

Real-Time Fraud Prevention with OrientDB

Banks and insurance companies lose millions of dollars in fraud every year. As online data grows, fraudsters have become increasingly capable of performing elaborate scams, identity theft, fraud rings and many other elusive ways to defraud customers and enterprises. Their methods are sophisticated and often times, their tactics go unnoticed until it is too late.

Detecting Fraud, especially while it is happening as opposed to after, is no easy task; yet it is not impossible. Relational databases are simply not capable of forming the correct, real-time connections needed to successfully detect crimes as they unfold. For this, companies have turned to graph databases as a means to detect weak or suspicious links between datasets. Insurance fraud, for example, is especially difficult to detect as they regularly involve multiple people, which on the surface are seemingly unrelated. Detection of these is dependent on discovering social links between participants making false claims.

Using relational databases to detect fraudulent claims can prove especially difficult. Table and columns are not suitable for forming complex relations between datasets. Joining tables can prove time consuming as well as taxing on system performance, which makes them difficult to use when attempting to detect crimes in real time. Contrary to relational databases, graph databases are relational in nature and are inherently capable of forming links between pieces of information, which can be easily traversed to detect suspicious activity.

Whereas relational databases rely on primary keys to join disconnected pieces of information, graphs work by forming a web of interconnected data and allows customer details, transactions and relations to be formed quickly, are easily observable and always available. In fact, a simple visual representation of a graph is enough to detect links between individuals and pieces of information. Graph databases are perfectly suited to store information and relations in a manner that lends itself to uncovering strange data patterns. However, normal graph DBs still make use of document databases in order to store transaction data. With regards to fraud detection, integrating multiple systems is not optimal when hoping to store secure data that must be travelled quickly.

How Does Bank Fraud Happen?

- Accounts are opened by seemingly normal customers
- They carry out transactions
- They open credit lines
- They get personal loans.
- Payments are made on time
- They may act alone or form fraud rings

Industry

Banking/Insurance/E-commerce

Challenge

Protect banking transactions from fraudulent activity by identifying suspicious patterns and links between account holders as well as ensuring safety for online commerce by verifying transaction accuracy and acting upon red flags.

Approach

Assign properties within relationships themselves as links in order to quickly traverse entire data trees and identify fraudulent activity.

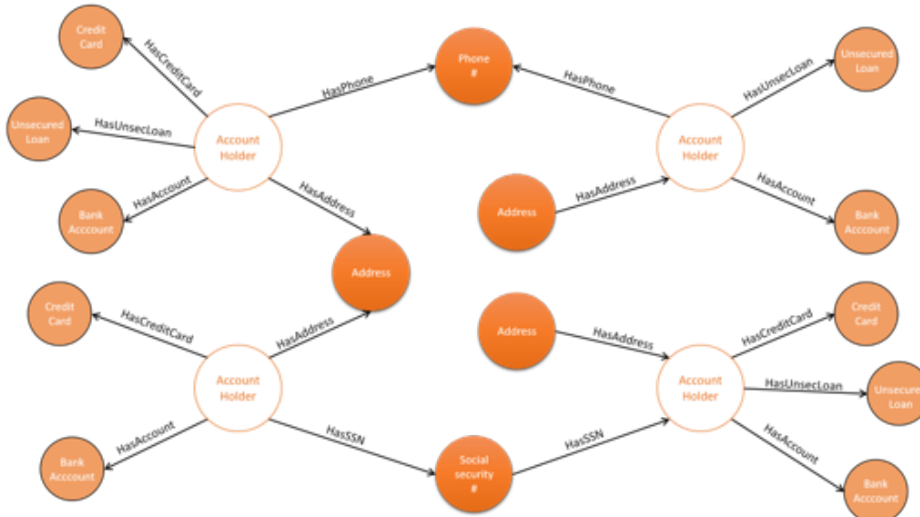
Solution

By using a graph database engine and harnessing the flexibility & power of documents, OrientDB is able to traverse entire trees of data in milliseconds. With its enhanced security features such as WAL (Write Ahead Log), Kerberos support, auditing and non-stop backups, data is safe from prying eyes or induced crashes.

Result

Quick, efficient and secure data retrieval capable of quickly identifying suspicious activity and fraudulent transactions.

- When least expected, they act quickly, maxing out credit cards and disappearing before they can be caught



Successful first party fraud is carried out by exploiting information that takes time to verify, that can be shared with other people, or that is simply overlooked due to the inability (or complexity) to properly link it to its source. By using real information such as telephone numbers and real addresses, scammers may appear to be regular clients, though these pieces of information can be used to create multiple identities.

How can OrientDB protect the Banking, Insurance and Online Retail industry?

By treating every edge and vertex as a JSON document, OrientDB allows properties to be assigned within relationships (links) themselves and does away with document stores all together. Its graph capabilities enable parts of or entire trees and graphs of records to be analyzed in just a few milliseconds. When it comes to quickly reading client data to find suspicious activity, multiple systems are simply not as effective.

E-COMMERCE

- E-commerce fraud relies on utilizing information which could possibly be shared with other clients
- IP addresses, credit card numbers, and cookies could all have multiple combinations

About OrientDB

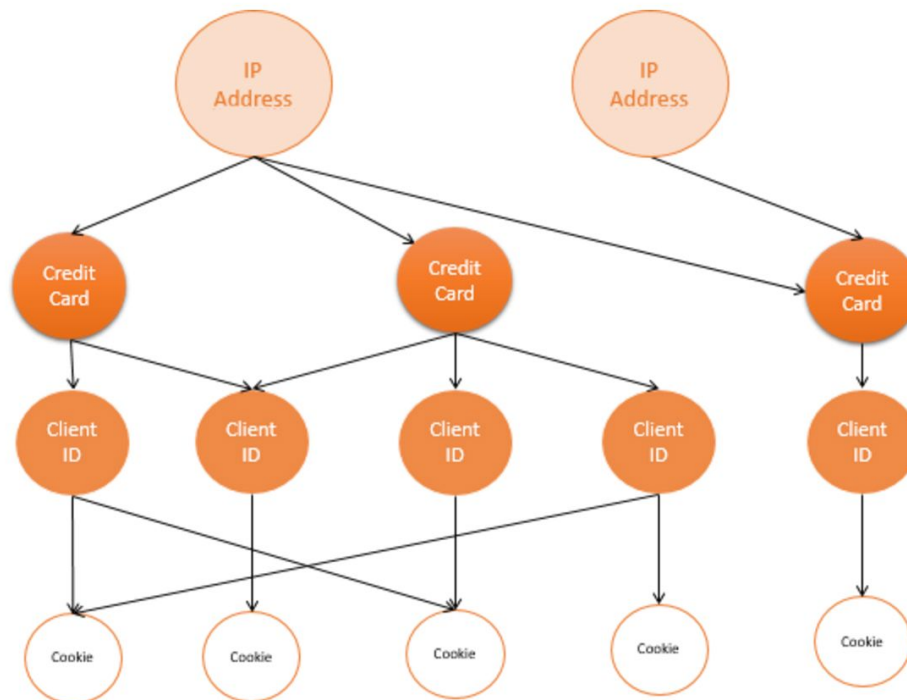
“With the release of OrientDB 2.1 and breakthrough innovation in OrientDB 2.2, we are building the industry’s first distributed document-graph database.” said Luca Garulli, CEO and Founder of OrientDB. “When I started to work on OrientDB back in 2010, I could barely imagine the pace of growth we’re seeing today thanks to our customers, users and advocates.” Ranked second most popular graph db by DB Engines, sixth document store and seventh key value store. It’s within the top ten in all three categories and steadily climbing the charts. Combining various models into one multi-model engine makes OrientDB a powerful, easy to use tool that doesn’t limit its users to adopt a single DB model.

Contact Info



enquiries@orientdb.com

- Detecting fraudulent transactions online is achieved through the correct analysis of suspicious patterns involving tracking cookies, user IDs, IP addresses and credit card information
- A single IP address utilizing multiple credit cards, with different Client IDs and shared cookies should raise flags for suspicious activity.



OrientDB guarantees Ecommerce Safety

System reliability is also of utmost importance for companies dealing with millions of transactions while safekeeping sensitive personal information. Server node crashes can lead to lost data as well as leave systems vulnerable. OrientDB uses WAL (Write Ahead Logging) to restore database content after a crash. Any pending transactions are automatically rolled back. Immediately, the server cluster redistributes the load across the available nodes and all the clients connected to the node in failure are automatically switched to an available server node with no fail-over to the application level.

The new security features introduced in OrientDB 2.2 provide an extensible framework for adding external authenticators, password validation, LDAP import of database roles and users, advanced auditing capabilities, and syslog support. OrientDB Enterprise Edition provides Kerberos authentication full browser SPNEGO support. When it comes to database encryption,



WHITE PAPER

Fraud & Security

starting with version 2.2, OrientDB can encrypt records on disk. This prevents unauthorized users from accessing database content or even from bypassing OrientDB security.

A Simple Choice

OrientDB is a 2nd Generation Open Source distributed graph-document database where every vertex and edge is a JSON Document. It supports schema-less, schema-full and schema-mixed modes, has a strong security profiling system based on user and roles and supports SQL amongst the query languages. It is incredibly fast, storing 220,000 records per second on common hardware and allows one to traverse parts of or entire trees and graphs of records in a few milliseconds. Its multi-model approach lends itself to easily and efficiently link database types to maximize performance.

Ranked 2nd most popular graph DB by DB engines, 6th document store and 7th key value store, it's within the top 10 in all 3 model categories and steadily climbing the charts. Combining various models into one engine makes it a powerful, easy to use tool that doesn't limit its users to adopt a single DB model.

OrientDB comes in two editions. The Community Edition is open source and free for any use (Apache 2 license). For those companies looking for Professional Support, Consultancy and additional advanced enterprise features, OrientDB Enterprise Edition is available upon request. Fortune 500 companies, government entities and startups all use this technology to build large-scale innovative applications. Clients include the United Nations, Ericsson, Sky, CenturyLink and Sonatype. OrientDB is the winner of the 2015 Infoworld Bossie award and has been covered by multiple media outlets.

Replacing your DBMS, once it no longer meets requirements, can be a huge cost in time and resources. Is your database powerful, scalable and flexible enough to grow with you? OrientDB also reduces the need to support multiple products to achieve your goals. See for yourself, give it a try! If you would like to receive more information about OrientDB and its capabilities, send us a message at enquiries@orientdb.com.