ITU Kaleidoscope 2015

Trust in the Information Society

AUTONOMIC TRUST MANAGEMENT IN CLOUD-BASED AND HIGHLY DYNAMIC IOT APPLICATIONS

Suneth Namal*, Hasindu Gamaarachchi*,
Gyu Myoung Lee**, Tai-Won Um***
University of Peradeniya*, LJMU**, ETRI***
namal@ce.pdn.ac.lk*

Barcelona, Spain
9-11 December 2015

Agenda

- Problem Statement
- Related Work
- Challenges of Trust Management in IoT
- Cloud Integration in IoT
- Decomposition of the Problem :
  - Use of MAPE-K Feedback Loop
- Trust as a Service (TaaS)
- Cloudifying TaaS
- Simulation and Results

Problem Statement

- Internet of Things (IoT) is seamlessly integrating physical objects to provide advanced and intelligent services for human beings

- Therefore, trust on IoT devices plays an important role in IoT based services and applications

- We present an autonomic trust management framework
  - based on MAPE-K feedback control loop
  - to evaluate the level of trust in an IoT cloud ecosystem

Related Work

- Yan et al., “A survey on trust management for Internet of Things” :
  - survey on trust management for IoT that discusses the current state of art, open issues and key challenges
- Chen et al., “Trm-iot: A trust management model based on fuzzy reputation for internet of things” :
  - trust model for IoT that uses fuzzy sets
- Noor et al., ““Trust as a service : a framework for trust management in cloud environments” :
  - framework for trust management in cloud environments called Trust as a Service

Challenges of Trust Management in IoT

- Existing trust management protocols do not scale well
  - due to limited storage and computation power

- IoT systems evolve with new applications, services, and nodes, frequently joining and leaving the systems

- Requirement of capability to compensate the human errors at some level

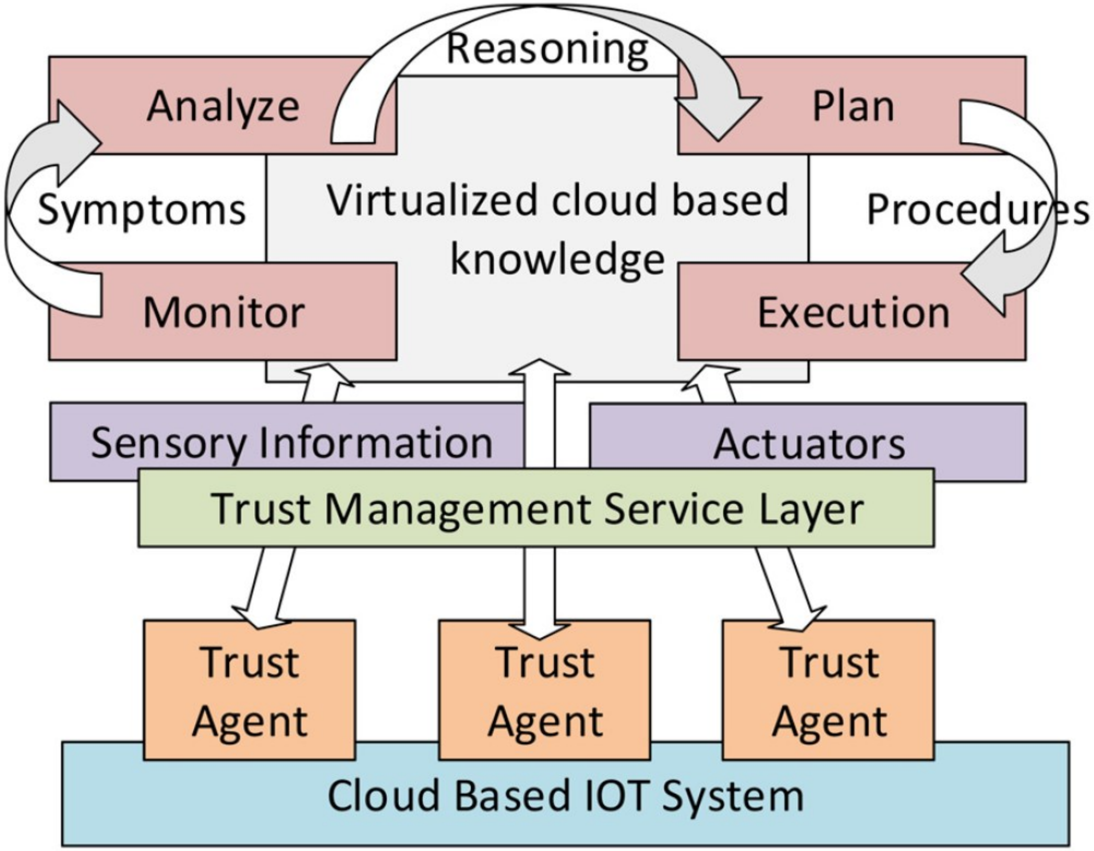
- IoT systems are frequent targets of many cyber attackers, since mostly accessible through wireless networks

Cloud Integration in IoT

- Computing and IoT have evolved independently on their own paths
- Cloud can benefit from IoT by extending to deal with real world things in a more distributed and dynamic manner
- Cloud acts as intermediate layer where it hides all the complexity and the implementation of functionalities
- So far no research carried out in trust management in cloud integrated IoT

Decomposition of the Problem

- MAPE-K feedback loops for adaptive trust agents



Use of MAPE-K Feedback Loop

- The system is highly dynamic : needs adaptive decision making and autonomic agents with control loops to manage resources

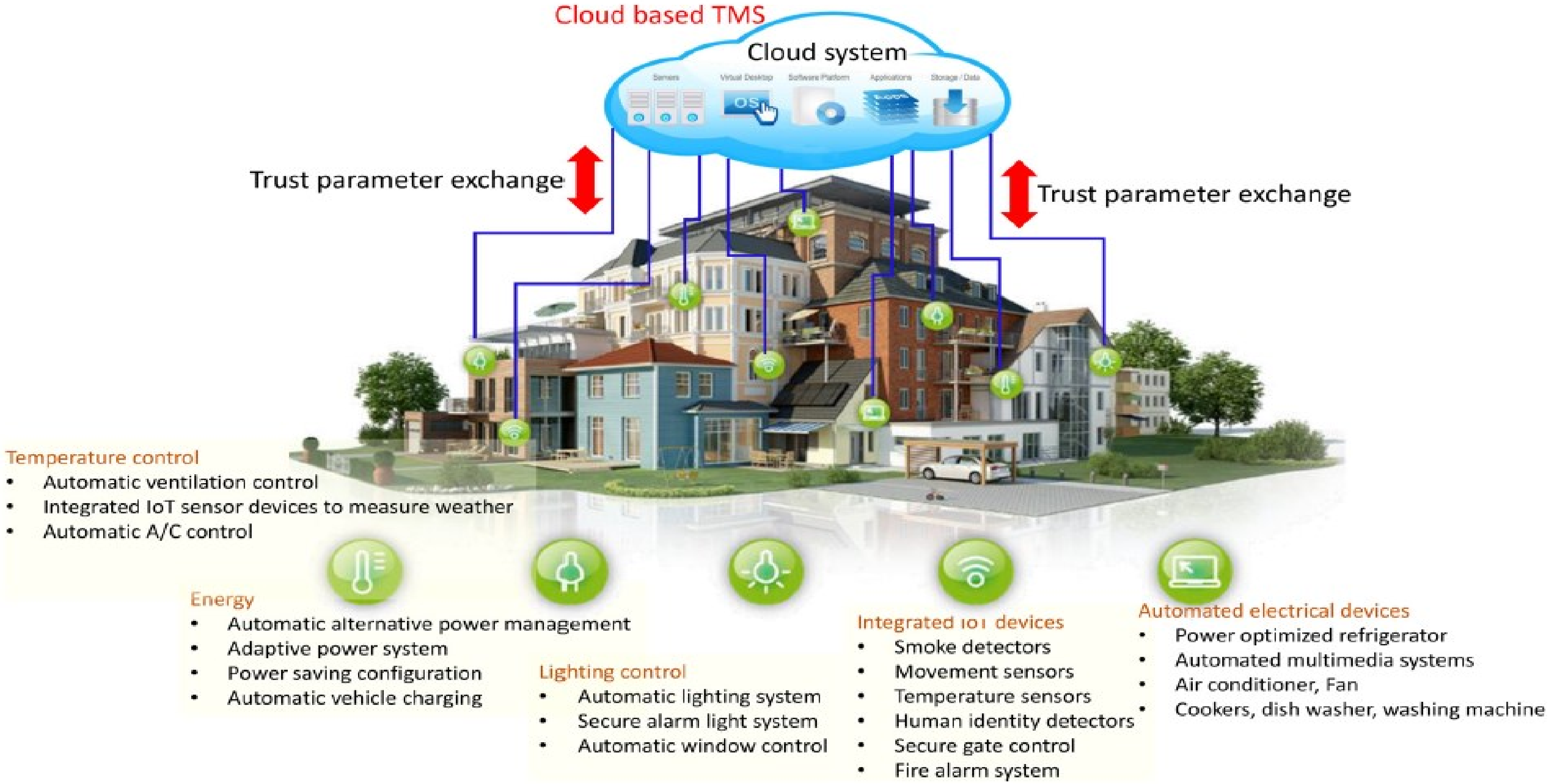
- A promising approach to handle such dynamics is self-adaptation realized by a MAPE-K feedback loop

Trust as a Service (TaaS)

- Cloud is a flexible framework to implement services : “Trust” can be thought of one of them
- An effective trust management system helps cloud service providers and consumers reap the benefits brought about by cloud computing
- But the trust on IoT devices and their applications in real-world is critical
- There have been many different approaches to enhance the trust over information and devices

Trust as a Service (TaaS)

- Smart home environment with the trust management system



Temperature control
- Automatic ventilation control
- Integrated IoT sensor devices to measure weather
- Automatic A/C control

Energy
- Automatic alternative power management
- Adaptive power system
- Power saving configuration
- Automatic vehicle charging

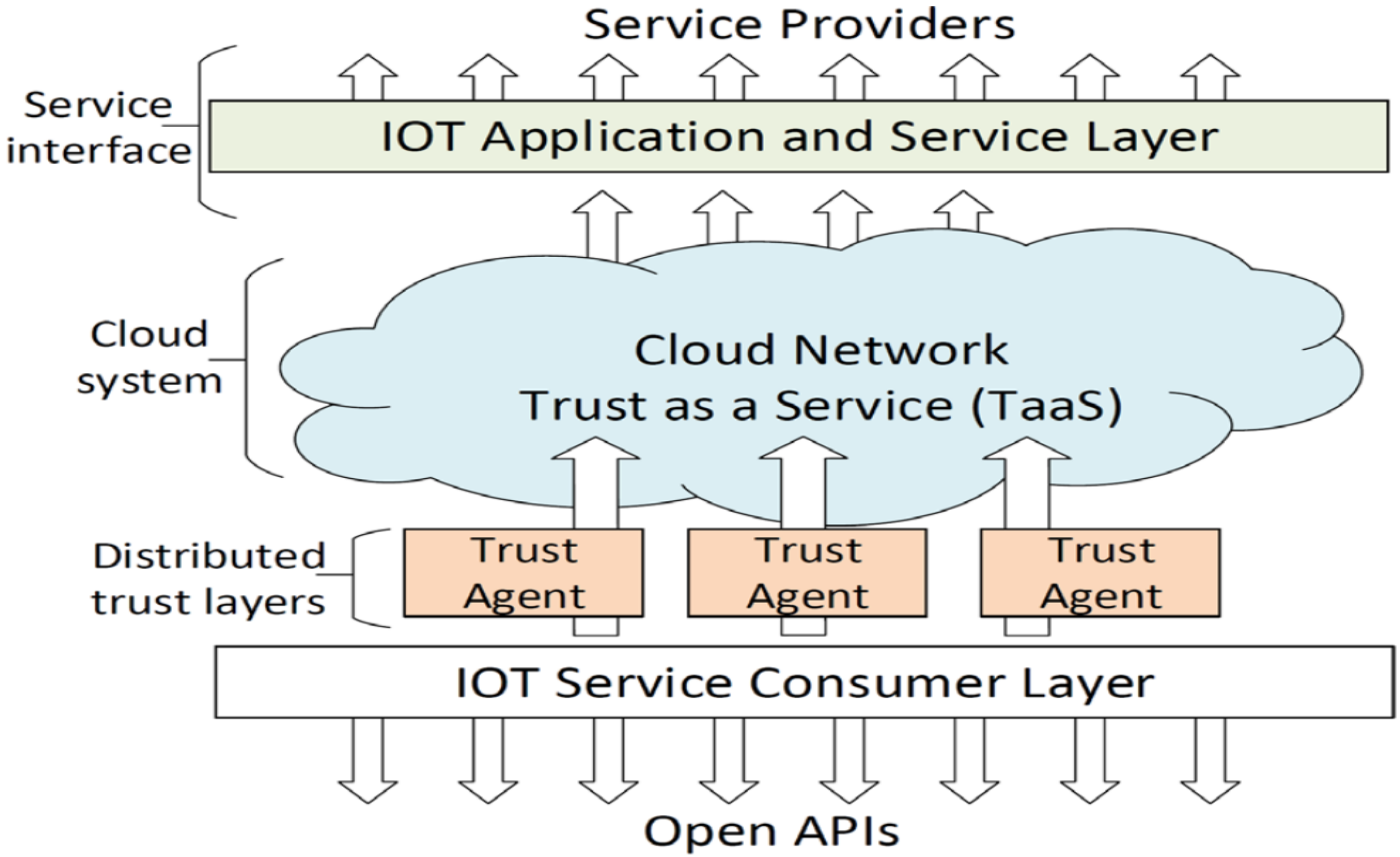
Lighting control
- Automatic lighting system
- Secure alarm light system
- Automatic window control

Integrated IoT devices
- Smoke detectors
- Movement sensors
- Temperature sensors
- Human identity detectors
- Secure gate control
- Fire alarm system

Automated electrical devices
- Power optimized refrigerator
- Automated multimedia systems
- Air conditioner, Fan
- Cookers, dish washer, washing machine

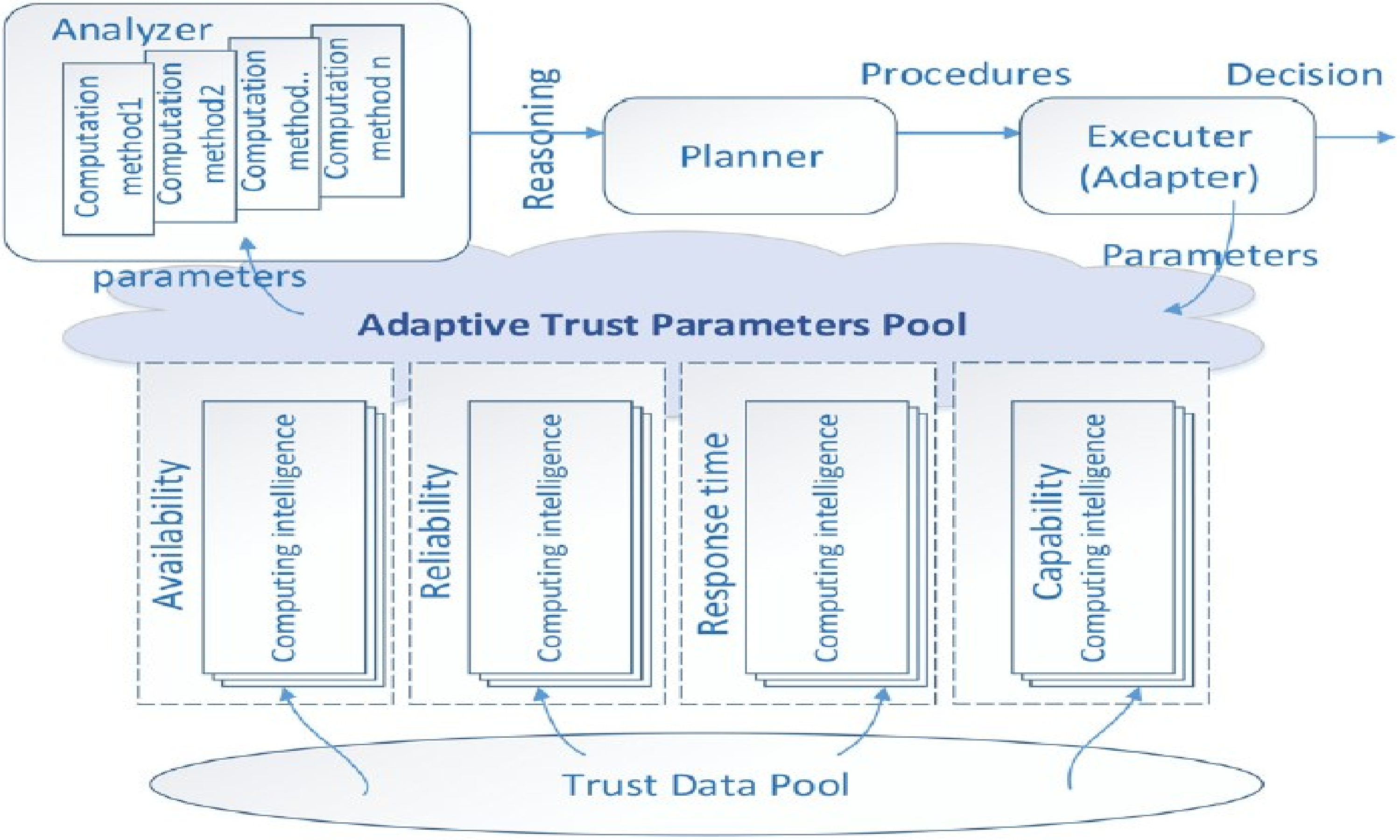
Cloudifying TaaS

- Overview of the solution architecture



Cloudifying TaaS

- State of art of trust agent

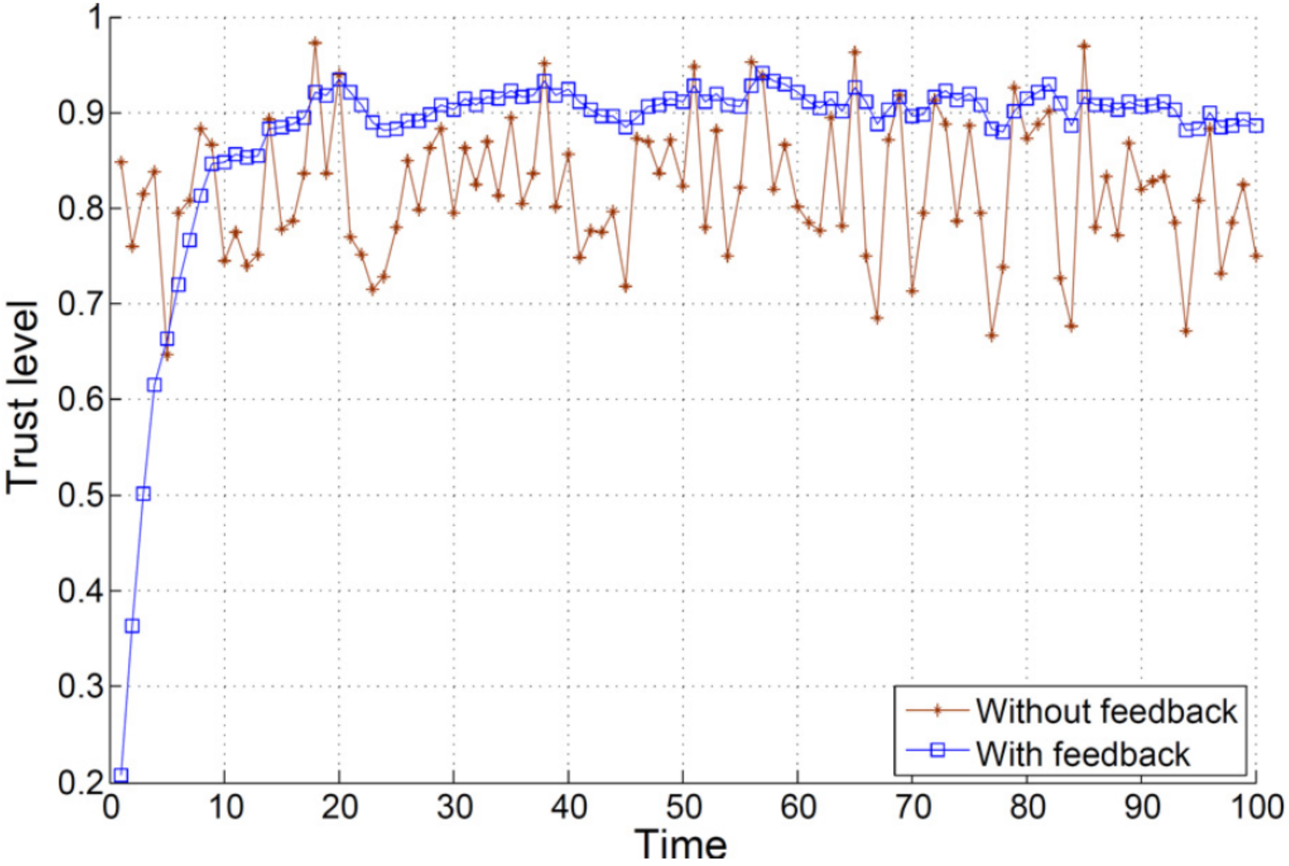


Cloudifying TaaS

- We consider four trust related parameters
  - **Availability** is making the resources available for users. The trustworthiness of a system lies on whether the resources are available when required.
  - **Reliability** defines the level of trust among two entities. A reliable system always produces correct information.
  - Irregularities in **response time** predicts possible intrusions in the system. That helps to identify changes from normal.
  - **Capacity** assures accessibility in one hand and scalability on the other hand.

Simulation and Results

- Effective level of trust (Aggregated availability, reliability, response time and capacity)


Trust level
Time
Without feedback
With feedback