The 8th IEEE Annual Computing and Communication Workshop and Conference

A Conceptual Framework for an IoT-Based Health Assistant and Its Authorization Model

S. M. Riazul Islam, Mahmud Hossain, Ragib Hasan, and Trung Q. Duong

Presented By
S. M. Riazul Islam, PhD
Assistant Professor, Dept. CSE
Sejong University, South Korea

Date: January 9, 2018
@University of Nevada, Las Vegas, USA
Contents

- Introduction

- IoT-Based Health Assistant Framework

- Security System Design
  - Hybrid Access Control Approach
  - Delegation-based Authorization Scheme
  - Experiment and Evaluation

- Concluding Remarks
Introduction

- IoT-based healthcare systems can be applied to a diverse array of fields, including care for pediatric and elderly patients.

Introduction

- IoT-based healthcare
  - Reduced Costs
  - Increased Quality of Life
  - Improved efficiency of healthcare services, providing easy and correct action, on time.

- IoT healthcare domain may become a target
  - IoT health devices and applications are expected to deal with important private information, including personal healthcare data.
  - Connected to worldwide information networks for access anytime and anywhere.

- Proposed a conceptual IoT-based healthcare framework and designed a security system (authorization aspect).
IoT-Based Health Assistant Framework

Cloud
- Provide
- Authentication
- Authorization
- Auditing

Databases
- Security Servers
- Health Computing Servers

HPA Gateway

Internet

Remote Caregiver
- Issue

SMART home
- Air Conditioning
- Refrigerator
- Other Smart appliances

Smart home

Smart Pill
- Medicine Box

Wearable Sensors
- EMG
- EEG
- Patient
- BP

Local Caregiver
- Digital Prescription

Patient Smartphone

Doctor’s Recommendation

A Conceptual Framework for an IoT-Based Health Assistant and Its Authorization Model
Proposed Security System Design

- Authorization: we propose a Delegated Context-aware Capability-based Access Control (DCCapBAC) scheme for ensuring protected access to medical sensors and actuators operate in the edge of the networks.

- A smart gateway, co-located with the personal area network, performs the SAT verification process on account of the medical devices.
A Conceptual Framework for an IoT-Based Health Assistant and Its Authorization Model

SAT Generation and JSON Envelop

Algorithm 1: Generate Security Access Token

```plaintext
1 function GenerateSAT (userID);
2     Input : User ID (userID)
3     Output: Signed SAT
4 end
5 if userID in revocationList then
6     return NULL ;
7 else
8     SAT ← new SATInstance();
9     SAT.add(userID);
10    role ← getRole(userID);
11    policies ← getPolicyXACML(role);
12 for policy in policies do
13       for permission in policy do
14          /*
15             * MSN = Medical Sensor Node
16             * Add permission for MSN
17           */
18          SAT.addResources(permission.MSN);
19          SAT.addActions(permission.MSN.Action);
20          /*
21             * EMR = Electronic Medical Record
22             * Add permission for EMR
23           */
24          SAT.addResources(permission.EMR);
25          SAT.addActions(permission.EMR.Action);
26 end
27 for res in SAT.Resources do
28     cc ← getContxtConstraint(res);
29     SAT.add(cc);
30 end
31 return Sign(SAT,PrivateKey);
32
```

SAT JSON Envelop

```json
{
  "ID": "9E371587234d004E19AE:d5C578702E94",
  "II": "2015-09-15T12:10:47z",
  "IS": "admin@users.iha.com",
  "SUB": "alice@users.iha.com",
  "SPK": "048E3408...684400D314",
  "SIG": "C27D4E5A9...DFDDEB7E5C42F5203BF9A0F",
  "SH": "F787B4E35...BDCE5BE5c4278702E945c42",
  "RES": "coap://node786/pacemaker",
  "AR": {
    "ACT": [
      "GET",
      "POST"
    ],
    "OB": {
      "NB": "08:00:00",
      "NA": "21:00:00"
    },
    "CT": {
      "DeviceContext": {
        "OperatingMode": "Energy Saving",
        "BatterySatus": "80%"
      },
      "UserContext": {
        "Location": {
          "33.50",
          "86.80"
        }
      },
      "CS": "SIG SPK DECRYPT HASH EQUALVERIFY
NB TIME GRATER THAN NA TIME LESS_THAN
OPERATION_MODE FORALL BATTERY_STATUS
FORALL LOCATION FORALL"
    }
  }
}
```
Access Control in IoT: Limitations

- **Role based access control (RBAC)**
  - It is challenging to assign and manage roles for billions of IoT devices
  - Centralized role management

- **Attributed based access control (ABAC)**
  - Policies are defined in XACML
  - Centralized policy management
  - Does not provide good scalability

- **Capability-based access control (CapBAC)**
  - Capability token are issued to IoT devices and users
  - Provides scalability at the cost of computation and communication overheads for token delivery and validation
Access Control in IoT: Proposed

- Mashup ABAC and CapBAC
- ABAC for managing access control policies
- CapBAC for scalability and to eliminate communication with the central entity
Contemporary SAT Verification Approaches

(a) Centralized approach.
In both the centralized and semi-distributed approaches, the ACLogic is implemented by an external entity, such as a central authorization server, located in the Cloud.
The gateway is located closer to the medical devices as compared to a Cloud authorization server used in the centralized, semi-distributed, and distributed approaches.

The delegation of the SAT verification task to the gateway, instead of delegating the task to the Cloud, results in a faster processing of a request.
Token Verification Approaches: Comparison

- **Distributed approach**
  - Is not suitable for IoT devices with limited processing power, memory, and communication bandwidth
  - Is not applicable for real-time requests

- **Centralized approach**
  - Do not provide better scalability
  - Is not applicable for real-time requests

- **Proposed Approach**
  - Delegate token validation to the Smart Gateway
  - Unburdens resource-constrained devices from computation and communication overheads
  - Reduces energy consumption
  - Enables devices to serve real-time requests.
Experiment and Evaluation

Experimental Setup

Experimental Network
Experimental Scenarios: U2D Interactions

(a) Distributed approach.

(b) Delegation-based approach.

A Conceptual Framework for an IoT-Based Health Assistant and Its Authorization Model
Experimental Scenarios: D2D Interactions

(a) Distributed approach.

(b) Delegation-based approach.
Correlation bet. Service Count and Packet Fragmentation.

- The more the number of packet fragments the more the packet processing delay and energy consumption.

- We avoid computation and communication overhead associated with packet fragmentation and reassembly by offloading the SAT verification to the Delegation Server.
Request Delivery Delay (RDD)

Security System Design: Results

Sejong University (CSE), Inha University (UWB ITRC)

A Conceptual Framework for an IoT-Based Health Assistant and Its Authorization Model
The CPU energy consumption increases as the size of a SAT increases for the distributed approach.
Concluding Remarks

- **Health Assistant**: The proposed theoretical framework for an IoT-based health prescription assistant helps a patient to properly follow his/her doctors recommendations.

- **Access Control**: Existing CapBAC approaches cannot achieve the low communication overhead, inexpensive computation, and load scalability requirements. The proposed DCCapBAC model resolves these issues by integrating ABAC model with the CapBAC model.

- **Token verification**: Delegation of computation intensive operations to the smart gateway co-located with the medical sensors and actuators in the distributed medical IoT networks. The delegation-based SAT verification approach is found energy efficient than the distributed approach.
Discussion