Privacy Preserving Energy Management

Holger Kinkelin, **Marcel von Maltitz**, Benedikt Peter, Cornelia Kappler, Heiko Niedermayer, Georg Carle

Chair for Network Architectures and Services

Department for Computer Science
Technische Universität München

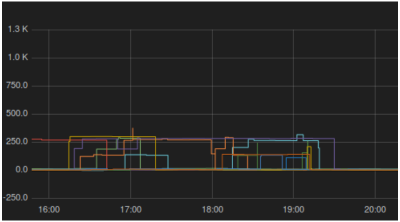
November 18, 2014

Energy Monitoring Systems (EMS)

EMS[1] generate fine-grained digital traces of energy consumption in a building.

Upon these traces essential savings of energy consumption can be achieved, by e.g.

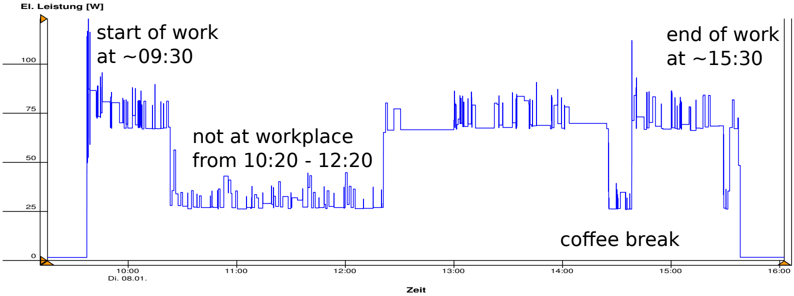
- finding inefficient or defect devices
- raising energy awareness among users



[1] Not to be confused with smart meters

EMS produce personal data

Scenario: Energy monitored office building
Digital traces give detailed insights into employee behaviour



start of work at ~09:30

not at workplace from 10:20 - 12:20

coffee break

end of work at ~15:30

⟹ raises conflicts with data protection laws, reduces user acceptance

⟹ data has to be secured, access control has to be enforced

Traditional access control not sufficient

Measurement values are unprotected in database, broker (DBMS or dedicated component) authenticates users and transfers data between them and DB.

Drawbacks

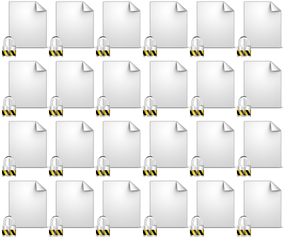
- Centralized data storage
- Data not inherently protected
- System administrator has full access

⟹ enforce access control on data level

Access control by encryption

Goal:
Retain data of finest granularity but protect it and enforce precise access control on data level

Approach:
Utilize *attribute based encryption* (Waters et al., 2007), which allows embedding of access policies by encryption



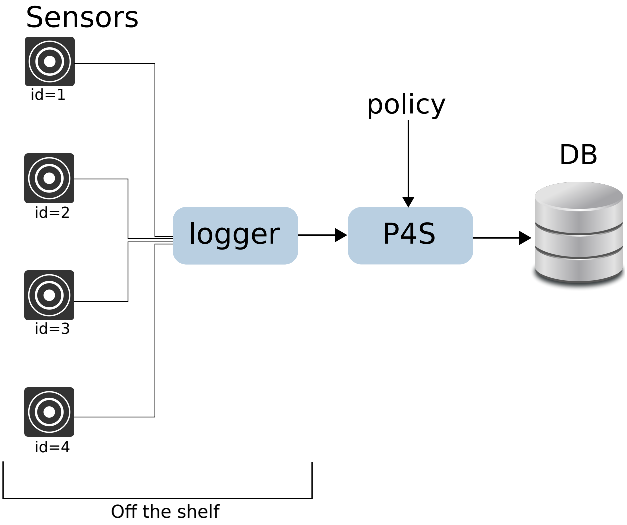
Access control by encryption

policy: role=“Energy manager” OR owner=“Joe”

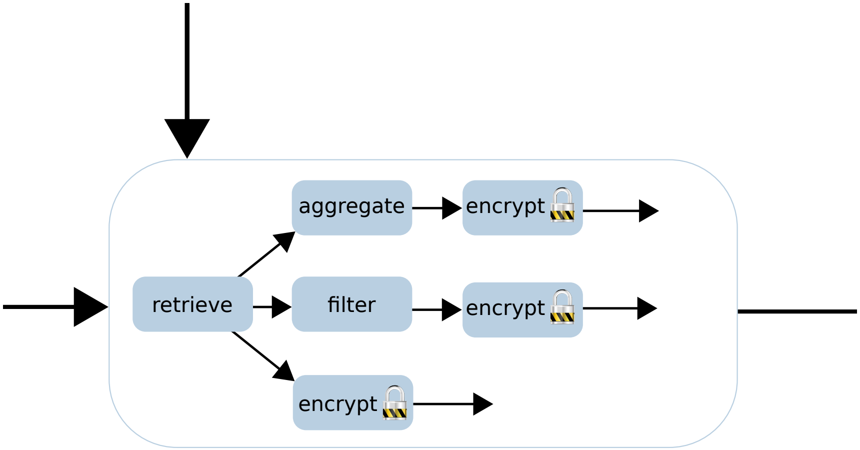
key: owner=“Trent”, role=(“Energy manager”, ”Employee“) ✓

key: owner=“Eve”, role=(“Employee”, “Accountant”) ✗

Architecture: Privacy Preserving Pre-Processing & Storage

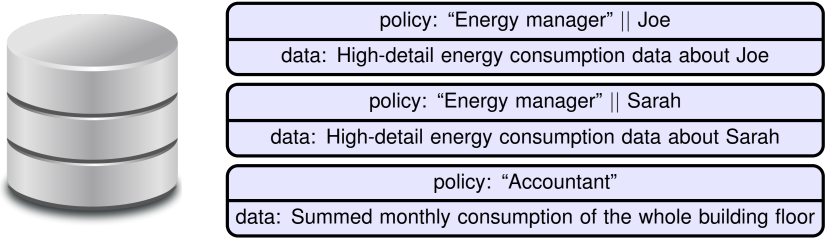


Architecture: Privacy Preserving Pre-Processing & Storage



Architecture: Privacy Preserving Pre-Processing & Storage

Database now stores values, preprocessed for different target groups, encrypted with apropriate policies.



policy: “Energy manager” || Joe

data: High-detail energy consumption data about Joe

policy: “Energy manager” || Sarah

data: High-detail energy consumption data about Sarah

policy: “Accountant”

data: Summed monthly consumption of the whole building floor

Evaluation: Security & Privacy

Benefits

- Support of distributed information generation and storage
- Data base does not hold plain information anymore
- Access control without running components
- Attacks on logger or P4S do no affect previous data
- Transport security also given by encryption

Problems

- Master private key necessary to derive user keys
- Energy manager's key allows full access
- Off the shelf components have to be trusted

Aggregation is not always applicable

Different roles exists with different requirements of granularity

- Accountant: Overall sum every month ✓
- Public Display: e.g. ranking without precise values ✓
- Employee: Own data in finest granularity, other's after permission ✗
- Energy manager: All data in finest granularity ✗

⟹ highest data resolution has to be preserved

Summary

Data streams like energy consumption is personal data and must be protected

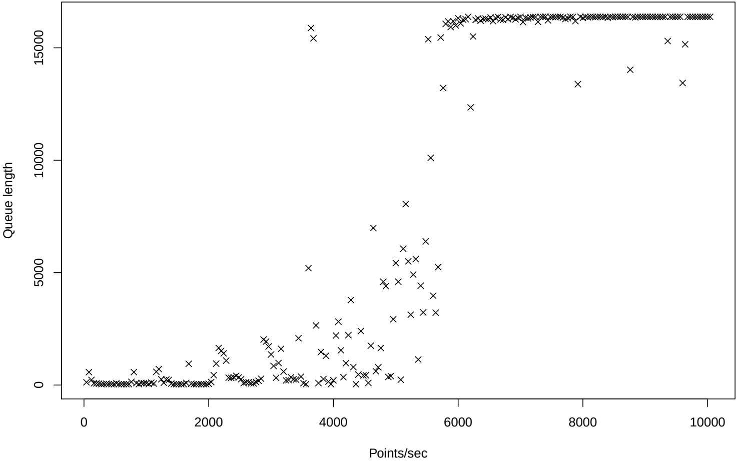
Established protection strategies are not always expedient

Proposal of new method:

- Specify data access policies (degree of detail, roles with access)
- preprocess raw streams to specified result streams
- realize access control by encryption on result streams
- distribute data in encrypted form
- carry out postprocessing on trusted user device

Evaluation: Performance

Quad-Core i5 @ 2.50 GHz, 3600 MB RAM, HD @ 5400 RPM


Queue length
Points/sec