An Access Control Framework for Cloud-Enabled Wearable Internet of Things

Smriti Bhatt, Farhan Patwa and Ravi Sandhu
Institute for Cyber Security (ICS)
Center for Security and Privacy Enhanced Cloud Computing (C-SPECC)
Department of Computer Science
University of Texas at San Antonio

3rd IEEE International Conference on Collaboration and Internet Computing
San Jose, California, USA, October 15 - 17, 2017

ravi.sandhu@utsa.edu
www.ics.utsa.edu
www.cspecc.utsa.edu
www.profssandhu.com

World-Leading Research with Real-World Impact!
Outline

- Introduction
- Background
- Contributions
- Classification of IoT Devices
- Wearable Internet of Things
  - Domains and Devices
- Access Control (AC) Framework
- Use Case
- AC Framework Objectives & Research Problems
- Conclusion and Future Work
Introduction

- **Internet of Things (IoT)**
  - Interconnection of Internet-enabled smart devices/things
  - Enabling technologies – *Internet, Cloud and Mobile computing, Big Data and Analytics, M2M technologies and communication protocols, ...*
  - Diverse and pervasive concept
  - Numerous IoT applications and services → various subfields of IoT

- **Wearable Internet of Things (WIoT)**
  - Revolutionizing industries like healthcare, and sports and fitness
  - Enabling technologies – *Internet, Smart phones, WSNs, and WBANs*

- Generally, IoT devices are resource constraint by nature
  - Limited storage, power, and computation
Cloud-Enabled Internet of Things (CEIoT)

Integration of Cloud and IoT

Major cloud services providers (e.g., AWS, Azure) utilize their cloud infrastructure to provide IoT solutions

Virtually unlimited resources with analysis and visualization capabilities

Security and privacy are primary concerns for IoT

Here, we present an Access Control (AC) framework for CEIoT in context of WIoT (i.e. CEWIoT)
Background

Fig 1: An Access Control Oriented (ACO) Architecture for the CEIoT [1]
Contributions

- Present a general classification of IoT devices to realize different sub-fields of IoT
- Enhance the ACO architecture for CEWIoT by adding an **Object Abstraction Layer**
- Develop an Access Control (AC) framework for CEWIoT based on our enhanced ACO architecture
- Develop a use case to capture different interactions between ACO layers and propose its possible enforcement in a commercial CEIoT platform, viz., AWS IoT
Classification of IoT Devices

Fig 2: A General Classification of IoT Devices
Fig 3: IoT Application Domains
Wearable Devices:

- smart watches
- smart clothing and accessories
- wireless body sensors
- ...

Types of Wearable Devices:

- In-Body
- On-Body
- Around-Body

Wearable devices data – highly privacy sensitive and confidential

A unified access control framework for CEWIoT securing IoT components and their interactions (communication and data exchange) is still lacking
Enhanced ACO Architecture for WIoT

Fig 5: Enhanced ACO Architecture for WIoT

a) Enhanced ACO Architecture for WIoT

b) IoT Components in ACO Layers

© Bhatt et al
Fig 6: Interactions Between ACO Layers

Each layer can interact with itself and up to two adjacent layers in each direction.

Two types of interactions:
- **Direct Interaction** (Interactions with itself and direct adjacent layers)
- **Indirect Interaction** (Interactions with second level of adjacent layers)
The access control (AC) framework –

- A set of access control models categorized into three main access control categories:
  - Object Access Control models
    - Object Layer and Object Abstraction Layer
  - Virtual Object Access Control models
    - Virtual Object Layer
  - Cloud Access Control models
    - Cloud Services Layer and Applications Layer
- Suitable access control models: Role-Based Access Control (RBAC), Attribute-Based Access Control (ABAC), Relationship-Based Access Control (ReBAC)
Fig 7: Access Control Framework Based on Interactions Between Different Layers of the ACO Architecture

AWS-IoTAC Model [3]
- Policy-based access control
- ABAC in limited form
  - Client Attributes
  - Target Attributes

Alshehri and Sandhu [2]
- VO-VO communications
- Operational and Administrative Access Control Models
  - ACLs, CapBAC, RBAC, ABAC

© Bhatt et al
World-Leading Research with Real-World Impact!
Fig 8: Types of Access Control Models
Use Case

Fig 9: Remote Health and Fitness Monitoring (RHFM) Example
Use Case (Contd.)

Fig 10: A sequential view of the RHFM Use Case

© Bhatt et al

World-Leading Research with Real-World Impact!
Based on our previous work [3], we propose a possible enforcement of our use case utilizing AWS IoT platform.

In [3], we configured a smart home use case (with smart sensors, lights, and thermostat) in AWS IoT.
AC Framework Objectives & Research Problems

- User-Based Device Authentication
- User-Centric Data Security and Privacy
- Edge Computing in WIoT (Cloudlets)
- Multi-Cloud Architecture for WIoT (Collaboration and Edge Computing)
Conclusion and Future Work

- Developed a conceptual AC framework for cloud-enabled wearable IoT (CEWIoT)
  - Enable development of a family of AC models with fine-grained access control for specific interactions in CEWIoT
- Discussed suitable access control models (e.g., RBAC, ABAC, ReBAC) for different AC categories
- Presented a WIoT use case and its possible implementation in AWS IoT

Future Work:

- Develop Cloud Access Control models (cross-tenant/account, multi-cloud models) – ABAC and other combinations


(...More in the paper)
Thank you!
Questions?