IoT Passport: A Blockchain-Based Trust Framework for Collaborative Internet-of-Things

Bo Tang, Hongjuan Kang, Jingwen Fan
Information Security Laboratory,
Sichuan Changhong Electric Co., Ltd.
{bo.tang, hongjuan.kang, jingwen.fan}@changhong.com

Qi Li
Institute for Network Sciences and Cyberspace,
Tsinghua University BNRist,
Tsinghua University
qli01@tsinghua.edu.cn

Ravi Sandhu
Institute for Cyber Security and Department of Computer Science, University of Texas at San Antonio
ravi.sandhu@utsa.edu

Blue Sky/Vision Track @ SACMAT`19
June 4, 2019
More “Things” than Human

• Passed a single connected object per person in 2008 and projected to 26 smart objects per human by 2020*

• What will be the foreseeable outcome?
  • AI helps us control objects in the background
  • Multi-factor User Interface with sensors
  • Collaborative IoT: things talk to each other

Smart Life

- Ubiquitous physical infrastructure with sensors and actuators
- Everything Connected
- Lifestyle with smart things towards better life
User Scenarios

• **S1.** On the way home, Alice converses with the AI assistant on her smart phone to check her food inventory. The smart refrigerator responds with a list and suggestions on grocery shopping. Moreover, the AI assistant provides a one-click option for same-day delivery.

• **S2.** The facial detectors at Alice’s authenticate her on arrival and further detect her mood as currently blue, so yellow lights will turn on and soft sound tracks from her favorites will play.
Inevitable Cross-Platform Collaboration

• Fragmented user needs inevitably lead to diverse brands and models of devices along time.
• Collaboration costs multiply with scenarios for on-device solutions but hardware capabilities are limited.
Centralized vs Decentralized

(a) Centralized solution: a single application manages collaboration among the participating devices and platforms

(b) Decentralized solution: a distributed application manages collaborative commands over the DCN
Goals

• Key objectives
  • Agreements between Platforms
  • Security and Privacy
  • Efficiency and Scalability
  • Sustainable Ecosystem

• Security Requirements
  • Decentralized Trust Framework
  • Access Control and Data Security
  • Hierarchical Synchronization
  • Incentive Policies
Federated Trust Requirements

• across platforms
  • Compatible with business needs and doubts
  • Transparency in data governance policy enforcement
  • Proper authority with managed devices (device citizenship)
  • User privacy concern properly addressed and enforced

• across devices
  • Federated authentication mechanisms
  • Authorization decisions are made in decentralized fashion
Related Works

- Centralized authentication and authorization for IoT

- Measurement-based trust models

- Distributed access control using blockchain

- Attribute-Based Access Control
  - Ravi Sandhu. 2012. The authorization leap from rights to attributes: maturation or chaos?. In 17th ACM SACMAT. ACM, 69–70.
Design Overview

Blockchain-Based Trust Framework (BBTF) in layers

- Application Layer: Collaborative IoT Services
- Network Layer: Trust-Based Collaboration, Hierarchical Trust Synchronization
- Perception Layer: Authentication, Trust, Authorization

Blockchain: Blockchain-Based Trust Framework (BBTF) in layers
IoT Passport

Source Platform
- User & Device Attributes
- Source Device
- IoT Passport Repository

Access Evaluation Rules
- User-Defined Policies
- Cross-Platform Trust Policies
- Access Control Policies

Blockchain
- Access Flow
- Reference Data Flow
- Smart Contract

Target Platform
- User & Device Attributes
- Target Device
- Provenance Data Repository
Hierarchical Trust Domains

- CAP Theorem selection: SC
  - Scalability
  - Consistency
  - Loose Decentralization on the Edge
Blockchain-Based Access Control

• Attribute-Based Access Control
  • Take subject attributes, object attributes and environment conditions into access evaluation
  • Blockchain guarantees the integrity, availability and non-repudiation of attributes
  • Attributes retrievable from blockchain and participating platforms

• Provenance-Based Access Control
  • Use provenance data as attributes
  • Persistent storage and proper sharing of the provenance data on blockchain
Incentive Policies

• Service-based
  • Service provider rewarded by consumer

• Capability-based
  • Capability provider rewarded by consumer

• Ecosystem-based
  • Public rankings of collaboration
Proposed Security Focused Research Agenda

• Context-aware access control for IoT
• Cross-platform trust models
• On-blockchain policy administration and verification
• Data on the Edge
Summary

• With the booming Internet of Things, cross-platform collaboration becomes inevitable

• Centralized solutions have limitations turning to decentralization

• Decentralized trust framework using blockchain

• IoT Passport
  • Hierarchical trust domains for better scalability and efficiency
  • Blockchain-based access control better enforcement with attributes
  • Incentive policies establish sustainable ecosystem

• Proposed security focused research agenda