19th International School on Foundations of Security Analysis and Design - FOSAD 2019

A Trusted Execution Environment-based Architecture to Protect Sensitive Data in Cloud/Fog-based IoT Applications

Dalton Cézane

Embedded Systems and Pervasive Computing Laboratory

Electrical Engineering and Informatics Center

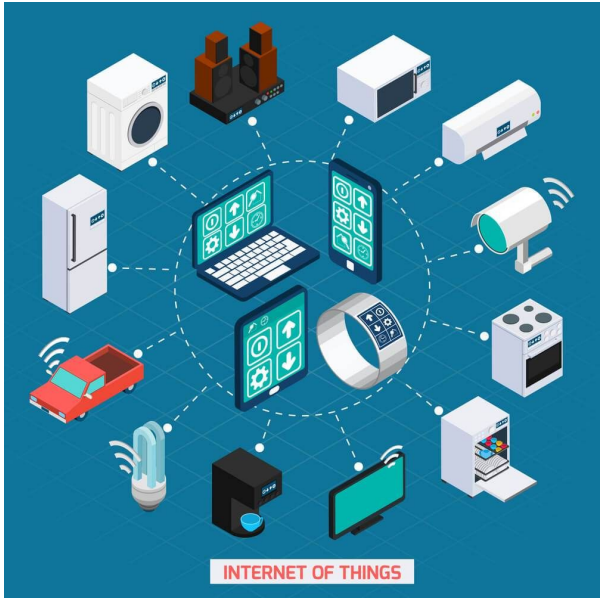
Federal University of Campina Grande

Agenda

- Introduction
- Basic IoT scenario
- Security/privacy concerns
- Research questions and threat model
- Solution principles and proposal
- Technologies used and preliminary evaluation
- Solution achievements and next steps
- Partial results

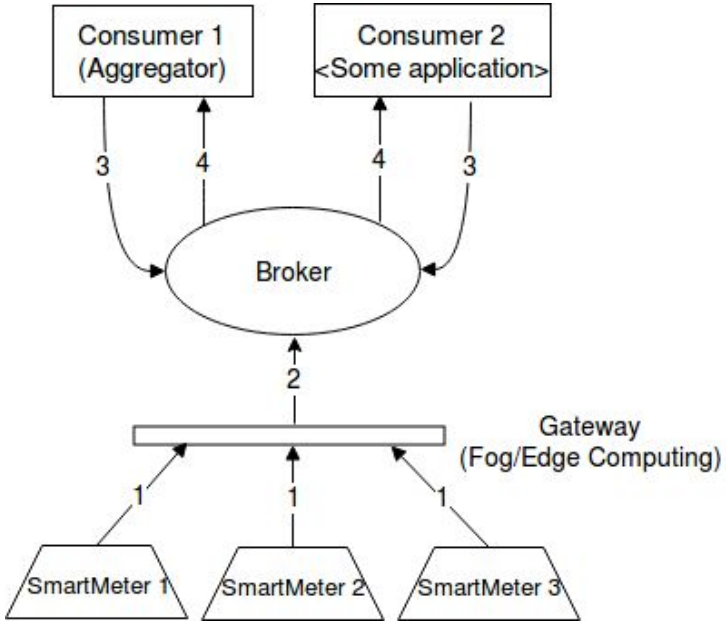
Introduction

- **Wide variety of IoT applications**
  - Distributed components
  - Cloud-based IoT (analysis, storage and processing)
  - Sensitive data (eg. Personally Identifiable Information) demand security/privacy concerns
  - Need for ensuring an acceptable level of trust



Basic Scenario

- **Smart Metering Application**
  - Producers (smart meters) generating energy consumption data
  - Producers sending data to a broker (e.g. publish/subscribe system)
  - Consumers receiving data through notifications
  - Consumers handling energy consumption data (eg. for billing purposes)



Basic architecture

Security/Privacy Concerns

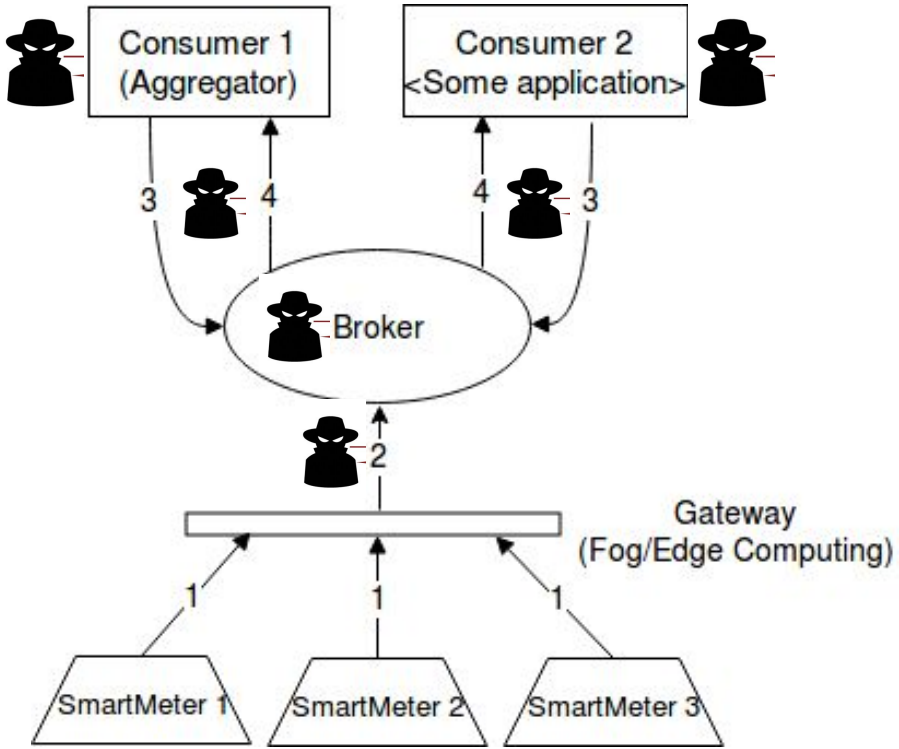
- **NIALM (Non Intrusive Appliance Load Monitoring) techniques**
  - Identify the use of household items/electronic devices by analysing energy consumption through time
- **An adversary can estimate**
  - What people are doing in a house?
    - *Taking shower? Watching TV? …?*
  - How many people are in the house?

Research Questions

- How to limit the need to trust the storage provider and the consumer?
- How to control access allowing only authorized entities to consume data?

Threat Model

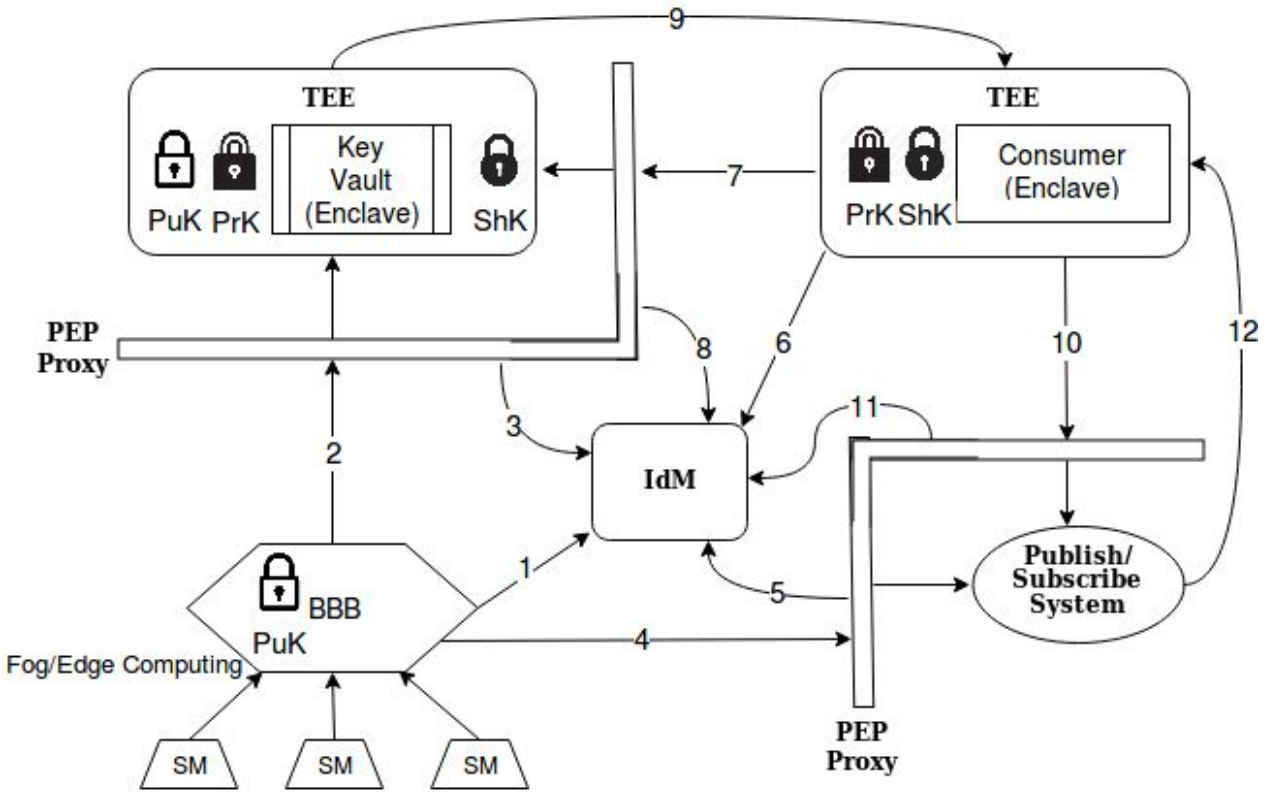
- **Three possible attack surfaces**
  - Consumers
  - Broker (Pub/Sub system)
  - Communication channel



Solution Principles

- **Manage identities and control access**
  - Authentication and authorization for producers and consumers
- **Apply cryptography for sensitive data (energy consumption)**
  - Encrypt data in the producers, in order to avoid data leakage
  - Decrypt only in a TEE (Trusted Execution Environment) consumer
- **Manage cryptographic keys**
  - Control the keys generation, distribution and storage within a TEE
- **Consider security for communication channel (TLS/HTTPS)**

Solution - Architecture



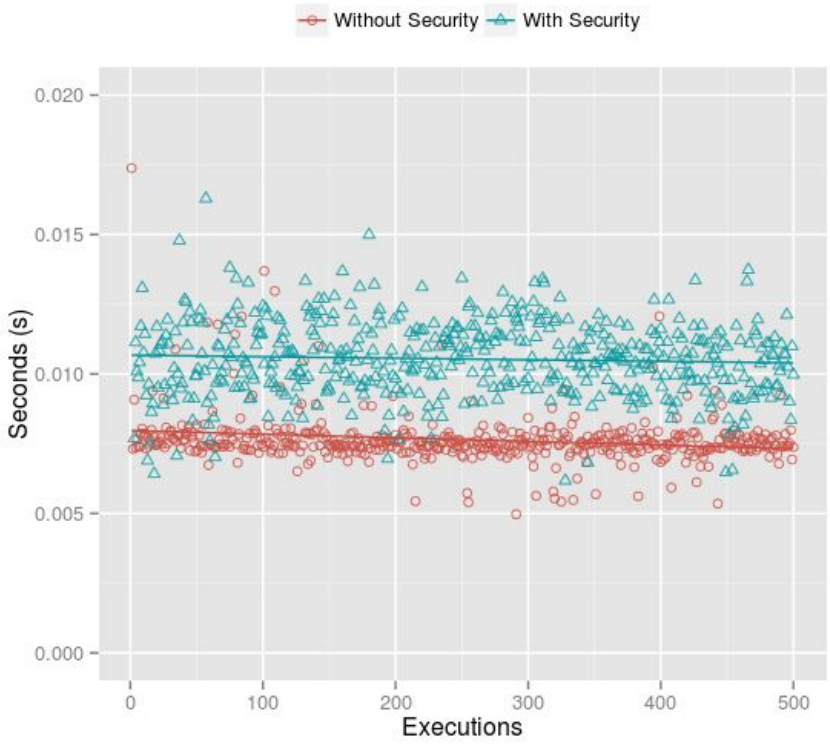
Solution Technologies

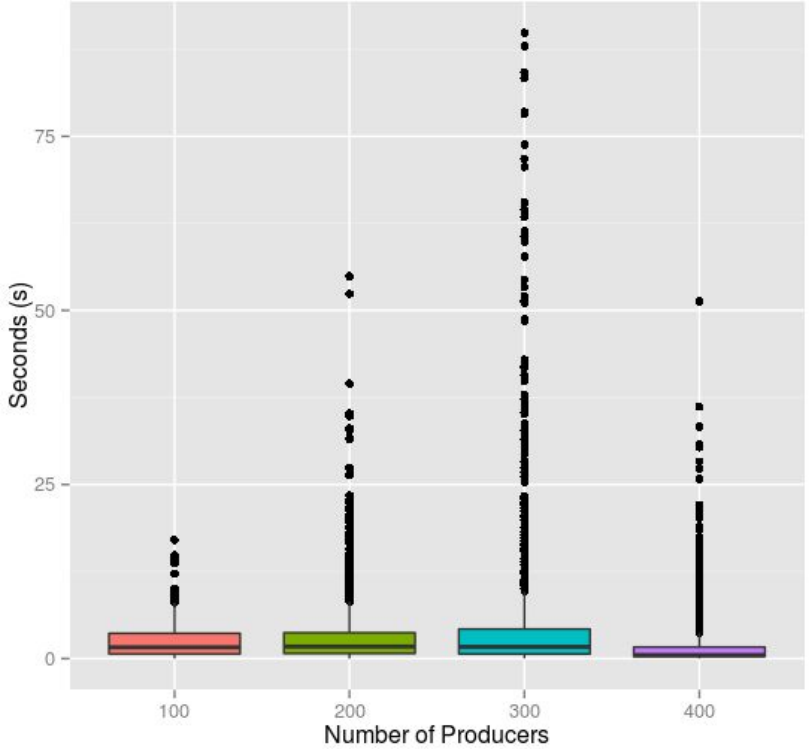
- **FIWARE Keyrock Identity Management (IdM)**
  - Authentication, OpenStack Keystone/Horizon modified and OAuth2 (tokens provisioning and validation)
- **FIWARE Wilma Policy Enforcement Point (PEP) Proxy**
  - Basic access control to applications, verifying OAuth2 tokens with Keyrock IdM
- **FIWARE Orion Context Broker**
  - Context data manager, Pub/Sub and RESTful API

Solution Technologies

- **Intel Software Guard Extensions (SGX)**
  - Creates an isolated protected region of memory (enclave)
  - Trusted applications protected even from high privilege users (eg. admin)
  - Remote attestation process enables third parties to validate if the application runs on a real Intel SGX
- **Key Vault (proposed component)**
  - Key generation, storage and distribution
  - Asymmetric cryptography (Public key for producers; Private key for consumers)
  - Running in Intel SGX (Attested by producers; Attest consumers)

Solution - Preliminary Evaluation



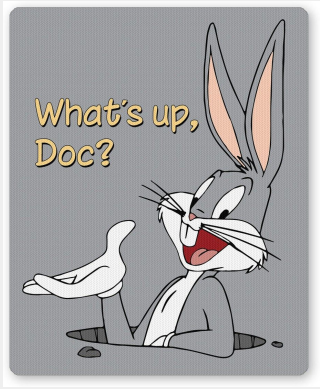


Achievements and next steps

- **Solution achievements**
  - Confidentiality, Integrity and Privacy (Data)
  - Authentication/Authorization (Producers and Consumers)
  - Secure communication (Channel)
- **Next steps**
  - Modelling the proposed architecture with a Coloured Petri Net (partially modelled)
    - *Communication flow and some threats, considering the threat model*
  - Doing a Systematic Literature Review (SLR) regarding the use of TEE for IoT applications
    - *Currently at "data extraction phase"*

Partial results

- VALADARES, D. C. G.; SILVA, M. S. L.; BRITO, A. E. M.; SALVADOR, E. M. **Achieving Data Dissemination with Security Using FIWARE and Intel Software Guard Extensions (SGX)**. In: International Symposium on Computers and Communications (ISCC). 2018, Natal, RN, Brazil. (**Best local paper award**)
- VALADARES, D. C. G.; PERKUSICH, A.; GORGÔNIO, K. C.; **A Trusted Execution Environment-based Architecture to Protect Sensitive Data in Cloud/Fog-based IoT Applications.** (Poster) In: Latin American Student Workshop on Data Communication Networks (SBRC/LANCOMM). 2019, Gramado, RS, Brazil. (**Selected as one of the best submissions**)



Questions?

A Trusted Execution Environment-based Architecture to Protect Sensitive Data in Cloud/Fog-based IoT Applications

Any suggestions or comments are welcome. Thank you!

Dalton Cézane Gomes Valadares, Kyller Costa Gorgônio and Angelo Perkusich

dalton.valadares@embedded.ufcg.edu.br
caruaru.ifpe.edu.br