Mert D. Pesé, Jay W. Schauer,
Murali Mohan, Cassandra Joseph,
Kang G. Shin, and John Moore

PRICAR: Privacy Framework for Vehicular Data Sharing with Third-Parties

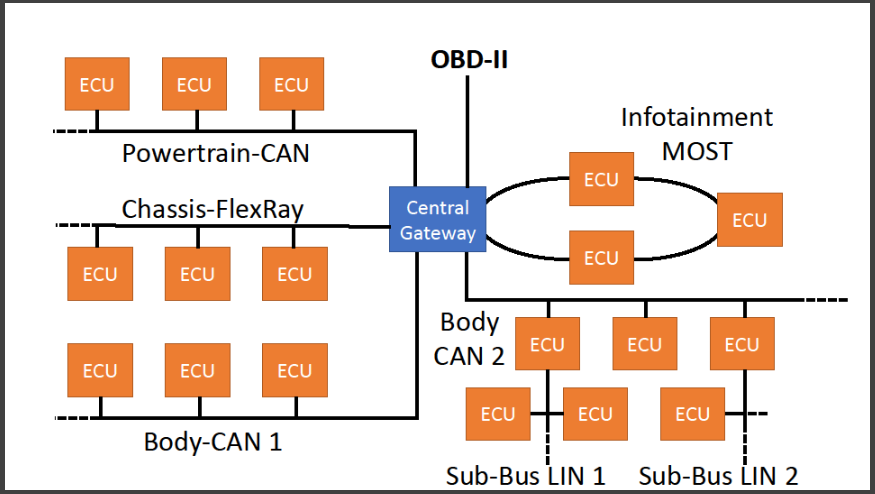
IEEE SecDev 2023, Atlanta, GA
10/20/23

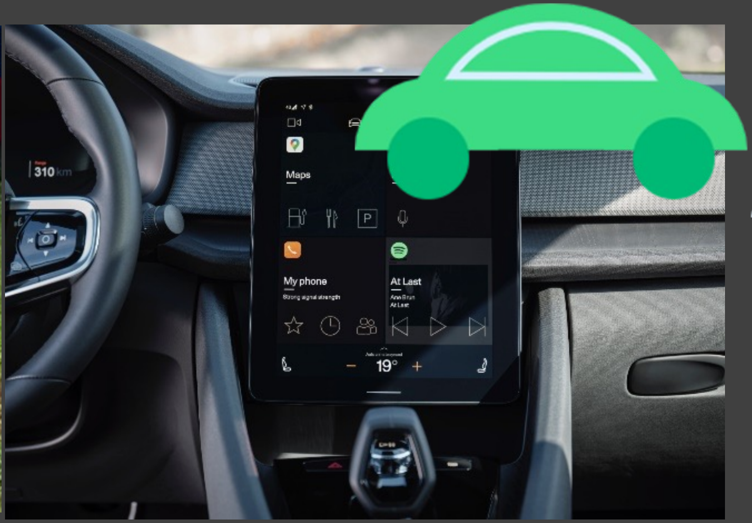
TigerSec Laboratory @ Clemson University

Real-Time Computing Laboratory @ University of Michigan, Ann Arbor

Ford

Security and privacy landscape is changing





First-Generation Attacks (~2010-2015)

Using physical interfaces

Second-Generation Attacks (~2015-2020)

Using wireless interfaces (e.g., IVI and TCU)

Third-Generation Attacks (~2020-?)

Using app eco-system on IVIs

Scalability

Risk / Damage Potential

Increased connectivity comes at a price

BMW CarData

Mercedes me

PROGRESSIVE

StateFarm

verizon

otonomo

Data Generation

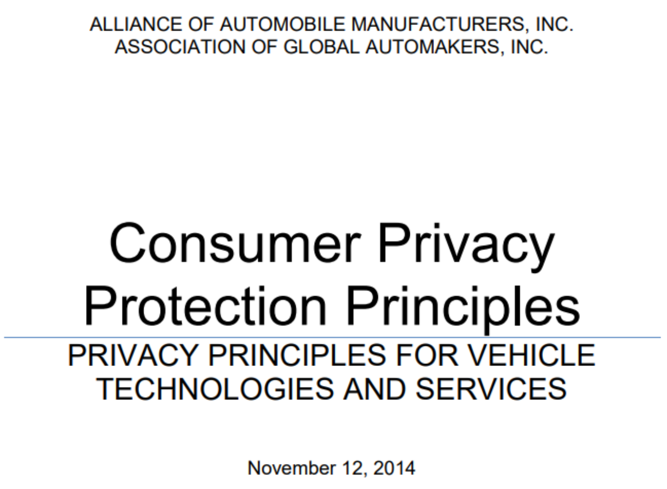
~25 GB/h (total)
~200 MB/h (CAN)

Data Connectivity

- 2016: 20%
- 2020: 75%
- 2021: 98%

Privacy Concerns

- Rising Awareness (e.g., Facebook-Cambridge Analytica incident)
- General Data Protection Regulation (GDPR)
- Increasing Number of Privacy Attacks in Cars

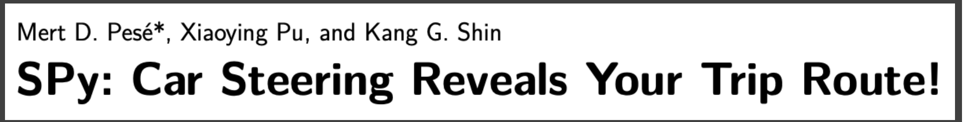


ALLIANCE OF AUTOMOBILE MANUFACTURERS, INC.
ASSOCIATION OF GLOBAL AUTOMAKERS, INC.

Consumer Privacy Protection Principles

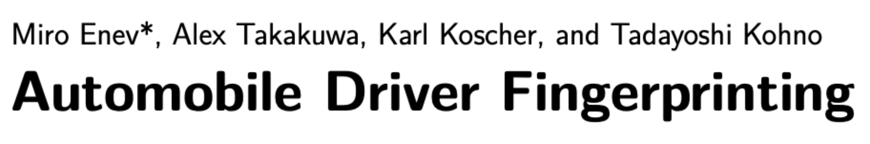
PRIVACY PRINCIPLES FOR VEHICLE TECHNOLOGIES AND SERVICES

November 12, 2014



Mert D. Pesé*, Xiaoying Pu, and Kang G. Shin

SPy: Car Steering Reveals Your Trip Route!

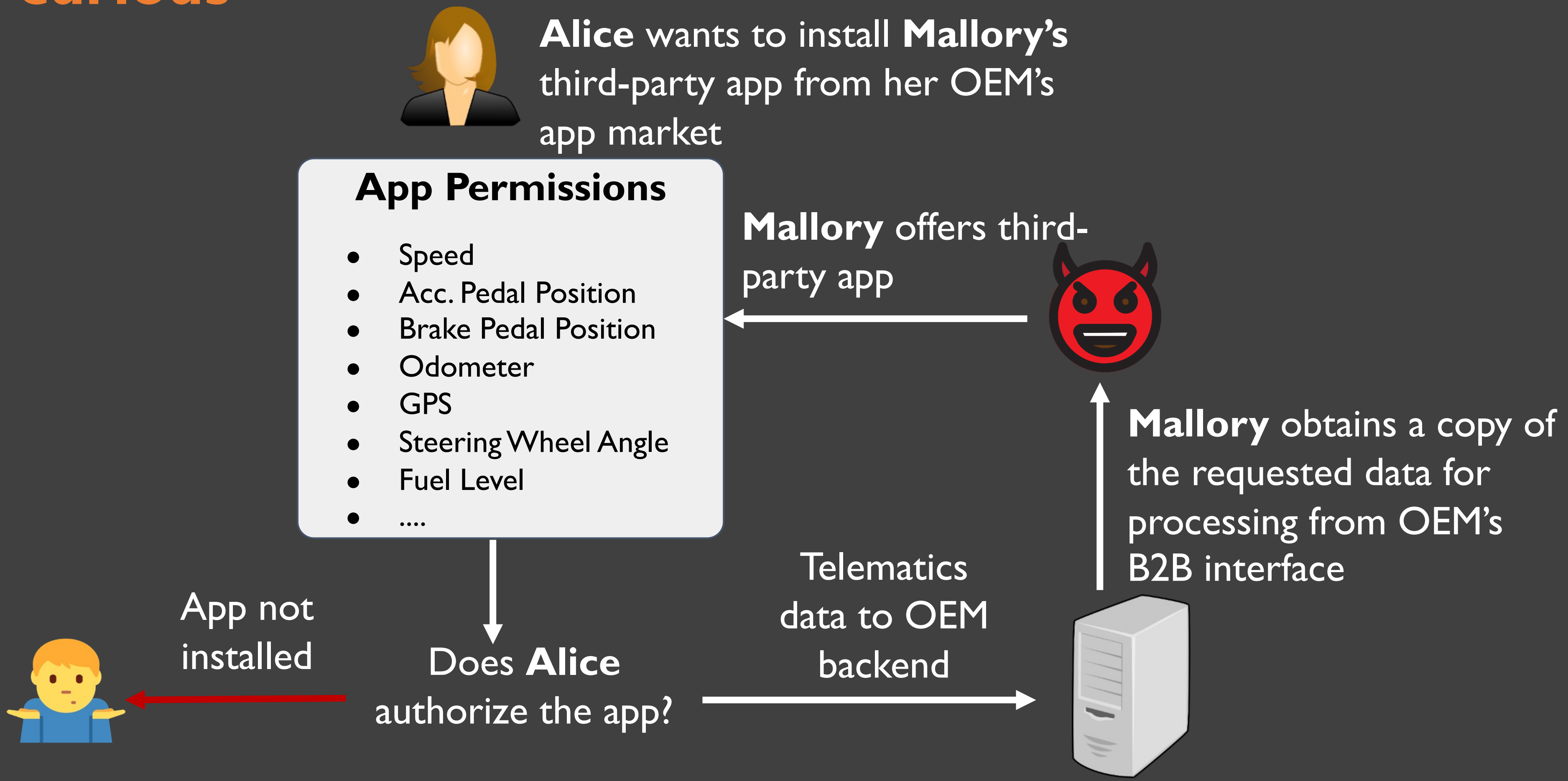


Miro Enev*, Alex Takakuwa, Karl Koscher, and Tadayoshi Kohno

Automobile Driver Fingerprinting

Data Collection

- Driving data is shared with third-party entities who can be **benign, but curious**



Alice wants to install **Mallory's** third-party app from her OEM's app market

App Permissions

- Speed
- Acc. Pedal Position
- Brake Pedal Position
- Odometer
- GPS
- Steering Wheel Angle
- Fuel Level
- ....

Mallory offers third-party app

Mallory obtains a copy of the requested data for processing from OEM's B2B interface

Telematics data to OEM backend

Does **Alice** authorize the app?

App not installed

General Data Protection Regulation (GDPR)

1. Lawfulness, Fairness and Transparency
2. Purpose Limitation
3. Data Minimization
4. Accuracy
5. Storage Limitation
6. Integrity and Confidentiality
7. Accountability

PRIVACY GOALS

🟩 Frontend
🟧 Backend

Minimization	Anonymization	Sanitization
Use of permission model	Remove PII from data	Prevent 3rd party from mining more context than agreed
1 2 3 4	2 6	2 5

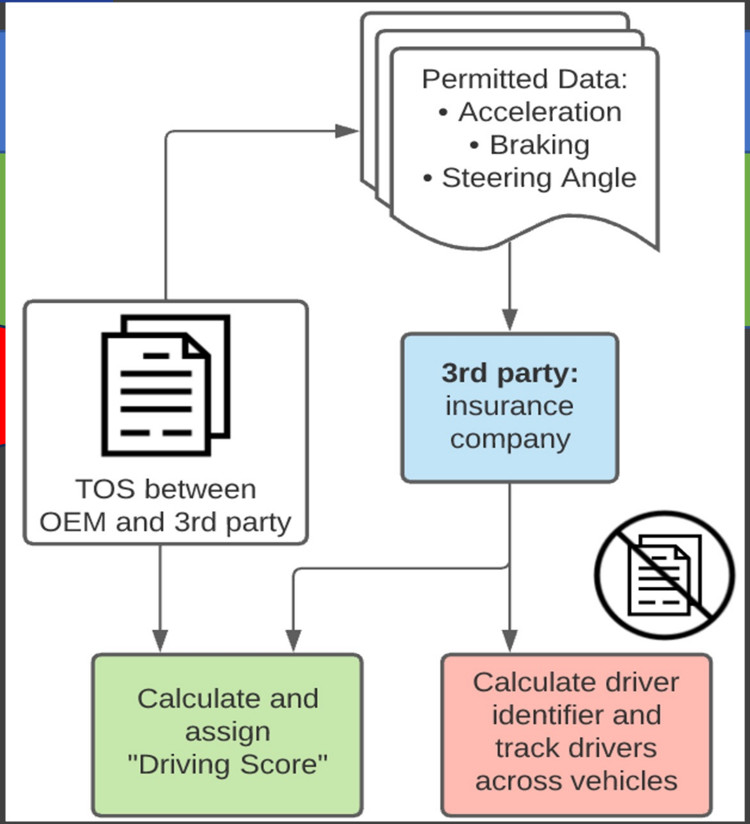
General Data Protection Regulation (GDPR)

1. Lawfulness, Fairness and Transparency
2. Purpose Limitation
3. Data Minimization
4. Accuracy
5. Storage Limitation
6. Integrity and Confidentiality
7. Accountability

PRIVACY GOALS

🟩 Frontend
🟧 Backend

1



Permitted Data:
- Acceleration
- Braking
- Steering Angle

TOS between OEM and 3rd party

3rd party: insurance company

Calculate and assign "Driving Score"

Calculate driver identifier and track drivers across vehicles

Sanitization

Prevent 3rd party from mining more context than agreed

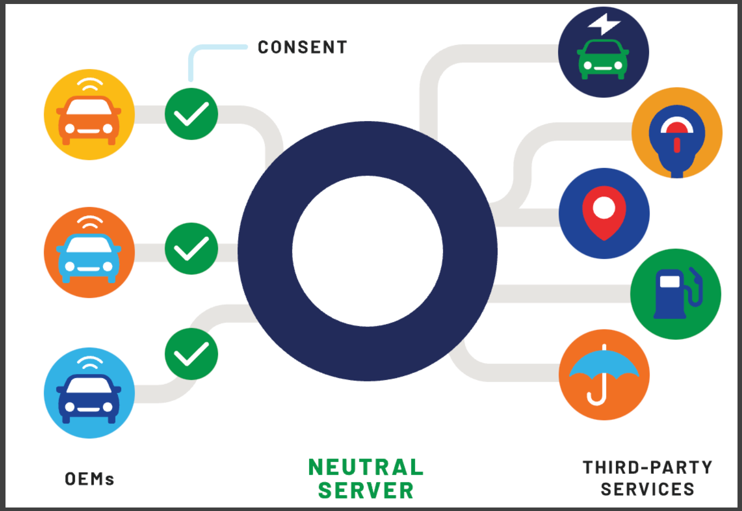
2 5

Data Sanitization

1. Lawfulness, Fairness and Transparency
2. **Purpose Limitation**
3. Data Minimization
4. Accuracy
5. **Storage Limitation**
6. Integrity and Confidentiality
7. Accountability

Existing Work

- Solid Project
- Neutral Server Concept (European Automobile Manufacturers' Association)

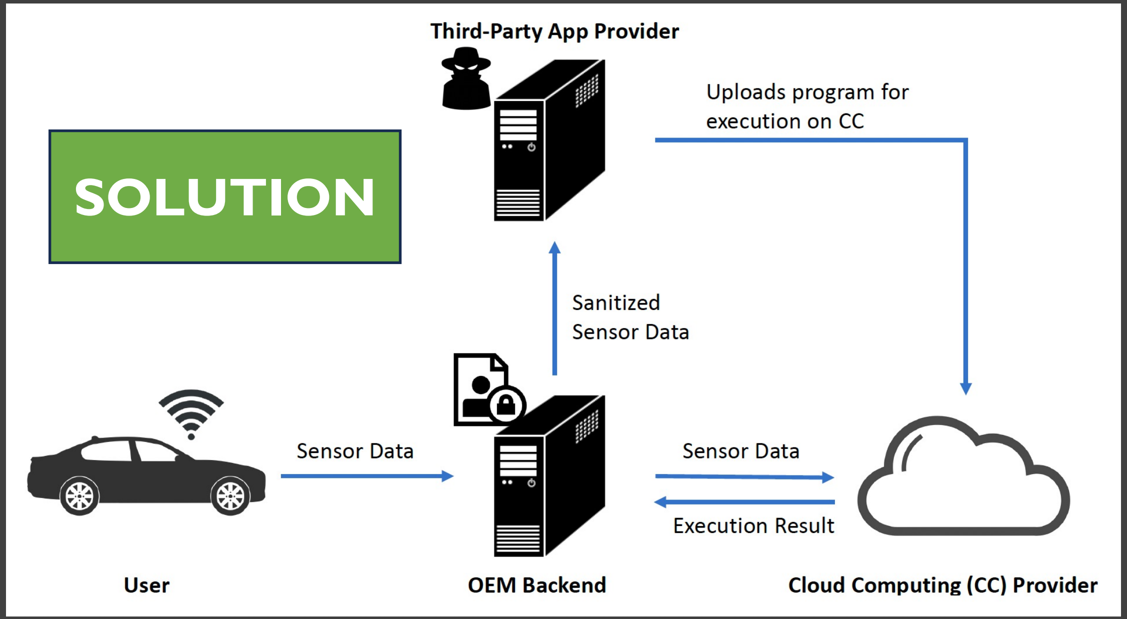

CONSENT

OEMs

NEUTRAL SERVER

THIRD-PARTY SERVICES

Problem: Rogue third-party can store data indefinitely **and** mine more context even if access is revoked!


SOLUTION

Third-Party App Provider

Uploads program for execution on CC

Sanitized Sensor Data

Sensor Data

Sensor Data

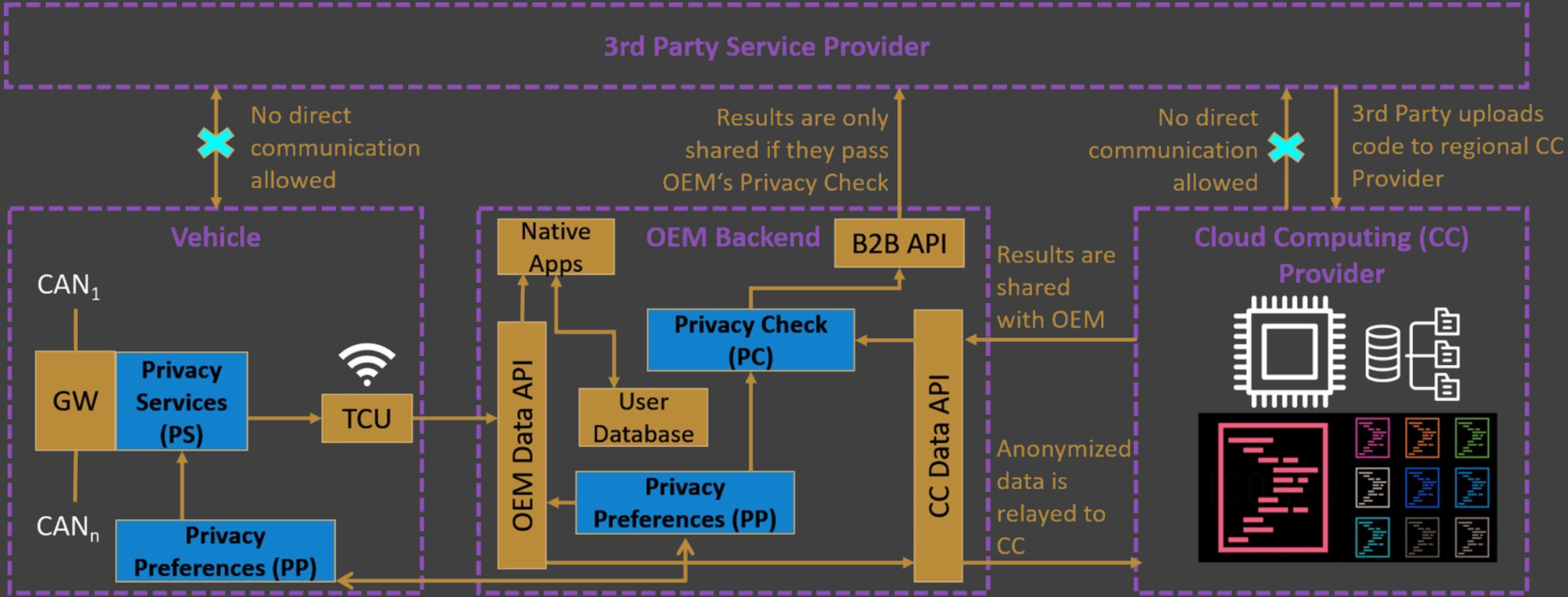
Execution Result

User

OEM Backend

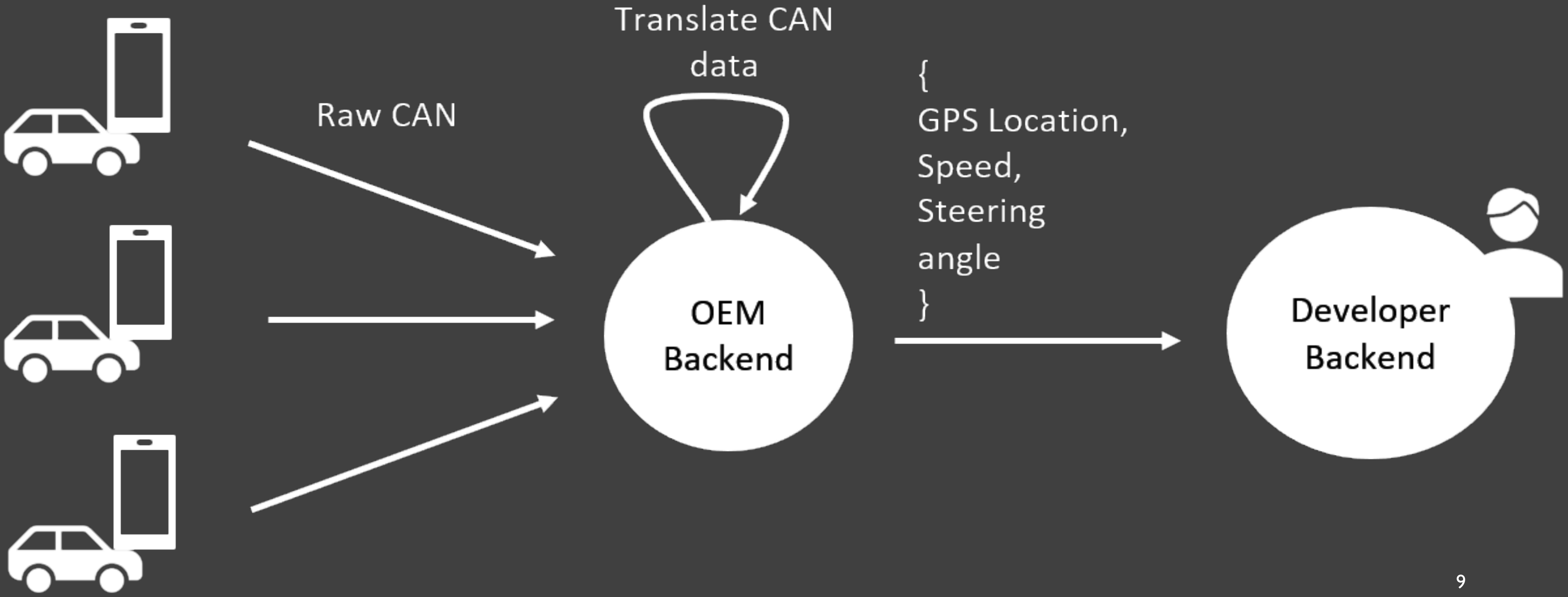
Cloud Computing (CC) Provider

Reference Architecture


3rd Party Service Provider
No direct communication allowed
Results are only shared if they pass OEM's Privacy Check
No direct communication allowed
3rd Party uploads code to regional CC Provider
Vehicle
CAN$_1$
GW
Privacy Services (PS)
TCU
CAN$_n$
Privacy Preferences (PP)
Native Apps
OEM Backend
B2B API
Privacy Check (PC)
OEM Data API
User Database
Privacy Preferences (PP)
CC Data API
Results are shared with OEM
Anonymized data is relayed to CC
Cloud Computing (CC) Provider

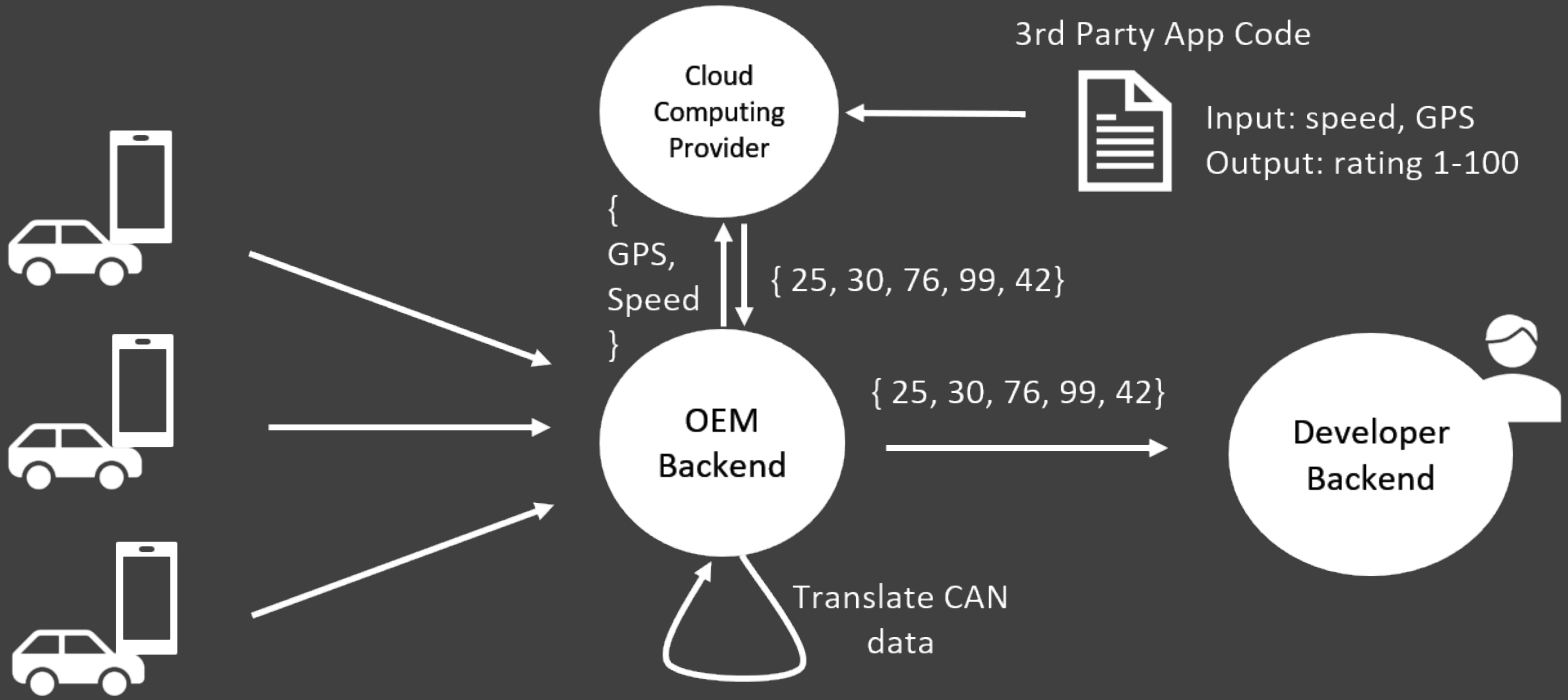
Example

Solves (2) Purpose Limitation + (5) Storage Limitation



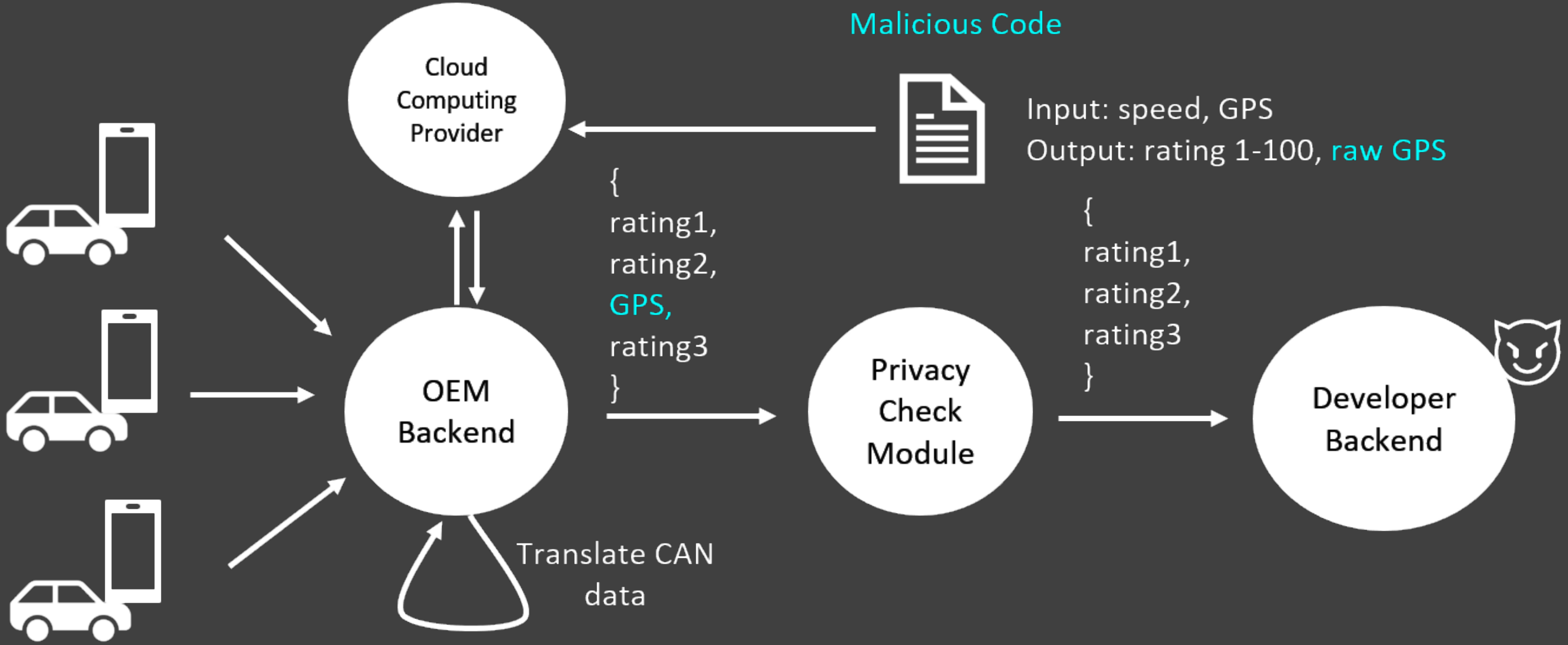
Example

Solves (2) Purpose Limitation + (5) Storage Limitation



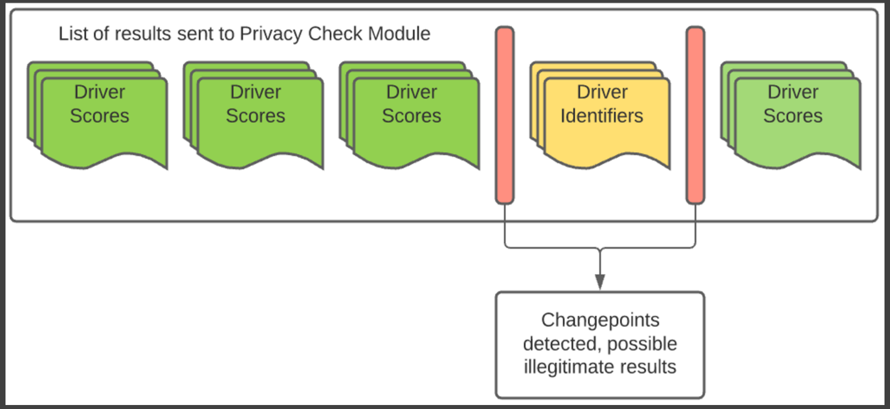
Example

Solves (2) Purpose Limitation + (5) Storage Limitation



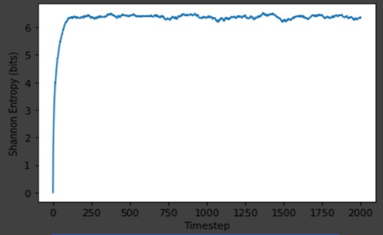
Privacy Check Module

- Goals
  - Approve legitimate results
  - Detect illegitimate results and stop transmission
  - Detect illegitimate results, even if disguised as legitimate
- Change-Point Detection (CPD)
  - Technique used for anomaly detection
- Entropy-Based Detection (EBD)
  - Use changes in the calculated entropy over time to find anomalies in input data $\mathrm{H}(X) = -\sum_{i=1}^{n} \mathrm{P}(x_i) \log \mathrm{P}(x_i)$

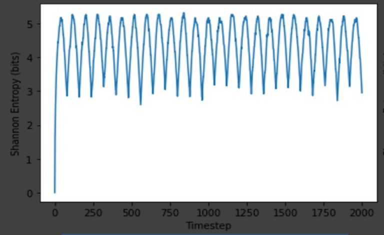


List of results sent to Privacy Check Module

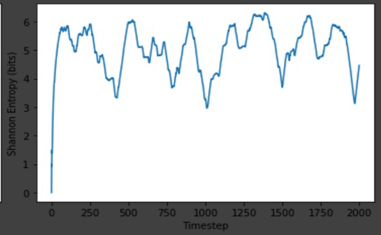
Changepoints detected, possible illegitimate results



No anomalies

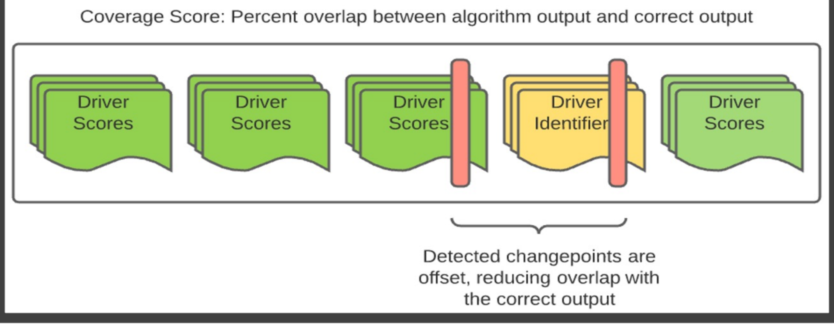


Periodic anomalies



Random anomalies

Evaluation: CPD



Coverage Score: Percent overlap between algorithm output and correct output

Driver Scores

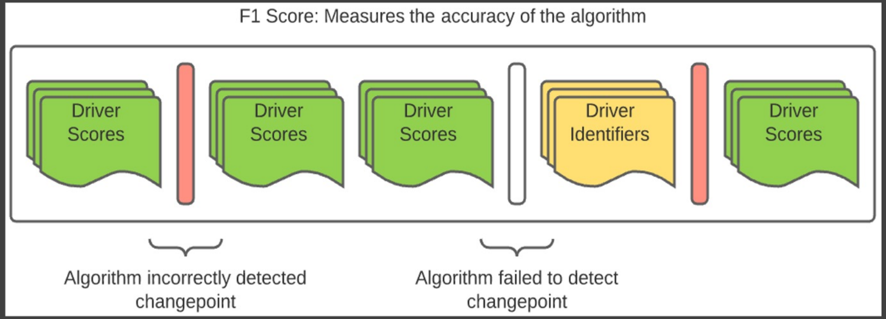
Driver Scores

Driver Scores

Driver Identifier

Driver Scores

Detected changepoints are offset, reducing overlap with the correct output



F1 Score: Measures the accuracy of the algorithm

Driver Scores

Driver Scores

Driver Scores

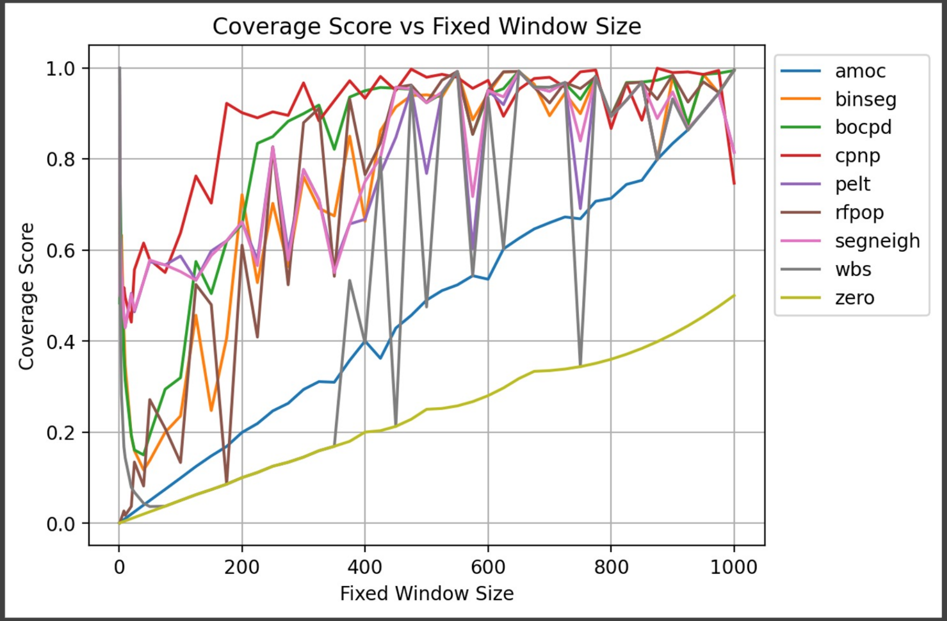
Driver Identifiers

Driver Scores

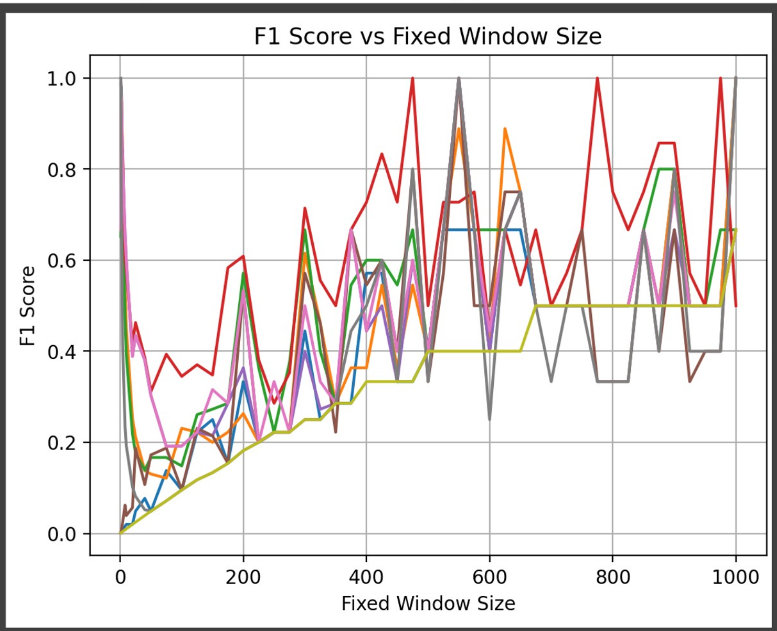
Algorithm incorrectly detected changepoint

Algorithm failed to detect changepoint

TPCDBench



Coverage Score vs Fixed Window Size

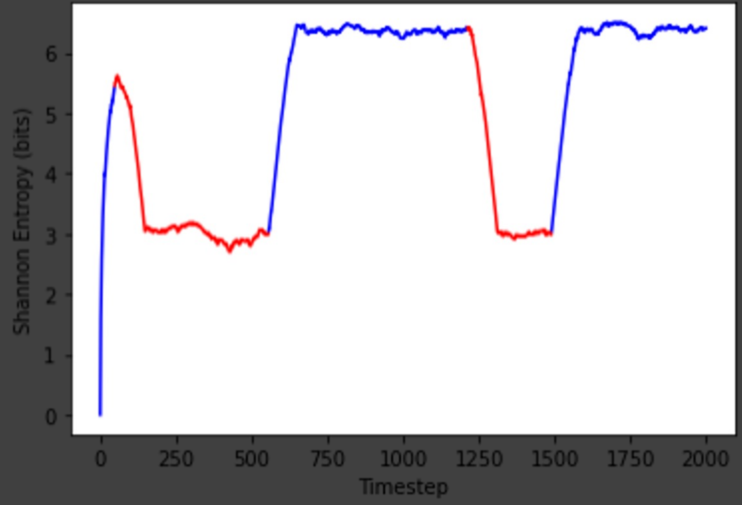


F1 Score vs Fixed Window Size

- Changepoint Detection can be used!
- Best average performance: CPNP and Pelt

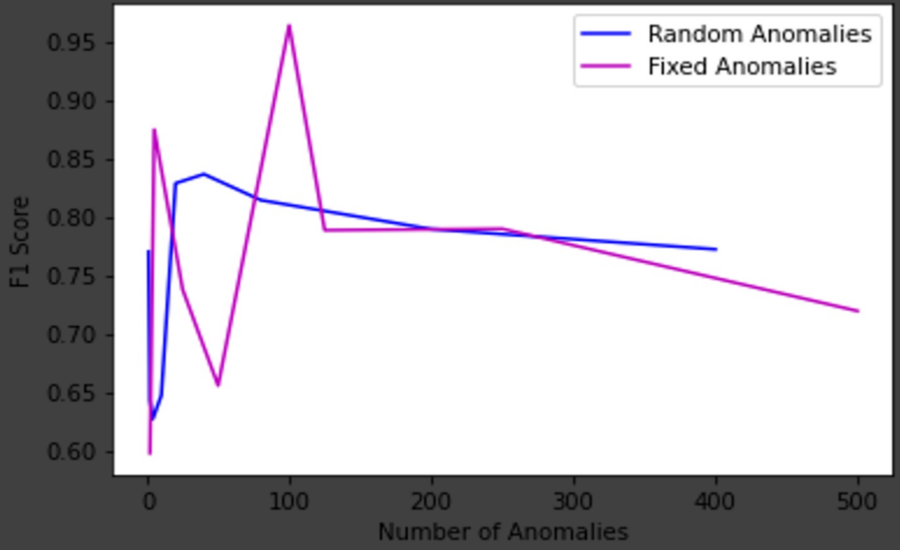
Evaluation: EBD

- Negative gradient changes in entropy correspond to changepoints



Red segments of data correspond to malicious data, while blue segments of data correspond to normal/benign data

- Good performance for both fixed and random anomalies



Conclusion

First Privacy-Preserving Vehicular Data Collection and Sharing Platform

Privacy Goals

Definiton of three privacy goals that satisfy GDPR regulation

Architecture Design

Production-ready reference architecture for OEMs

Data Sanitization

Adapted and evaluted two anomaly detection techniques for data sanitization

Q & A

Mert D. Pesé, Ph.D.
mpese@clemson.edu