Federated Cybersecurity Testbed as a Service (FCTaaS) – Use Cases in University of Arizona

Sicong Shao
University of Arizona

Cloud and Autonomic Computing Center
Semi Annual IAB Meeting

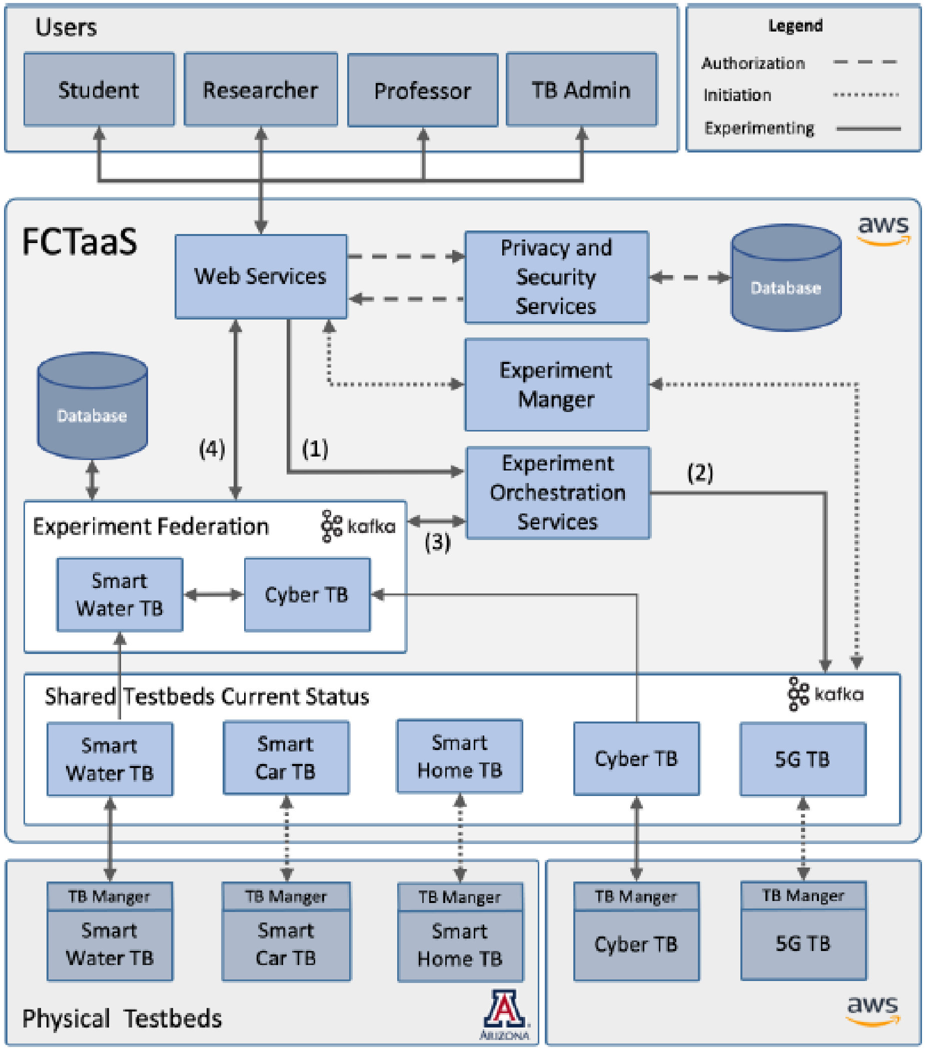
Outline

- □ Background
- □ FCTaaS Architecture
- □ FCTaaS Tasks: Overview
- □ Use Cases
  - ■ Federation of smart city water treatment and distribution services
  - ■ Blockchain Based Methodology for Zero Trust Modeling and Quantification for 5G Networks
- □ Conclusion

Background

- The global acceptance and deployment of smart infrastructure provide personalized and efficient services to the users, improving their quality of life.
- Although smart infrastructure enables a better life, it exposes users and systems to more attack vectors when compared to isolated environments.
- Researchers need realistic testbeds to collect research data, perform experiments, and evaluate their security approaches to address these security problems.
- Such complex smart infrastructure testbeds are challenging to build and expensive to operate, highlighting the need for community testbeds that researchers can utilize to create complex security scenarios and perform realistic experimentation.

FCTaaS Architecture



Cloud and Autonomic Computing Center

Process of FCTaaS Tasks

Setup Phase

1) Testbed Discovery and Integration

2) Beacon Transmission

Experimentation Phase

3) Experiment Setup

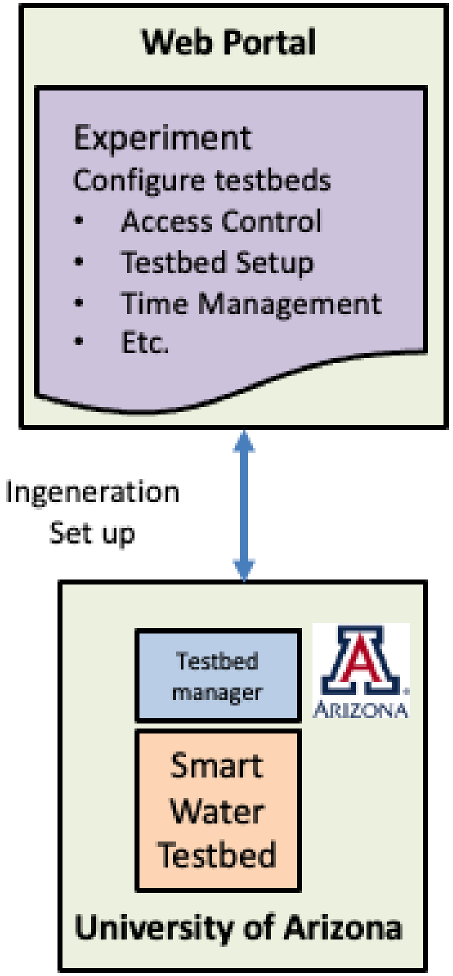
4) Experiment Initialization

5) Experiment Performance

6) Experiment Finalization

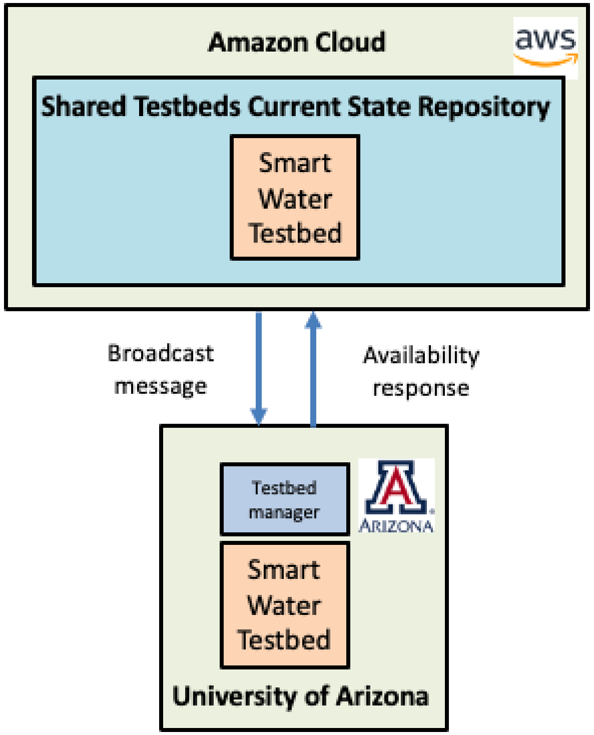
Task 1: Testbed Discovery and Integration

- A method to initiate the integration of a new testbed into the federation.
- Testbed manger is responsible for listing new testbed into the system, according to the user preference.
- Accordingly, the testbed will be available to authorized users when needed.



Task 2: Beacon Transmission

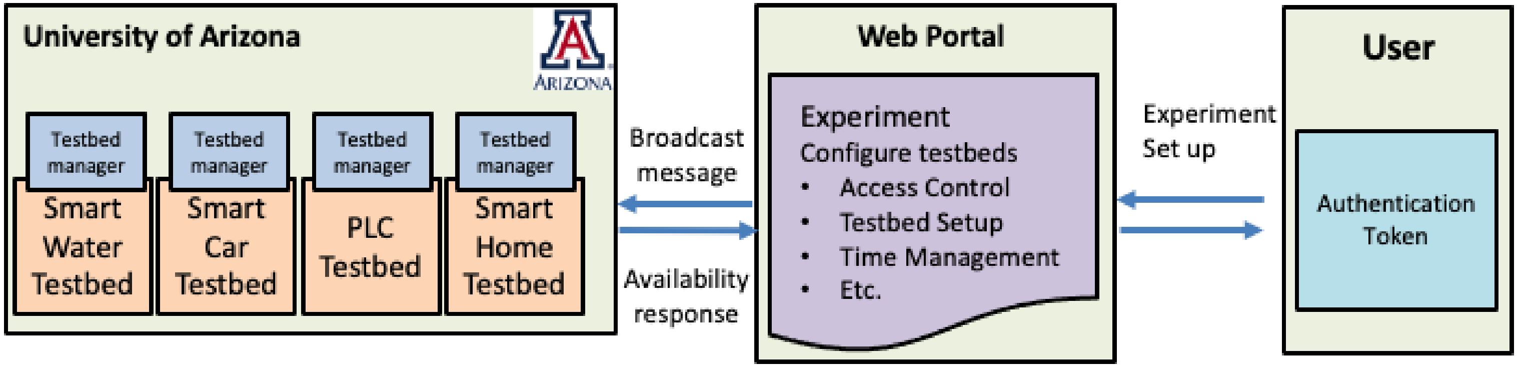
- This step ensures the availability of unutilized testbed within federation.
- A beacon message is broadcasted to testbeds initialized in the federation.
- The testbed manger report the current status of the testbed, thus informing the user of the available mechanics to utilize.



Task 3: Experiment Setup

- During this phase, the user communicate the desired experiment set up to the FCTaaS including testbeds in the experiment, time of use and desired configuration to perform security checks before granting access to testbeds

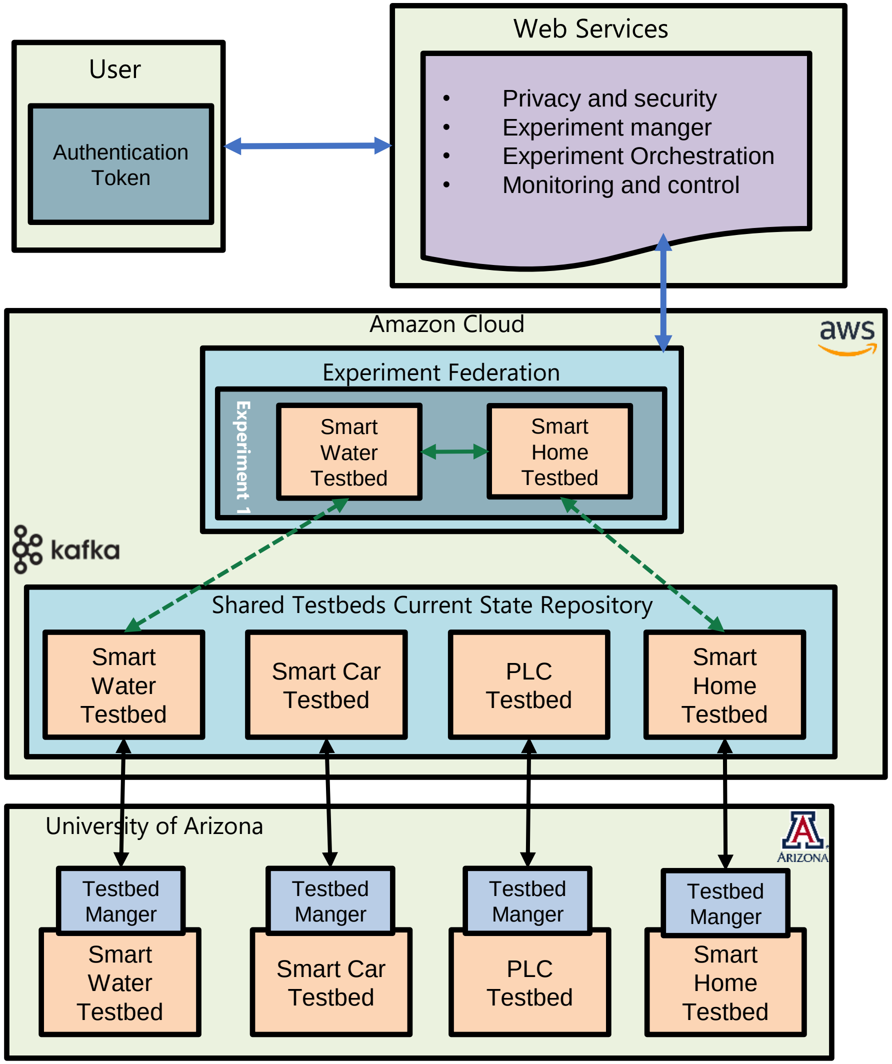
- A beacon message is broadcasted to the selected testbeds to ensure the availability where the testbed manger report back the availability status.



Task 4: Experiment Initialization

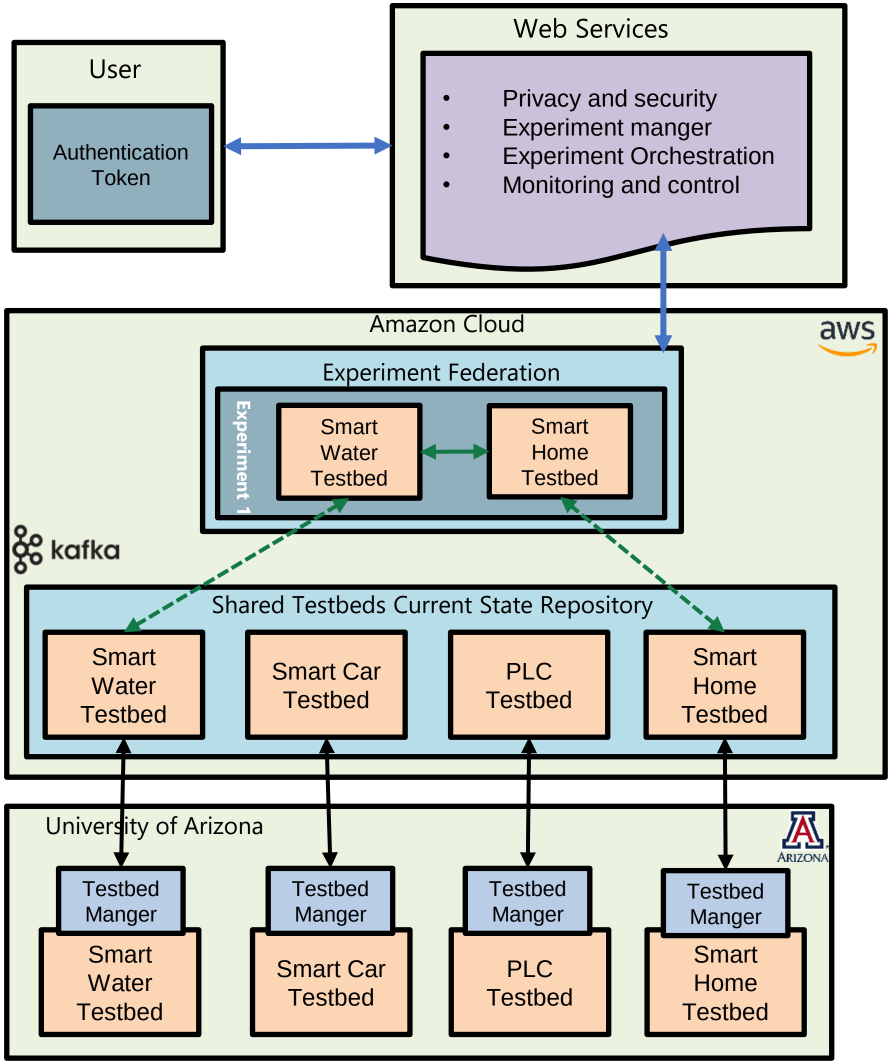
- Different experiments may have variation in the setup based on the number of testbeds involved in the scenario and desired topology.

- Thus, we ensure the initialization phase orchestrate the experiment maintain the current state in real time utilizing digital twin concept via shared memory.



Task 5: Experiment Performance

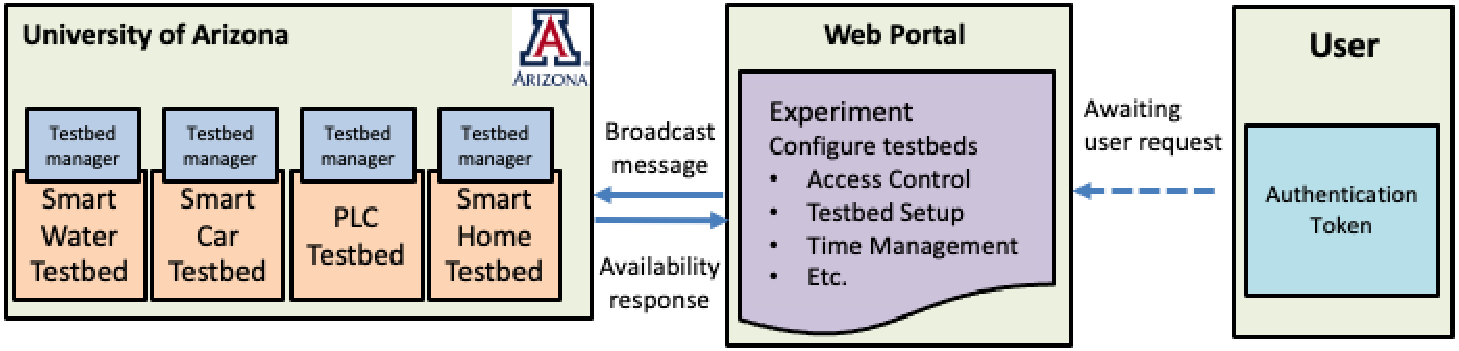
- The Federation performance Experiment creation for each user within the federation.
- Data information is observed as a message and transmitted over to the digital twin.
- Destination testbed/user read the messages in near real-time performance.



NSF CAC Cloud and Autonomic Computing Center TEXAS TECH UNIVERSITY THE UNIVERSITY OF ARIZONA UNIVERSITY OF DETROIT MERCY Universidad de Sonora UNT EST. 1890

Task 6: Experiment Finalization

- Once the experiment is complete, the recently used testbed will be released, thus enable further utilization for upcoming experiments by other users.

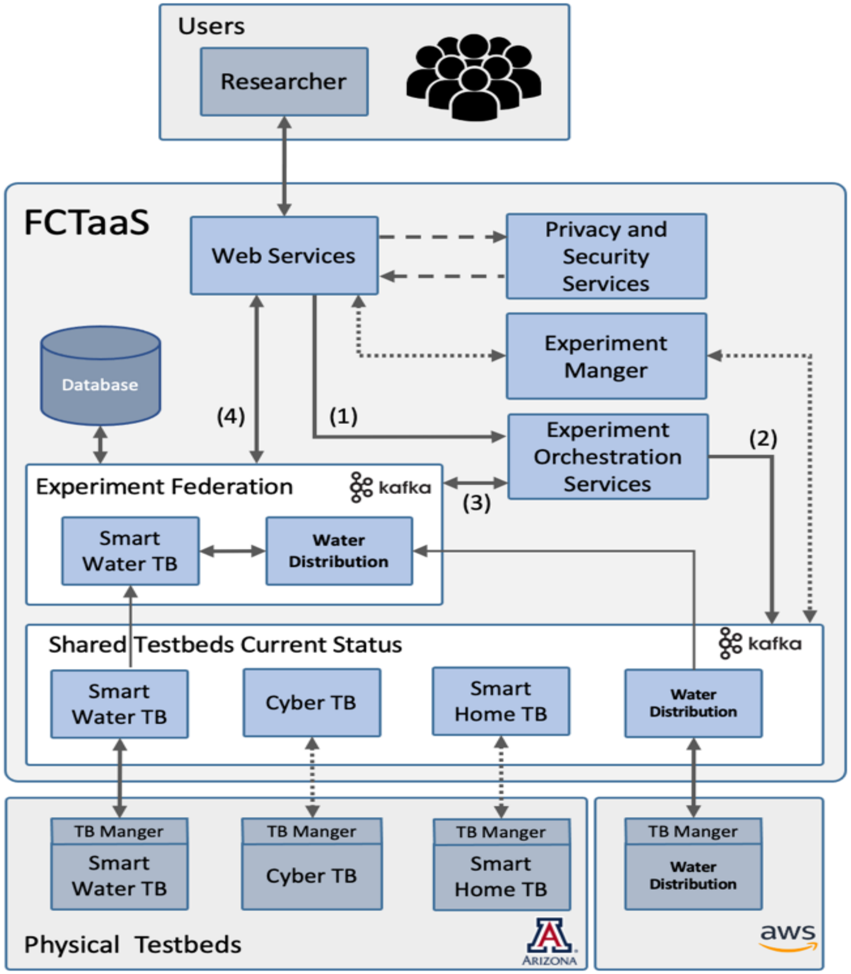


Use Cases

- Use Case 1: Federation of smart city water treatment and distribution services

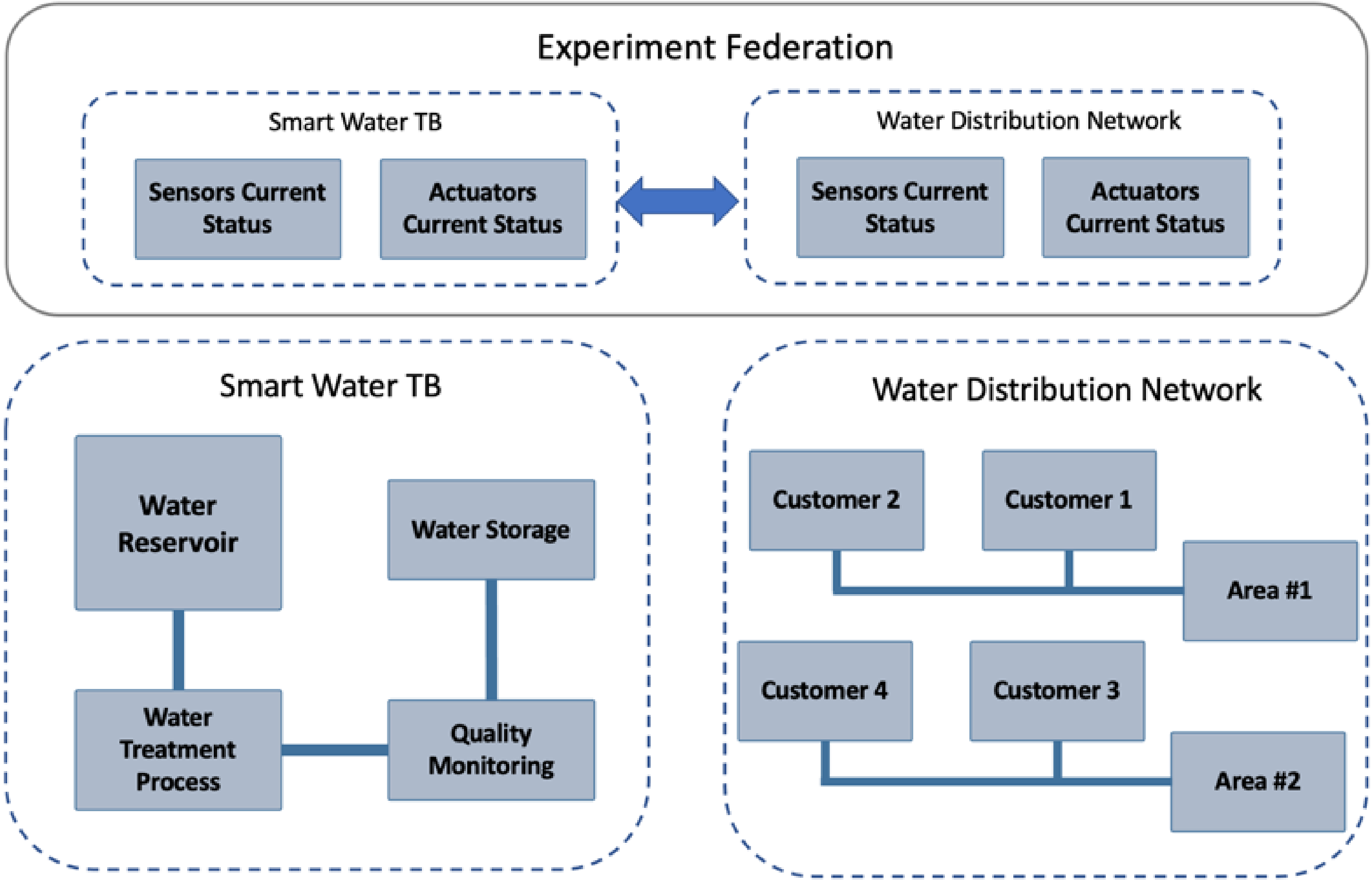
- Use Case 2: Blockchain Based Methodology for Zero Trust Modeling and Quantification for 5G Networks

Federation of Smart Water Treatment



Cloud and Autonomic Computing Center

Federation of Smart Water Treatment

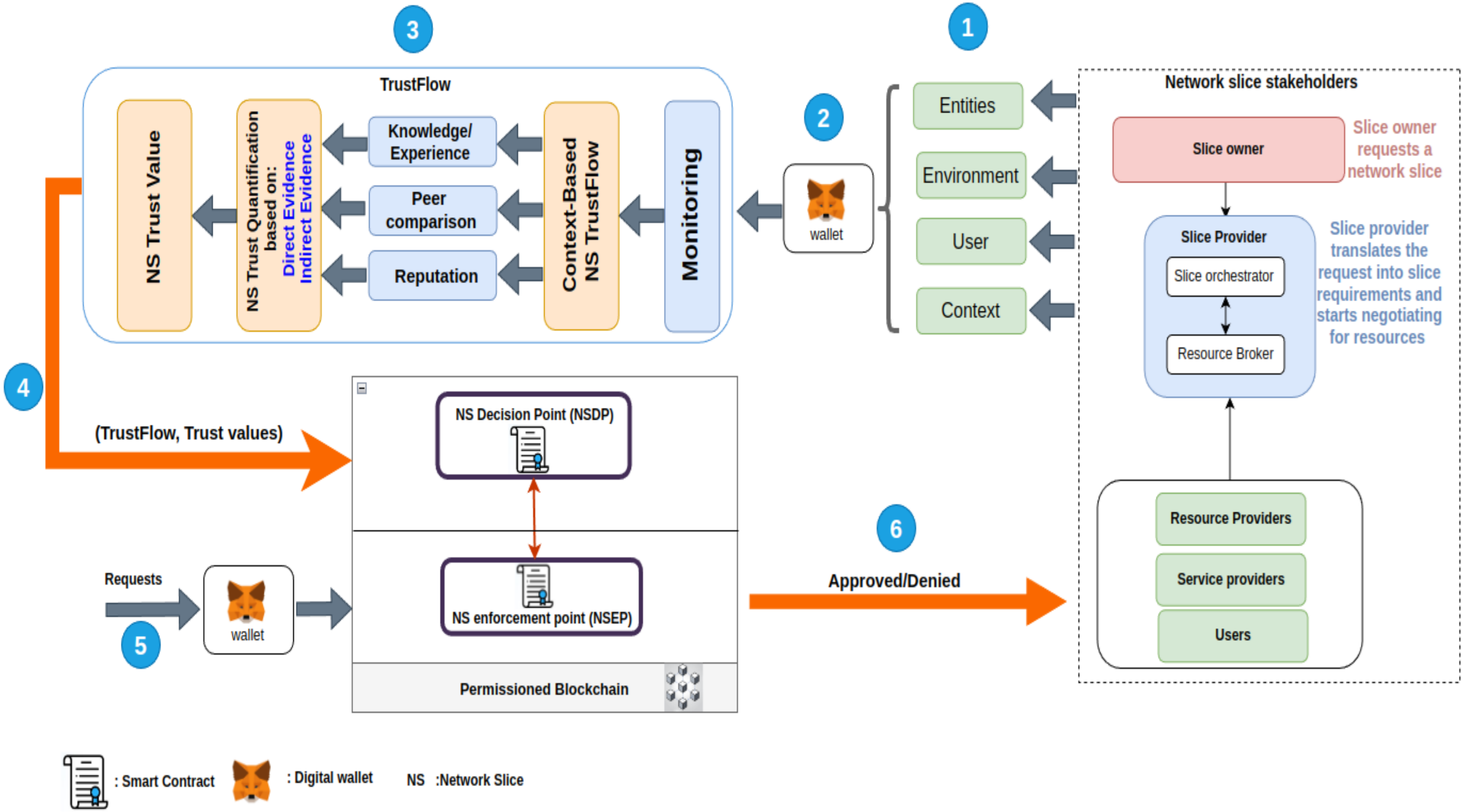


Blockchain Based Methodology for Zero Trust Modeling and Quantification for 5G Networks

Motivation

- In 5G networks, a network slice is defined as a logical network created by partitioning a shared physical infrastructure.
- Each slice is customized and optimized to meet customers’ needs.
- Network slicing brings unprecedented security challenges because of its dynamic and diverse structure.
- Trust in the 5G ecosystem is a cornerstone for global adaptation and tackling security and privacy risks.
- In this research, we shed light on the Zero Trust concept in 5G using distributed ledger (Blockchain).
- We will be using blockchain technology to establish trust between network slice stakeholders (i.e., slice owners, users, slice resource providers, and service providers).

Zero Trust in 5G Network Slicing



3

TrustFlow

NS Trust Value

NS Trust Quantification based on: Direct Evidence Indirect Evidence

Knowledge/ Experience

Peer comparison

Reputation

Context-Based NS TrustFlow

Monitoring

2

wallet

1

Entities

Environment

User

Context

Network slice stakeholders

Slice owner

Slice owner requests a network slice

Slice Provider

Slice orchestrator

Resource Broker

Slice provider translates the request into slice requirements and starts negotiating for resources

Resource Providers

Service providers

Users

4

(TrustFlow, Trust values)

NS Decision Point (NSDP)

NS enforcement point (NSEP)

Permissioned Blockchain

Requests

5

wallet

6

Approved/Denied

: Smart Contract : Digital wallet NS :Network Slice

NSF CAC Cloud and Autonomic Computing Center

TEXAS TECH UNIVERSITY

Universidad de Sonora

THE UNIVERSITY OF ARIZONA

UNT EST. 1890

UNIVERSITY OF DETROIT MERCY

Zero Trust in 5G Network Slicing Tasks

- Task 1: Implementing a data collection tool to gather relevant data from the network slice/system.

- Task 2: Develop the TrustFlow module that processes realtime date and quantifies the trust of an entity using:
  - Deterministic-based Quantification.
  - Machine Learning-based Quantification.

- Task 3: Developing a Zero Trust Architecture using blockchain technology with two smart contracts.

Summary

- The primary goal of this FCTaaS is to develop framework to facilitate the discovery and integration of isolated and geographically dispersed testbeds.

- Our experimental setup facilitate reproducing cybersecurity experiments and can add additional cybersecurity testbeds into our existing experiment setup.

- FCTaaS allows researchers to explore different research questions while building on top of existing hardware without owning individual testbeds.