Smarter Meters

Team 7

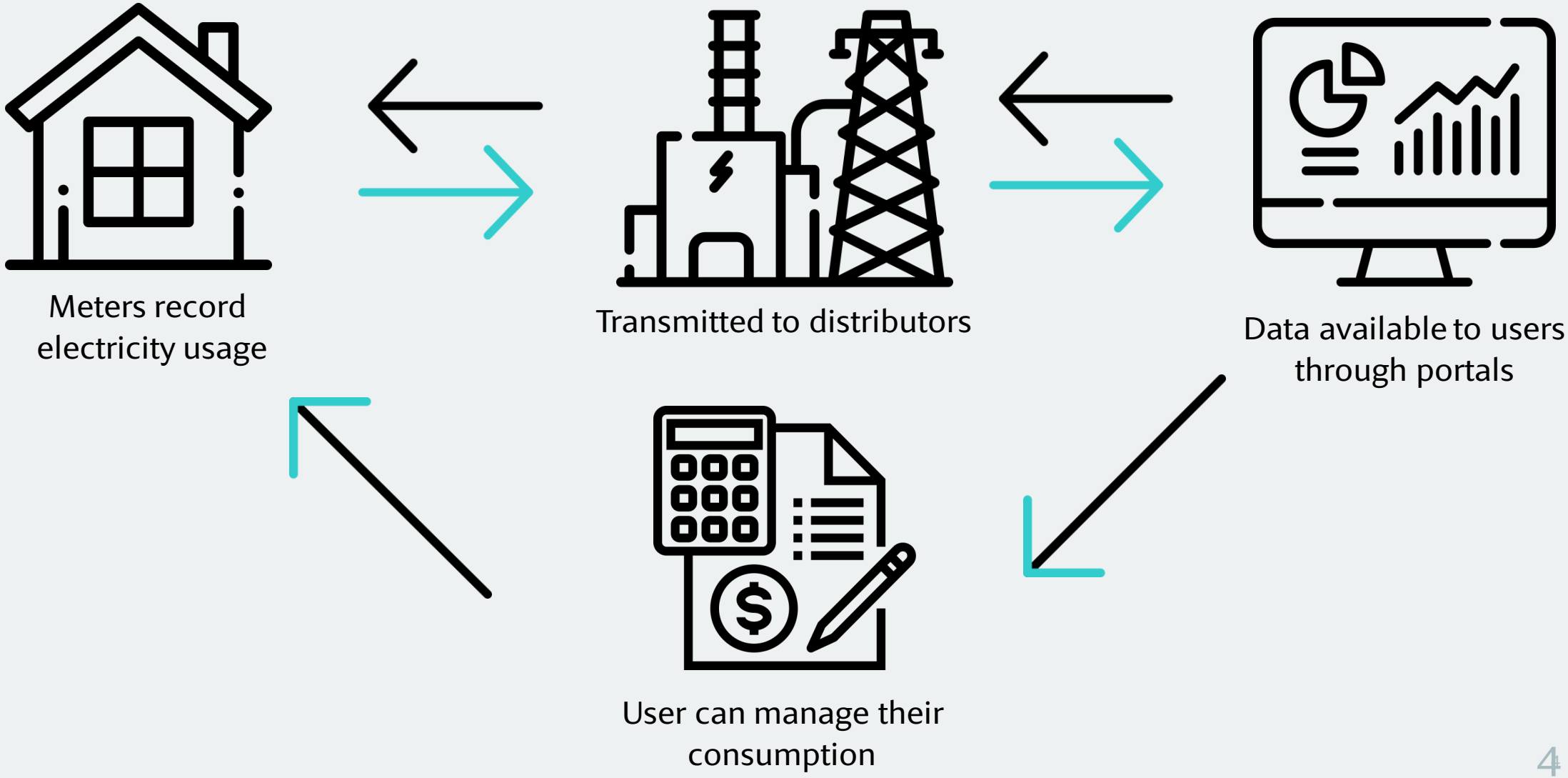
Ella Reck - Soumaia Bouhouia

Felicia Sun - Vanessa Akhras

Recap: Smart Meters

Keeps track of your electricity consumption in real time

Recap: Smart Meter Communication System

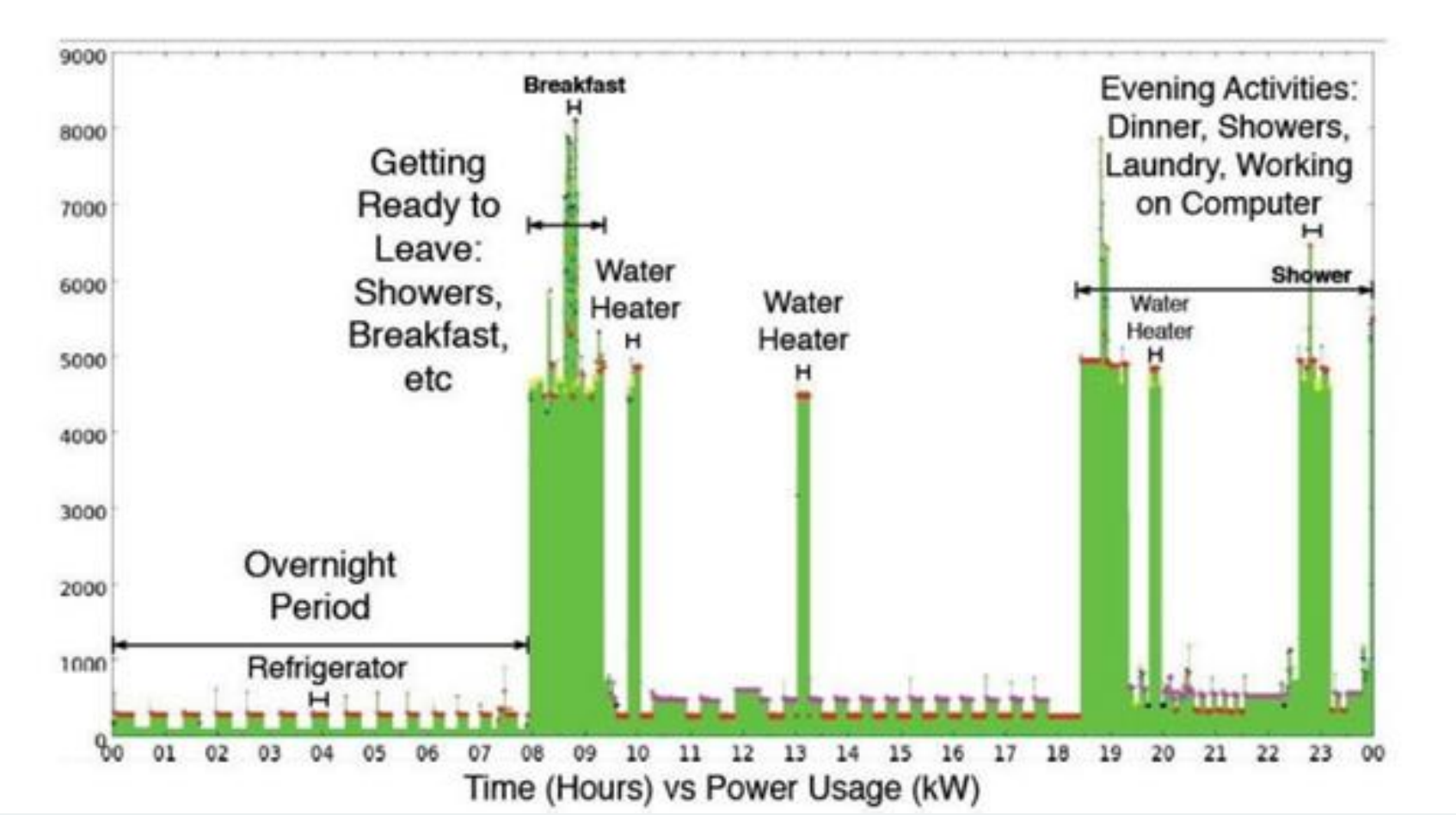


Recap: Smart Meters

- Omnipresent
- Used for billing
- Used for detecting and predicting

Beyond Energy Monitoring: Threats

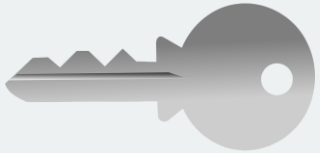
- Allows for identification
- Main concern: inferring consumer routines and behavior
- Energy disaggregation



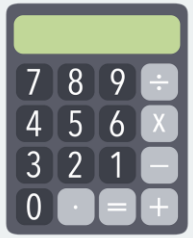
Features
Functional Requirements

Private Access to Detailed Data

(User)



End-to-End Encryption +Secure Communication



Billing Data + Aggregated Insights

(Supplier)

Data Accuracy + Timely Processing

Privacy Goals

Anonymization

Remove identifiable information + Aggregate individual consumption data

Encryption

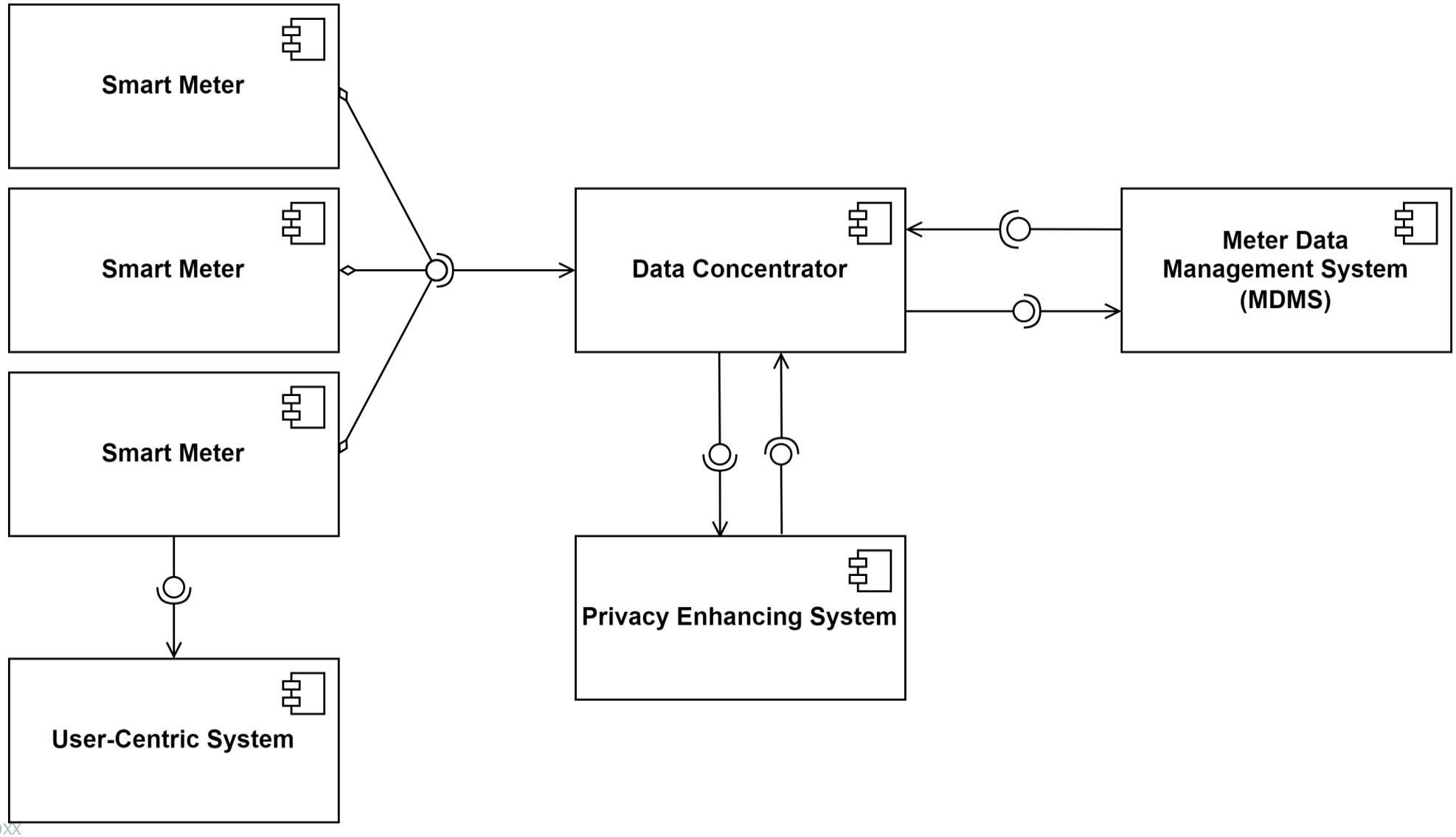
Encrypt data in transit and at rest

Data Minimization

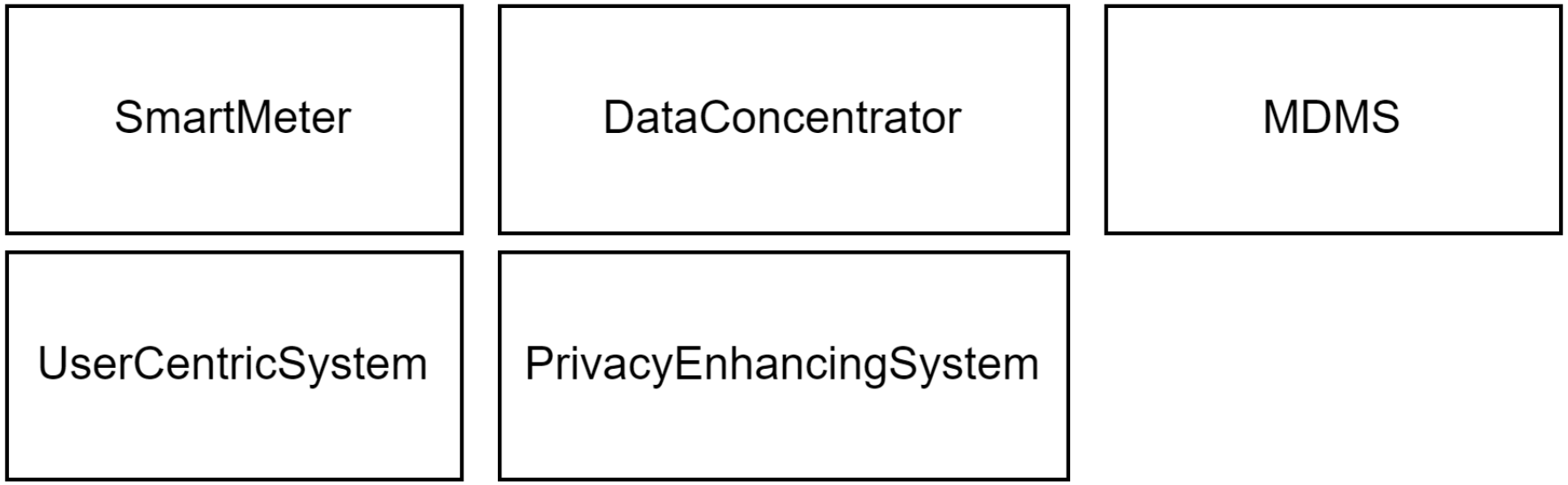
Collect only the necessary data required and incrementing the time between data collection.

Our System

General Overview

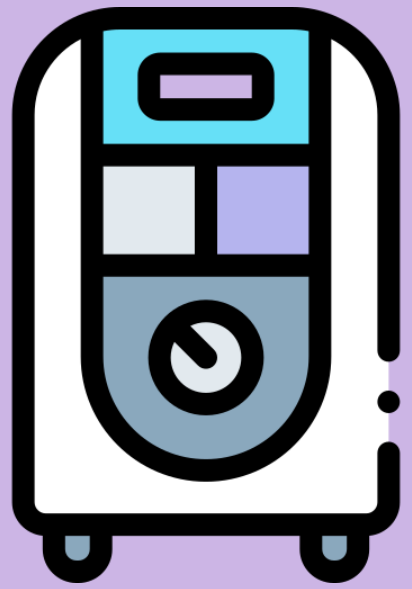


General Overview



The Smart Meters

- Simulation of the hardware
- Database of meter readings
- Immediate AES encryption

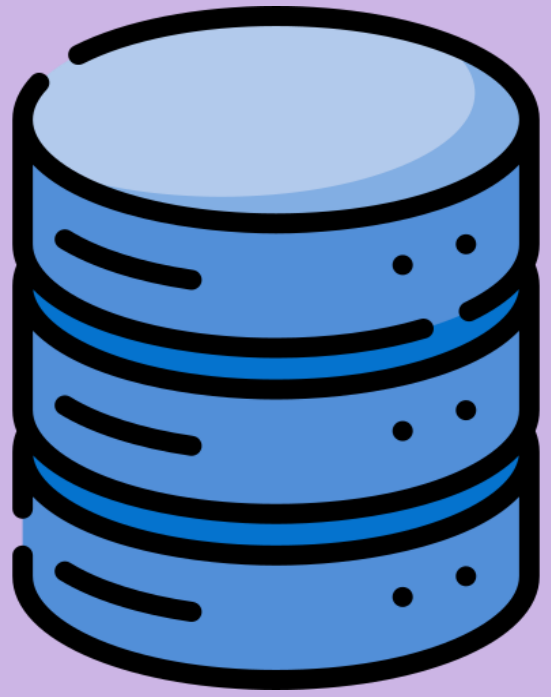


The Data Concentrator

- Acts as the middleman
- Transfers data
- No processing

The Privacy-Enhancing System

- Main focus
- Paillier Encryption
- Aggregates the data and forwards it to the data concentrator



The Meter Data Management System (MDMS)

- Secure communication between smart meters and MDMS
- Stores aggregated RSA encrypted data
- Pallier overhead is problematic for the MDMS
- Data already aggregated in PES and less granular by Pallier
- Real systems use algorithms such as RSA

The User-Centric System

- User access to their own data
- Hashed passwords

Privacy: Before and After

	Before	After
Anonymization	**Depends**	**Yes,** by aggregating
Encryption in transit	**Yes**	**Yes**
Encryption at rest	**No**	**Yes,** pallier encryption allows us to work with encrypted data.
Data Minimization	**No**	**Yes,** collect only the necessary data required for billing and system operation

Demo of Simulation

Videos:

- UCS demo
- PES demo
- UI/MDMS demo

Limitations

- Paillier encryption performance overhead
- Decryption and immediate re-encryption
- Possibility of function creep (soft privacy)

Thank You!