Context-Aware Access Control Model for Services Provided from Cloud Computing

Ichiro Satoh

Researcher, National Institute of Informatics /

The chairman of working group for technical issues on personal data, the Cabinet Secretariat of Japan

E-mail: ichiro@nii.ac.jp

Outline

- Motivation
- Problem statement
- Requirements
- Design and Implementation
- Evaluation
- Conclusion

A framework to enable context-aware services in mobile and pervasive computing to be provided from cloud computing.

It can bridge a gap between context-based access control model and role-based access control model used in commercial cloud computing platforms.

Introduction

- Context-aware services tend to be used in pervasive computing settings
  - Such computers have limited computational resources.
  - Context-aware services themselves are often provided from cloud computing.
  - The final goal is to support city-level context-aware systems with a large number of users for multiple purpose on IoT infrastructures

- However, access control models for context-aware services and in cloud computing are different.
  - The purpose of this work is to bridge gaps between context-aware models in context-aware services and cloud computing.

Background

- Our projects had many experiments on context-aware services in the real world, e.g., shopping malls and museums.
  - For example, our context-aware visitor navigation services had been used in several museums, e.g., national science museum of Japan
    - The services supported annotations about exhibits according to visitors' context and behaviors in the museums.
- Services were provided from cloud computing platforms in addition to local pervasive or mobile computers.

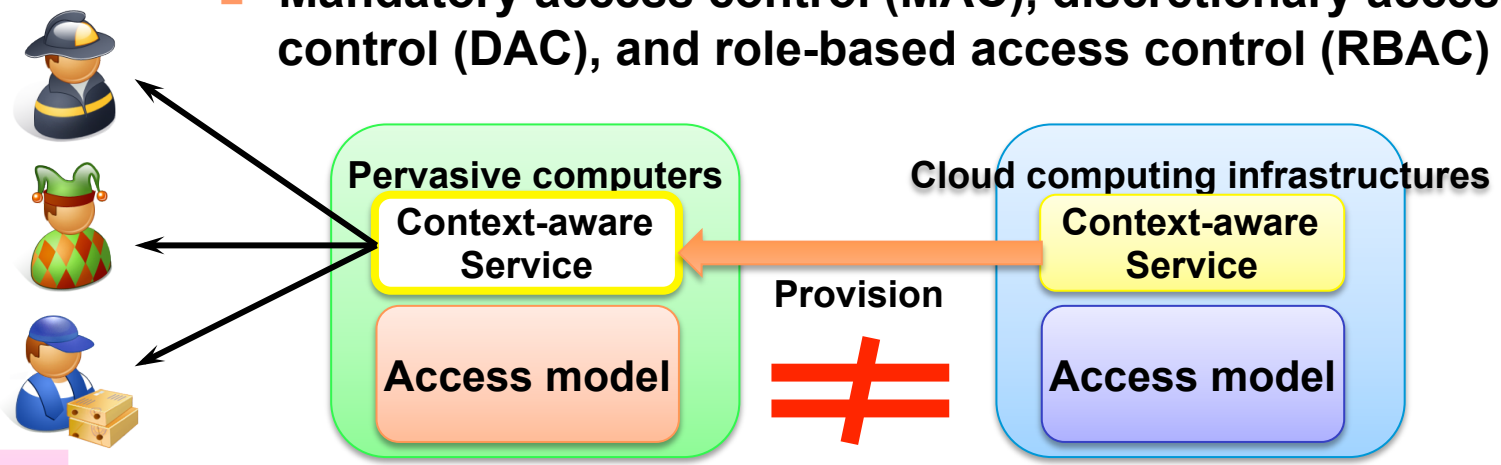
Introduction

- Context-aware services tend to be used in pervasive computing settings
  - Such computers have limited computational resources.
  - Context-aware services themselves are often provided from cloud computing.
  - The final goal is to support city-level context-aware systems with a large number of users for multiple purpose on IoT infrastructures

- However, access control models for context-aware services and in cloud computing are different.
  - The main contribution of this work is to bridge gaps between context-aware models in context-aware services and cloud computing.

Gap Between Access Control Models

- When services are provided from cloud computing, there are gaps between security mechanisms, e.g., access control models, in pervasive computing in cloud computing.
  - In context-aware computing:
    - Access controls based on context or subject in the real world
  - In cloud computing:
    - Mandatory access control (MAC), discretionary access control (DAC), and role-based access control (RBAC)



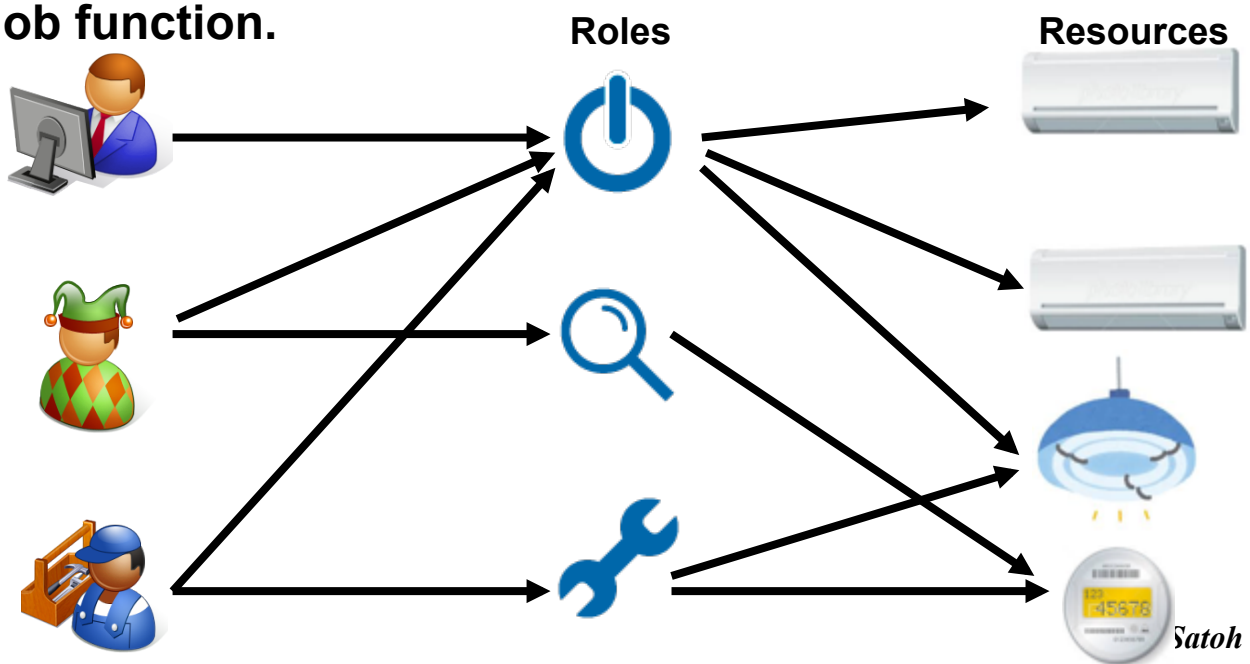
- There is mismatches between access control models in pervasive computing and cloud computing.

Our goal is to bridge gaps between them.

Access Control Models in Cloud

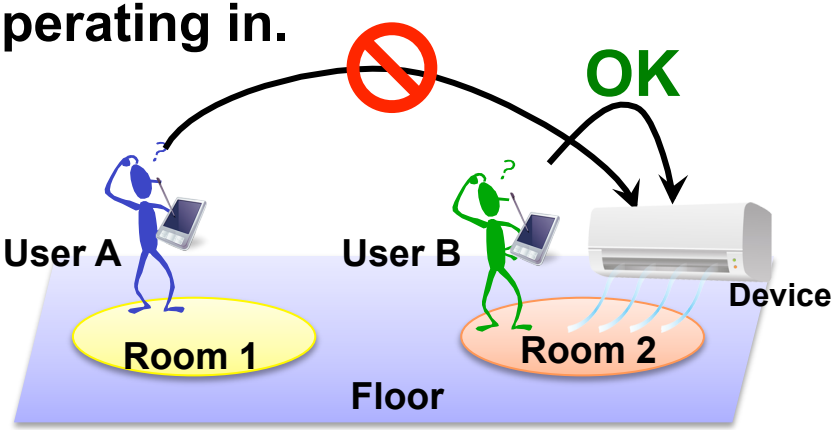
- Most commercial cloud computing platforms support conventional access control models, e.g., Mandatory access control (MAC), discretionary access control (DAC), and role-based access control (RBAC)
  - For example, role-based access control (RBAC).
    - A user has access to resources according to his/her assigned role.
    - Roles are defined based on job functions.
    - Permissions are defined based on job authority and responsibilities within a job function.

Such models may be useful in server-sides, but in pervasive computing context-aware access control models are needed.



Context-based Access Model

- **In context-aware services, permissions should be associated with contexts, and subsequently subjects are associated with the contexts they are currently operating in.**

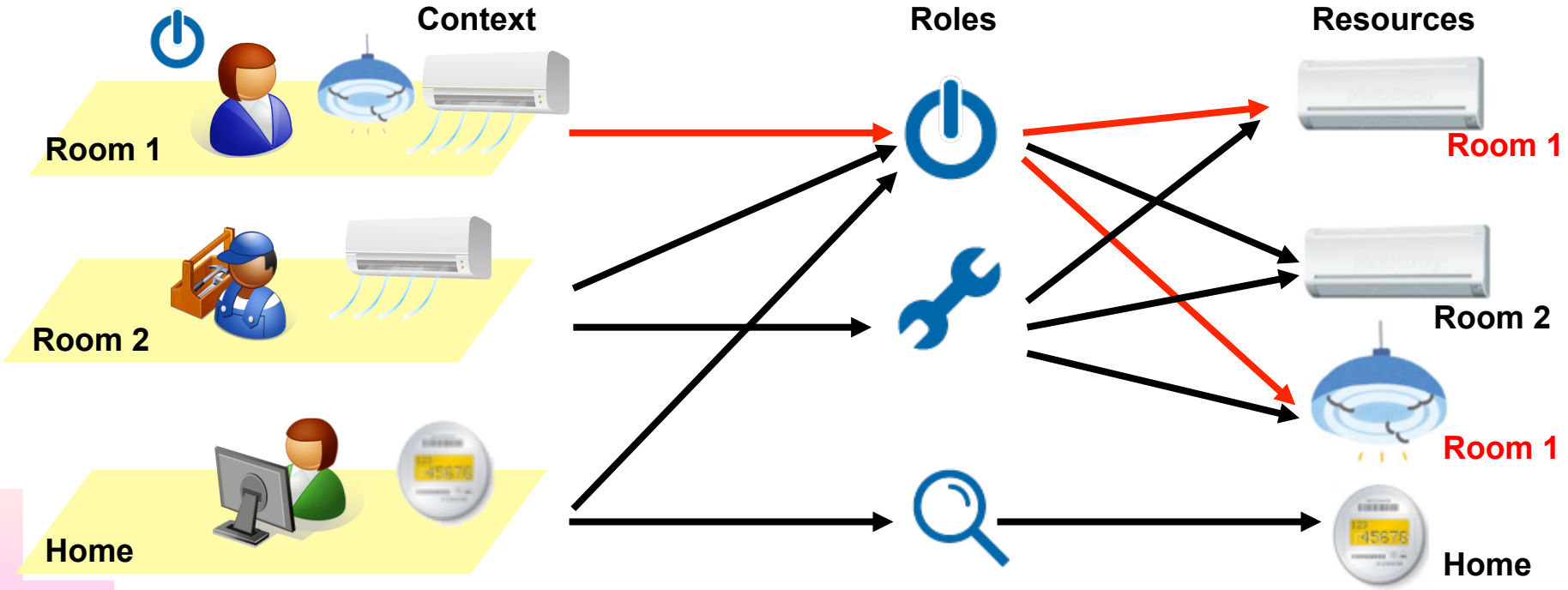


Example scenarios:

- **Only while a user is in the room, his/her smart phone should have the capability to control the devices in the room.**
- **Anyone who are not in the room should not.**
- **Administrators should have the capability of managing devices in the house (subject-based AC)**

Connecting Context-centric AC to Role-based AC

- When services are provided from cloud computing, context-aware services need to be managed based on the access control supported in cloud computing, e.g., RBAC.

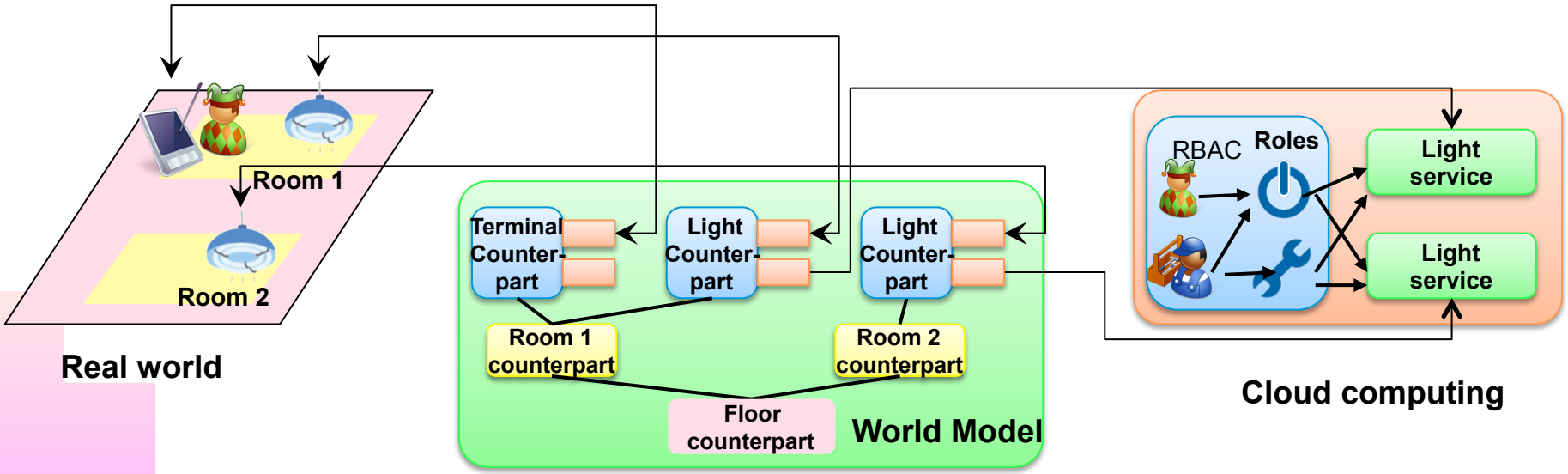


- Our framework maps from contexts to roles.
- It needs to access only the targets according to context.

Ichiro Satoh

Approach

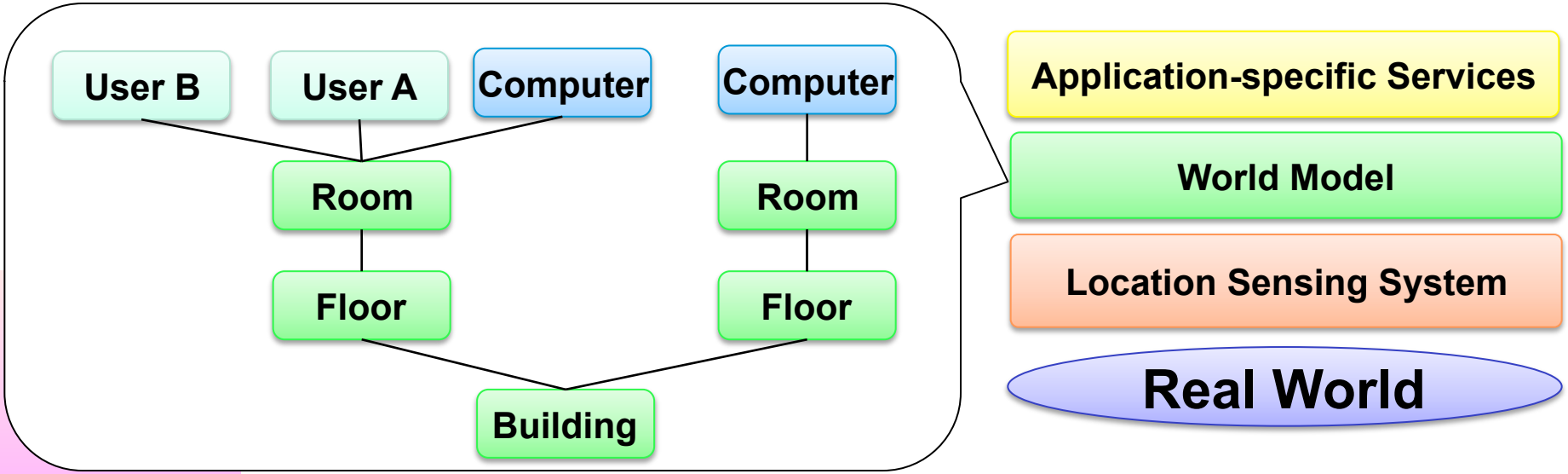
- To support context-based access control, our approach introduces a world model to represent contexts in the real world and to connect between pervasive computers and services provided from cloud computing.
  - The model consists of counterparts as representations of their targets, e.g., person, objects, and spaces, in the real model.
  - The model supports a context-aware service broker to find and invoke services support in cloud computing, which is managed in RBAC and so on.



- Subject-based access control in pervasive computing is supported by using Cloud's RBAC.

World Model

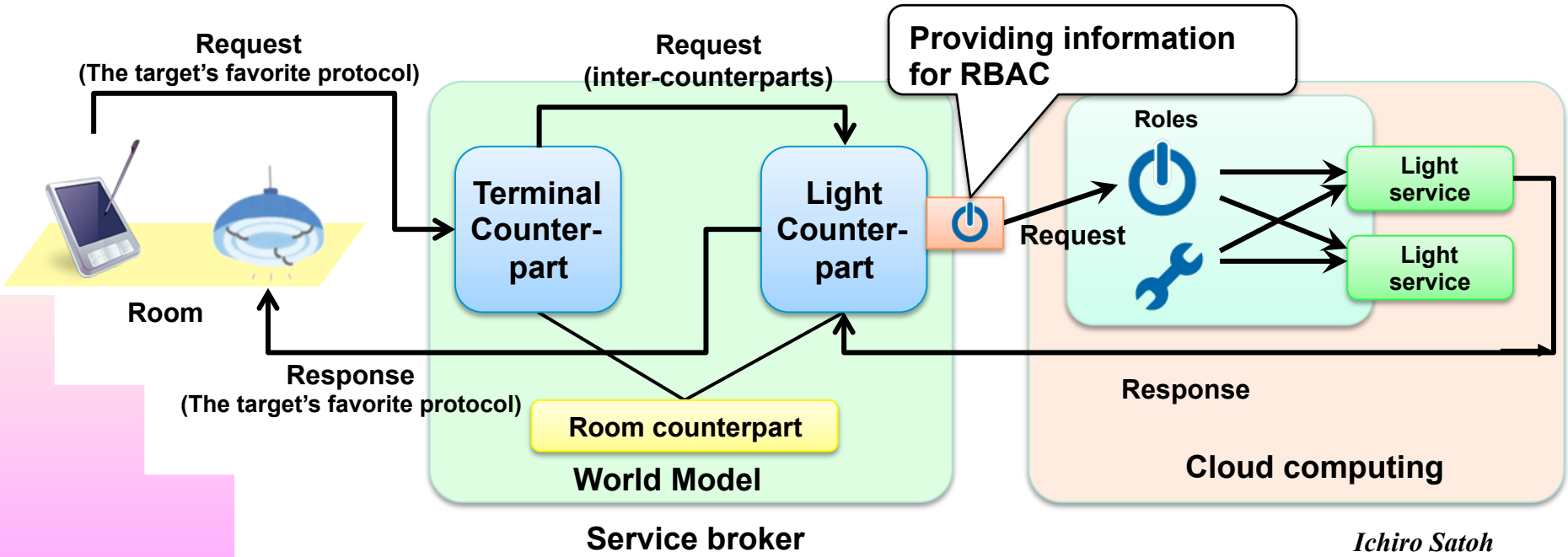
- Counterparts are representatives of their targets and programmable entities and used as proxies to access cloud services on behalf of the targets
  - They are structurally organized according to containment relationships between them by using several location-sensing systems.
    - e.g., Active RFID, WiFi-based TDoA locating systems
- The model manages location-based access control.
  - Each counterpart can access the services that are coupled with its neighboring and descendant counterparts via the model.



The author is a member of ISO SC31 (for RFID and real-time locating systems) *Ichiro Satoh*

Connection between Context-Aware AC and Cloud's AC Models

- Services in cloud are loosely coupled to the counterparts of their targets, e.g., users' smartphones and appliances
  - The framework abstract away differences in access control models used in cloud computing, e.g., RBAC, DAC, and MAC
  - It enables pervasive devices to indirectly interact with services via their counterparts organized in a tree structure based on the containment relationships between people, devices, and spaces.

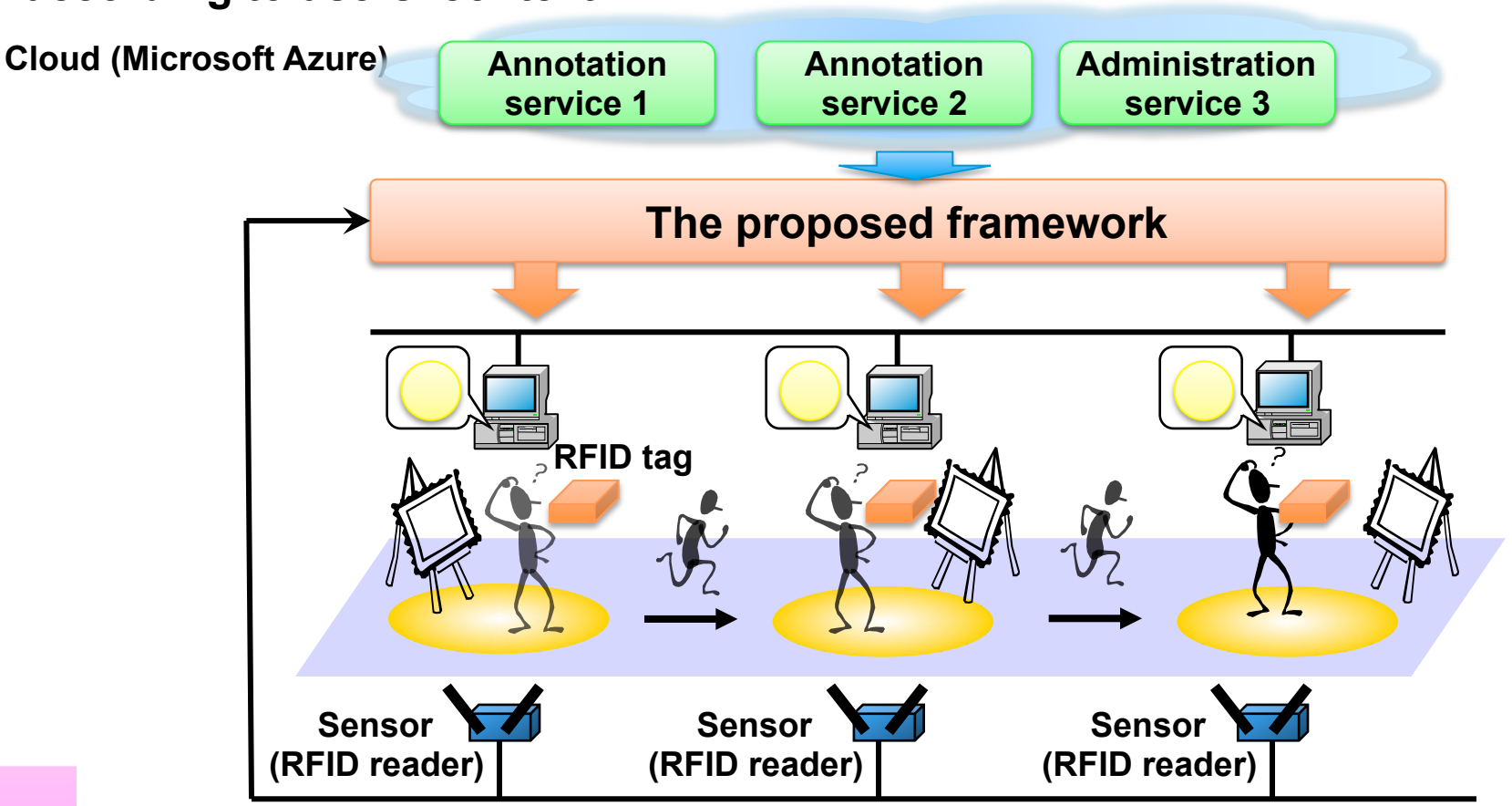


Ichiro Satoh

Experiment

In the experiment at the Museum of Nature and Human Activities (Hyogo, Japan) for a month.

- When a user moves to an exhibit in a museum, it automatically presents annotations at computers close to the exhibit in a museum with RFID.
  - Services provided from MS Azure (under RBAC) could be controlled according to users' context.



The author is a member of ISO SC31 (for RFID and real-time locating systems)

Ichiro Satoh

Lesson Learns from Experiences

- Sensing errors
  - Sensing and computing systems are not perfect.
    - There is no perfect solution, but
    - The framework could inform such errors to context-aware services, administrators, and users.
- User-conflicts
  - The framework could explicitly inform services when detecting multiple users beyond services' assumptions.

Conclusion

- A framework could bridge a gap between access control models in context-aware services and cloud computing.
  - It could abstract away access control models in commercial cloud computing platforms and be independent of implementations of services in cloud.
  - This mismatches are general when providing context-aware services from cloud computing.

- Future work.
  - The current implementation was a little ad-hoc because its original purpose was to construct a practical (and ad-hoc) system used in an experiment in the real world.
  - We plan to reconstruct the framework as an academic prototype system.