HITACHI
Inspire the Next

Advanced Access Control Mechanism for Mobility as a Service Platform

Anjali Rajith, Sakurai Soki

anjali.rajith.he@hitachi.com, soki.sakurai.mk@hitachi.com

SECURWARE 2022,
Lisbon, Portugal

Research & Development Group,
Hitachi Ltd., Yokohama, Japan

October 17-20, 2022

About Me

Anjali Rajith joined Research & Development Group, Hitachi Ltd, Japan in December 2015. She graduated from Tokyo Institute of Technology, Tokyo Japan in 2015.

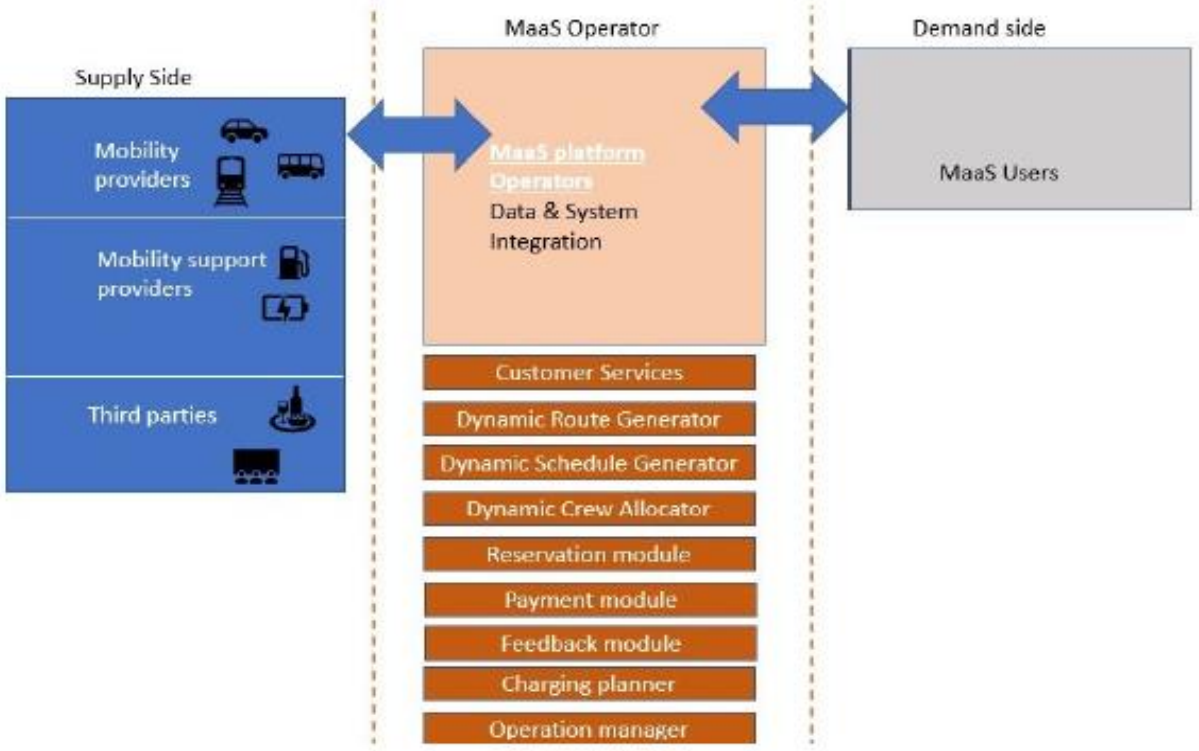
She has involved in various projects related to Industrial IoT platform, data management and analysis, dynamic risk management in autonomous vehicles, functional safety, STAMP-based accident causality models, access control and authentication in different domains such as cross-industrial collaboration platforms, MaaS platforms etc.

Contents

1. Introduction: What is Mobility as a Service (MaaS)?

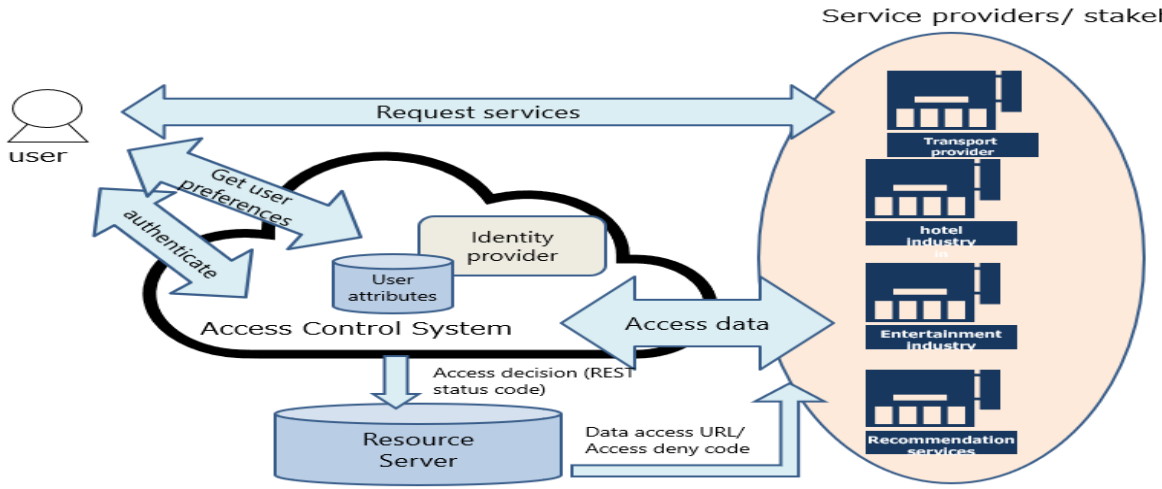
HITACHI
Inspire the Next

- Mobility as a Service (MaaS) is a digital platform that integrates multiple transport providers and third-party service providers into a single platform where customers can easily book and pay for services through a single channel.
- It consists of a supply side, a demand side and a stack of services to coordinate users and services.



1. Introduction: Security Challenges of MaaS platform

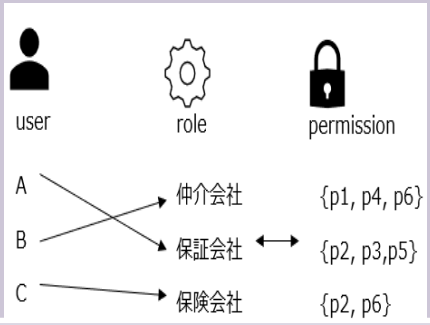
- **Challenge 1: Misuse of personal information of customers.**
  - Confidential customer information that flow through the MaaS can be used by third party services without their knowledge. Therefore, it is necessary to ensure that the platform complies with personal information protection acts.
  - Consider giving of power of consent/revocation to customers.
- **Challenge 2: Accidental data leakage of sensitive information.**
  - Ensure that only minimum necessary information is provided to each service.
  - Protect sensitive information even in the event of accidental data leakage.
- **Challenge 3: Handle insider threats such as service maliciousness which use data for favouring a business/ personal benefits.**
  - Continuous monitoring of trust factor of participating parties in a quantitative manner.



2. Background - Access Control Mechanisms

There are different types of access control mechanisms, whose advantages and disadvantages are studied.

Role-based Access Control (RBAC)



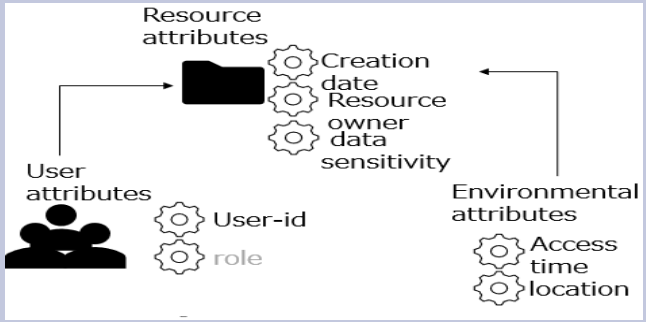
- Each user is associated with roles and roles define permissions.

Enforce rules that provide discretionary access control based on user profiles/ job functions

- Static permission list, permission is given before access attempt

- Less control on access

Attribute-based Access Control (ABAC)



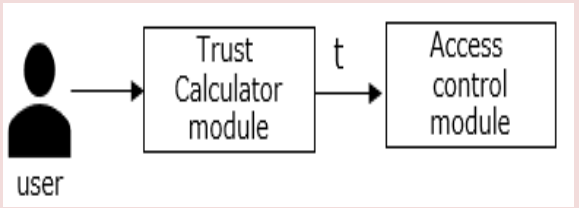
- Access policies are associated to users based on their attributes.

- Access decision is based on meeting the conditions in the policies based on user attribute values during access time

- Not flexible and dynamic.

- Difficulty in traceability.

Trust-based Access Control (TBAC)



- Assigns additional dynamic trust value to users, for mitigating risks, such as fraudulent activities.

- Makes application process smooth and risk-free.

- Probabilistic approach. Lot of security loopholes if implemented alone.

3. Overview of Proposed System

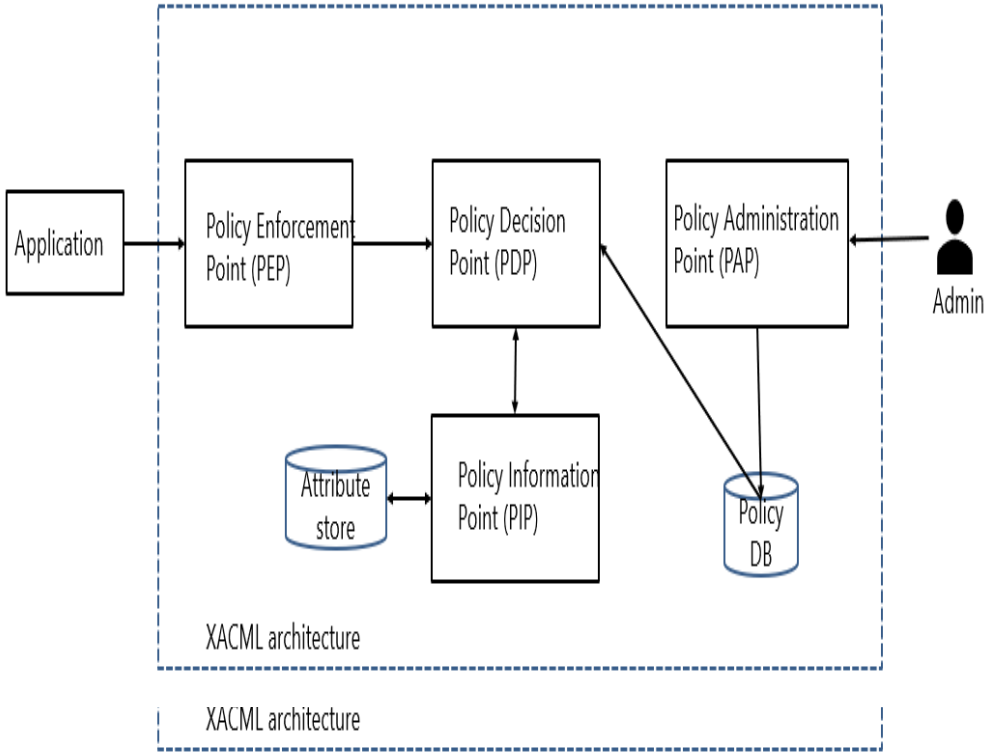
- **An advanced access control system is proposed, which is a combination of fine-grained and quantitative trust computing approach by adding new functionalities to standard XACML* architecture.**
  - **Context-based system:**
    - Data access context is determined based on the context of data access, normal or emergency.
  - **Customer-centric approach:**
    - Customers are given the power to control access to their personal information.
  - **Access logging:**
    - Access logging function logs the data request and response attributes associated to a data requester to an access log database.
  - **Trust computation:**
    - It calculates the trust score of the data requesters based on trust parameters logged in the access log database, as well as security monitoring system.

XACML* : Extensible Access Control Mark Up Language

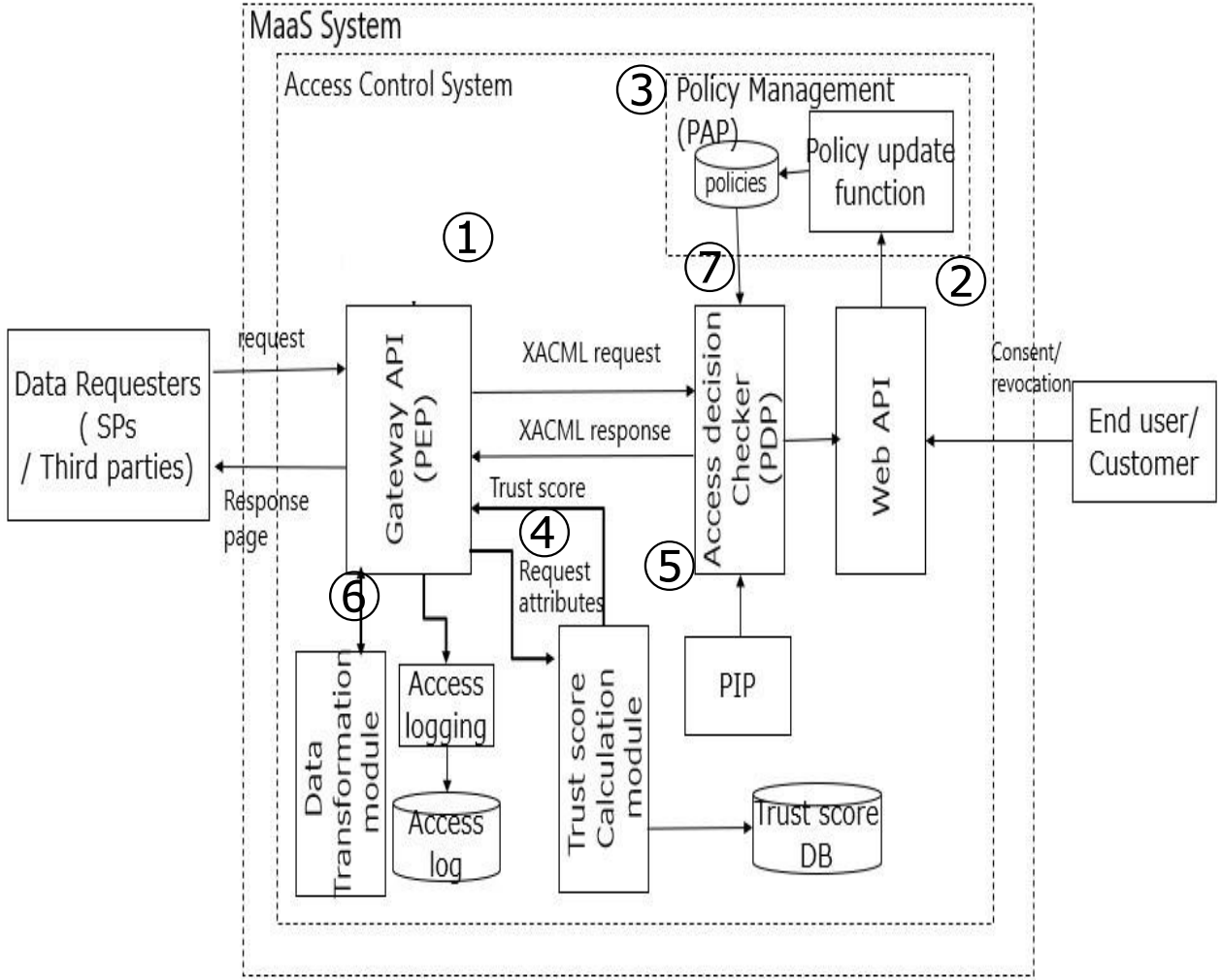
4. Architecture of proposed system

HITACHI
Inspire the Next

The proposed system adds additional functionalities to the standard XACML architecture.



Standard Access Control Architecture of XACML



Proposed approach

4-1 Main components of proposed architecture

HITACHI
Inspire the Next

① Gateway API – Receives the data request/ response and has a context evaluator function.

② Web API – A user interface that allows customers to interact with the MaaS data management layer.

③ Policy Management – Manages the policies and triggers real-time policy update function upon changes.

④ Access logging – logs the access parameters of the data requesters upon trust score calculation.

⑤ Trust calculation module – calculates the trust score of the data requesters and stores in trust score database.

⑥ Data transformation module – masks the sensitive customer information.

⑦ Access decision checker - provides access decision based on the policies defined.

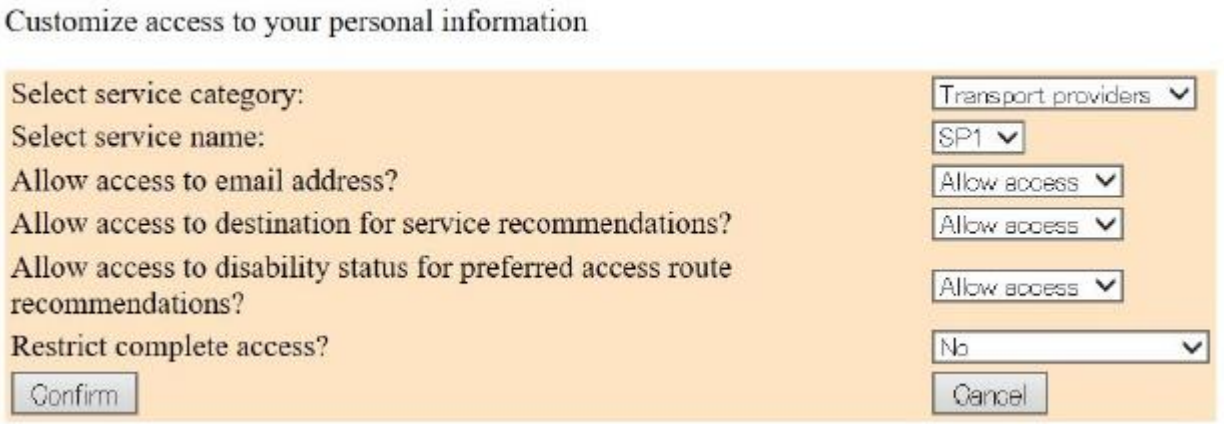
4-2 Context evaluation system

- Context evaluation is a function that enables to alter the data flow handling in the event of emergencies, where safety is preferred over security. In the life-threatening situations, data from MaaS platform is used for emergency evacuations etc.
- The context-evaluator component in the gateway API receives the real-time request attributes, composed of [$\text{subject}_{\text{real-time}}$, $\text{action}_{\text{real-time}}$, $\text{environment}_{\text{real-time}}$].
- Based on the attribute values, the value of “context” variable is judged as [normal, emergency].
- If normal, the data flow handling is performed in the normal manner. If context is “emergency”, the trust computation is bypassed.

4-3 Customer-centric Approach

HITACHI
Inspire the Next

- The customers are given the power to control access to their personal information. This is realized through the policy management and web API module.
- The customers can enable or disable access to selected information through the web API.
- The dynamic policy management and data transformation functions supports this feature.



Security preference form

Customer Name	Email address	Destination	Disability status	Smoking preference
sam	sam1@gmail.com	bokutho hosptial	N	not smoking
cathy	******@gmail.com	****	****	smoking
yamamoto	yamamoto99@gmail.com	bakurocho station	N	not smoking
suzuki	******@yahoo.com	****	****	not smoking
miura	******@hotmail.com	****	****	not smoking
akiko	akiko@gmail.com	sumida community center	N	not smoking

Transformed data

4-4 Data access logging

- Data access logging is performed for trust score computation and access audit purpose.
- All request and response attributes, authentication id, name, service category, access time, action, resource id, access decision etc. are logged to access database.
- Any unfortunate incident of access by an unauthorized person is reported and prompts the admin for immediate policy definition’ review.

4-5 Trust computation

HITACHI
Inspire the Next

- Trust computation of data requestors is performed to quantitatively estimate their trust factor.
- Trust score computation is performed at the time of data access request, based on the access log data.
- The trust score computation approach is critical in issuing security warnings to the admin user and data requesters, restricting access to confidential information, and auditing purpose.

4-6 Trust computation - parameters

- In the current implementation, a trust score is calculated based on 3 parameters:

Parameter1:

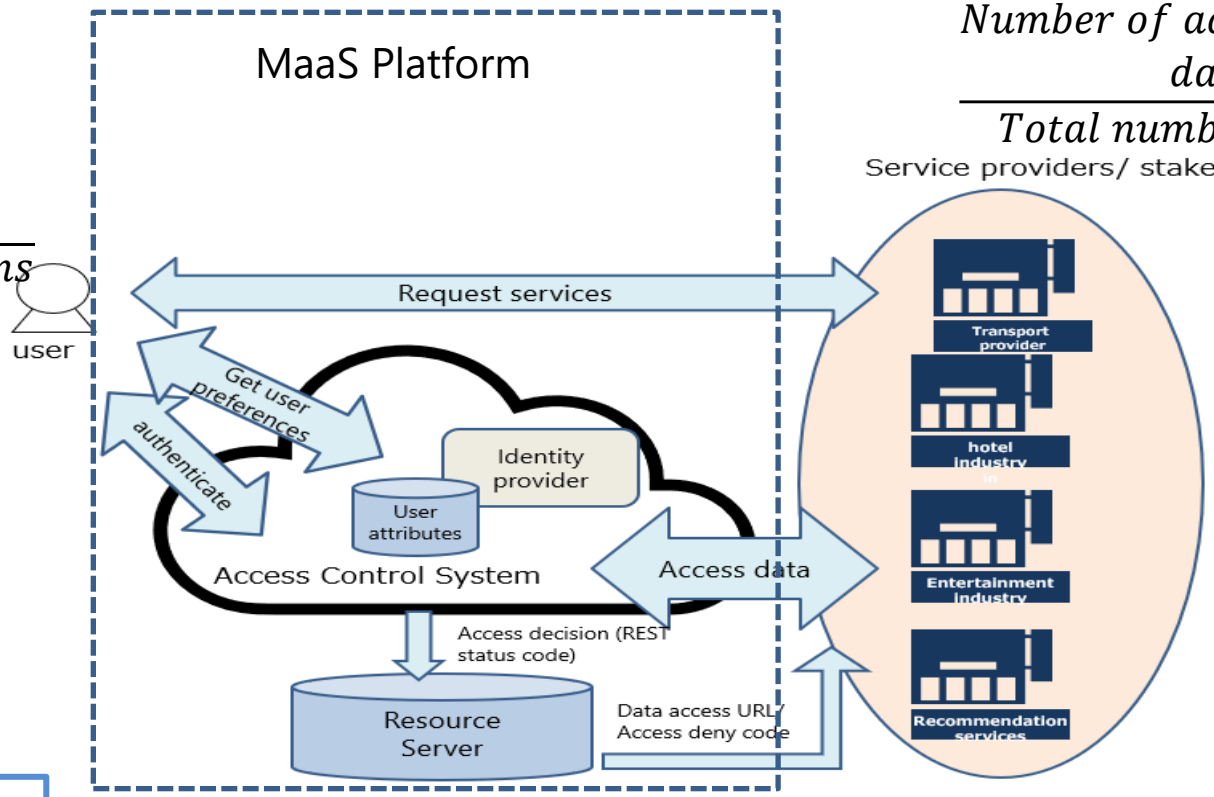
$$Transaction\ rate = \frac{Number\ of\ successful\ transactions\ by\ a\ Stakeholder}{Total\ number\ of\ successful\ transactions\ by\ users\ in\ same\ category}$$

Parameter2:

User feedback level
In the range 0-1

Parameter3:

$$Access\ frequency\ rate = \frac{Number\ of\ access\ requests\ from\ the\ data\ requester}{Total\ number\ of\ access\ requests}$$



Parameter4:
Weighted impact score from security monitoring system, based on encryption measures, suspicious packet count etc.

Parameter5:

$$Invalid\ access\ attempt\ rate = \frac{Number\ of\ invalid\ attempts\ \ by\ a\ data\ requester}{Total\ number\ of\ access\ attempts}$$

Trust score of a stake holder is:

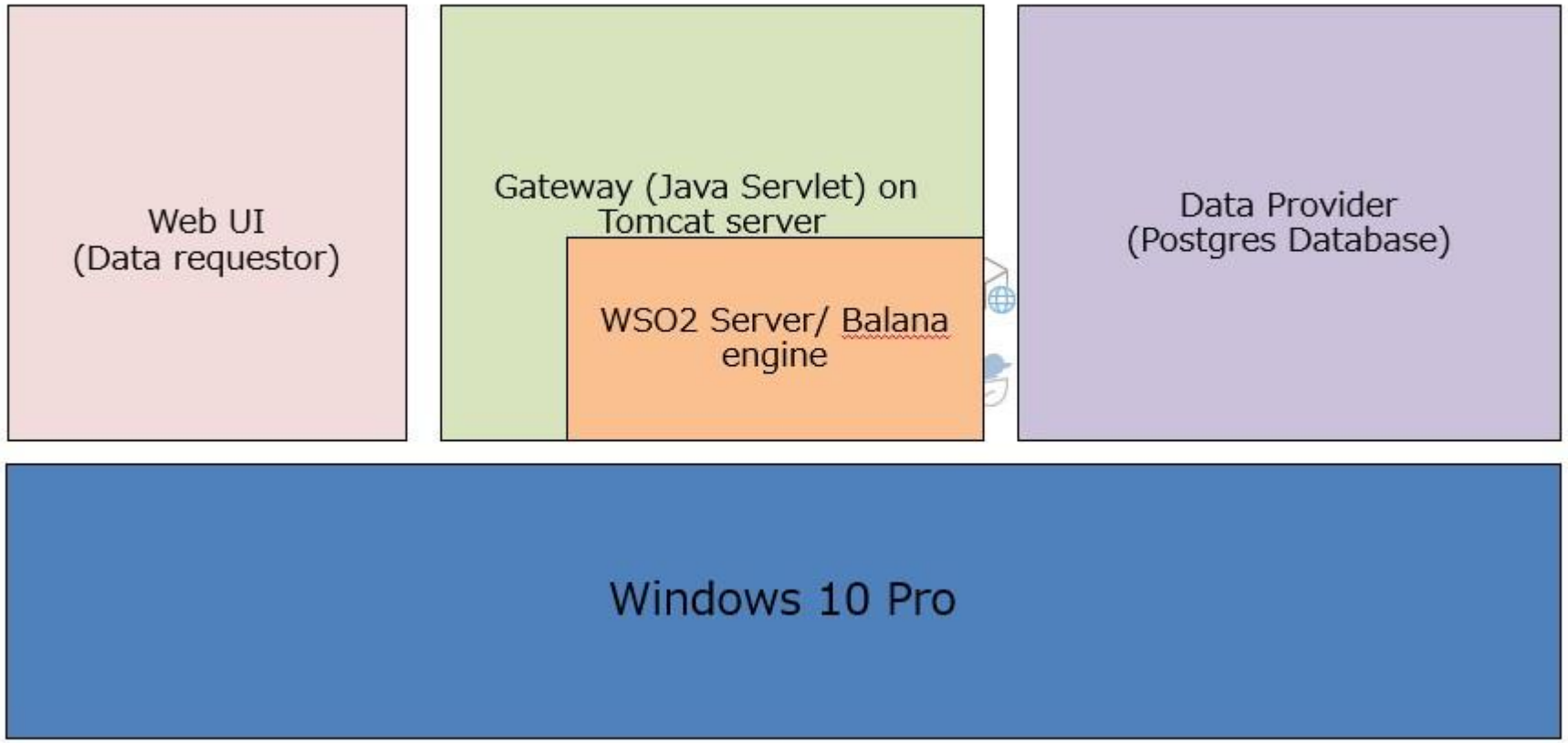
$$T^n = \sum_{w=i}^{j} w_i * p_i$$

p_i are the j parameters used, w_i are the weights of p_i parameters

5-1. Technology Stack of implementation

HITACHI
Inspire the Next

An open source tool, WSO2 identity server/ Balana engine is used as access decision engine.



5-2. Implementation

The combined fine-grained and trust computation approach formulates an access decision based on:

- Trust score computed at the time of access request based on access log data.
- Checking real-time data request attribute values against policies defined.
- If all conditions are satisfied, access is granted, else rejected.

Rule 1 {
description: "Only service providers of category transport providers, with trust score greater than 0.6 are allowed by customer1 to read the data"
subject:"SP1"
action:read
object:"customer#1.data"
condition:"SP1.service_category==transport_provider && SP1.trust_score ≥ 0.6"
decision: permit}

Policy rules

Trust score of data requestors

6. Summary

- A dynamic user-centric hybrid access control approach is implemented by combining fine-grained access control and quantitative trust-based access control approach such that the security threats in a MaaS platform is minimized:
  - Misuse of sensitive customer information
  - Accidental data leakage
  - Insider threats such as service maliciousness.

<u>Future issues</u>

- Need to investigate on dynamic selection of trust parameters.
- System performance in terms on number of concurrent users.