

Fraud Detection



Fraud detection

Fabian Fromwald

Peter Kain

Korrekturleser: Peter Kain

Einleitung

Banken und Versicherungen verlieren jährlich mehrere Milliarden Dollar wegen Betrug. Traditionelle Methoden der Betrugserkennung spielen immer noch eine wichtige Rolle um die Verluste zu minimieren.

Jedoch haben Betrüger eine Vielzahl von Wegen gefunden, sich der Entdeckung zu entziehen. Sie organisieren sich in Gruppen und Ringen. Sie verwenden gefälschte oder gestohlene Identitäten und benutzen gehackte Geräte.

Graph-Datenbanken bieten moderne Möglichkeiten Betrugsringe und andere komplexe Betrugsfälle zu erkennen und in Echtzeit zu stoppen.

Keine Betrugserkennung kann je perfekt sein, aber eine Möglichkeit ist es zwischen die Daten zu blicken, nämlich den Verbindungen zwischen ihnen. In herkömmlichen relationalen Datenbanksystemen bleiben solche Verbindungen unentdeckt, bis es zu spät ist.

Fraud Detection

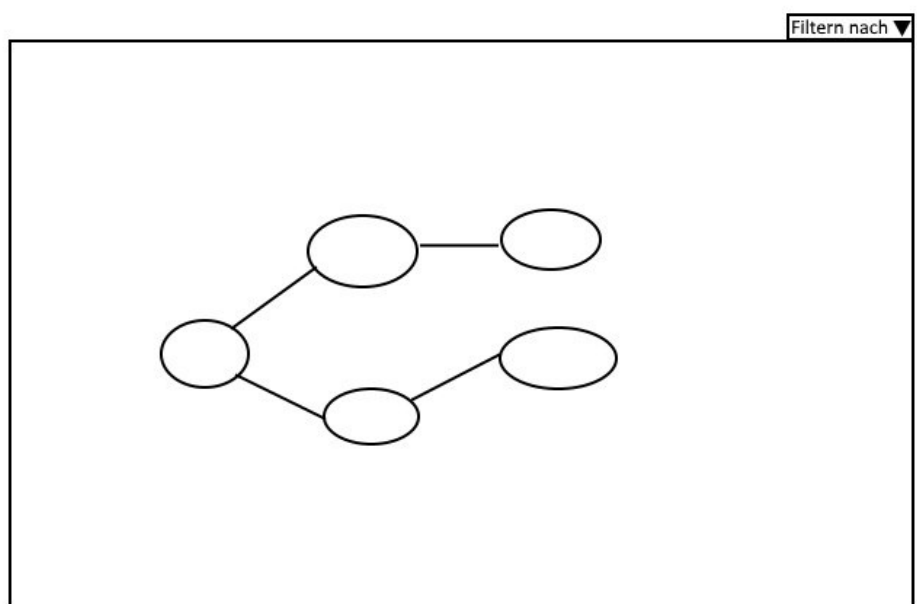
Deshalb arbeitet Fraud Detection mit Graph-Datenbanken. Die Software bietet Ihnen verschiedene Modi die Betrugsfälle zu erkennen. Diese Modi sollen sicherstellen, dass sie immer nur das für Sie Wichtigste angezeigt bekommen. Es gibt zwei verschiedene Modi zur Auswahl: Abteilungsleiter und Sacharbeiter.

Abteilungsleiter

Datenbank auswählen

Abteilungsleiter ▼

Filtern nach ▼	
Transaktion 1	20%
Transaktion 2	15%
Transaktion 3	5%

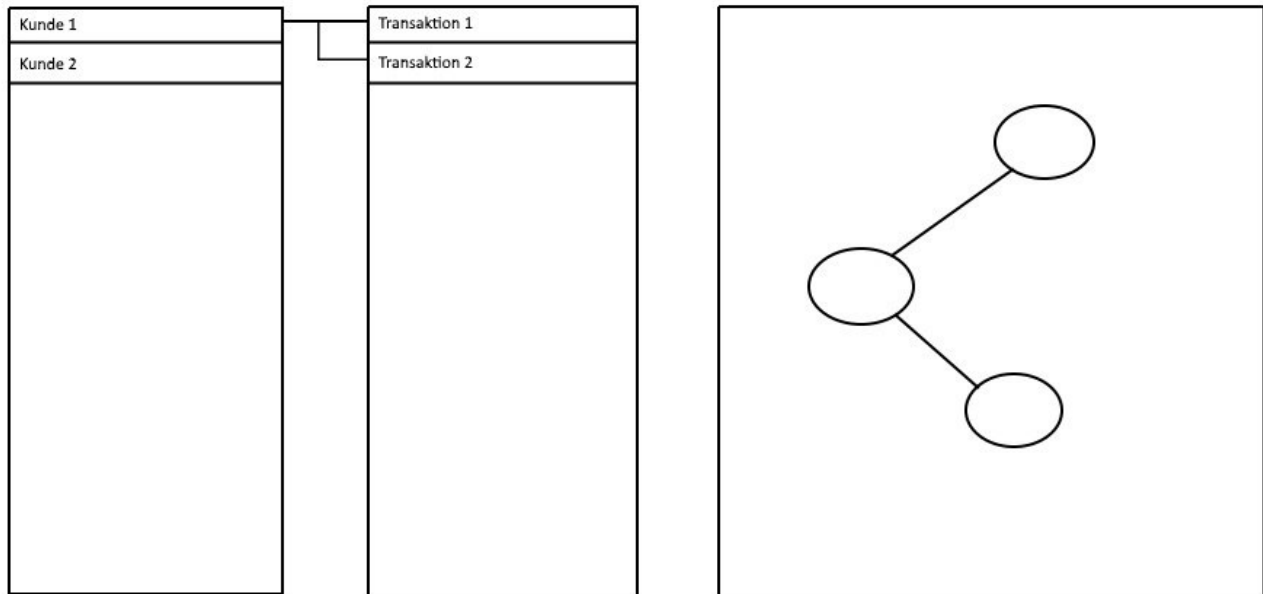


Als Abteilungsleiter können Sie sich alle Transaktionen nach Betrugswahrscheinlichkeit sortiert anzeigen lassen, diese werden im Graph rechts dargestellt. Außerdem können Sie sowohl den Graphen, als auch die Liste der Transaktionen nach bestimmten Merkmalen (Zeit, Ort, Kunde) filtern.

Sacharbeiter

Datenbank auswählen

Sacharbeiter ▼



Als Sacharbeiter bekommen Sie eine Liste der Kunden angezeigt. Durch Auswahl eines Kunden in der Liste bekommen Sie in der Liste und ganz rechts die Transaktionen als Liste, beziehungsweise als Graph angezeigt.

Fraud Detection kann von jedem PC aus mit einem JavaScript-fähigen Browser aufgerufen werden. Es ist keine Installation auf Ihrem Gerät nötig.

Typischer Betrugsfall

Der genaue Ablauf von Betrugsfällen variiert zwischen den einzelnen Fällen, aber das Muster zeigt wie Betrugsringe für gewöhnlich arbeiten:

1. Eine Gruppe von zwei oder mehr Leuten organisiert als Ring
2. Der Ring teilt sich eine Menge von echten Kontaktinformationen, zum Beispiel Telefonnummern und Adressen, welche sie nutzen um gefälschte Identitäten zu erstellen.
3. Sie eröffnen neue Konten mit diesen Identitäten.

4. Neue Konten werden zu den Originalen hinzugefügt
5. Die Konten werden normal benutzt mit regelmäßigen Ausgaben und pünktlichen Zahlungen.
6. Banken erhöhen den Kreditrahmen im Laufe der Zeit, wegen dem verlässlichen Kreditverhalten.
7. Eines Tages zerbricht der Ring. Sie koordinieren ihre Aktivitäten, nutzen das Maximum ihres Kreditrahmens aus und verschwinden.
8. Manchmal gehen die Betrüger einen Schritt weiter und bringen all ihre Kontostände durch gefälschte Rechnungen kurz vor dem vorherigen Schritt auf Null.
9. Die uneinbringlichen Schulden werden abgeschrieben.

Solche Betrugsfälle zu erkennen, bevor sie passieren, ist eine schwierige Aufgabe. Mit traditionellen Datenbanken ist dies bei größeren Datenmengen kaum möglich, da die Graphen darüber als eigene Tabellen modelliert werden müssten. Dies macht die Abfragen komplizierter und langsamer. Graph-Datenbanken sind das ideale Werkzeug um diese Hürden zu umgehen.

Technisches

Unser Produkt arbeitet mit Neo4j, einer Graph-Datenbank. Ihre Bestandsdaten können einfach von einem Relationalen Datenbankmanagementsystem zu Neo4j migriert und auch in "Real Time" synchronisiert werden. Somit kommt es zu keinen Abweichungen zwischen den beiden Systemen und Sie sehen immer den aktuellsten Stand. Die Integration in Ihre bestehende IT ist somit einfacher als Sie denken.

Diese Schnittstelle wird intern für unsere GUI verwendet, lässt sich aber auch leicht in bestehende Anwendungen einbinden.