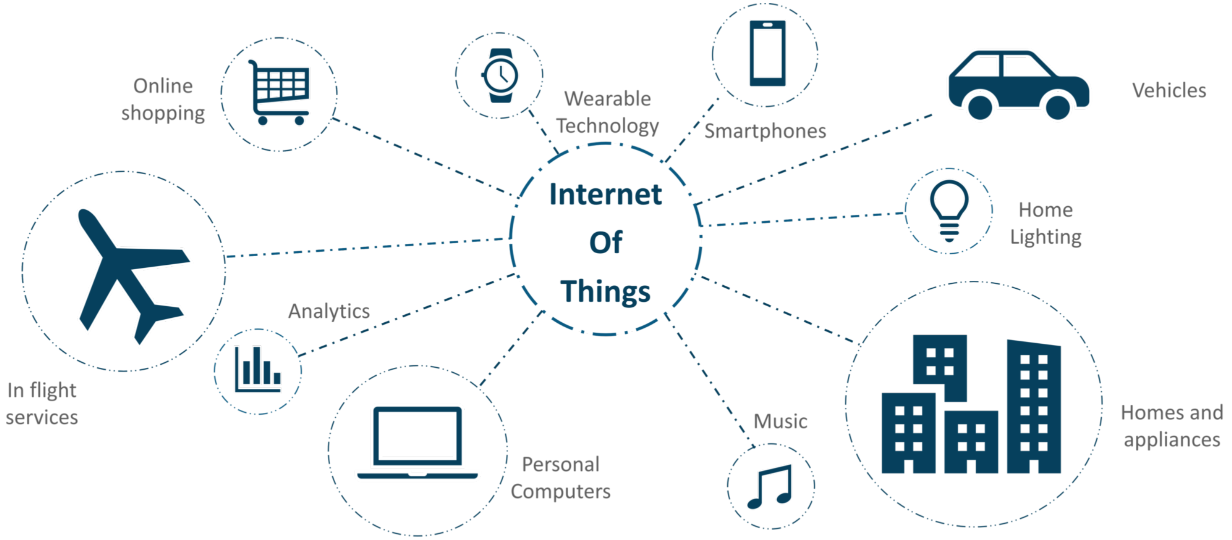
Blockchain-Based Administration of Access in Smart Home IoT

Mehrnoosh Shakarami, James Benson, and Ravi Sandhu

Institute for Cyber Security (ICS),
Department of Computer Science,
University of Texas at San Antonio (UTSA)

ACM Workshop on Secure and Trustworthy Cyber-Physical Systems (SaT-CPS'22)
April 27, Baltimore-Washington DC Area, United States

Introduction



- Tailored authorization and access control for IoT.
  - Many proposals remained at conceptual level.
- Hype around using blockchain for IoT access control.
- Operational vs. Administrative access control.

Access Control in IoT Environments

		🏠	🏢	🚗	❤	🏭
Policy Specificatio n	Granularity	●	●	●	●	●
	Context Awareness	●	●	●	●	●
Policy Management	Handling the complexity of Environment	○	●	●	◑	●
	Usability	●	○	○	●	○
	Multi-domain Administration	○	●	●	◑	●
Policy Enforcement	Minimum user involvement	◑	●	●	●	●
	Light-weight	◑	◑	◑	●	●
	Reliability and Availability	●	●	●	●	●

- We recognize smart home IoT unique characteristics necessitate oriented authorization models to be particularly designed, managed and enforced.

- Little attention has been paid to administration of access in IoT environments.

Blockchain for Access Control

Benefits:

- Decentralized Control
- Transparency and Auditability
- Distributed Information
- Tamper-proof

Why NOT Blockchain for Operational Access Control:

- IoT Constraints
- Long Transaction Confirmation Time
- Financially Prohibitive

Why Blockchain for Administrative Access Control:

- Less Frequency of Administrative Tasks
- Posteriori Analysis
- Scalable
- No need for IoT devices to be engaged in blockchain

Threat Model and Blockchain Benefits

Threat Model:

- Insider Attack: Spoofing, Tampering, Privilege Escalation, Repudiation.

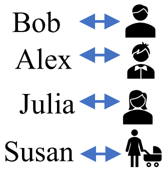
Assumptions:

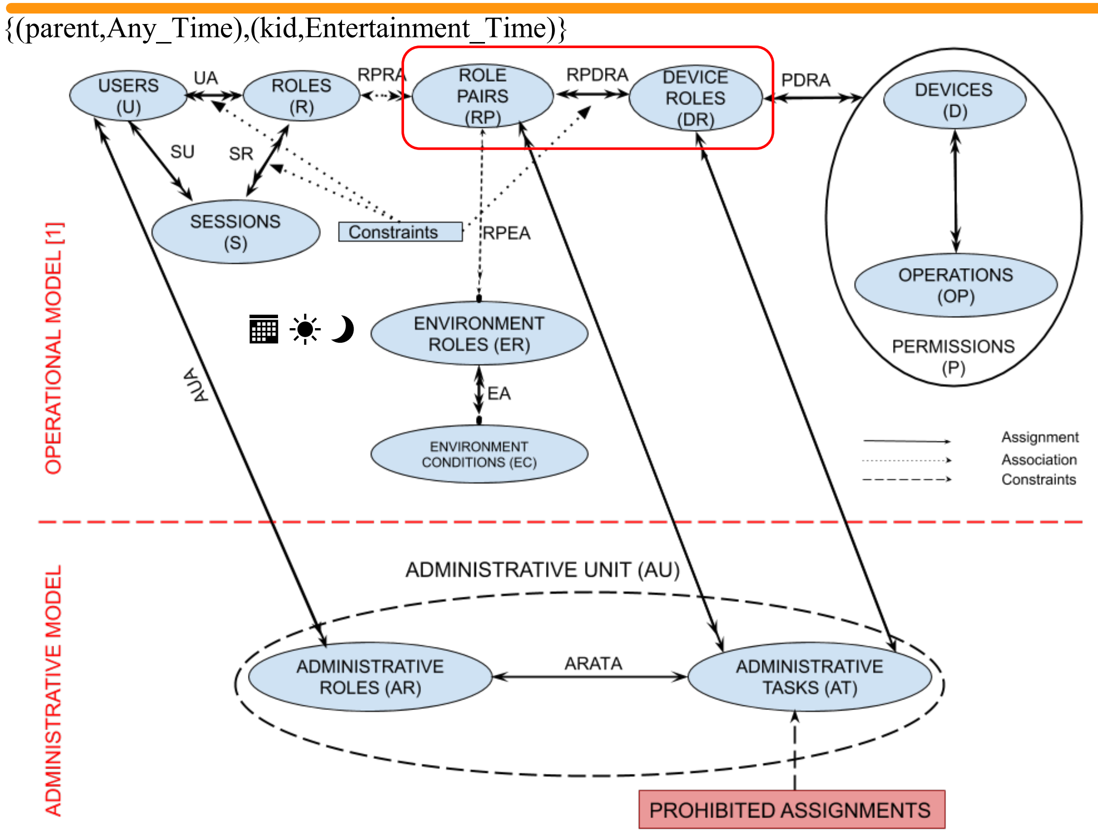
- Users' communication with edge is secure over local network.
- Routing attacks are out-of-scope.
- Attacks against Web3 API are out-of-scope.
- Attacks against user's private key in their wallets considered to be out-of-scope.

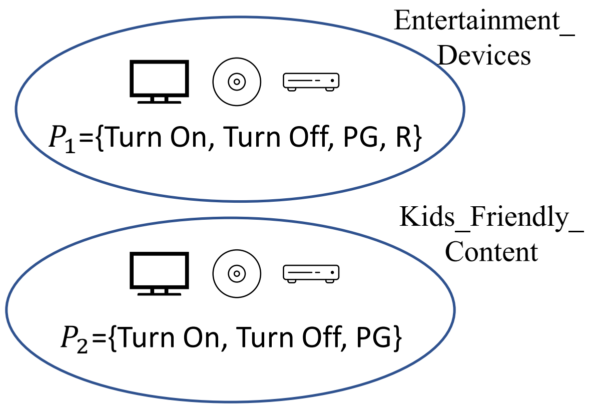
Blockchain Security Benefits:

- Administrator account cannot be faked.
- Administrative policy is encoded in a smart contract recorded to ledger via consensus.
- System is equipped with transparency and auditability.

PEI: Policy – Basic Administrative Model



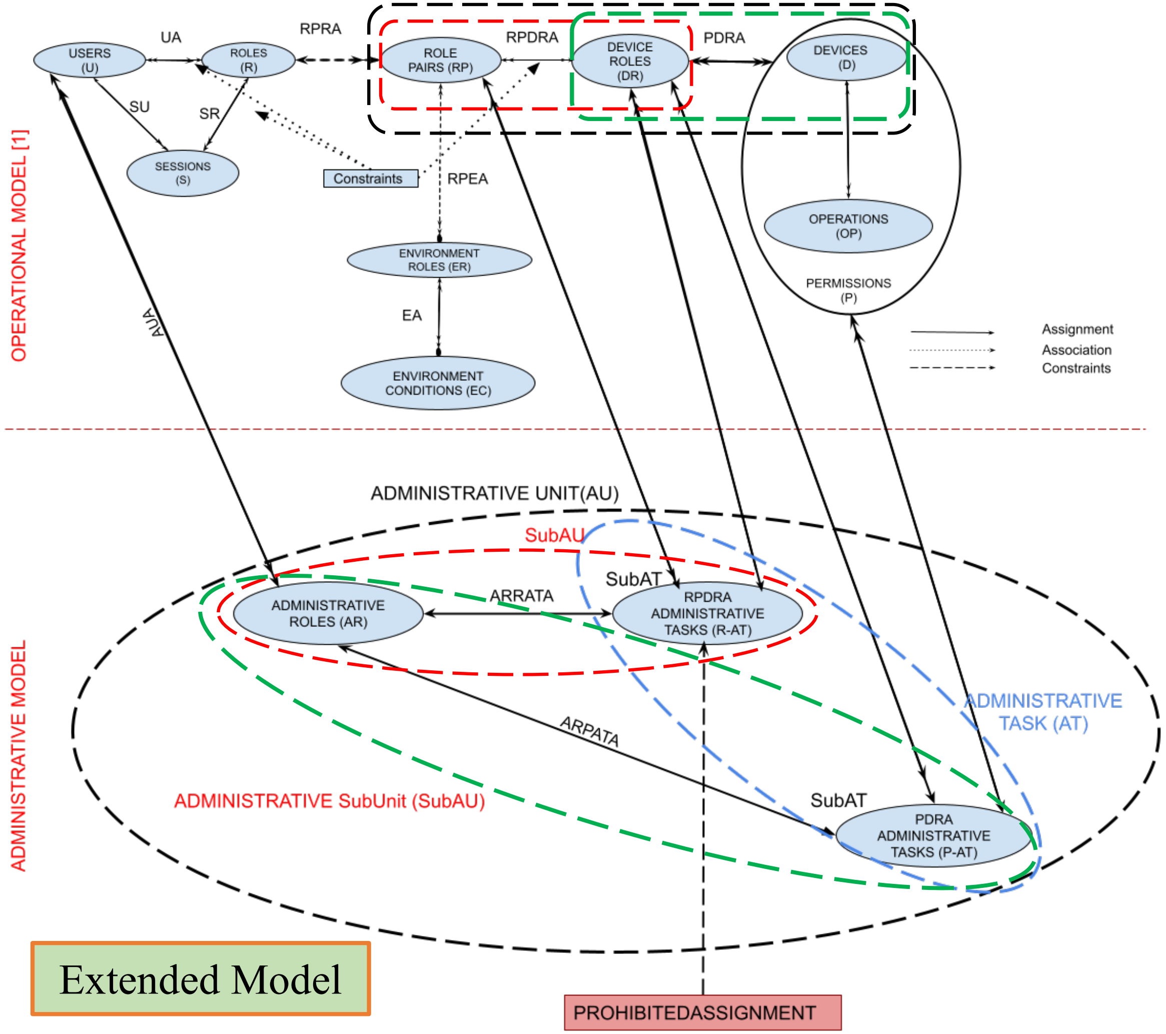



Entertainment_ Devices
P_1={Turn On, Turn Off, PG, R}
Kids_Friendly_ Content
P_2={Turn On, Turn Off, PG}

Basic Model to manage RPDRA Assignment

- We recognize administration is best to be done decentralized. Decentralization provided through Administrative Units (AU).
- We define one administrative unit per operational assignment to be managed, which includes a unique administrative role (AR) and a set of administrative tasks (AT).
- Authorization is scoped as a set of administrative tasks defined to manage corresponding assignments in the operational model.

PEI: Policy – Extended Administrative Model



Extended Model

- We extended our administrative model by defining one administrative unit per operational assignment to be managed.
- Each administrative unit includes a unique administrative role which controls a predefined set of administrative tasks which represents its scope of administration.

au_1 = Entertainment_Management

ar_1 = Entertainment_Manager

at_1= {DR={ENTERTAINMENT_DEVICES, KIDS_FRIENDLY_CONTENT}
RP={(KID, ENTERTAINMENT_TIME), (PARENT,ANY_TIME), (GUEST, ANY_TIME)}}

au_2 = Adult_Management

ar_2 = Adult_Manager

at_2= {DR={ADULT_CONTROLLED}
RP={(PARENT,ANY_TIME), (BABY_SITTER, ANY_TIME)}}

((KID,ENTERTAINMENT_TIME), ENTERTAINMENT_DEVICES)

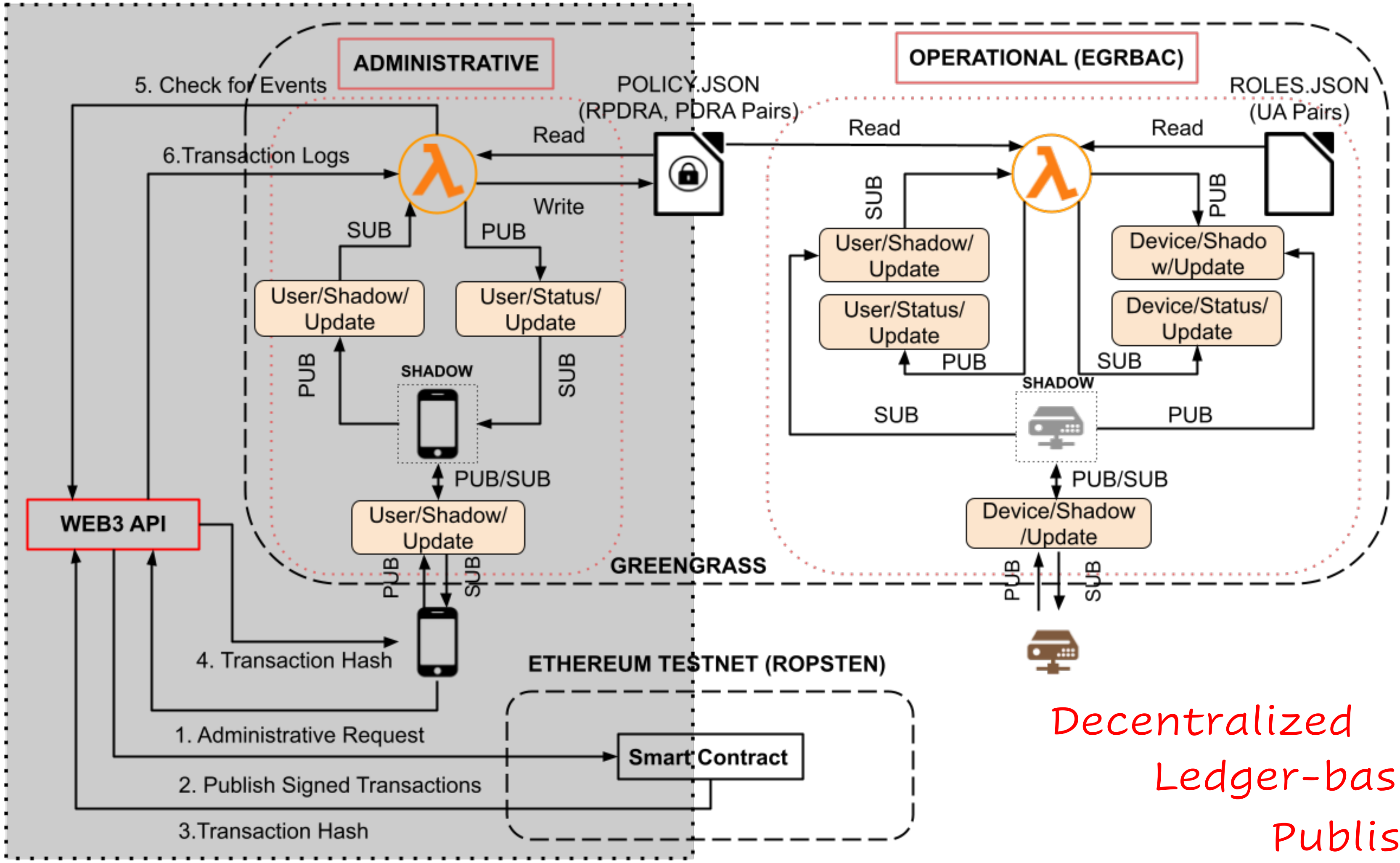
Prohibited Assignments

au_3 = Ownership_Control

ar_3 = Home_Owner

at_3= {DR={OWNER_CONTROLLED}
RP={(PARENT,ANY_TIME)}}

PEI: Enforcement Architecture

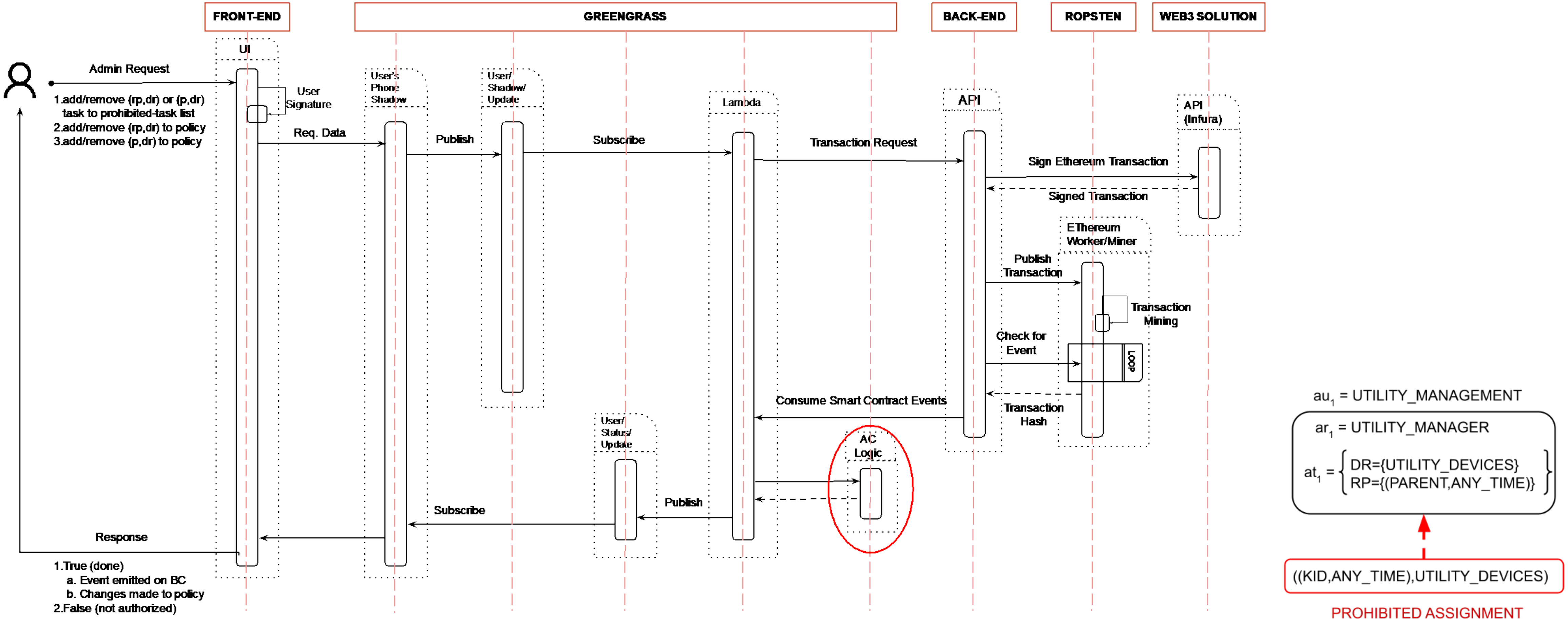


Decentralized

Ledger-based

Publish-subscribe

Sequence Diagram



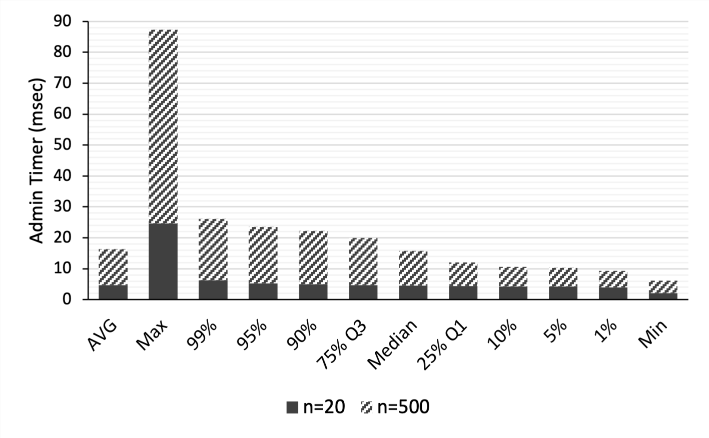
PEI: Implementation Setup

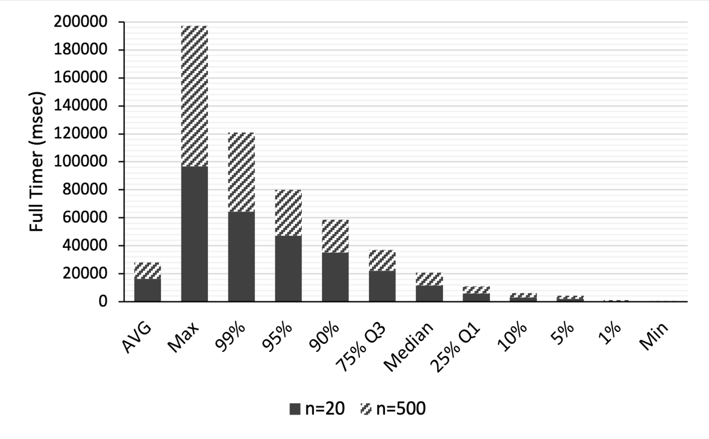
- Administrative access control policy implemented in a single smart contract on the Ropsten.
- Different administrative controls are coded as functions, which would be triggered by transactions.
- Smart contract is programmed in Solidity and tested it on Remix IDE.
- Infura is used as web3.0 API to interact with blockchain.

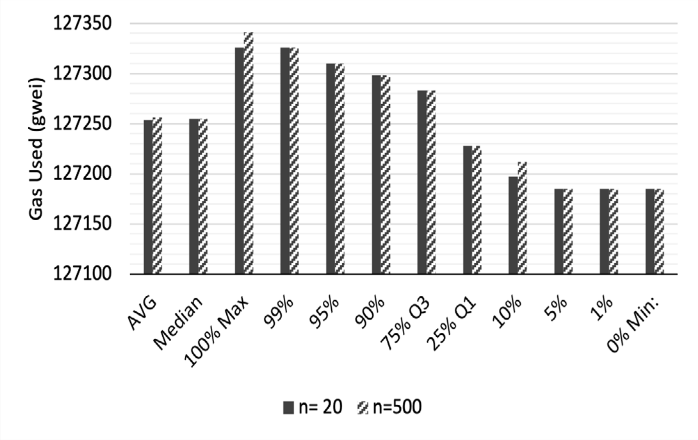
- Experiment Environment:
  - AWS IoT Greengrass v1.
  - Greengrass runs on a dedicated virtual machine: one virtual CPU, 2 GB of RAM and 20 GB hard drive.
  - The virtual machine's operating system is Ubuntu 20.4.2 LTS and it is connected to a 1 Gbps network.
  - Our AWS lambda code on the Greengrass is written in Python 3.8 and is running in a long-lived isolated runtime environment with limited RAM of 256 MB

- Experiments are done for a normal distribution with a 99.9% confidence interval.
- We ran our experiments in two settings with the policy sizes of n=20 and n=500.
  - Both experiments were run for a total of 500 times.

Implementation Results







Admin Timer: After a transaction has been successfully mined, Lambda checks the logs to search out the succeeded transactions. Then, it makes appropriate changes to the “policy.json” file and publishes the results to the User/Status/Update to inform the user about his/her administrative request.

Full Timer: Complete cycle of an administrator submitting a request, to that request being mined, and the lambda function processing the results and updating as necessary.

Gas Used: the actual amount of gas which was used during execution. Gas prices are denoted in GWEI, which equals to 10^{-9} ETH. We calculated the monetary cost of each transaction to be 28 cents.

Discussions

- Our administrative model features:
  - Decoupled Assignment and Revocation
  - Symmetric Assignment and Revocation
  - Generalizability
  - Transparency and Auditability
  - Privacy

- Security considerations specific to our architecture:
  - Smart Contract Security
  - Device-Cloud Communications

- Limitations:
  - Continuous Access control and Mutability
  - Handling Conflicts

- Our implementation results are reassuring that although the use of blockchain for operational access control is NOT promising, BUT it is promising to be utilized at administrative level.

Blockchain Hype

EGRBAC is not chosen as a de-facto!

Q&A

Acknowledgement

- This work is partially supported by NSF CREST Grant 1736209.

Thanks for your time and attention!

- Any Questions?