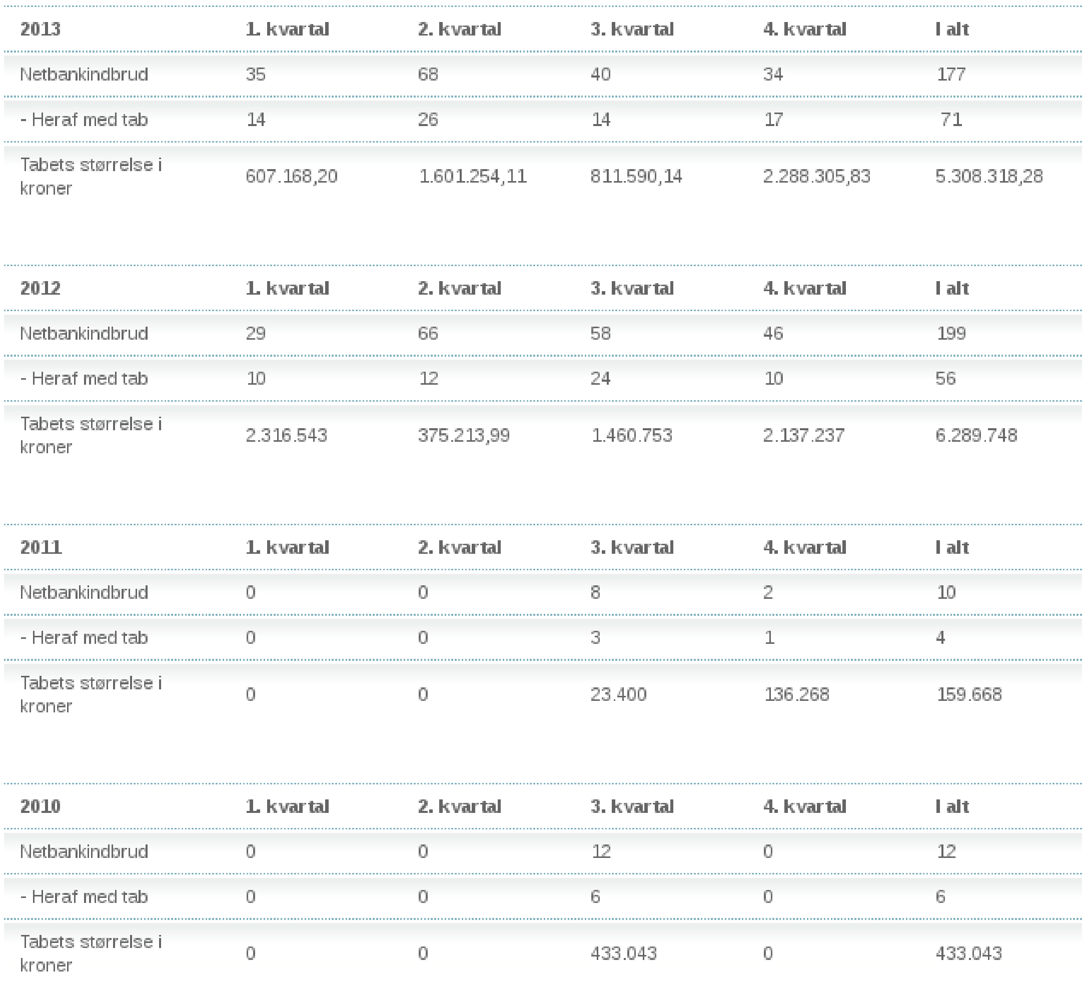
Machine Learning for Fraud Detection

Dídac Rodríguez Arbonès
didac@di.ku.dk

Fraud

- Fraud in Denmark is a substantial issue.
- The financial institutions are keen on prevention.
- It is a very difficult problem to solve.
- Substantial resources are dedicated to fight against it.



2013	1. kvartal	2. kvartal	3. kvartal	4. kvartal	I alt
Netbankindbrud	35	68	40	34	177
- Heraf med tab	14	26	14	17	71
Tabets størrelse i kroner	607.168,20	1.601.254,11	811.590,14	2.288.305,83	5.308.318,28

2012	1. kvartal	2. kvartal	3. kvartal	4. kvartal	I alt
Netbankindbrud	29	66	58	46	199
- Heraf med tab	10	12	24	10	56
Tabets størrelse i kroner	2.316.543	375.213,99	1.460.753	2.137.237	6.289.748

2011	1. kvartal	2. kvartal	3. kvartal	4. kvartal	I alt
Netbankindbrud	0	0	8	2	10
- Heraf med tab	0	0	3	1	4
Tabets størrelse i kroner	0	0	23.400	136.268	159.668

2010	1. kvartal	2. kvartal	3. kvartal	4. kvartal	I alt
Netbankindbrud	0	0	12	0	12
- Heraf med tab	0	0	6	0	6
Tabets størrelse i kroner	0	0	433.043	0	433.043

http://www.finansraadet.dk/tal--fakta/Pages/statistik-og-tal/netbankindbrud---statistik.aspx

NEM ID

Avtale Giro

DK

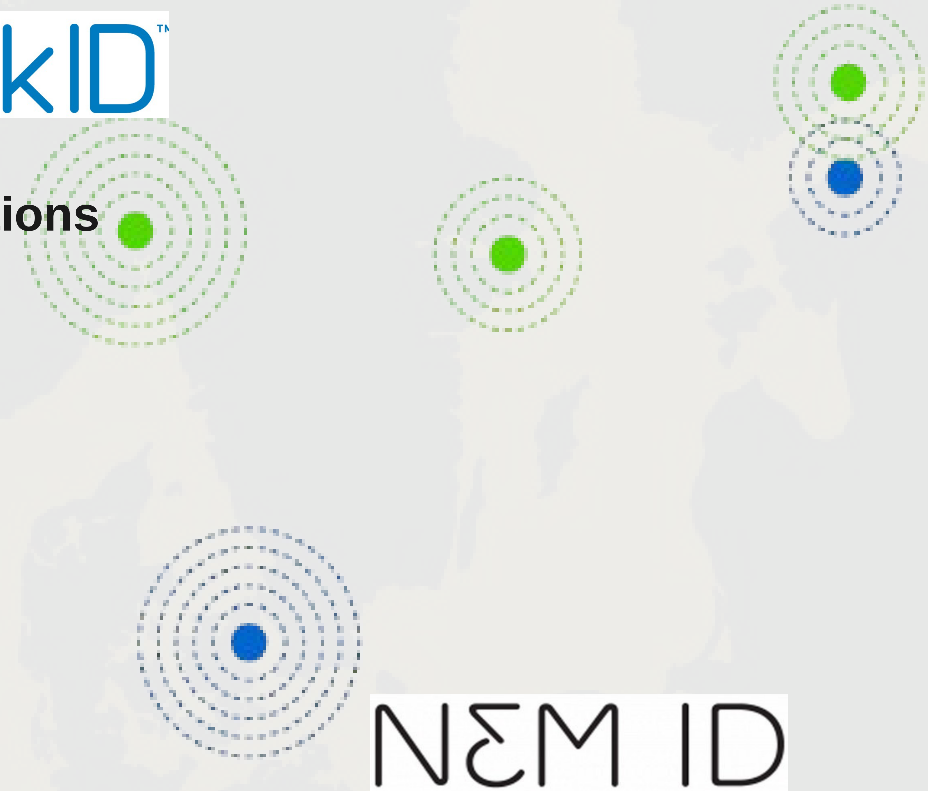
nets

e Faktura

e Boks.dk

BS BETALINGSSERVICE

Coverage



bankID

6 M users
~500 M transactions

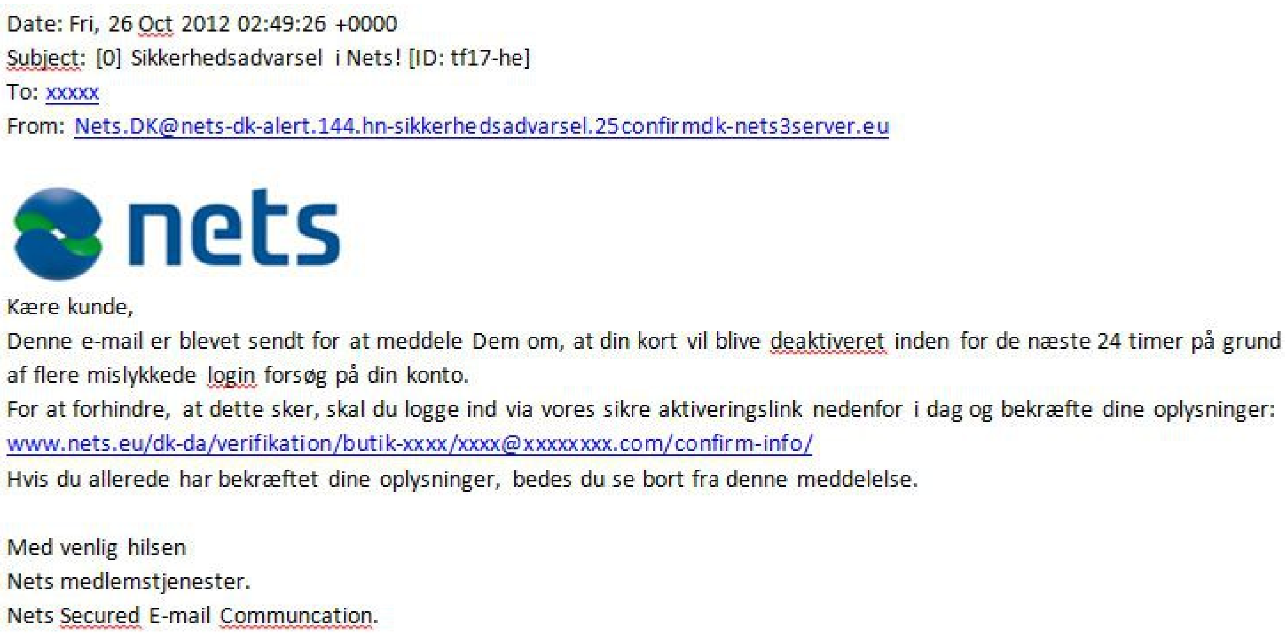
NEM ID

4,5 M users
~145,5 M transactions

Overview of project

- Develop a prevention mechanism against online banking cyber-crime using machine learning (ML).
- Detection capable of identifying fraudulent authentication sessions in NemID.
- Possibility of working within other company IT assets.
- Project to be deployed to BankID in Norway and NemID in Denmark adding to the security measures currently in place.
- Self-updating and minimal operation intervention.

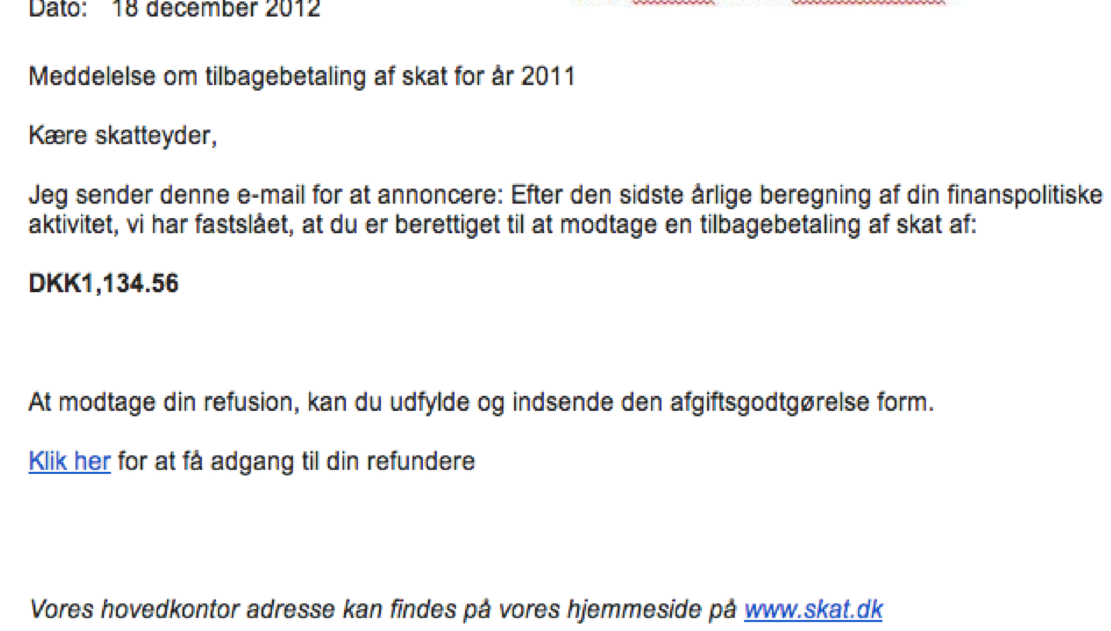
Phishing



Date: Fri, 26 Oct 2012 02:49:26 +0000
Subject: [0] Sikkerhedsadvarsel i Nets! [ID: tf17-he]
To: xxxxx
From: Nets.DK@nets-dk-alert.144.hn-sikkerhedsadvarsel.25confirmdk-nets3server.eu

Kære kunde,
Denne e-mail er blevet sendt for at meddele Dem om, at din kort vil blive deaktiveret inden for de næste 24 timer på grund af flere mislykkede login forsøg på din konto.
For at forhindre, at dette sker, skal du logge ind via vores sikre aktiveringslink nedenfor i dag og bekræfte dine oplysninger:
www.nets.eu/dk-da/verifikation/butik-xxxx/xxxx@xxxxxxxx.com/confirm-info/
Hvis du allerede har bekræftet dine oplysninger, bedes du se bort fra denne meddelelse.

Med venlig hilsen
Nets medlemstjenester.
Nets Secured E-mail Communcation.



Dato: 18 december 2012

Meddelelse om tilbagebetaling af skat for år 2011

Kære skatteyder,

Jeg sender denne e-mail for at annoncere: Efter den sidste årlige beregning af din finanspolitiske aktivitet, vi har fastslået, at du er berettiget til at modtage en tilbagebetaling af skat af:

DKK1,134.56

At modtage din refusion, kan du udfylde og indsende den afgiftsgodtgørelse form.

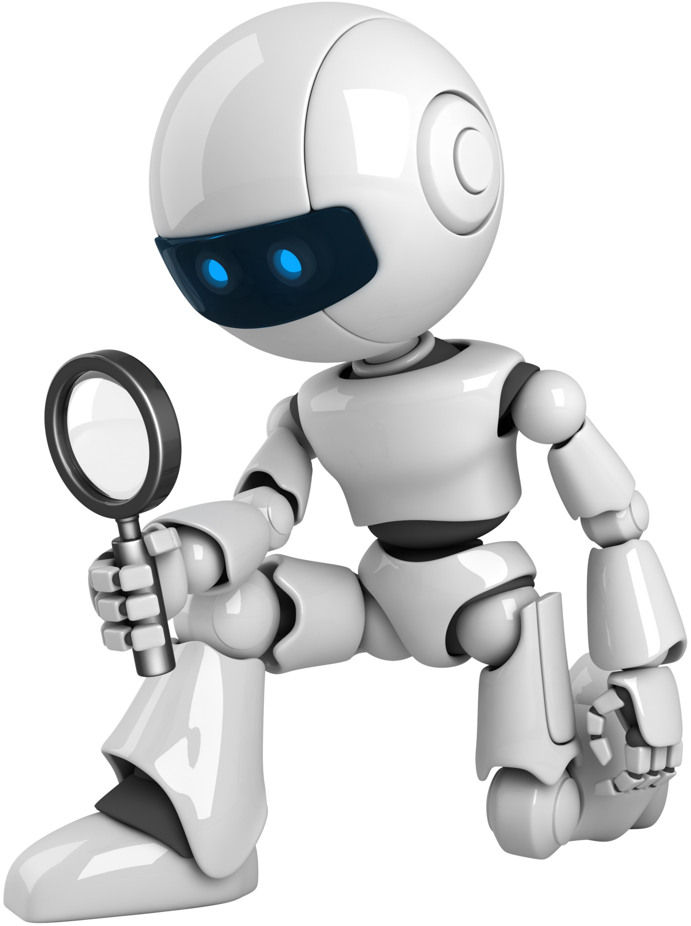
Klik her for at få adgang til din refundere

Vores hovedkontor adresse kan findes på vores hjemmeside på www.skat.dk

- It consists on redirecting the user to a malicious webpage.
- The user is unaware who is the information recipient.
- The criminals can use the credentials to authenticate to the systems.

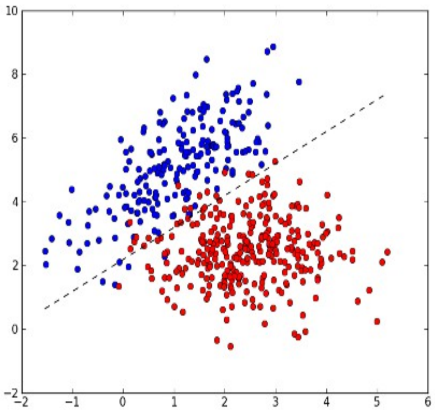
Machine learning

- Part of artificial intelligence.
- Ecompasses many algorithms to learn from data and make decisions on new events.
- Its power comes from the available information from the system.
- There is no one-size-fits-all, it is as good as the data it relies on.
- There are two major types:
  - Supervised
  - Unsupervised

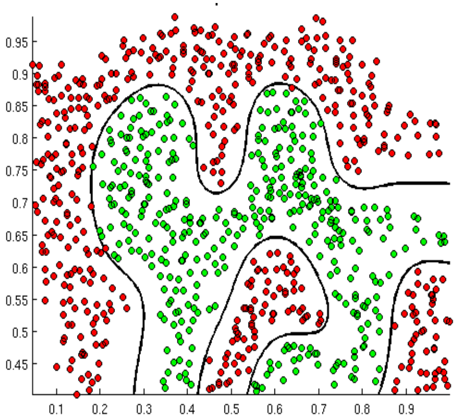


Machine learning

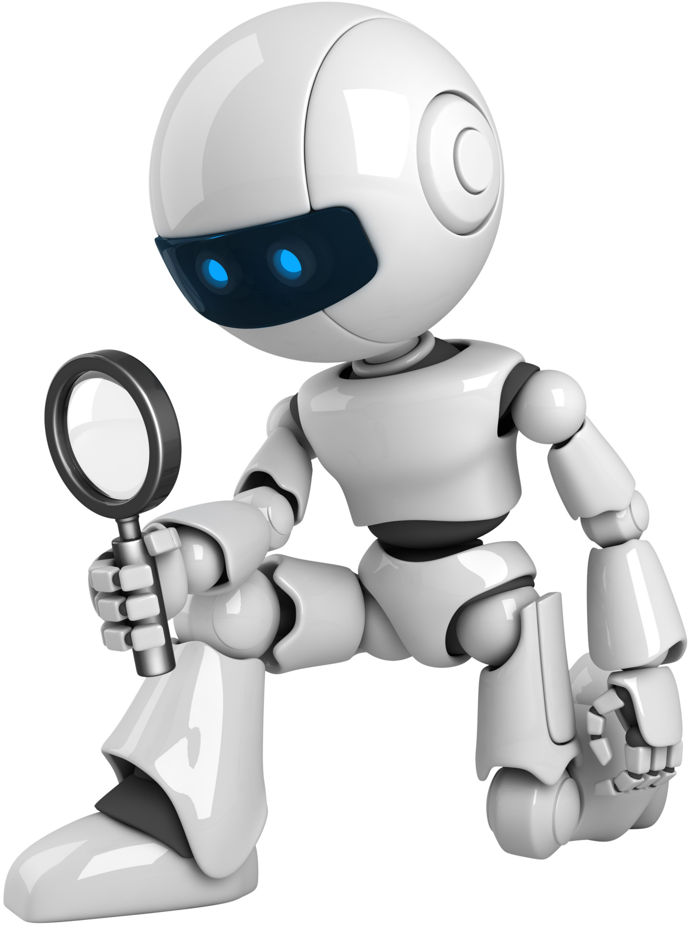
- Various levels of performance and requirements.
- Ensemble systems possible.
- Feature space reduction.



LDA

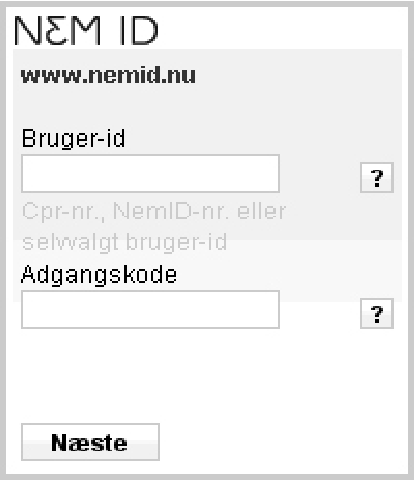


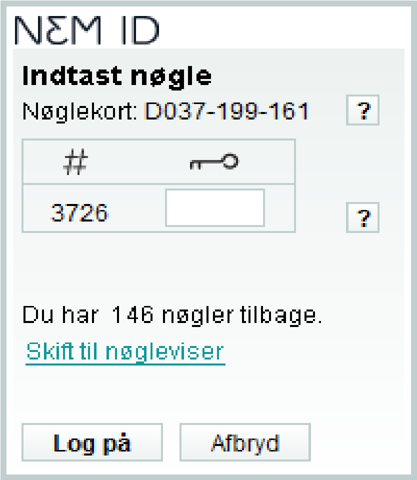
SVM



Data source

- The data is preprocessed and **anonymized** after it is collected from the login applet of the BankID.
- The data is complex and heterogenous:
  - Geographic information
  - Browser information
  - OS information
  - Timing information
- There are no reliable labels to be used for analysis.





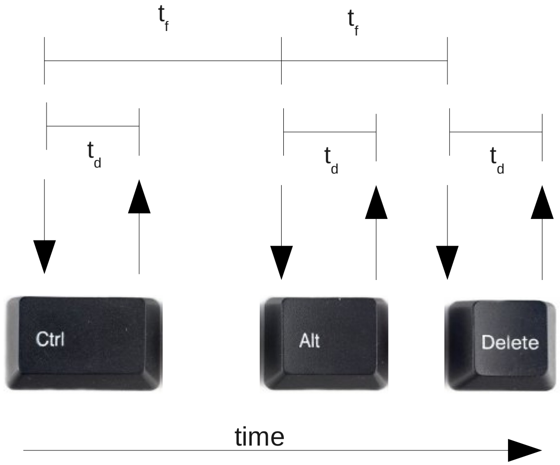
Nøglekort: D037-199-161

3726

Du har 146 nøgler tilbage.

Data source

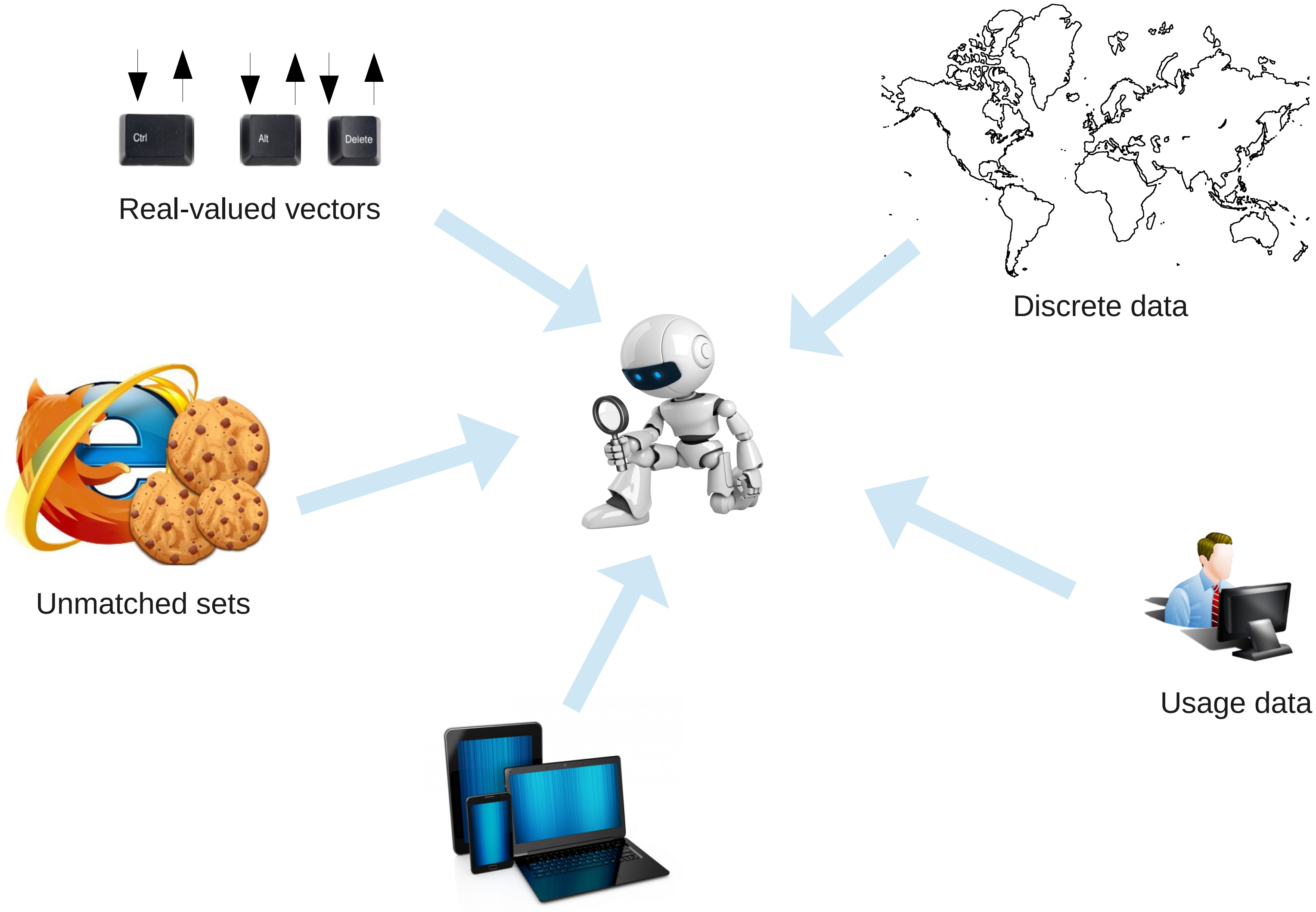
- An example of user data are keystrokes:



- There have been previous studies[1] achieving good results in classification only with this type of data.
- It relies on heavily on previous user knowledge.
- Unfortunately, this type of data is not enough on its own for a reliable fraud detection.

(1) Killourhy, Kevin S., and Roy A. Maxion. "Comparing anomaly-detection algorithms for keystroke dynamics." Dependable Systems & Networks, 2009. DSN'09. IEEE/IFIP International Conference on. IEEE, 2009

Data source



Real-valued vectors

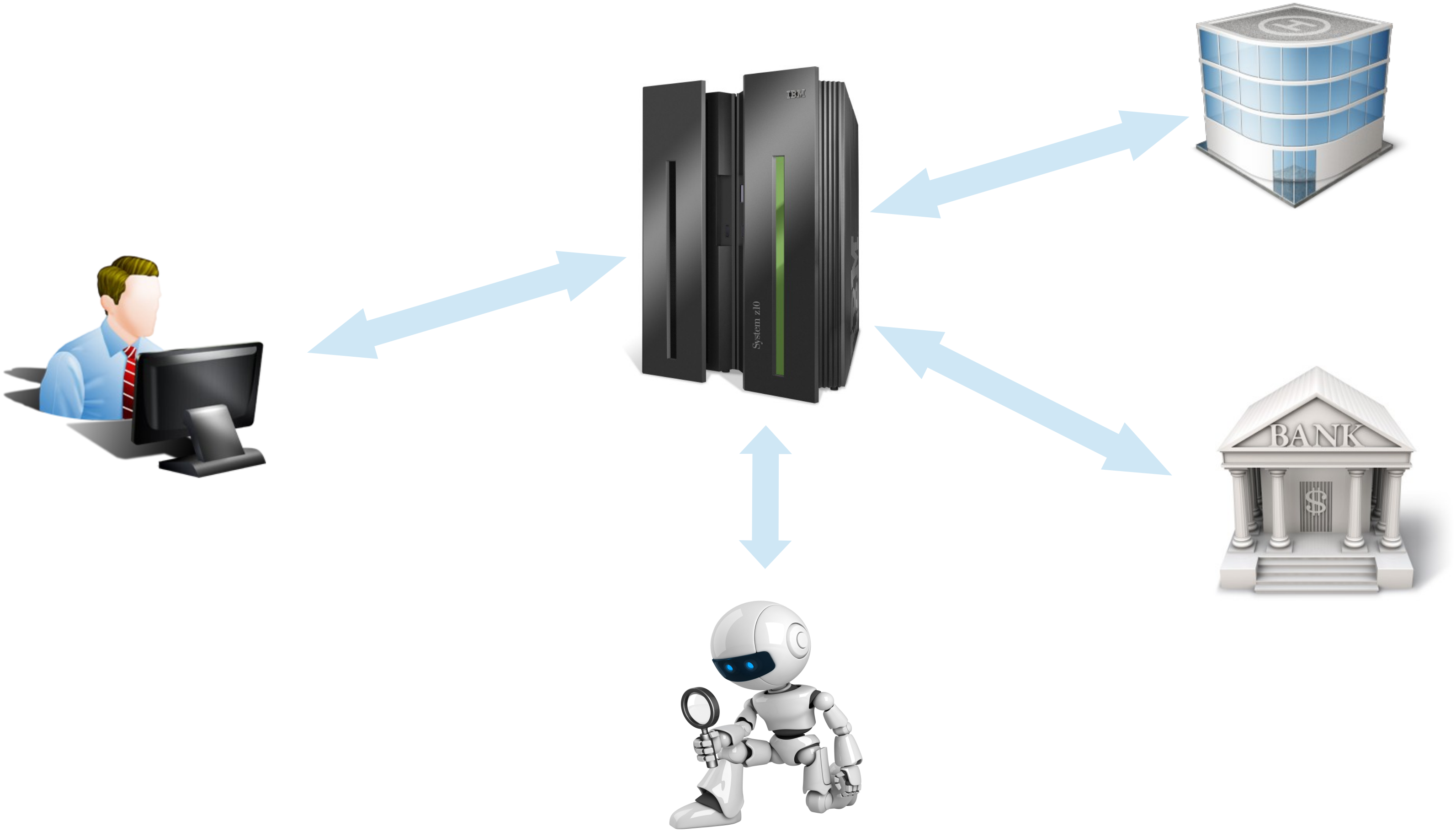
Discrete data

Unmatched sets

Usage data

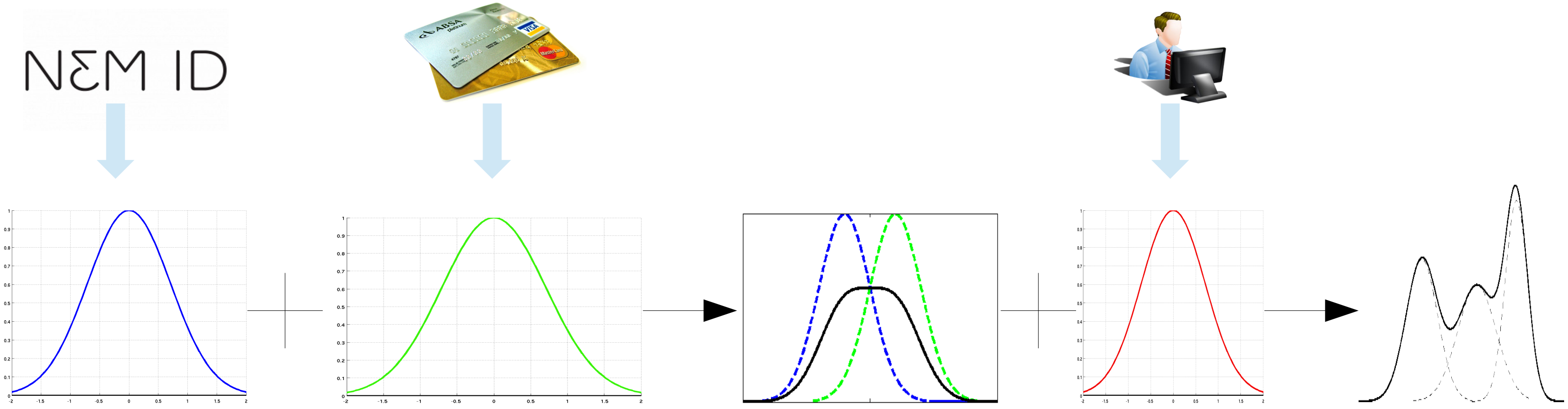
Device information

System overview



Other information sources

- Credit cards
- Individual transactions
  - Person-to-person
  - Crowd-to-person
- Web service usage
- Customer profiling



Challenges & expectations

- Thieves are smart.
- Sometimes **very** smart.
- There exist numerous companies around the globe with the only goal of illicit financial gain.
- It is humanly impossible to detect and stop them without unlimited resources.
- Legal & marketing concerns make datasets scarce and incomplete.

- Machine learning is an excellent candidate to pursue these actions in a scalable manner with low expense and effort.
- It can find patterns not directly obvious to humans.
- It can self-adapt to new events.

Industrial PhD practicalities

Danish Agency for Science Technology and Innovation
Ministry of Science Technology and Innovation

- The programme is funded by the Ministry of Higher education and Science (DASTI[1]).
- There are several application reviews during the year. It typically takes 2-4 months to receive an answer.
- The company is required to have physical presence in Denmark.
- The student is formally employed at the company.
- There is a supervisor both at the university and at the company.
- Time allocation is roughly 50%, if not otherwise agreed.
- There is a budget allocated for the university expenses and a subvention for the company.
- Usually any patent or profitable outcome from the project is property of the company (IP agreement), but there has to be a scientific dissemination component.

(1) http://ufm.dk/en