ISACA Netherlands Chapter
Risk Event 2023

Investing in and building (fin)techs, does AI play a role?

Observations from the experience of building DEGIRO and beyond

Jasper Anderluh

November 16th – ISACA Risk Event 2023 Bussum

What is this presentation NOT about?

Not about “how to use ChatGPT for IT Risk Audit”

A topic like this could be better treated by an IT Risk Auditor

Not About “how to use ChatGPT for Software Development”

Would be very interesting theme, certainly important to consider from IT Risk perspective.

Then, what IS it about?

The wholy grail (fin)tech platform

From the DEGIRO adventure in a nutshell to where to go next.

How does AI fit into achieving this holy grail platform

What data is collected and how AI could be applied to achieve the goals of the where-to-go next platform.

What are the IT Risk considerations because of the application of AI

Try to give some insights based on an example platform architecture.

DEGIRO

Started in 2013 with 35 people, 1 country, 0 clients, in-house system build.

Active in 18 European countries in 2015 with 150.00 clients (in top 20 of European Brokers)

Sold in 2019 with 650.000 clients (in top 5 of European Brokers)

Now with over 2.5 million clients all over Europe, the number 1 and only true pan-European Broker

Illustratie: Rhonald Blommestijn voor het FD, Sept 12th 2020

Fintech companies are the symbiosis of ONLINE PLATFORMS and FINANCIAL SERVICES

ONLINE PLATFORM

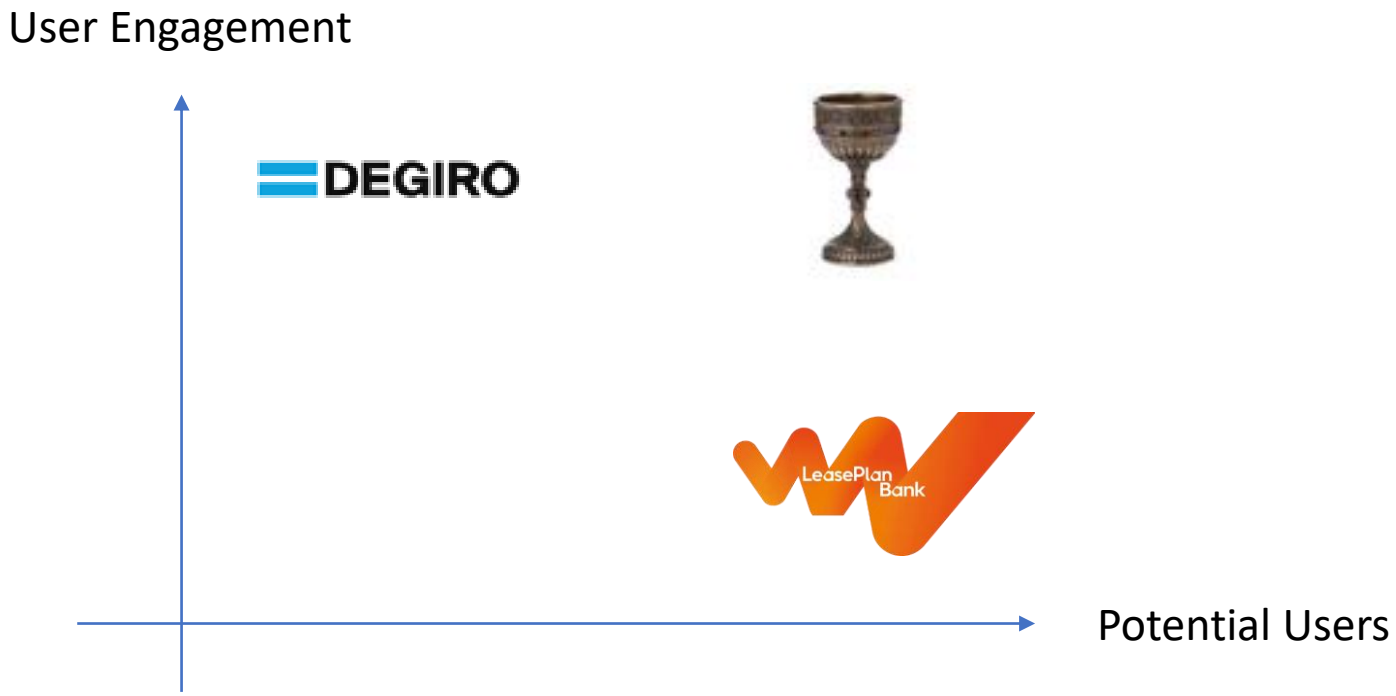
So, on one side you have branding and marketing automation to get users in for the right CPA, then try to engage, activate, upsell and retain them. All to create the growth potential of an online platform / tech company with economies of scale.

PRIVACY

FINANCIAL SERVICES

On the other side you are Regulated and have the KYC, AML, Market Abuse, Target Group, Information Transparancy, Business Integrity, Compliance

The **Holy Grail** is to find an offering that is of interest to many users and has a high user engagement.



What pieces of the puzzle should be there (at least)?

Online, easy to complete but compliant, cost-savvy onboarding flow for users.

Streamlined, efficient and automated business processes, where system follows process and not the other way around.

AI

Relevant (preferably personalized) product offering which is lived up to. In order to generate growth, good retention rates make a huge difference.

Correct and efficient regulatory and geographical setup, otherwise competition beats you.

A well-functioning, hands-on, problem-solving, product believing TEAM.

Holy Grail

Payments / Purchases by Consumers

Neo Banks
PSD2 licencees
Relevant Reach

What are examples of AI modelling that could contribute to the holy grail?

Transaction categorisation for budgetting features

Transaction behaviour analysis for credit worthiness

Transaction behaviour analysis to target individuals for services

Transaction recognition for subscriptions

Transaction analysis for loyalty

Transaction analysis for market segmentation

SCOUPY

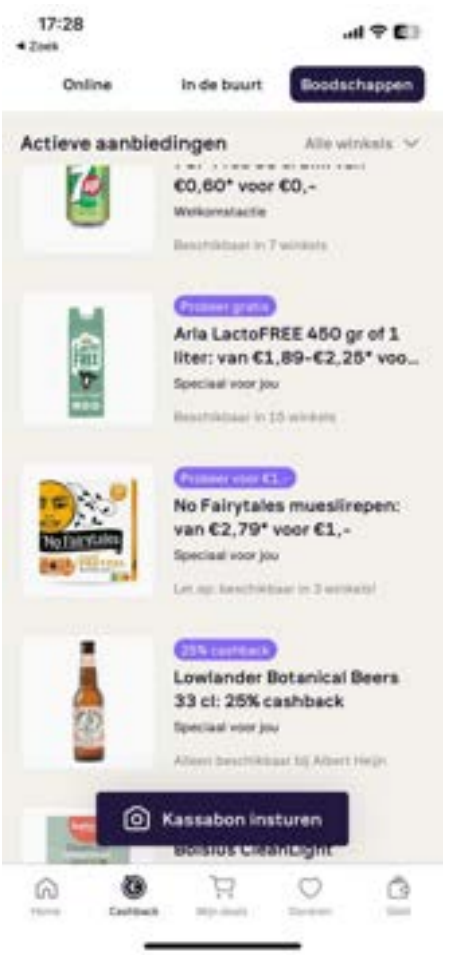
OCR Receipts
Product recognition
Brand recognition
Category recognition

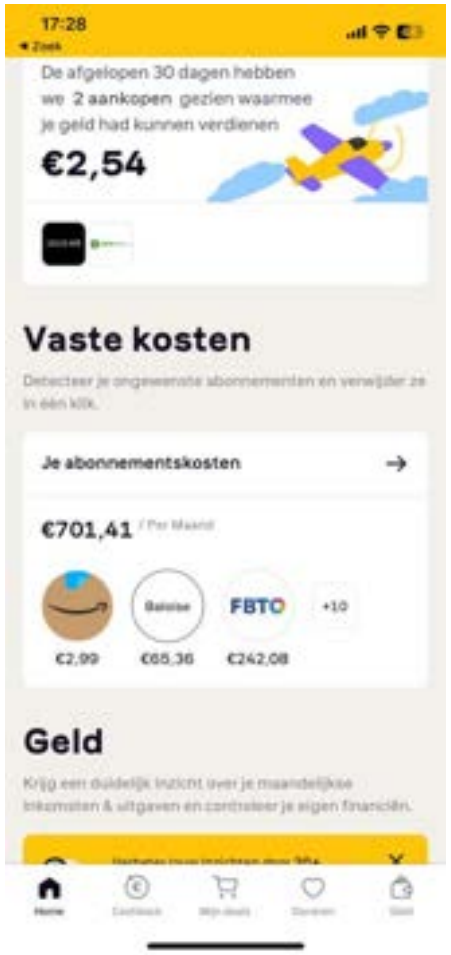
budgetbakers

Connect bank
Categorise transactions
Merchant recognition

Relevant offerings

woolsocks
the money app





IT Security Risks

The Risk : Personal Data Leakage

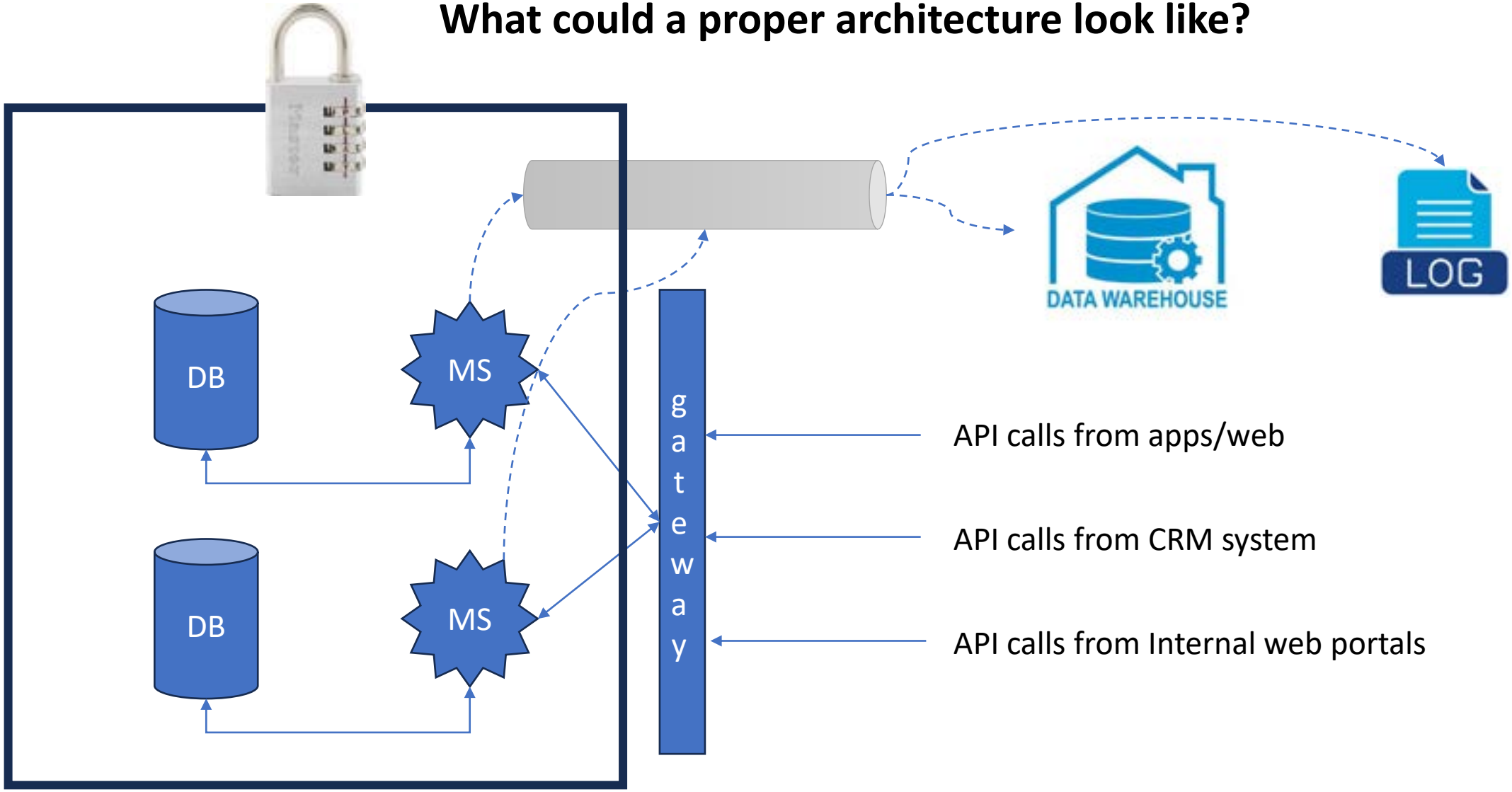
AI models are trained using (personal) data: where is it stored (think of dedicted tools), etc.
AI models can detect patterns in, at first sight, non-personal data and make those data personal data. Is data classification taking this into account?

Another Risk : Unfair treatment

AI models might be trained using biased data: how to detect this?

Model-only based decisions should be possible to explain to users. How to in a black-box?

What could a proper architecture look like?



What about the data

Encryption and Secrets

Personal Data is encrypted in the databases **and** in the data warehouse

Individual, per-user Encryption keys should be used

Rotating secrets injected into micro services

Locked Production Environment

Production environment only contains automated, 4-eyes approved, deploys (e.g. Jenkins)

Logs are stored outside of production environment and should **not** contain personal data. No developer access needed for IT ops.

Api access only for authorized access and refresh tokens.

To Summarize….

Modern Holy Grail Platform

Contains a lot of (personal) data

Uses AI modelling to perform some functions

Is developed by pragmatic, hands-on and well-motivated team

IT Risks to be considered

Data is distributed over (sub)systems: could AI discover patterns in the non-personal data in these isolated (sub)systems that make it personal?

Even if data in databases is encrypted, where is the data stored for training the models and is this safely done?

Is the conflict between the pragmatic, hands-on team and needed “lock” on the production environment balanced?

?

Thank you