GreenFlux
Smart charging

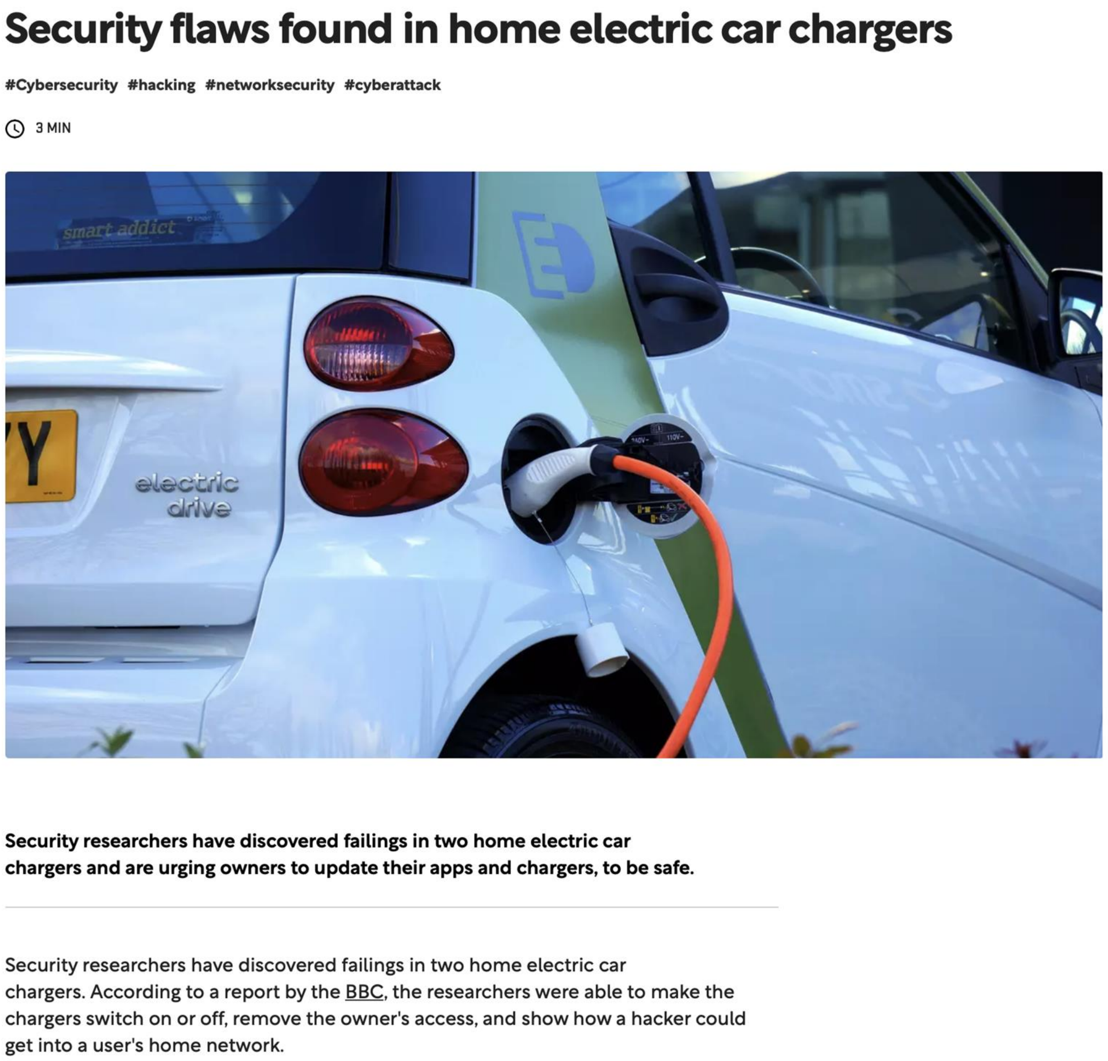
CARAMEL

Electromobility Pillar

2nd OEM Workshop

16-11-2021

Security flaws in EV charge stations



Security flaws found in home electric car chargers

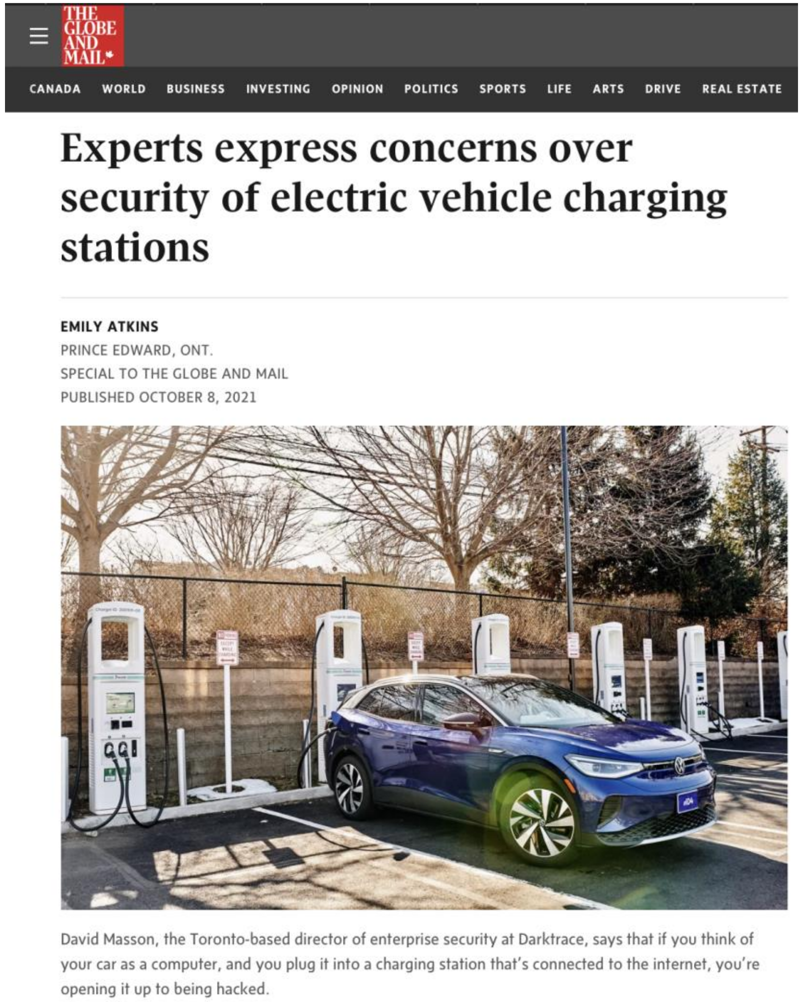
#Cybersecurity #hacking #networksecurity #cyberattack

3 MIN

Security researchers have discovered failings in two home electric car chargers and are urging owners to update their apps and chargers, to be safe.

Security researchers have discovered failings in two home electric car chargers. According to a report by the BBC, the researchers were able to make the chargers switch on or off, remove the owner's access, and show how a hacker could get into a user's home network.

Retrieved from cybermagazine.com, 1 August 2021



Experts express concerns over security of electric vehicle charging stations

EMILY ATKINS
PRINCE EDWARD, ONT.
SPECIAL TO THE GLOBE AND MAIL
PUBLISHED OCTOBER 8, 2021

David Masson, the Toronto-based director of enterprise security at Darktrace, says that if you think of your car as a computer, and you plug it into a charging station that's connected to the internet, you're opening it up to being hacked.

Retrieved from theglobeandmail.com, 8 October 2021

Agenda

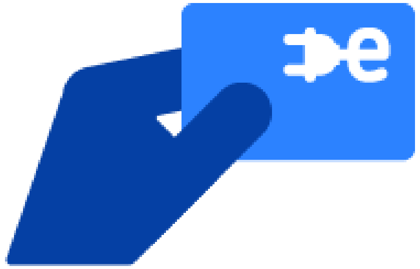
1. Recap
2. Communication Protocols
3. Communication Architecture
4. Preliminary anomaly detection results
5. ML Pipeline deployment

Recap

EV Charging Ecosystem

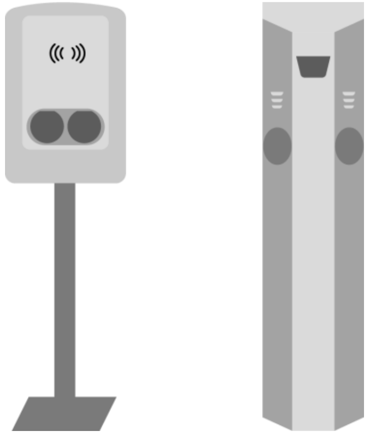
eMSP

An e-Mobility Service Provider (eMSP) is a market role offering an EV charging service to EV drivers. An eMSP provides value by **enabling access to a variety of charge stations** around a geographic area.



CPO

A CPO is responsible for installation, operation and maintenance of charge stations. A CPO provides value by **connecting smart charging devices to eMSPs**

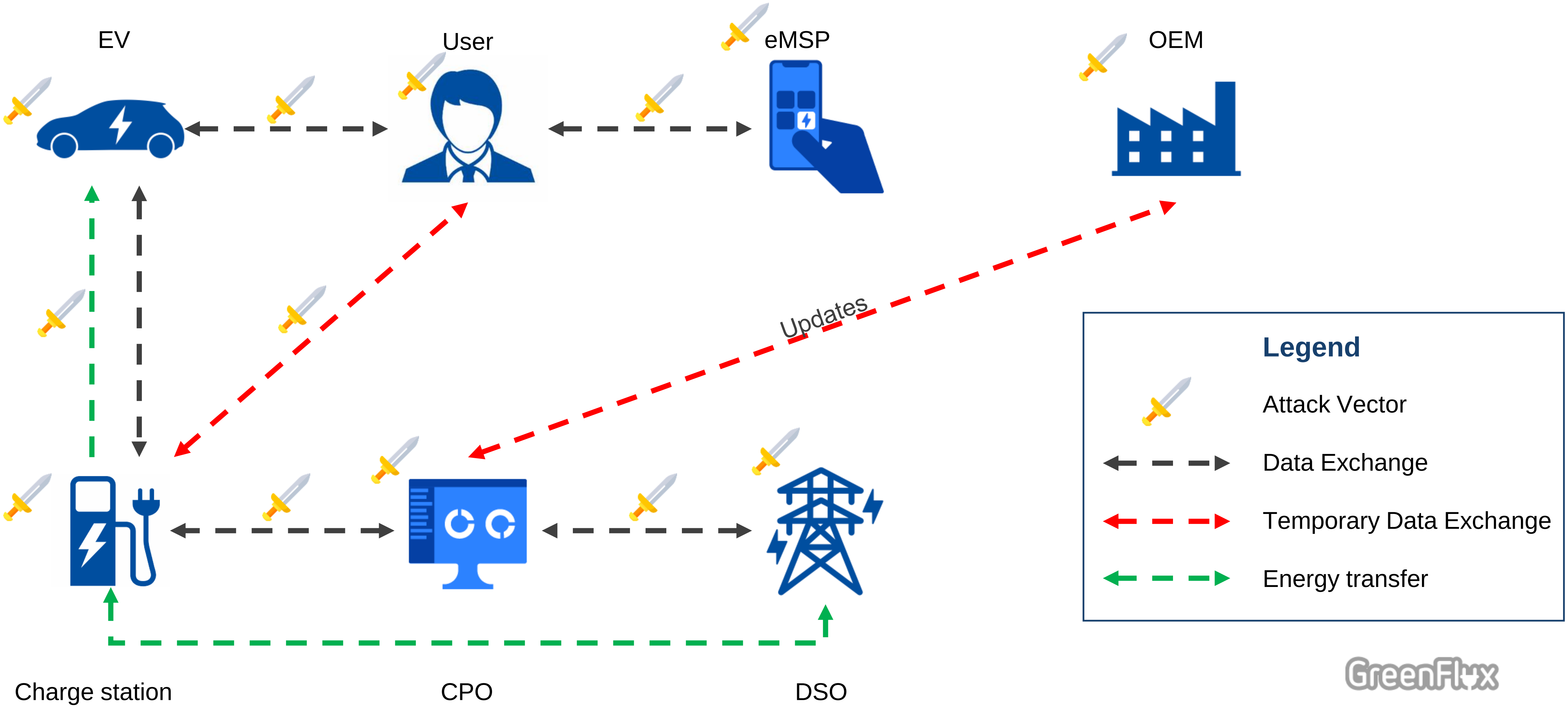


White label CPO & eMSP platform

- Billing and transaction management
- Remote management and support
- Global Roaming via open standards
- Smart Charging
- App
- Interfaces / API

EV Charging ecosystem

Attack vectors



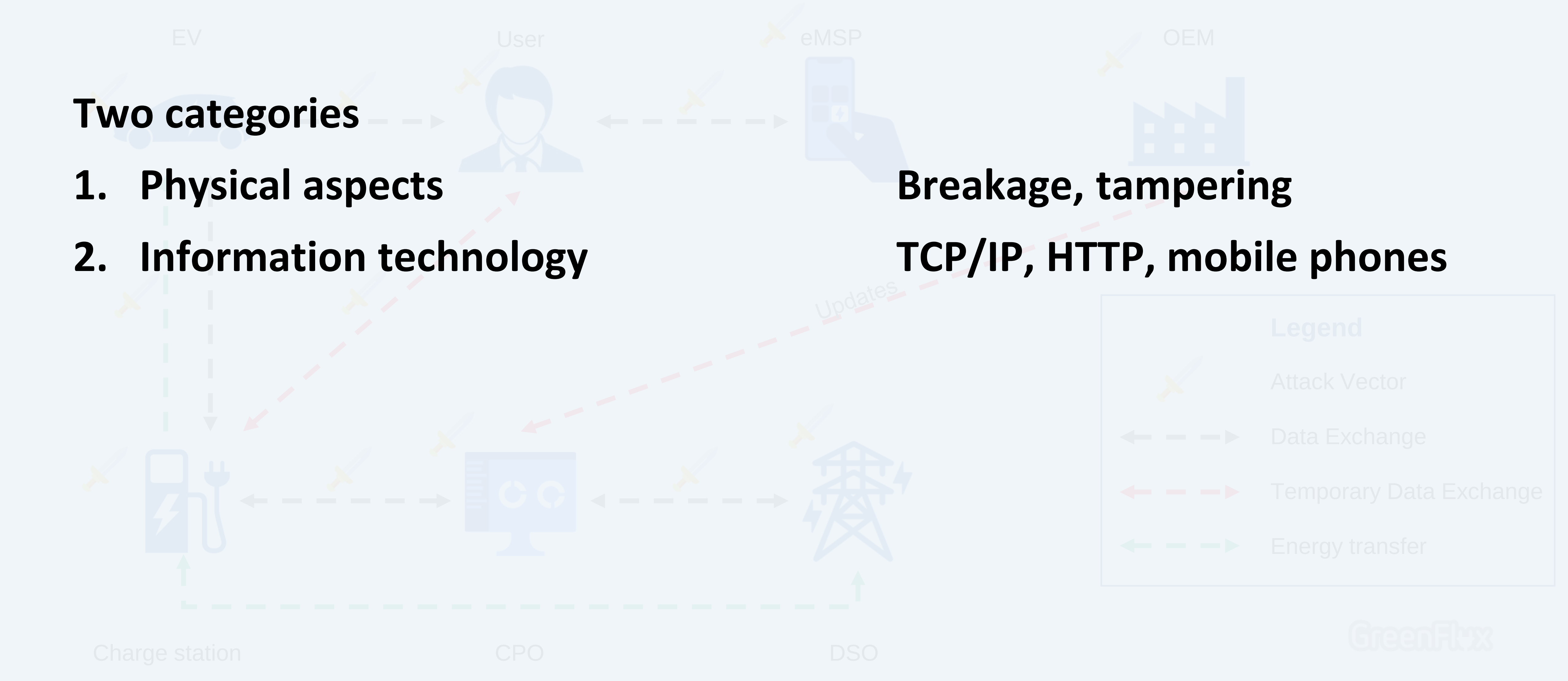
GreenFlux

EV Charging ecosystem

Attack vectors

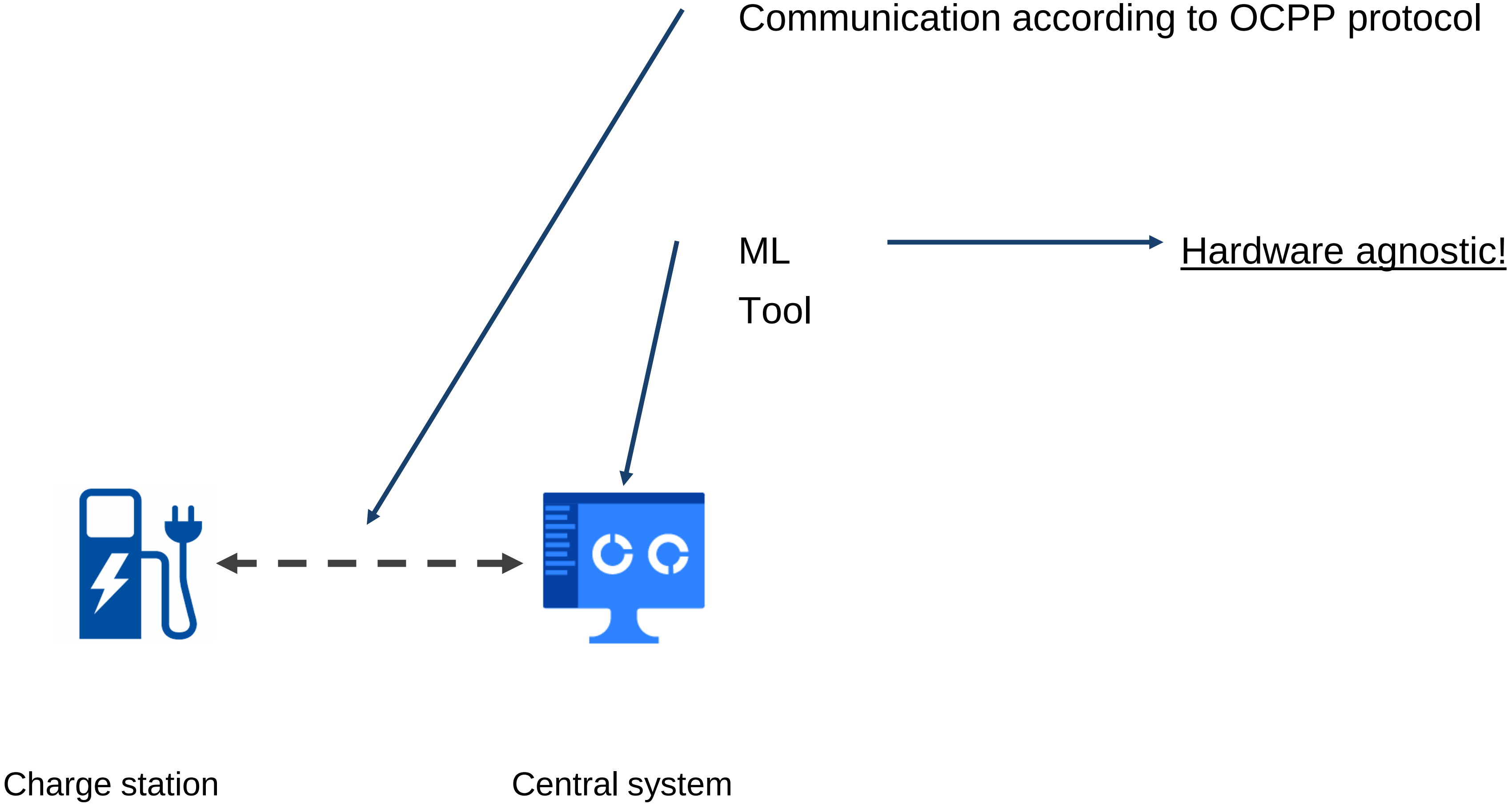
Two categories

1. **Physical aspects** — **Breakage, tampering**
2. **Information technology** — **TCP/IP, HTTP, mobile phones**



EV Charging ecosystem

Attack vectors



Communication according to OCPP protocol

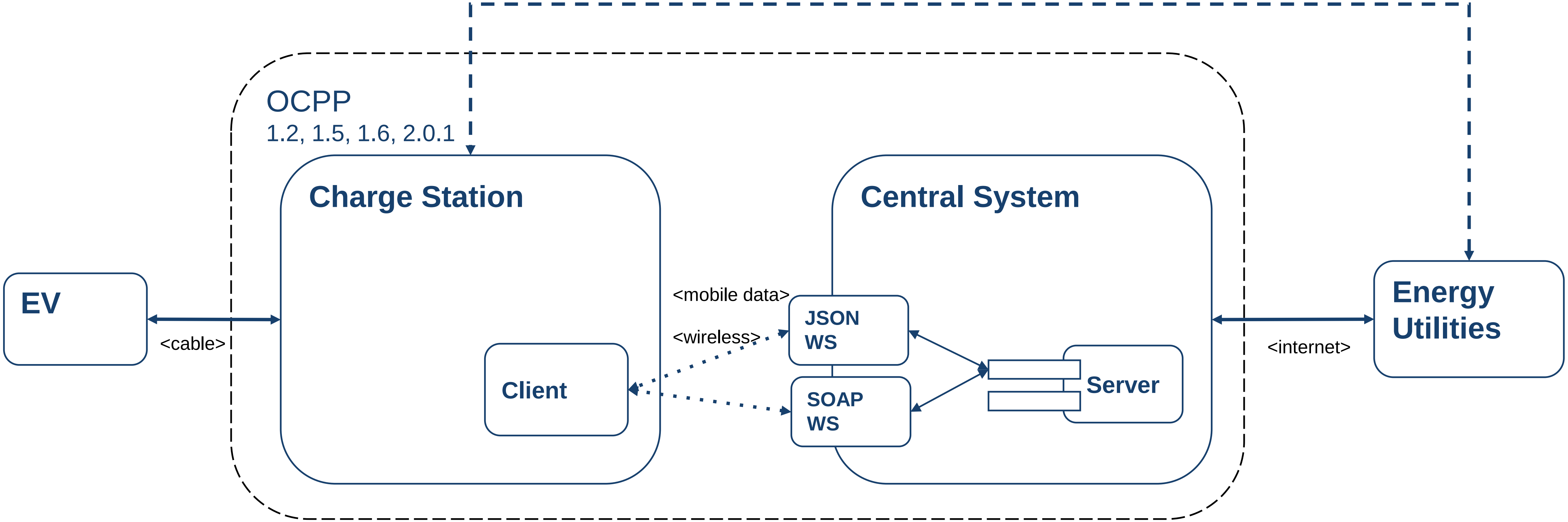
ML Tool → Hardware agnostic!

Charge station

Central system

Open Charge Point Protocol

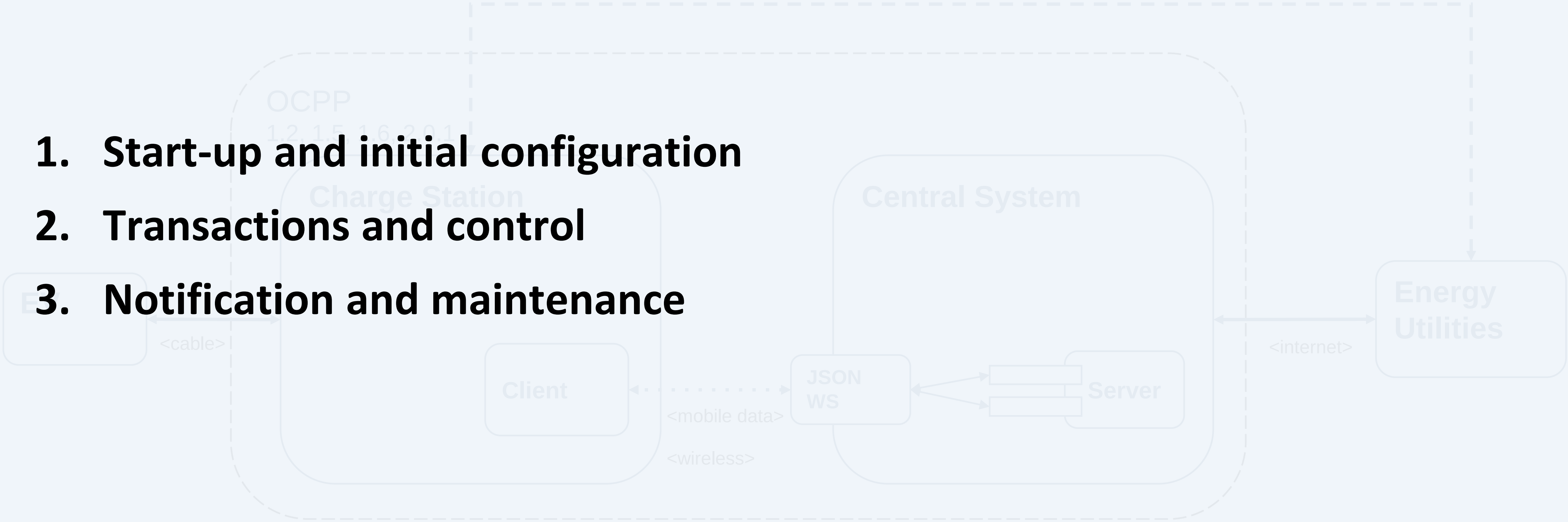
Deployment Diagram



Open Charge Point Protocol

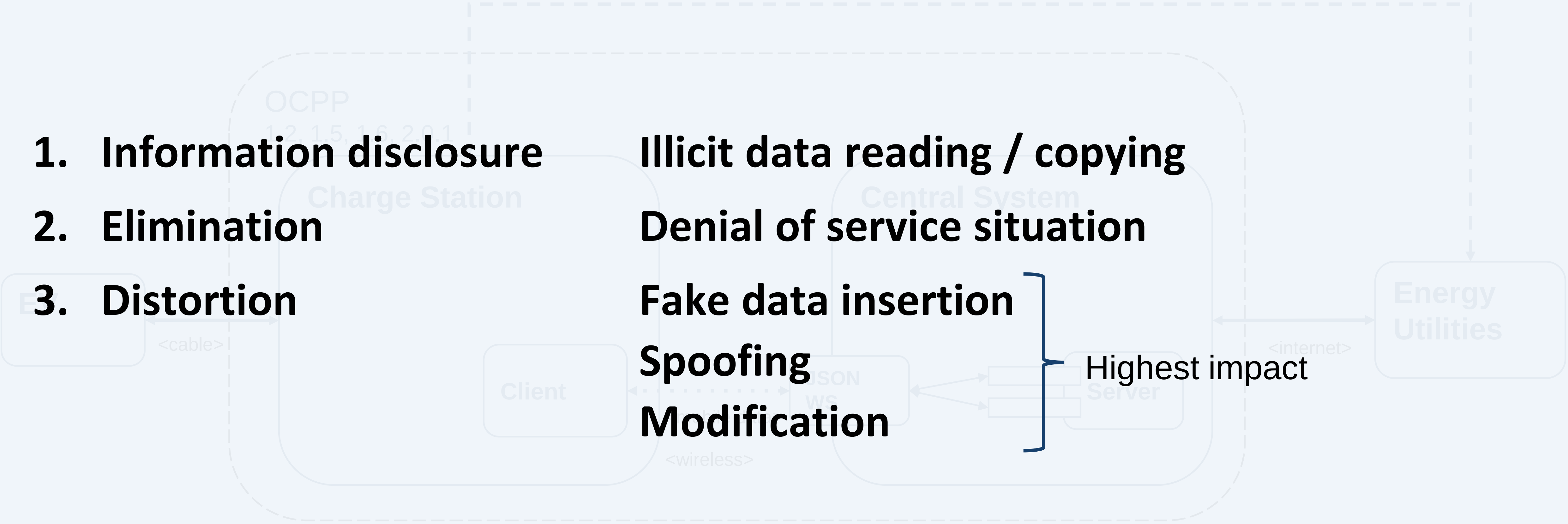
OCPP 1.6 Command stages

1. Start-up and initial configuration
2. Transactions and control
3. Notification and maintenance



Open Charge Point Protocol

Threat scenarios



1. Information disclosure	**Illicit data reading / copying**	
2. Elimination	**Denial of service situation**	
3. Distortion	**Fake data insertion** **Spoofing** **Modification**	Highest impact

Open Charge Point Protocol

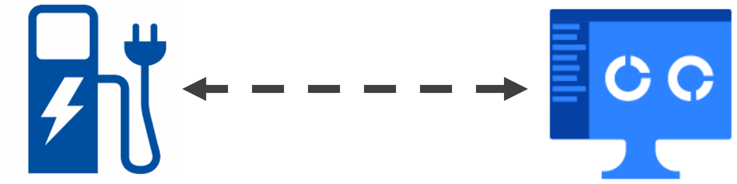
Message types and data share

OCPP1.5 consists of 24 Message Types

OCPP1.6 consists of 28 Message Types

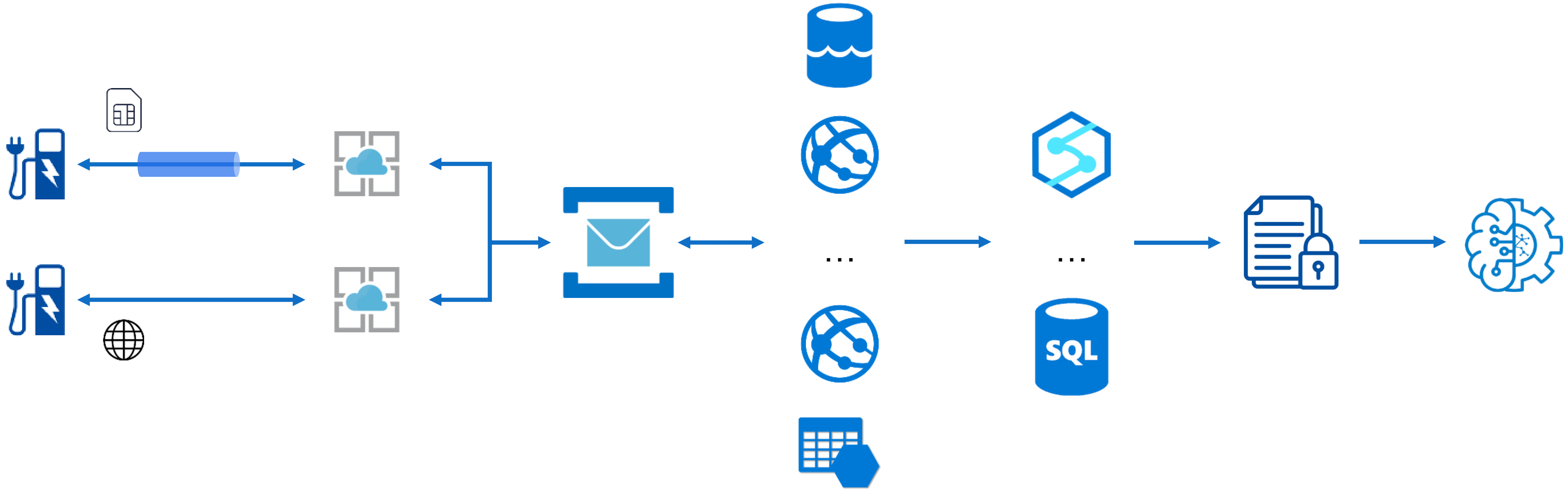
Distrubution in GreenFlux logs:

MeterValues	55%
Start- StopTransactions	20%
Other	*25%*



Charge station communication

Training data for ML pipeline



VPN Tunnel

Charge stations

Socket Server (Private/public) (SOAP/JSON)

Service Bus

GFX Services

GFX Databases

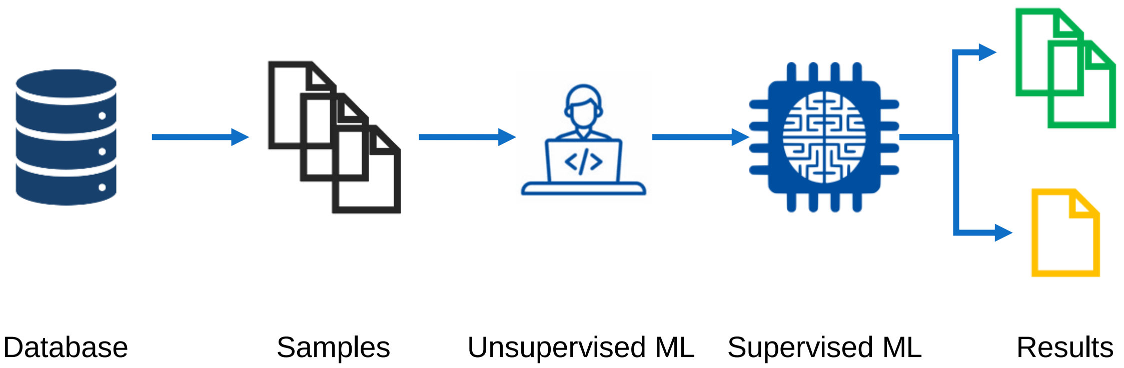
Data anonymization

Anomaly detection

Preliminary results

Anomaly detection

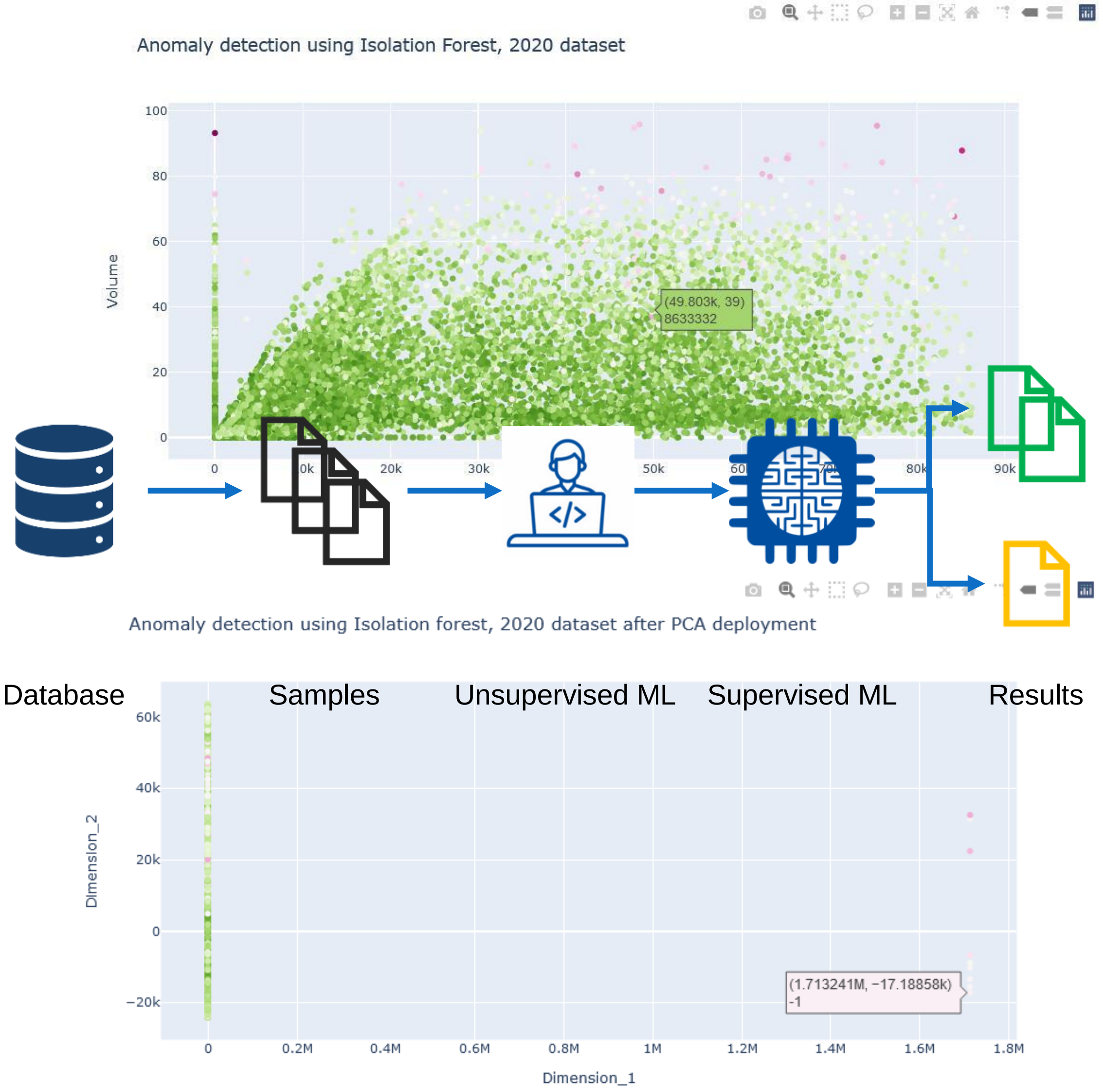
- Trained on 4 million entries
- 2018Q1, 2019Q1, 2020Q1



Preliminary results

Anomaly detection

- Trained on 4 million entries
- 2018Q1, 2019Q1, 2020Q1
- Principal Component Analysis (PCA)
- 2018 CDR bug detected



Anomaly detection using Isolation Forest, 2020 dataset

Anomaly detection using Isolation forest, 2020 dataset after PCA deployment

Database

Samples

Unsupervised ML

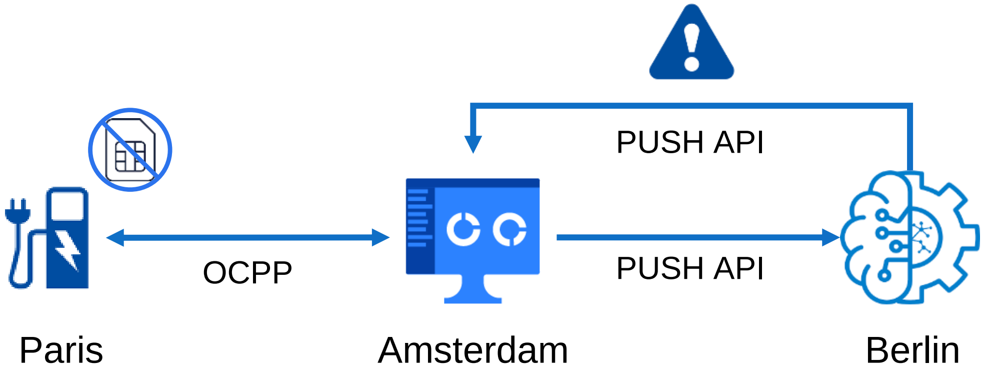
Supervised ML

Results

Deployment

Anomaly detection flow

- Charge station sends OCPP messages
- GFX Platform pushed data to ML Tool
- Anomalies are reported back to GFX
- Mitigation action taken by GFX



CARAMEL

Artificial Intelligence-based Cybersecurity for Connected and Automated Vehicles

T · · ·   i2cat   KATECH   nextium by idneo   ETRI Electronics and Telecommunications Research Institute   Panasonic AUTOMOTIVE   University of Cyprus   ubiwhere   8 Bells

S   AVL   Capgemini engineering   mobigen Make The Best For Smart Business   EXALENS   GreenFlux   Atos

Contact

Bob Elders

bob.elders@greenflux.com

Thanks for your attention!