

Intel® AI Technologies Help Onesait Smart Fraud Reduce Fraudulent Activities

2nd Gen Intel Xeon® Scalable processors help recognize new fraud patterns, giving fraud analysts stronger, more accurate detection, and management tools



Intel®
AI Builders
Member



minsait

Fraud detection is an expensive catch-up game. Bad actions are detected through a rules engine that looks at transactions—often after they have taken place. Fraud analysts then review activities to determine if a fraudulent activity occurred. Some modernized systems with in-memory computing solutions can detect activities in real-time. But whether the action is detected as it happens or after the fact, many of these activities end up being false positives, meaning that the transactions were genuine and not fraudulent.

False positives are costly. They take up precious time by experts who need to focus on real fraudulent activities. They also can impact customer experience by rejecting a transaction—40 percent of U.S. shoppers experience blocked or questioned transactions¹—or even freezing an account, requiring the customer to intercede on his or her own behalf. Those blocked transactions result in billions of dollars in lost revenue each year for merchants.² So, while fraud itself costs e-commerce merchants 7.6 percent of their annual revenues, false positives result in 2.8 percent of lost revenues each year.³

The financial and payments sectors have heavily relied on rule-based systems, which often capture limited knowledge about fraud patterns, cannot detect fraud based on new schemas, and do not leverage customers' regular activity profiles. As a result, advanced fraud goes undetected, and the fraud analysts' team must handle thousands of false positives on a daily basis, which increases fraud management costs.

Onesait Smart Fraud—AI-based Fraud Detection

Today's layering of the best fraud detection schemes is not enough. [Minsait](#), an [Indra](#) company, developed [Onesait Smart Fraud](#), a customer-centric, real-time fraud detection solution for financial services, banking, and electronic payments and transfers. With pioneering artificial intelligence (AI) and machine learning (ML) techniques capable of replicating the experience, procedures, and working methods of specialized banking analysts, the solution greatly enhances the levels of fraud protection, reducing both fraud and false positives.

AI-powered Fraud Detection

Onesait Smart Fraud leverages a unified data model and a wide range of detection techniques that go beyond rule-based systems to track customer activities across multiple channels and data sources. The solution features machine learning algorithms to detect known fraud patterns, neural networks to detect unknown fraud techniques, and an in-memory computing profiling system to spot suspicious customer behavior. It also supports context-based and workflow-based rules that leverage existing fraud expertise in the organization. Finally, it provides a full-featured web-based interface—called Smart Fraud Manager—to support fraud management processes across its lifecycle.

Onesait Smart Fraud comprises the following components:

- **Smart Fraud Engine** – implements detection capabilities based on low-latency ML and AI models, an in-memory computing profiling system, and a rules-based engine.
- **Smart Fraud Manager** – provides a management interface for fraud analysts and supervisors to investigate cases.
- **Smart Fraud Training System** – features offline machine learning training processes required for ML, AI, and model profiling.
- **NoSQL database** – a MongoDB database.

The solution can be deployed in any enterprise infrastructure on modern Linux distributions, including Red Hat Enterprise Linux (RHEL), CentOS, and Ubuntu. The software and algorithms are built on TensorFlow, Keras, scikit-learn, and Python.

Taking advantage of 2nd Gen Intel Xeon Scalable Processors

Smart Fraud leverages advanced artificial intelligence and machine learning techniques. These accurately model legitimate customer behavior and generalize fraud patterns, making them more suitable for detecting unknown fraud patterns and reducing false positives.

The techniques and algorithms are accumulated into the Smart Fraud ML Training System component built on industry-standard frameworks and programming languages. The Smart Fraud Training System benefits from tools for ML workloads on 2nd Gen Intel® Xeon® Scalable processors, including Intel Optimizations for TensorFlow with AI-enabled Intel Math Kernel Library for Deep Neural Networks (Intel MKL-DNN) and Intel Distribution of Python. These Intel AI technologies leverage the built-in capabilities of Intel architecture to accelerate machine learning training, which

allows new models to be quickly deployed to the Onesait Smart Fraud solution.

Results

Smart Fraud, with its advanced AI-powered fraud detection capabilities, reduces fraud management operational costs, decreases false positives ratios, and increases accuracy of fraud detection compared to rule-based solutions. The solution is being used by fraud analysts across a number of banking and payments companies to detect fraud cases. Analysts are able to quickly investigate and prevent funds from reaching bad actors' accounts.

Bankia and Minsait are collaborating on a market-leading implementation for fraud detection and prevention and cybersecurity anomaly recognition. [Bankia](#) is a nationwide Spanish financial institution. With a universal banking model based on multichannel management, it specializes in providing services to individuals and companies.

The collaboration between Minsait and Bankia will leverage both organizations' AI and machine learning expertise and algorithms and Bankia data, plus other work being done together in machine learning and neural networks. Together they "envis-age the development of an anti-fraud solution with a rapid and reliable response capability that will make it possible to address current and future challenges in this field."⁴

Conclusion

Intel AI technologies can reduce the effort required to train new Onesait Smart Fraud models to accelerate deployment. In a dynamic and ever-changing environment like banking and payments fraud, being able to retrain models in a timely manner is key to detecting new fraud patterns and stopping most recent fraud schemas.

For more information about Minsait, visit [minsait.com](#)

Learn more about the Intel AI Builders program at [builders.intel.com/ai/membership](#)

Intel®
AI Builders
Member

Minsait is a digital transformation consultancy and IT firm with offices in Spain and Latin America. Minsait possesses a high degree of specialization and knowledge in applying modern technologies, such as AI and machine learning, to solve some of the most demanding problems that business and industry face.

Rafael San Miguel Carrasco, Senior Specialist, and Adrián López de Lucas, Data Solutions Architect, were both involved in this project with Intel on behalf of Minsait.

¹ <https://www.creditcards.com/credit-card-news/fraud-alert-blocked-poll.php>

² <https://www.javelinstrategy.com/press-release/false-positive-card-declines-push-consumers-abandon-issuers-and-merchants>

³ https://www.lloydsbankcardnet.com/content/pdf/Lloyds_AI_Fraud_Whitepaper.pdf

⁴ <https://www.minsait.com/en/news/media-room/bankia-and-minsait-team-reduce-bank-fraud-and-cybersecurity-anomalies>

Performance results are based on testing as of dates shown in configuration and may not reflect all publicly available security updates. No product can be absolutely secure. See configuration disclosure for details.

Intel's compilers may or may not optimize to the same degree for non-Intel microprocessors for optimizations that are not unique to Intel microprocessors. These optimizations include SSE2, SSE3, and SSSE3 instruction sets and other optimizations. Intel does not guarantee the availability, functionality, or effectiveness of any optimization on microprocessors not manufactured by Intel. Microprocessor-dependent optimizations in this product are intended for use with Intel microprocessors. Certain optimizations not specific to Intel microarchitecture are reserved for Intel microprocessors.

Performance tests, such as SYSmark and MobileMark, are measured using specific computer systems, components, software, operations and functions. Any change to any of those factors may cause the results to vary. You should consult other information and performance tests to assist you in fully evaluating your contemplated purchases, including the performance of that product when combined with other products. For more complete information visit: <http://www.intel.com/performance>

© Intel Corporation. Intel, the Intel logo, and other Intel marks are trademarks of Intel Corporation or its subsidiaries. Other names and brands may be claimed as the property of others.