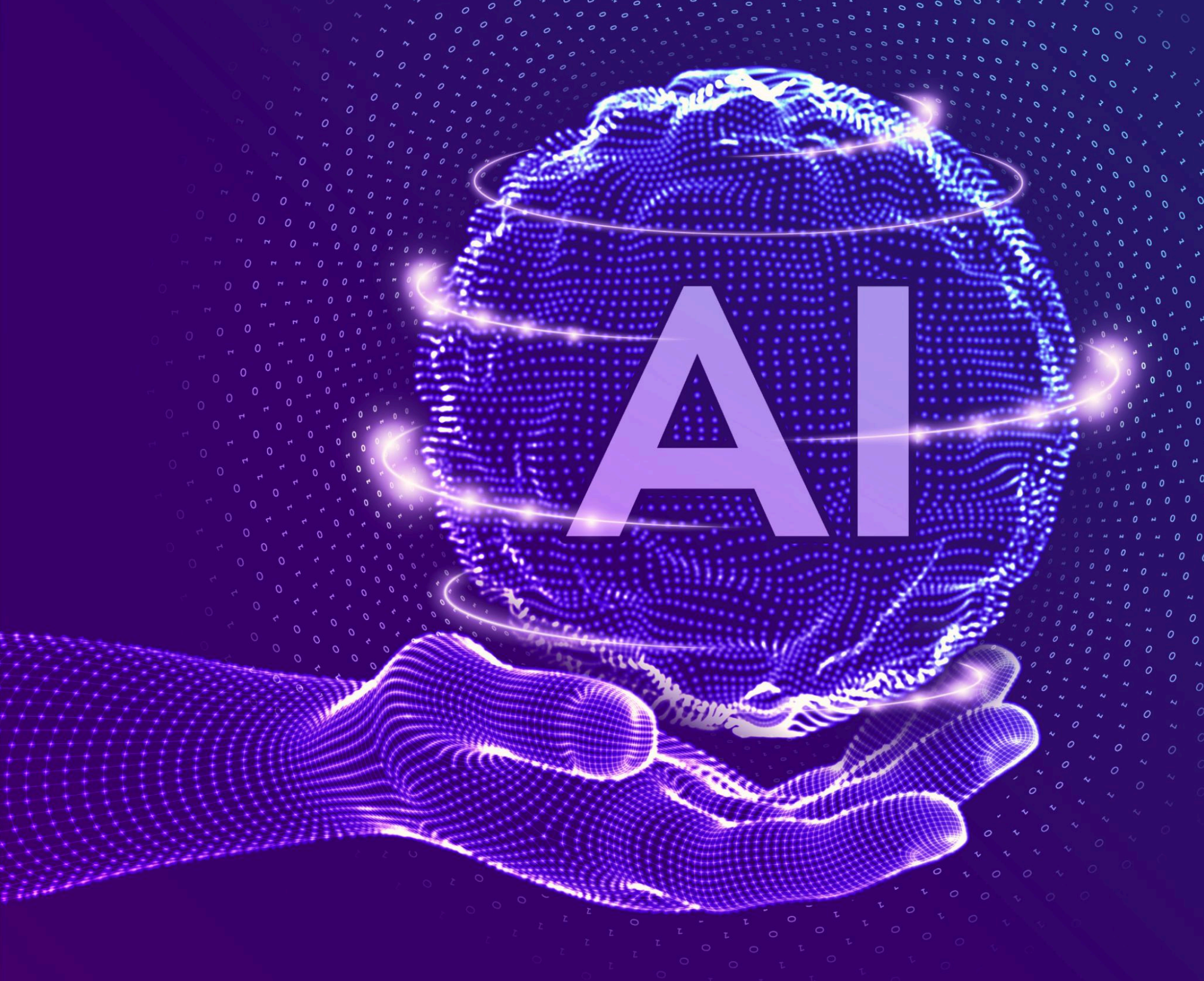
FRIENDLY TECHNOLOGIES
ZFORT GROUP



AI/Big Data

Case Study

Detecting Scammers

Overview

Fighting fraud is a noble cause. Using Artificial Intelligence to fight fraud is a smart strategy.

Background

Our client runs a service that detects scammers and spammers within customers' platforms. There are thousands and thousands of users over hundreds of projects. These projects are totally different in nature and niche, but they have something in common:

- Thousands of legit users.
- Hundreds of fraudsters.

Our client has been fighting the malevolent users for years - algorithmically. What if we utilize AI on this mission?

Challenges

- Number of users we have to analyze is several million.
- The number of profile parameters we have to take into account is 100+.
- In addition to just pieces of data, we have to analyze behavior.
- The profile patterns and behavior patterns evolve over time.

Solution / Approach

- Build a service that ingests data about users and stores it in a format suitable for several different neural networks.
- Prepare a dataset of users that are 100% good or 100% scammers.
- Train the neural networks on the provided dataset.
- Analyze the rest of the users and assign them a risk score based on feedback from the neural networks we used.
- Implement a notification service.
- Automate the majority of operations, so that the Scammer Detection Service can start from scratch in as little time as possible.

Workflow / Analysis Phase

- We identified the profile data pieces that can be used by AI.
- We identified the UGC (user-generated content) that can be used by AI.
- We identified the events triggered by users that can be used by AI.
- We identified the suitable neural networks that can take advantage of the data.
- We designed a storage model compatible with the data and the neural networks.

Workflow / Implementation Phase

- We ran several ad hoc tests to see if the results were acceptable. They were great.
- We built the full cycle analysis service and deployed it to 2 different projects.
- We observed the functioning of the service for several months and adjusted the system regularly.
- Once we were sure we did at least 80% of what we could do, we deployed the service to a multitude of projects.
- We automated the most frequent operations so that the service can be managed by personnel without any specific knowledge.

Technologies

- TensorFlow
- PyTorch
- Apache Spark
- Google BigQuery
- Docker
- PHP + React
- GCP

Team Size

- Business Analyst / Data Analyst
- Architect
- Tech Lead
- AI Specialist
- Back-End Developer
- Front-End Developer
- QA Engineer
- DevOps
- Project Manager

Outcomes

- Hidden scammers revealed.
- New scammers detected **70%** faster than in the previous approach.
- The human experts need to spend **50%** less time reviewing complex cases.
- Users feel more protected and trust the client project more.

Lessons Learned

- The more data you have the better results of AI / ML implementations.
- Two neural networks are better than one. Three is better than two.
- Modern fraudster problems require modern solutions.

Contact Information

To coordinate next steps please contact:

✉ Mail: **contact@zfort.com**

☎ Tel: **+1 202 9602900**

LinkedIn: **zfort-group**

ZFORT GROUP - YOUR RELIABLE PARTNER