zu den Betrugsmustern im Online-Handel hat ergeben, dass es verschiedene Ansätze gibt, mit denen Betrüger versuchen, sich Ware zu erschleichen. Im Mittelpunkt des Projekts standen Betrugsfälle, die mit bisherigen Standardmethoden nicht erkannt werden können. Transaktionen, die von einem Betrüger oder einer Betrügergruppe stammen und bei denen sich der Name, Benutzername und die Adresse unterscheiden, können bisher nur schwer erkannt werden. Um dem entgegenzuwirken, wurde der Ansatz entwickelt, einzelne Transaktionen als Knoten zu betrachten und dann aus diesen Netzwerke zu bilden. Dadurch lassen sich Gemeinsamkeiten dieser einzelnen Transaktionen kennzeichnen und visualisieren und so Zusammenhänge aufdecken. Prinzipiell versuchen Betrüger in solchen Szenarien, ihre echte Identität durch die Nutzung einer oder mehrerer virtueller Identitäten zu verschleiern. Dabei gibt es mehrere Möglichkeiten vorzugehen: Zum einen werden Zahlungen mit falschen, gestohlenen oder öffentlich zugänglichen Bankverbindungen getätigt. Lieferungen gehen nicht an den Betrüger selbst, sondern an Packstationen, leerstehende Häuser oder Wohnungen oder an Komplizen. Eine weitere Möglichkeit besteht darin, seine eigenen Daten leicht abzuändern. Der Postbote kennt allgemein die Namen und dazugehörigen Lieferadressen auf seiner Route und geht bei einer leichten Abänderung meist von einem Fehler aus. Dementsprechend gibt er das Paket an den Betrüger.

Somit ist es ein starkes Indiz für einen Betrugsversuch, wenn mehrere Transaktionen viele Ähnlichkeiten aufweisen und sich beispielsweise, durch einen Tausch von Vor- und Nachnamen, kleinere Abänderungen des Namens oder auch Ziffernverdopplungen der Hausnummer (5 → 55) ergeben. Der Ansatz des Projektes war es, 1. Gruppen aus *ähnlichen* Transaktionen (und somit ähnlichen virtuellen Identitäten) zu bilden, 2. zu bewerten und 3. zu visualisieren, um derartige Zusammenhänge aufzudecken.

Hierbei hat sich gezeigt, dass nicht nach einem einzelnen Muster in den Transaktionen gesucht wird, um Betrüger zu finden. Vielmehr müssen mehrere Ähnlichkeitsindikatoren in die Bildung des Netzwerkes und in seine Bewertung einbezogen und gewichtet werden.

4.2 Datenaufbereitung

Während der Datenaufbereitung zeigte sich die Problematik der Datenqualität, die eine unmittelbare Konsequenz aus der Nutzung heterogener externer Daten ist. Um die Daten effizient in das entwickelte System laden zu können, müssen diese vorher bereinigt und angepasst werden. Dabei stand man vor der Herausforderung, dass die bereitgestellten Daten teilweise doppelt vorhanden und in den Attributen Straße und Hausnummer nicht atomar sind. Des Weiteren gab es Postleitzahl-Einträge, welche „NULL“, einen Ortsnamen oder „Deutschland“ enthielten. Je mehr die Daten an das Zielsystem angepasst sind, desto mehr Zeit wird bei der Datenaufbereitung gespart. Während dies durchaus üblich für entsprechende Anwendungen ist, hat es jedoch Design-Konsequenzen: Da Betrugsfälle zeitnah erkannt werden müssen, ist eine aufwändige einzelfallbezogene Datenbereinigung nicht zielführend. Da die Daten in dem Szenario von externen Partnern stammen, ist auch eine Bereinigung an der Datenquelle keine gangbare Option. Es müssen vielmehr ETL-Routinen zur automatisierten Datenaufbereitung genutzt werden – was für eine Einbindung in vorhandene BI/DWH-Landschaften spricht.

4.3 Prototypische Umsetzung

Während des Projekts wurde ein lauffähiger Prototyp umgesetzt, der mittels Netzwerkanalyse auf Basis einer Neo4j-Graphdatenbank Gruppen identifiziert und bewertet. Diese können in dem Visualisierungstool Linkurious detailliert betrachtet werden. Als Ergebnis liefert der Prototyp die nach Auffälligkeit sortierten Gruppen, um durch diese im Anschluss manuell navigieren zu können.

Der Aufbau des Prototyps folgt mehreren Schritten, die automatisch durchlaufen werden:

1. Im ersten Schritt werden die Daten mit Hilfe einer selbst implementierten Lösung bereinigt und eingelesen.
2. Daraufhin wird mit einer selbsterstellten Komponente aus jeder Transaktion ein Knoten in der Graphdatenbank erzeugt und Duplikate herausgefiltert. Gleichzeitig wurde sichergestellt, dass nicht verschiedene Transaktionen desselben Nutzers als „ähnlich“ gekennzeichnet werden. Mit Schritt 2 konnte die Datenmenge in der Graphdatenbank halbiert werden.
3. Im nächsten Schritt werden Beziehungen zwischen Knoten berechnet und Gruppen gebildet.
4. Folgend werden Knoten und Verbindungen in CSV-Dateien gespeichert und in die Neo4j-Graphdatenbank importiert.
5. Zuletzt werden die Knoten nach Auffälligkeit kategorisiert.

Danach kann die Visualisierung und Navigation mit dem Tool Linkurious stattfinden.

4.4 Ähnlichkeitsmaße, Gruppenerkennung und -bewertung

Das entwickelte Verfahren ist zweistufig:

1. Bildung von Netzwerken aus ähnlichen Transaktionen (Gruppenbildung)
2. Bewertung der Netzwerke anhand ihrer Auffälligkeit (Gruppenbewertung)

Ad 1: Um *Gruppen bilden* zu können, werden von dem System alle Transaktionen miteinander verglichen und auf Ähnlichkeiten geprüft. Hierfür wurden für verschiedene Attribute gewichtete Ähnlichkeitsmaße berechnet. Um irrelevante Gruppen zu vermeiden, werden Kanten zwischen Transaktionen erst dann gezogen, wenn die aufsummierten Ähnlichkeitsmaße einen definierten Schwellwert überschreiten (die Gewichtungen wurden in einem längeren Prozess durch Kalibrierung gewonnen).

Die bereitgestellten Daten bestehen aus diskreten Attributen sowie der Lieferadresse, wobei nur Daten aus Transaktionen herangezogen werden. Insgesamt wurden acht verschiedene Attribute auf Gleichheit und/oder auf Ähnlichkeit geprüft. Eine weitere Anreicherung mit externen Informationen wurde auf Wunsch von arvato Financial Solutions vermieden (arvato Financial Solutions legt erheblichen Wert darauf, seine Informationsdienstleistungen mit maximaler Datensparsamkeit und unter vollständiger Berücksichtigung von Datenschutzzielen zu erbringen).

Als besonders relevant hat sich eine Prüfung erwiesen, bei der analysiert wurde, ob Vor- und Nachname komplett vertauscht wurden oder ob diese sehr ähnlich zu anderen Namen sind. Dieser Fall, wie auch identische Hash-IDs[1], E-Mail Adressen und ähnliche E-Mail Adressen im gleichen PLZ Bereich werden direkt mit dem Schwellenwert versehen. Sie bilden dadurch unmittelbar eine Kante und gehen direkt in die Gruppenbildung ein. Des Weiteren werden Ähnlichkeiten in der Lieferadresse mit einem hohen Gewicht versehen, wobei das Gewicht mit zunehmender örtlicher Nähe steigt. Weniger kritische Attribute werden mit einem niedrigen Gewicht versehen und kommen primär in Verbindung mit weiteren Attributskombinationen zum Tragen.

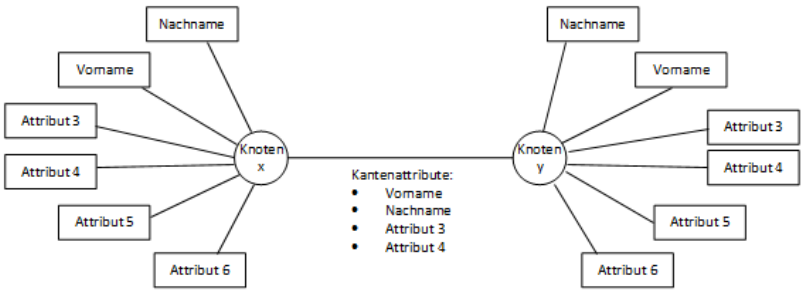

Abbildung 1: Visualisierung des Datenmodells

[1] Hash-ID: Zusammengesetztes Merkmal zur Identifikation von Hardware.

Eine besondere Herausforderung bestand in der Bestimmung von Ähnlichkeiten von Personen- und Straßennamen sowie E-Mail-Adressen. Für diese drei Typen von Attributen wurden jeweils eigene Metriken erstellt und kalibriert. In diese gingen jeweils unterschiedlich gewichtete Summen aus phonetischen (Kölner Phonetik & Soundex) [25][26] und syntaktischen (Jaro-Winkler-Distanz) [27] Ähnlichkeitsmaßen ein.

Gleiche und ähnliche Attribute werden auf die Kante zwischen zwei Transaktionen geschrieben (folglich als „Kantenattribut“ bezeichnet), damit der Algorithmus für die Bewertung der Gruppen darauf zugreifen kann. Dies wird in Abbildung 1 verdeutlicht: Die Knoten x und y weisen insgesamt vier gleiche oder ähnliche Attribute auf. Diese werden als Kantenattribut auf der Kante selbst vermerkt. Dabei gibt es kritische Attribute, die unmittelbar dafür sorgen, dass eine Kante gezogen wird, unter anderem die Hash-ID oder die E-Mail Adresse.

So kann beispielsweise eine Gruppe gebildet werden, die im Namen, der Adresse, der Email-Adresse und der Hash-ID gleiche oder ähnliche Attribute aufweist (vgl. Abbildung 2; im Beispiel mit einem vereinfachten und reduzierten Attributsatz).

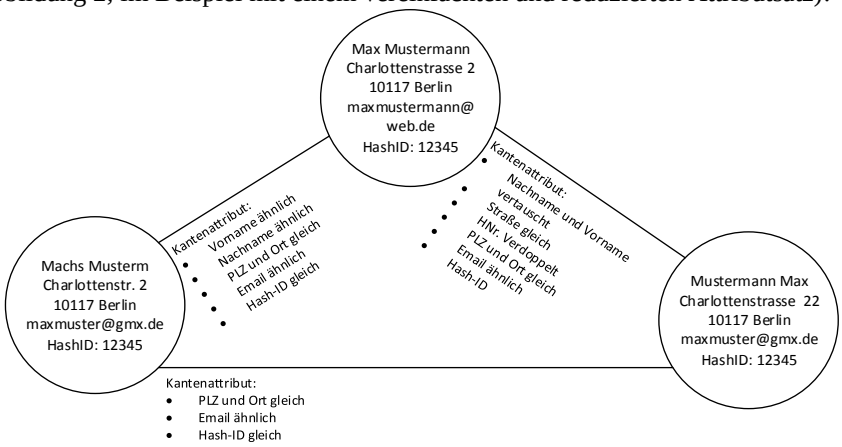

Abbildung 2: Beispiel einer Gruppe

Ad 2: Die *Bewertung der Gruppen* erfolgt nach einem ähnlichen Ansatz wie die Gruppenbildung: Es werden die Kantenattribute mit Ähnlichkeitswerten versehen und dann summiert (wobei hierbei andere Gewichtungen zum Tragen kommen). Anhand von weiteren Schwellwerten wird eine Kante in eine von drei Kategorien einsortiert, wobei die dritte die auffälligste Kategorie darstellt. Die Vorgaben sind dabei selektiver gewählt und zielen stärker auf die Kennzeichnung tatsächlicher Betrugsfälle ab als bei der initialen Gruppenbildung. arvato Financial Solutions hat hervorgehoben, dass Gruppen besonders dann als auffällig gelten, sobald mit einzelnen Attributen „gespielt“ wird. Dies kann anhand kleiner Abänderungen der Daten erkannt werden, die sich v.a. per Augenmaß ähneln. Dies wurde bei der Gewichtung berücksichtigt. Im Knoten selbst wird jetzt ebenfalls eine Kategorie vermerkt, damit eine Graph-Traversierung angewandt werden kann. Außerdem hat dies den Vorteil, Knoten je nach Kategorie in der Visualisierung einfärben zu lassen. Hierfür erhält jeder Knoten eine Einordnung entsprechend der maximalen Kategorie aller anliegenden Kanten.

Die Kategorie wird darauf folgend im Graph mit einer Tiefe von zwei an die Nachbarknoten weitergegeben, sofern diese bislang eine niedrigere Kategorie haben.

Schließlich wird für jede Kategorie eine Datei angelegt, welche die ihr zugeordneten Gruppen enthält. Die per Netzwerkvisualisierung aufbereiteten Gruppen sind dafür konzipiert, einem menschlichen Entscheider vorgelegt zu werden (keine Vollautomatisierung) und sollen diesen in der Identifikation möglicher Betrüger unterstützen. Dies ist konform mit dem Vorgehen von arvato Financial Solutions und insbes. zur Vermeidung von False-Positives auch notwendig.

4.5 Visualisierung und Datenhaltung

Während der Entwicklung wurde die Erkenntnis gewonnen, dass es sinnvoll ist, die *netzwerkorientierte Datenhaltung und -auswertung* von der *netzwerkorientierten Visualisierung* zu trennen, da sich die Anforderungsprofile als zu unterschiedlich erwiesen haben (funktional mächtige Datenhaltung und -abfrage vs. performante Darstellung und interaktive Navigation). Die Datenhaltung für die Transaktionen mit ihren Verbindungen sowie die Traversierung erfolgt im Prototyp mit der Graphdatenbank Neo4j, die Visualisierung über das Tool Linkurious. Linkurious ist ein Werkzeug für die Visualisierung von Graphdaten, dessen Vorteile darin liegen, eine performante Visualisierung und Suche von Netzwerken, eine einfache Kopplung mit Neo4j, eine Möglichkeit, Knoten anhand der Attribute einzufärben sowie eine einfache Ergänzung neuer Knoten und Kanten zu bieten. Abbildung 3 zeigt beispielhaft eine Gruppe mit Knoteneinfärbung nach Kategorie der Auffälligkeit.

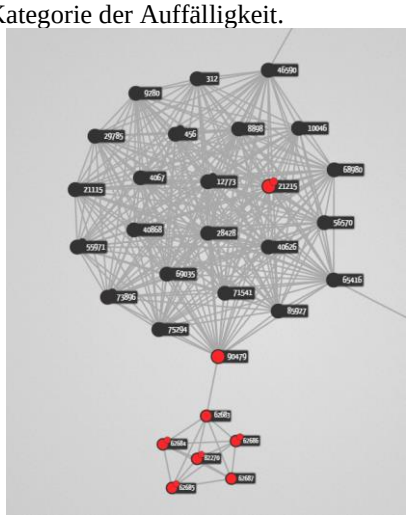

Abbildung 3: Visualisierungsbeispiel aus dem Prototyp

4.6 Big-Data-Kontext

Eines der Hauptprobleme während des Projekts war die Zeit, die benötigt wurde, um das gesamte Netzwerk initial aufzubauen. So benötigte der Prototyp zum Erstellen des gesamten Netzwerkes auf einem handelsüblichen PC ca. 21 Tage. Die Ursache für

diese lange Laufzeit liegt darin, dass das Programm für jede neue Transaktion nach ähnlichen, bereits vorhandenen Transaktionen sucht, was zu einer quadratischen Laufzeitentwicklung führt (Datensatz Berlin – 90.000 Knoten: 50 Minuten; Datensatz NRW – 648.000 Knoten: 33 Stunden, bereinigter Komplettdatenauszug – 5 Mio. Knoten: 21 Tage). Soll später auf den vollständig historisierten Datenbestand zurückgegriffen werden, so ist auch eine Aufrüstung des Analyserechners (vertikale Skalierung) keine Option.

Wie man Diagramm 1 entnehmen kann, benötigt bereits die Suche nach ähnlichen Datensätzen zu einem Referenzdatensatz für den genutzten Datenbestand 70 bis 80 Sekunden. Um Auffälligkeiten im Bestellvorgang zu entdecken und damit potentielle Betrugsabsichten effektiv zu verhindern, bedarf es aber eine Near-Real-Time bzw. in bestimmten Anwendungsfällen sogar eine Real-Time-Unterstützung. So entstehen beispielsweise Online-Händlern pro verlorenem Dollar insgesamt 3,10 $ Kosten [28]. Je früher ein Betrugsversuch daher auffällt, desto mehr Kosten kann ein Unternehmen einsparen. Eine solche Real-Time-Unterstützung kann jedoch mit einer benötigten Zeit von 70 Sekunden pro Transaktion nicht gewährleistet werden.

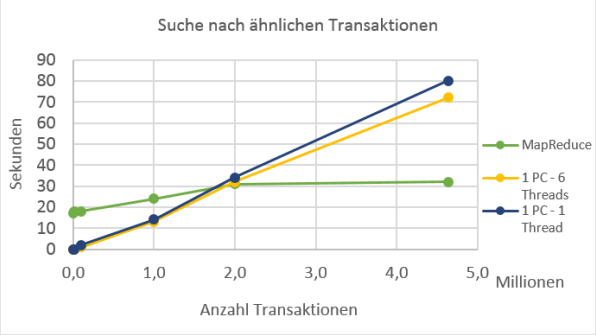

Diagramm 1: MapReduce – Suche nach ähnlichen Transaktionen

Um die Möglichkeit einer Real-Time-Unterstützung zu erproben, wurde exemplarisch eine Realisierung auf einem Hadoop-Cluster durchgeführt. Der Prototyp wurde dahingehend verbessert, dass er, anstatt die Suche nach ähnlichen Transaktionen lokal auf einem Rechner durchzuführen, die Aufgabe an einen MapReduce-Job weiterreicht, der die Rechenleistung eines kleineren Hadoop-Clusters (5 PCs) nutzt, um die Suche zu beschleunigen. Durch dieses Vorgehen wird Laufzeit dahingehend gespart, dass die einzelnen Vergleiche zur Suche von Verbindungen zwischen den Transaktionen auf mehrere nebenläufige Prozesse aufgeteilt werden. Wie man Diagramm 1 entnehmen kann, ergibt sich dadurch eine Laufzeiteinsparung für die gesamte Datenmenge von ca. 40 Sekunden pro Suche. Dieses Ergebnis deutet darauf hin, dass eine Weiterentwicklung des Prototyps in diese Richtung deutliche Vorteile bringen kann.

4.7 Resultierende Architektur

Zur Diskussion der architektonischen Konsequenzen einer Einbettung der entwickelten Lösung in ein bestehendes BI-Umfeld (wie etwa von arvato Financial Solutions angestrebt) wird ein generischer BI-Ordnungsrahmen benutzt, der zwischen den

operativen Daten, der Datenbereitstellung und der Informationsgenerierung /-distribution unterscheidet [6]. Bei den *operativen Daten* handelt es sich im gegebenen Fall um die Daten, die von den Online-Shops zur Überprüfung bereitgestellt werden. Die anfallenden Transaktionen werden bereits heute bei arvato Financial Solutions für die *Datenbereitstellung* auf einem Hadoop-Cluster abgelegt. Diese Datenbereitstellungsschicht dient dazu, allen vorhandenen Systemen dieselbe Datengrundlage zu bieten und kann später auch für Parallelisierungsaufgaben etwa in der Ähnlichkeitsanalyse eingesetzt werden. Darüber hinaus ist der Einsatz einer übergreifenden ETL-Komponente (als Ersatz für die separaten Routinen des Prototyps) sinnvoll, da dadurch allen nachfolgendenden Systemen bereits harmonisierte Daten zur Verfügung gestellt sind und möglicher Mehraufwand, wie z.B. Adressbereinigung, vermieden werden kann (vgl. auch 4.2). Sowohl die neue Transaktion als auch die Verbindungen zu anderen Transaktionen werden daraufhin in die Graphdatenbank geladen. Diese nimmt für den Prototyp die Funktion eines Data Marts für die Netzwerkanalysen ein, der parallel zu dem etablierten, reportingorientierten DWH steht. Hier ist der Gesamtbestand an Ähnlichkeitsbeziehungen zwischen Transaktionen hinterlegt.
In die Schicht der *Informationsgenerierung bzw. -distribution* lassen sich Systeme zur Visualisierung von Netzwerken und zur visuellen Analyse einordnen, etwa auf der Basis von Werkzeugen wie Linkurious, Qlikview oder KeyLines. Diese greifen auf jeweils zu betrachtende Auszüge des Data Marts zu.

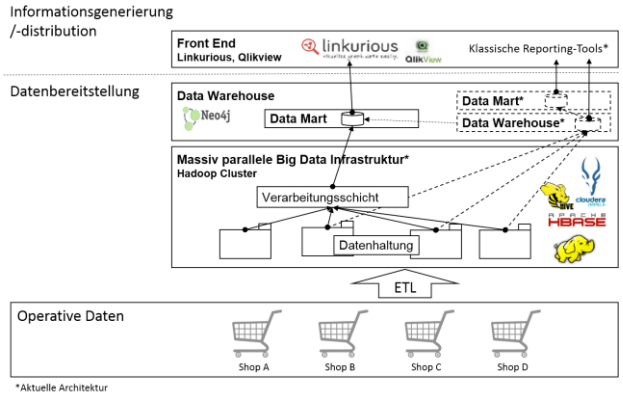

Abbildung 4: Architekturskizze

5 Diskussion

Der Forschungsbeitrag der Arbeit besteht in dem Entwurf einer Lösung einer netzwerkorientierten Betrugserkennung, die lediglich auf Ähnlichkeiten zwischen Transaktionen aufbaut. Dies umfasst insbes. die Architektur sowie die Bildung der Ähnlichkeitsmetriken und des Algorithmus zur Identifikation und Bewertung der Gruppen. Das Konzept kann auf ähnliche Fälle der Betrugserkennung übertragen werden. Vorstellbar sind auch Anwendungen im Controlling oder im Marketing, sofern für bestimmte Fragestellungen lediglich Daten aus Bestellvorgängen vorliegen. Wie die Ausführungen unterstreichen, handelt es sich um eine Lösung für ein relevan-

tes Problem, dessen Einsetzbarkeit mit dem lauffähigen Prototyp auch gezeigt wurde. In der Evaluation konnten auch tatsächlich potentielle Betrugskandidaten identifiziert werden, die von den Analysten von arvato Financial Solutions als hochrelevant betrachtet wurden. Auch wurden testweise bereitgestellte reale Betrugsfälle im Prototypen auch als auffällig gekennzeichnet. Der Prototyp stuft ca. 19% aller Knoten als auffällig ein, wir gehen jedoch davon aus, dass dieser Anteil durch weitere Bereinigungsschritte noch deutlich reduziert werden kann.
Eine methodische Grenze des Vorhabens bestand darin, dass die Güte der Betrugserkennung nur qualitativ durch Befragungen geprüft werden konnte. Es gab keinen Satz von eindeutigen Testfällen. Zudem waren Daten zu Zahlungsausfällen nur lückenhaft vorhanden und unzureichend für einen statischen Test, mit dem Alpha- und Betafehler quantitativ hätten bestimmt werden können. Auch konnten die Ähnlichkeitsmetriken in dem Zeitrahmen des Projektes lediglich durch iteratives Testen unter Feedback von arvato Financial Solutions erstellt werden. Es ist auch zu berücksichtigen, dass es mit dem Verfahren nicht möglich ist, einmalige Betrugsversuche aufzuzeigen (da noch keine Transaktionen zum Vergleich vorliegen) oder von Fällen zu unterscheiden, bei denen ein „Nichtbezahlen“ unabsichtlich war. Des Weiteren ist eine perfekte Täuschung, bei der es keine Ähnlichkeiten zu anderen Transaktionen gibt, mit dem Prototyp nicht auffindbar. Schließlich ist der Ansatz bislang noch nicht auf virtuelle Güter übertragbar, da in der Ähnlichkeitsanalyse ein wichtiger Fokus auf der Lieferadresse liegt. In einem Anwendungsfall mit virtuellen Gütern ist des Weiteren die Zeit noch wesentlich kritischer: Bei derartigen Gütern muss innerhalb weniger Sekunden geprüft werden, ob eine Transaktion zustande kommen soll bzw. welche möglichen Zahlungsarten dem Kunden angeboten werden sollen.

Der Prototyp kann noch in vielfacher Weise weiterentwickelt werden. Ein besonderer Aspekt ist hierbei der Ausbau der Ähnlichkeitsanalyse durch zusätzliche Attribute und deren Verfeinerung. Dafür sollte auch geprüft werden, ob durch andere, komplexere Algorithmen, wie z.B. Phonet [29], die Genauigkeit der Ähnlichkeitsanalyse (in Bezug auf Zeichenketten) verbessert, oder deren Zeitbedarf durch Vorprüfung mit effizienteren Vergleichen wie z.B. der Bag-Distance [30] verringert werden kann. Die Arbeit weist auch auf weiteren Forschungsbedarf im Rahmen der Namensähnlichkeit hin. Diese benötigt eine tiefere und feinere Abstimmung, etwa für die Berücksichtigung fremdsprachiger Namen. Die Anreicherung mit Geodaten stellt ebenfalls eine vielversprechende Weiterentwicklung dar. Hierdurch kann präziser ermittelt werden, ob es auffällige Häufungen von Transaktionen innerhalb eines Gebietes gibt. Wird eine Umsetzung mit Geodaten in Betracht gezogen, ist es eine wesentliche Anforderung, personenbezogene Daten nicht an unsichere Drittanbieter zu geben, weshalb diverse weitverbreitete Services nicht in Anspruch genommen werden dürfen. Methodisch wäre eine Integration mit weiteren Verfahren zur Betrugserkennung erforderlich, insbes. auf der Grundlage von Klassifikationsalgorithmen für die Feinjustierung der Gruppenbewertung.

Des Weiteren ist eine Ausweitung auf ein Realtime-System mit Active Data Warehousing sinnvoll, um zu gewährleisten, dass eine neue Transaktion nach dem Hinzufügen zeitnah von einem zuständigen Bearbeiter geprüft und bewertet wird. Wird auf ein Real-Time System zusätzlich ein Active Data Warehousing Ansatz implemen-

tiert, können definierte, automatisierte Aktionen häufig anfallende Aufgaben bearbeiten. Während des Projekts wurden bereits exemplarisch einige solche Event-Condition-Action-Regeln erstellt und mit arvato Financial Solutions diskutiert. Sie dienen damit als Grundlage für die weitere Umsetzung. Mit Hilfe solcher Regeln lässt sich beispielsweise die Information über den Zahlungsausfall einer Transaktion an die damit verbundenen Transaktionen weitergeben und es können Maßnahmen angestoßen werden, um weitere Zahlungsausfälle zu verhindern.

Schließlich ist zu beachten, dass der Ansatz als *Ergänzung* zu bestehenden Scoring- und klassifikationsbasierten Systemen zu verstehen ist und nicht als deren *Ersatz*. Es besteht sowohl Forschungsbedarf hinsichtlich des Designs eines kombinierten Systems als auch bezüglich dessen Ergebnisgüte. Zu beachten ist dabei, dass wir Fälle gefunden haben, die ausschließlich in einer Netzwerksicht identifizierbar sind und es hier unseres Wissens auch bislang kein alternatives System gibt, dass dies leistet.

Trotz der angeführten Limitationen legen die Resultate insofern deutlich nahe, dass und wie mit dem verfolgten Ansatz ein wertvoller Beitrag zur Entscheidungsunterstützung realisiert werden kann und welche architektonischen und methodischen Anforderungen sich daraus ergeben. Es ist zu betonen, dass arvato Financial Solutions plant, den Prototypen in einem Anschlussprojekt in Richtung eines produktiv laufenden Systems weiterzuentwickeln.

References

1. Ngai, E. W. T., Hu, Y., Wong, Y. H., Chen, Y., & Sun, X.: The application of data mining techniques in financial fraud detection: A classification framework and an academic review of literature. Decision Support Systems, 50. Jg., Nr. 3, S. 559-569 (2011)
2. Chan, P. K., Fan, W., Prodromidis, A. L., & Stolfo, S. J. .: Distributed data mining in credit card fraud detection. Intelligent Systems and their Applications, IEEE, 14. Jg., Nr. 6, S. 67-74 (1999)
3. Brause, R., Langsdorf, T., Hepp, M.: Neural data mining for credit card fraud detection. In: Tools with Artificial Intelligence, 1999. Proceedings. 11th IEEE International Conference on. IEEE, S. 103-106 (1999)
4. Chen, H., Chiang, R., Storey, V.C.: Business Intelligence and Analytics: From Big Data to Big Impact. MIS quarterly, 36. Jg., Nr. 4, S. 1165-1188 (2012)
5. Baars, H., Funke, K., Müller, P. A., & Olbrich, S.: Big Data als Katalysator für die Business Intelligence – Das Beispiel der informa Solutions GmbH. HMD Praxis der Wirtschaftsinformatik, S. 1-11 (2014)
6. Kemper, H.-G., Baars, H., Mehanna, W.: Business Intelligence – Grundlagen und praktische Anwendungen. Springer (2010)
7. Laney, D.: LANEY, Doug. 3D data management: Controlling data volume, velocity and variety. META Group Research Note, 6. Jg. (2001)
8. Brewer, E. A.: Towards robust distributed systems. In: PODC, S. 7 (2000)
9. Cattell, R.: Scalable SQL and NoSQL data stores. ACM SIGMOD Record, 39. Jg., Nr. 4, S. 12-27 (2011)
10. Angles, R., Gutierrez, C.: Survey of graph database models. ACM Computing Surveys (CSUR), 40. Jg., Nr. 1, S. 1 (2008)
11. Oxford Dictionary, http://www.oxforddictionaries.com (Zugegriffen am: 22.10.2014)

12. Kou, Y., Lu, C. T., Sirwongwattana, S., & Huang, Y. P.: Survey of fraud detection techniques. In: Networking, sensing and control, 2004 IEEE international conference on. IEEE, S. 749-754 (2004)
13. Phua, C., Lee, V., Smith, K., Gayler, R.: A comprehensive survey of data mining-based fraud detection research. arXiv preprint arXiv:1009.6119 (2010)
14. Bolton, R. J., Hand, D. J.: Statistical fraud detection: A review. Statistical Science, S. 235-249 (2002)
15. Sadowski, G., Rathle, P.: Fraud Detection: Discovering Connections with Graph Databases (2014)
16. Chau, D. H., Pandit, S., Faloutsos, C.: Detecting fraudulent personalities in networks of online auctioneers. In: Knowledge Discovery in Databases: PKDD 2006. Springer Berlin Heidelberg, S. 103-114 (2006)
17. Wasserman, S., Faust, K.: Social network analysis: Methods and applications. Cambridge University Press (1994)
18. de Nooy, W., Mrvar, A., Batagelj, V.: Exploratory social network analysis with Pajek. Cambridge University Press (2011)
19. Freeman, L. C.: Centrality in social networks conceptual clarification. Social networks, 1. Jg., Nr. 3, S. 215-239 (1979)
20. Hevner, A. R., March, T. S., Park, J., Ram, S.: Design science in information systems research. MIS quarterly, 28. Jg., Nr. 1, S. 75-105 (2004)
21. Warmbrodt, J., Sheng, H., Hall, R.: Social network analysis of video bloggers' community. In: Hawaii International Conference on System Sciences, Proceedings of the 41st Annual. IEEE, S. 291-291 (2008)
22. Holsapple, C., Hsiao, S., Pakath, R.: Business Social Media Analytics: Definition, Benefits, and Challenges. Proceedings of the Twentieth Americas Conference on Information Systems, Savannah (2014)
23. Putzke, J., Fischbach, K., Schoder, D., Oster, D.: Business Intelligence und die Analyse unternehmensinterner Kommunikationsprozesse. In: Multikonferenz Wirtschaftsinformatik (2008)
24. Gregor, S. and Jones, D.: The anatomy of a design theory. Journal of the Association for Information Systems, 8. Jg., Nr. 5, S. 1 (2007)
25. Wilz, M.: Aspekte der Kodierung phonetischer Ähnlichkeiten in deutschen Eigennamen. Diss. Magisterarbeit an der Philosophischen Fakultät der Universität zu Köln (2005)
26. Raghavan, H., Allan, J.: Using soundex codes for indexing names in ASR documents. In: Proceedings of the Workshop on Interdisciplinary Approaches to Speech Indexing and Retrieval at HLT-NAACL 2004. Association for Computational Linguistics, S. 22-27 (2004)
27. Cohen, W., Pradeep R., Fienberg, S.: A comparison of string metrics for matching names and records. In: KDD Workshop on Data Cleaning and Object Consolidation, S. 73-78 (2003)
28. LexisNexis: 2013 LexisNexis® True Cost of Fraud^{SM} Study - Merchants Struggle Against an Onslaught of High-Cost Identity Fraud and Online Fraud (2013)
29. Hofmann, P.: Information Retrieval Seminar: Phonetische Suche. In: Seminar, Johannes Gutenberg-Universität Mainz (2010)
30. Bartolini, I., Ciaccia, P., & Patella, M.: String matching with metric trees using an approximate distance. In: String Processing and Information Retrieval. Springer Berlin Heidelberg, S. 271-283 (2002)