

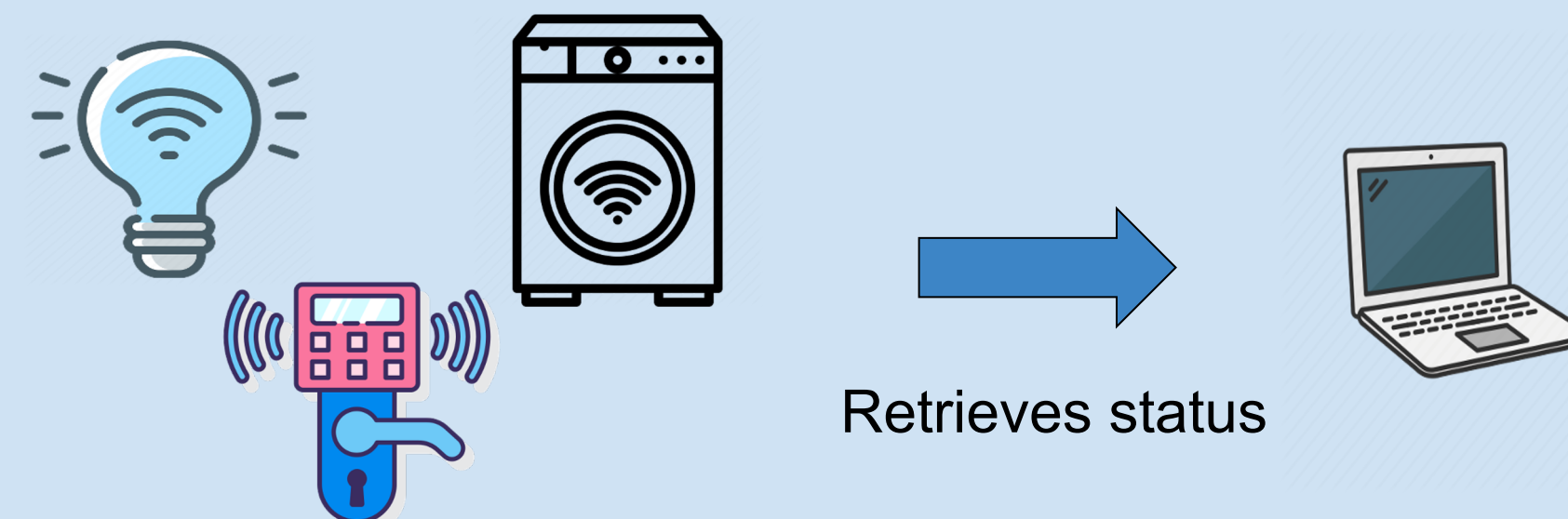
Motivation

- ❑ Unexpected security risks in the IoT systems deployed in smart homes
- ❑ Rising privacy concerns of the smart home device users
- ❑ Lack of early threat detection systems for smart homes

How our framework works?

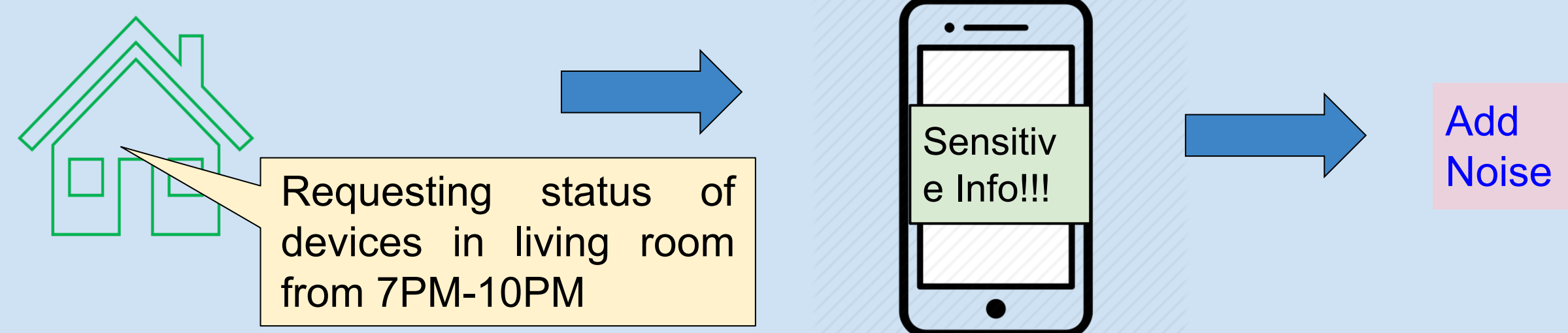
1) Data collection:

- Collect behavioral data from IoT devices
- Integrate them based on timestamp



2) Preserve privacy

- Access Control
- Adding noise

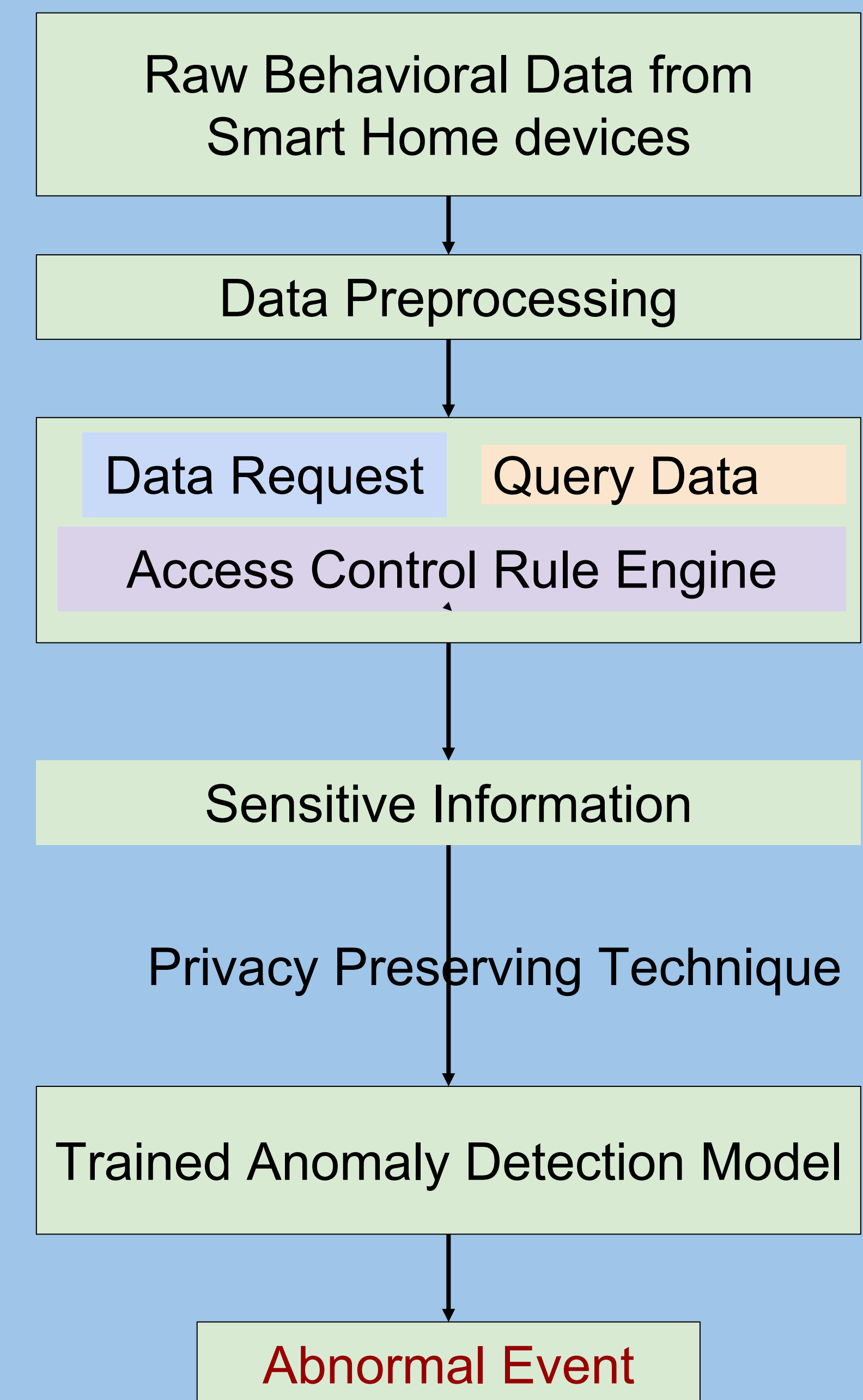


3) Detect Anomalous Scenarios

- Train the models with the noise added data
- Calculate the threshold score for the trained model
- Identify abnormalities whenever a sequence exceeds threshold score
- Alert the user



Architecture



Conclusion and Future Work

- ❑ We collected data for a period of three weeks from deployed IoT devices and detected anomalous scenarios.
- ❑ In our future work, we would add noise to sensitive information and measure accuracy of anomaly detection model.

