



Credit Card Fraud Detection

Anastasia Wawilow

- Einleitung
- Allgemeine Grundlagen
 - Aufbau einer Kreditkarten
 - Kreditkartenarten
 - Kreditkartenbetrug
 - Techniken der Kreditkartenbetrüger
- Techniken zur Erkennung eines Kreditkartenbetrugs
 - Clustering
 - Neuronale Netze
 - Entscheidungsbäume
 - Hidden Markov Model

- Kreditkarten – meistgenutztes Zahlungsmittel
 - 1,8 Milliarden Karten
 - 15 Millionen Akzeptanzstellen
- Verführung zum Betrug

- Einleitung
- **Allgemeine Grundlagen**
 - Aufbau einer Kreditkarten
 - Kreditkartenarten
 - Kreditkartenbetrug
 - Techniken der Kreditkartenbetrüger
- Techniken zur Erkennung eines Kreditkartenbetrugs
 - Clustering
 - Neuronale Netze
 - Entscheidungsbäume
 - Hidden Markov Model

Aufbau

- Deutschland
 - 'echte' Kreditkarten
 - Chargekarten
 - Debitkarten
 - Prepaidkarten
- England
 - 'echte' Kreditkarten
 - teilweise Prepaidkarten





- Echte Kreditkarten
 - Inhaber bekommt eine Rechnung
 - Girokonto wird nicht direkt belastet
 - Rechnung
 - Sofortige Bezahlung
 - Ratenzahlung



- Chargekarten
 - ähnlich wie echte Kreditkarten
 - Rechnung soll ein Monat später beglichen werden
- Debitkarten
 - Girokonto wird sofort belastet
 - Funktioniert, wie herkömmliche EC / Maestro Karte



- Prepaidkarten
 - Basiert auf Guthabenbasis
 - Nur Online – Akzeptanzstellen
 - Ohne Bonitäts – und Schufaprüfung
- Virtuelle Kreditkarten
 - Keine Plastikkarte
 - Geeignet für Transaktionen im Internet
 - Basiert auf Guthabenbasis

- Insolvenzbetrug
 - Ein Betrug ist schwer vorhersagbar
 - Pre - Check
 - Schufa Holding AG = Schutzgemeinschaft für allgemeine Kreditsicherung
 - Ziel: Banken von Forderungsausfällen zu bewahren

– Prozess:

- Verbraucher möchte einen Kredit aufnehmen
- Kreditinstitut holt sich die Auskünfte über Bonität des Antragstellers bei Schufa ein
- Bank entscheidet über Vergabe eines Kredits

- Score - Wert = Wahrscheinlichkeit für ein Kreditausfall
 - Berechnung basiert auf dem logischen Regressionsmodell
 - Abhängig von Werten, wie Anzahl der Wohnungswechsel, Anzahl der Bankkonten, Länge der Kredithistorie usw.

- Diebstahl / Fälschung
 - Diebstahl der physischen Karte
 - Fälschung der Kreditkartendaten
 - Schutzmechanismus der Kreditkarten ist im Vergleich zu Bankkonten deutlich unausgereifter
 - Räuber brauchen
 - Kreditkartennummer
 - Gültigkeitsdatum
 - Prüfziffer
 - Name des Inhabers

- Neue Technologie – 3 D Secure Code
- Chargeback Verfahren
 - Karteninhaber können die Buchungen stornieren
 - Der Betrag wird wieder gutgeschrieben
 - Entstandene Kosten trägt der Zahlungsempfänger

- **Anwendungsbetrug**
 - Identitätsdiebstahl
 - Benutzung personenbezogener Daten einer anderen Person
 - Betrüger kommen an diese Daten, z.B. durch das Durchwühlen unseres Abfall



- Skimming = “abschöpfen”
 - Magnetstreifen werden mittels spezieller Lesegeräten kopiert
 - Es werden Kartenduplikate hergestellt
- Vertauschen der Karte



- Software zur Generierung von Kreditkartennummer
 - Generierung von gültigen Kreditkartennummer, Ablaufdatum und Kreditkartengesellschaft
- Triangulation
 - Online Shop mit stark reduzierten Preisen

- Einleitung
- Allgemeine Grundlagen
 - Aufbau einer Kreditkarten
 - Kreditkartenarten
 - Kreditkartenbetrug
 - Techniken der Kreditkartenbetrüger
- Techniken zur Erkennung eines Kreditkartenbetrugs
 - Clustering
 - Neuronale Netze
 - Entscheidungsbäume
 - Hidden Markov Model

- Clustering
 - Ziel: Ähnlichkeit innerhalb einer Gruppe maximieren, außerhalb der Gruppe zu minimieren
 - Peer group analysis
 - Verfahren zur Überwachung vom Verhalten im Laufe der Zeit
 - Peer Gruppen = Sammlung von mehreren Karten
 - Breakpoint analysis

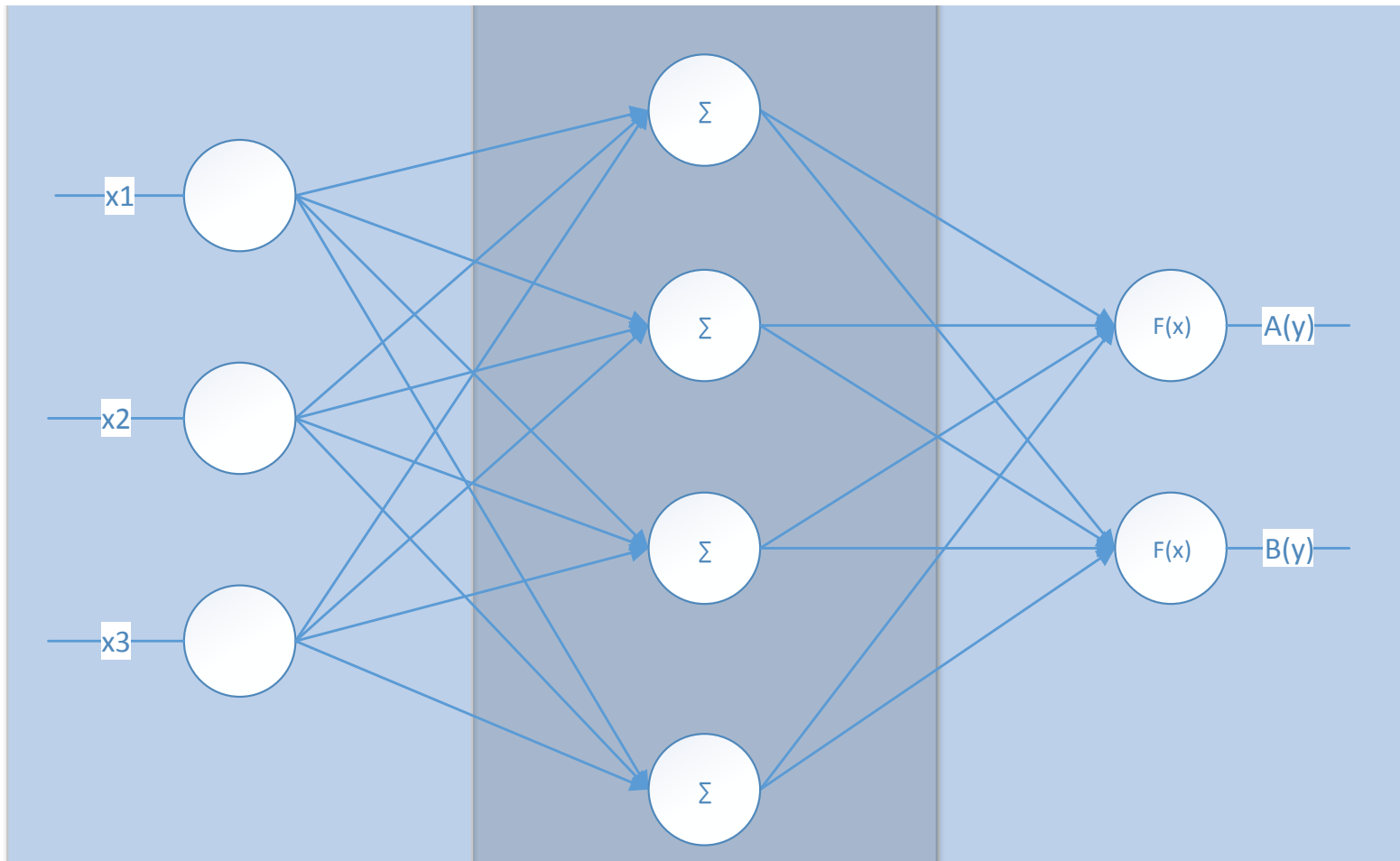
- Einleitung
- Allgemeine Grundlagen
 - Aufbau einer Kreditkarten
 - Kreditkartenarten
 - Kreditkartenbetrug
 - Techniken der Kreditkartenbetrüger
- Techniken zur Erkennung eines Kreditkartenbetrugs
 - Clustering
 - Neuronale Netze
 - Entscheidungsbäume
 - Hidden Markov Model

- Neuronale Netze
 - Nachbildung von Leistungsfähigkeit des menschlichen Gehirn
 - Geeignet für unvollständige, unreine und widersprüchliche Daten
 - Berücksichtigung nicht nur einzelner Faktoren, sondern ihre Kombination
 - Neuronale Netze sind flexibel, können schnell angepasst werden

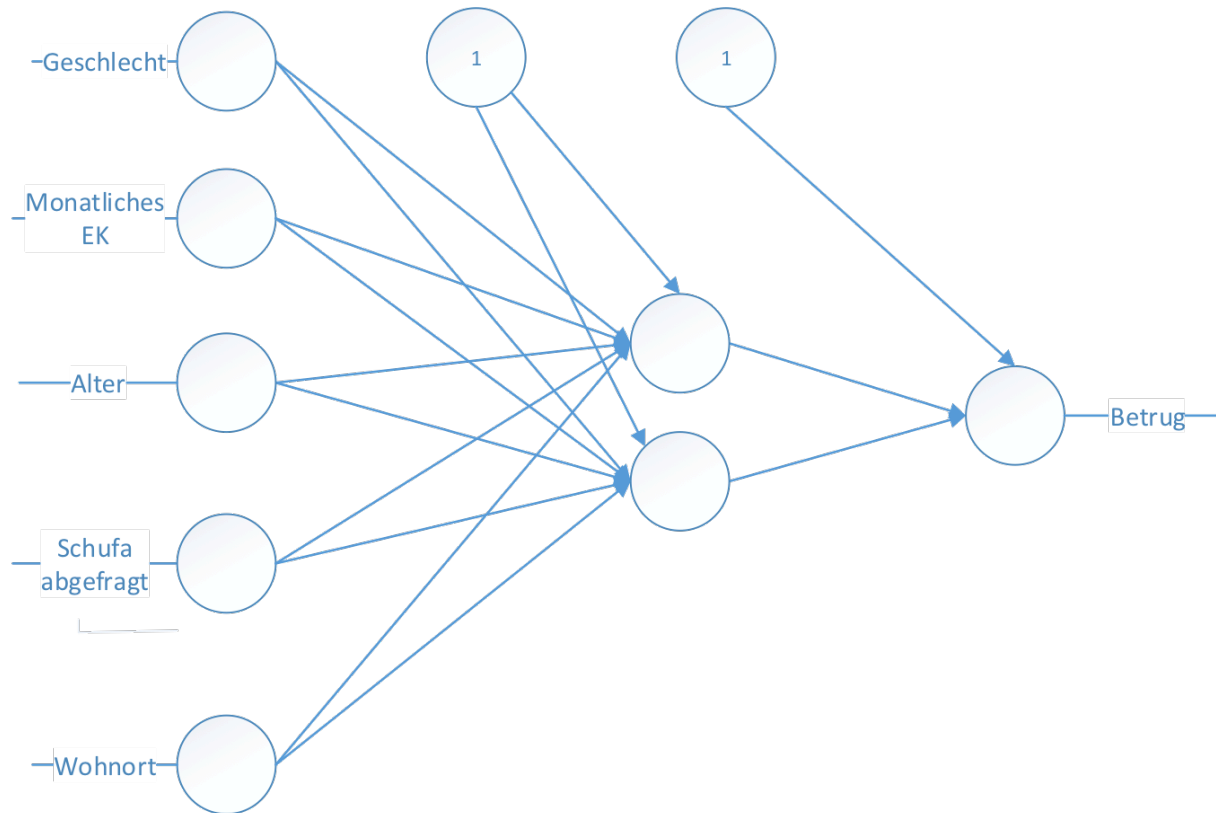
- Neuronale Netze – Aufbau
 - Bestehen aus Neuronen
 - Neuronen verarbeiten die Eingabegröße zu einer Ausgabe
 - Eingabegröße ist mit einer bestimmten Intensität mit dem Neuron verbunden

- Neuronales Netz besteht
 - Aus drei Schichten
 - Eingabeschicht – leitet die Eingabe weiter
 - Versteckte Schicht
 - Ausgabeschicht – gibt Entscheidung an Außenwelt zurück
 - Aktivierungsfunktion
 - Trainingsmenge = Eingabedaten + erwartete Ausgabe

Techniken

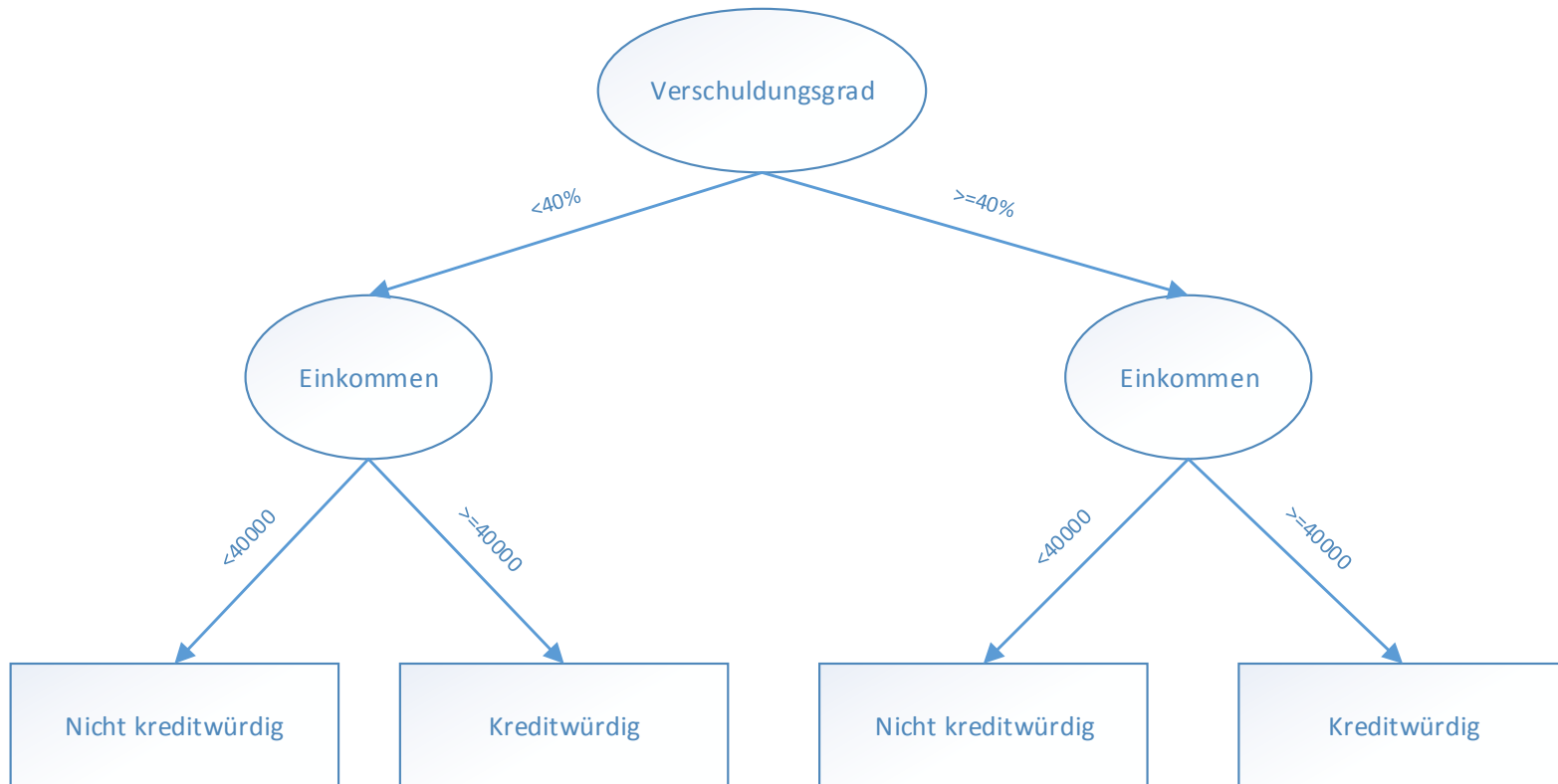


Techniken



- Einleitung
- Allgemeine Grundlagen
 - Der Begriff 'Kreditkarten,
 - Kreditkartenarten
 - Kreditkartenbetrug
 - Techniken der Kreditkartenbetrüger
- Techniken zur Erkennung eines Kreditkartenbetrugs
 - Clustering
 - Neuronale Netze
 - Entscheidungsbäume
 - Hidden Markov Model

- **Entscheidungsbäume**
 - Eine Methode zur Klassifikation
 - Geordnete, gerichtete Bäume
 - Repräsentation
 - Blätter – Klassen
 - Knoten – Attribute
 - Kanten – Attributwerte
 - Entscheidungsbäume werden für die Prognose der Klassenzugehörigkeit von bisher noch nicht aufgetretenen Objekten verwendet

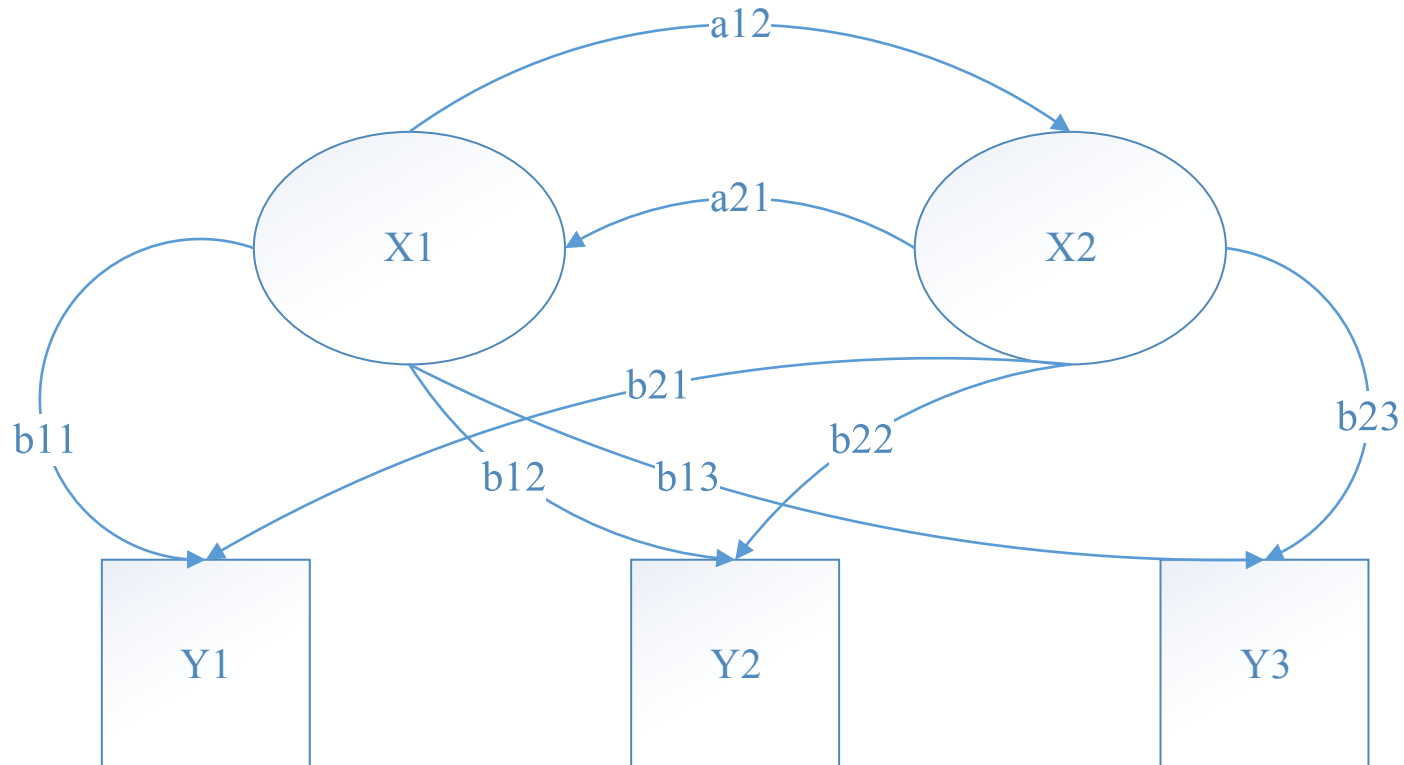


- Entscheidungsbäume
 - Algorithmen für die Erstellung
 - ID3, CART, C4.4
 - Informationsgehalt wird ermittelt
 - Das informativste Attribut ist die Wurzel
 - Baum wird weiter rekursiv aufgebaut
 - Ziel: Modellgenerierung, mit der die Ereignisse vorhersehbar werden können
 - Vorteil: leichte Ablesbarkeit von Entscheidungsregeln

- Einleitung
- Allgemeine Grundlagen
 - Aufbau einer Kreditkarten
 - Kreditkartenarten
 - Kreditkartenbetrug
 - Techniken der Kreditkartenbetrüger
- Techniken zur Erkennung eines Kreditkartenbetrugs
 - Clustering
 - Neuronale Netze
 - Entscheidungsbäume
 - Hidden Markov Model

- Hidden Markov Model
 - HMM wird mit “normalem” Verhalten von Kreditkarteninhaber trainiert
 - HMM akzeptiert nicht eine eingehende Transaktion → eine verdächtige Transaktion
 - Stochastisches Modell
 - Modellierung durch eine Markow – Kette mit unbeobachteten Zuständen

- Hidden Markov Model besteht aus
 - Endliche Menge von Zuständen
 - Ausgabesymbolen - Emissionen
 - Konstante Übergangswahrscheinlichkeit
 - Abhängig von aktuellen Zustand
 - Wahrscheinlichkeit von Ausgabesymbole
 - Beobachtungssequenz



X - Zustände

Y – Emissionen

a - Übergangswahrscheinlichkeiten

b - Emissionswahrscheinlichkeiten

- HMM wird von Betrugserkennungssystem benutzt
- System empfängt
 - die Karteninformationen
 - Summe von Einkäufen
- System überprüft, ob
 - Transaktion verdächtig ist oder nicht



Vielen Dank!