Access Control for Smart Home IoT: Introduction and GRBAC Model

Safwa Ameer
James Benson
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

Safwa.ameer@my.utsa.edu

L11-1

Spring 2020

Introduction

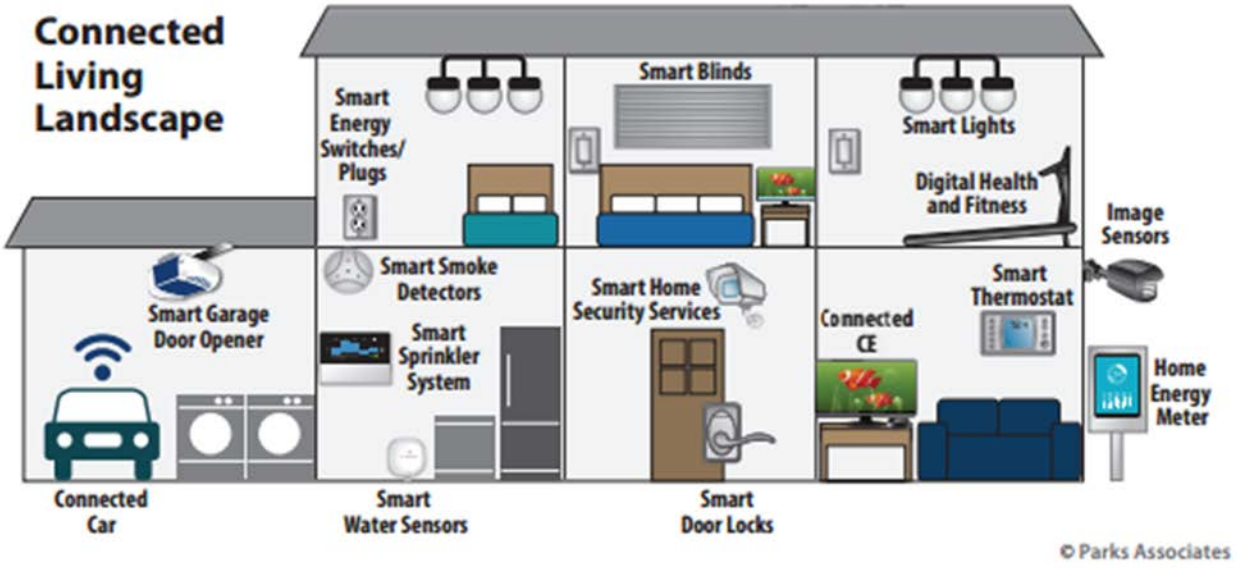
- The Internet of Things (IoT) is a new technology paradigm envisioned as a global network of machines and devices capable of interacting with each other.

- Currently, IoT is one of the most talked about topics in technology, it has already become indispensable components of our lives.

Introduction

- One of the most popular domains for deploying smart connected devices is the smart home.

- The global smart home market is forecast to reach a value of more than 53 billion US dollars by 2022.



Motivation

- Surprisingly, little attention has been paid to AC in home IoT.
- AC issues have been explored extensively for many different domains.
- Home IoT is significantly different from traditional domains in:
  - In home IoT we have many users who use the same device, for example: smart door lock, smart light,.. .

Motivation

- House residents usually have complex social relationship between them, which introduce a new threat model, e.g. an annoying child trying to control the smart light in his sibling's room, a current or ex-partner trying to abuse one or all house residents.

- The majority of IoT devices do not have screens and keyboards making them hands free for convenience while making authentication and access control more challenging.

- Smart home things are usually constrained resources in term of computational power, and storage.

Motivation

- He et al [1] have recently proposed a new perspective of access control policies specifications for home IoT. They re-envisioned access control and authentication for the home IoT through a 425-participant user study.

- They concluded that the characteristics that make IoT distinct from prior computing domains necessitate a rethinking of access control and authentication.

- Ouaddah et al [2] provided and extensive review of different access control solutions in IoT within the Objectives, Models, Architectures, and Mechanisms (OM-AM).

- They believe that the need arises for a dynamic and fine-grained access control mechanism, where users and resources are constrained .

Our Criteria for Smart Home IoT Access Control Models

- Based on the literature review that we have done, we believe that a smart home IoT access control model (whether it is device to device (D-D), user to device (U-D) or both) should exhibit, at least, the following characteristics:

1. **Dynamic,** to capture environment and object contextual information..
2. **Fine-grained**, so that a subset of the functionality of a device can be authorized rather than all-or-nothing access to the device.
3. **Suitable for constrained home environment**. IoT AC model should not require extensive computation or communication on the part of resource constrained devices. Furthermore, any access control solution for smart home IoT should consider the fact that a generic interoperability standard among IoT devices is still missing.

Our Criteria for Smart Home IoT Access Control Models

4. **Constructed specifically for smart home IoT or otherwise be interpreted for the smart home domain such as by appropriate use cases.** To ensure that the model is suitable for smart home different specifications such as, social relationships between house members (which implies He et al second characteristic), cost effectiveness, usability, and so on

5. **The model should be demonstrated in a proof-of-concept,** to be credible using commercially available technology with necessary enhancements.

6. **The model should have a formal definition**, so that there is a precise and rigorous specification of the intended behavior.

- We investigated literature's IoT access control models that govern user to device access against our criteria, and notably no model satisfies all desired specifications.

Our Criteria for Smart Home IoT Access Control Models

Model Type	Model	U-D or D-D	Dynamic	Fine Grained	Suitable for constrained home environment	Designed or interpreted for smart home IoT	Implemented	Provides a formal Access Control Model
RBAC Model	EGRBAC, this paper	U-D	yes	yes	yes	yes	yes	yes
RBAC Model	GRBAC, Covington et al [3]	U-D	yes	no	yes	yes	no	no
RBAC Model	Zhang et al [4]	U-D and D-D	yes	yes	yes	no	no	yes
RBAC Model	Barka et al [5]	U-D and D-D	no	yes	no	no	no	utilizes RBAC [51]
RBAC Model	Jindou et al [6]	U-D	no	yes	no	no	yes	yes
RBAC Model	Kaiwen et al [7]	U-D	yes	yes	yes	no	no	yes
RBAC Model	Liu et al [8]	U-D	no	yes	yes	no	no	no
ABAC Model	Ye et al [9]	U-D and D-D	yes	no	no	no	no	yes
ABAC Model	Bandara et al [10]	U-D	no	yes	yes	no	yes	utilizes XACML [49]
ABAC Model	Mutsvangwa et al [11]	U-D	N/A	N/A	no	no	no	no
ABAC Model	Xie et al [12]	U-D and D-D	N/A	N/A	no	no	no	no
UCON Model	Martinelli et al [13]	U-D	yes	yes	yes	no	yes	utilizes U-XACML [12, 36]
CapBAC Model	A survey is provided in [2]	Not adequate for the constrained environment of smart homes as explained in Section 3.						

Analysis of Published IoT Access Control Models Based on Desirable Characteristics

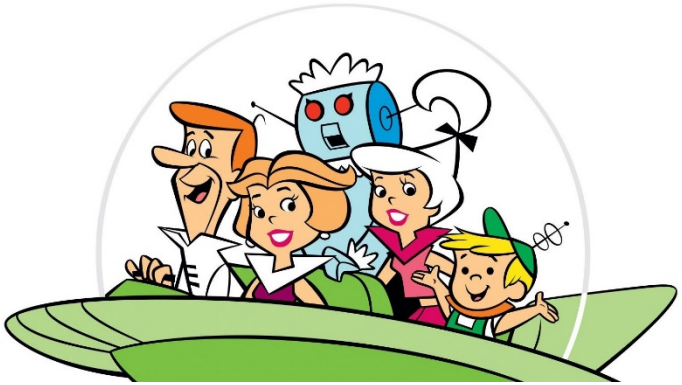
Our Threat Model

- In smart houses we have two types of adversaries:

a- Outsider hacker who is trying to get digital or physical access to the house by exploiting system vulnerabilities.

b- The household members themselves, that is insiders who have legitimate digital and physical access to the house, such as family members, guests, and workers.

- **The central focus of our paper** is making sure that those legitimate users get access only to what they are authorized to by the house owner.



Our Threat Model

- There are other types of insider threats such as, Revocation evasion, and logging evasion. We didn't consider them for the following reasons:

1. Revocation evasion:

   In our adopted architecture, the user cannot access the smart devices directly, each request must go through the smart hub which contains the access policies. If a revocation happened, the access policies will be updated, and this will be reflected in any future access request.

2. Logging evasion:

   We believe that this threat is implementation specific more than design specific.

The GRBAC Model

- Covington et al introduced the Generalized Role-Based Access Control (GRBAC) model [14].
- In addition to the usual concept of Subject Role, GRBAC incorporates the notion of Object Roles and Environment Roles.
- A subject role is analogous to a traditional RBAC role.
- An object role is defined as the properties of the resources in the system, such as images, source code, streaming videos, devices.
- An environment role is defined as the environment state during access.

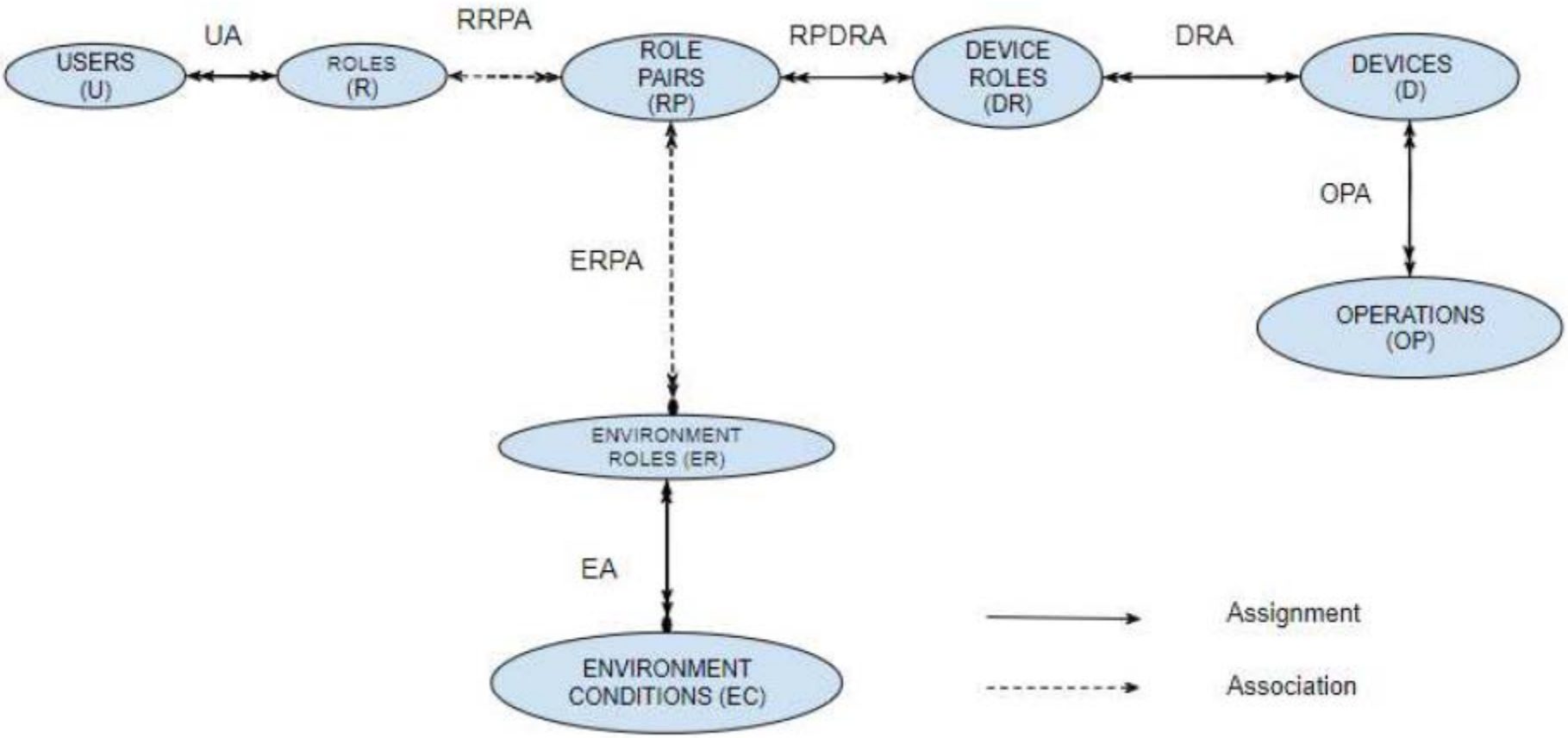
The GRBAC Model

- In [3] they subsequently provided a high level but incomplete formal definition of environment role-based access control model, building upon [15].

- They neither considered formalizing the object role part of GRBAC, nor provided a model diagram.

- We provide a complete detailed formalization of GRBAC accompanied with a model diagram.

Our view of GRBAC



Our formalization of GRBAC

Users, Roles and Devices

$-U, R, D, OP$ and DR are sets of users, roles, devices, operations and device roles respectively

$-UA \subseteq U \times R$, many to many users to role assignment (home owner specified)

$-OPA \subseteq OP \times D$, many to many assignment between operations and target devices (manufacturers specified)

$-DRA \subseteq D \times DR$, many to many devices to device roles assignment (home owner specified)

Environment Roles and Environment Conditions

$-ER$ and EC are sets of environment roles and environment conditions respectively

$-EA \subseteq 2^{EC} \times ER$, many to many subsets of environment conditions to environment roles assignment (home owner specified)

Role Pairs

$-RP \subseteq R \times 2^{ER}$, a set of role pairs specifying all permissible combinations of a user role and subsets of environment roles (home owner specified)

– For convenience for every $rp = (r_i, ER_j) \in RP$, let $rp.r = r_i$ and $rp.ER = ER_j$

$-RRPA \subseteq R \times RP$, one to many role to role pairs association, where $RRPA = \{(r_m, rp_n) \mid rp_n \in RP \wedge rp_n.r = r_m\}$

$-ERPA \subseteq ER \times RP$, many to many environment roles to role pairs association, where $ERPA = \{(er_m, rp_n) \mid rp_n \in RP \wedge er_m \in rp_n.ER\}$

Role Pair Assignment

$-RPDRA \subseteq RP \times DR$, many to many role pairs to device roles assignment (home owner specified)

Authorization Predicate

– For a user u_i to perform operation op_k on device d_j when the set of environment conditions EC_m is active:

$(op_k, d_j) \in OPA \wedge$

$(\exists\, r_x \in R, rp_y \in RP, dr_l \in DR)$, where:

$(u_i, r_x) \in UA \wedge rp_y.r = r_x \wedge (rp_y, dr_l) \in RPDRA \wedge$

$(d_j, dr_l) \in DRA \wedge$

$rp_y.ER \subseteq \{er \in ER \mid (\exists EC'_m \subseteq EC_m)[(EC'_m, er) \in EA]\}$

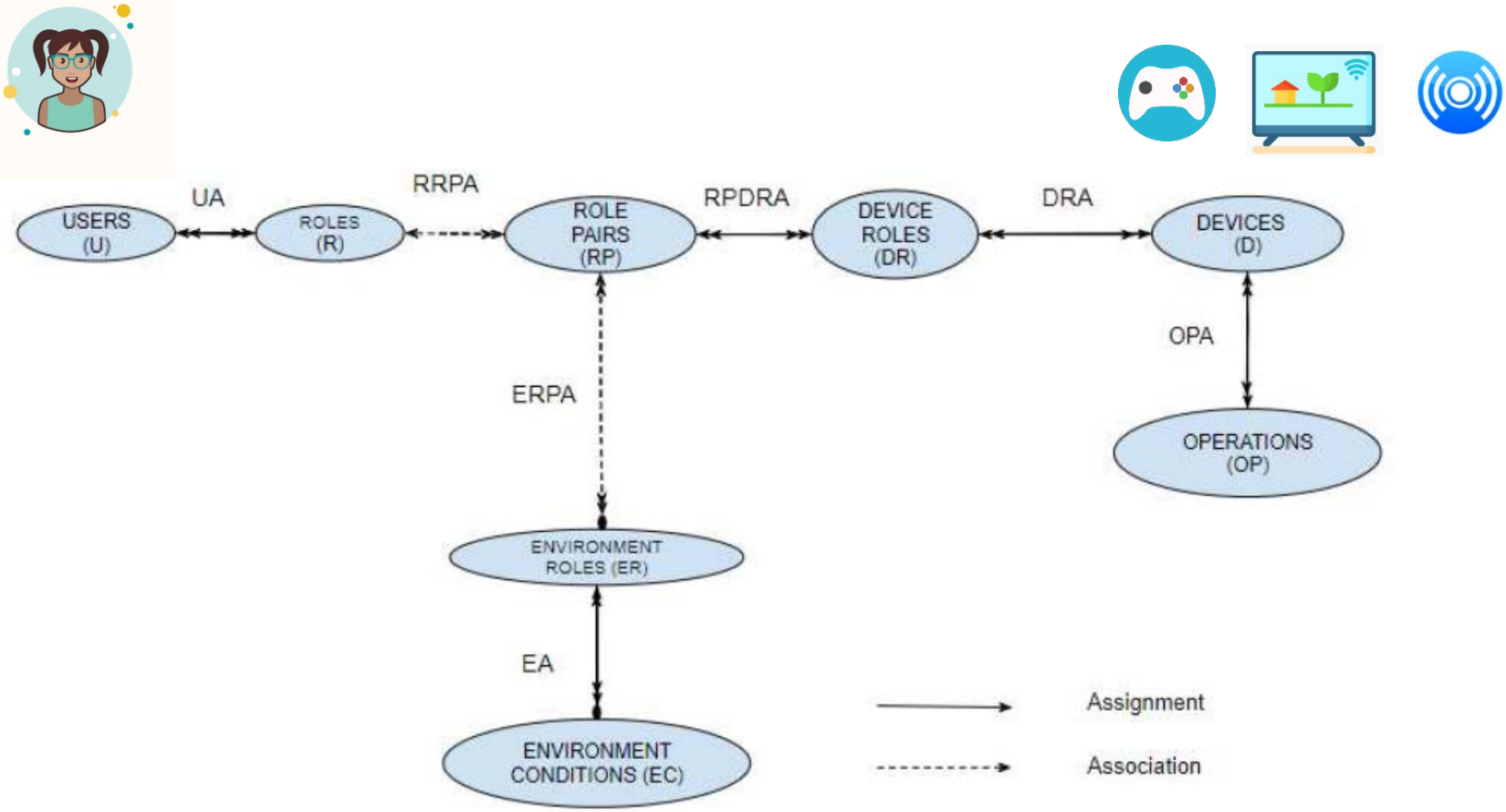
Use Case 1.A Configuration in GRBAC

$$U = \{alex, bob, \ldots\},\ R = \{kids, parents, \ldots\}$$
$$UA = \{(alex, kids), (bob, parents), \ldots\}$$
$$D = \{TV, DVD, Playstation, \ldots\}$$
$$OP_{TV} = \{ON, OFF, G, PG, PG13, R, NC-17, \ldots\}$$
$$OP_{DVD} = \{ON, OFF, G, PG, PG13, R, NC-17, \ldots\}$$
$$OP_{Playstation} = \{ON, OFF, A3, A7, PG12, A16, A18, BuyGames, InternetBrowsing, Texting, VoiceMessaging, \ldots\}$$
$$OP = OP_{TV} \cup OP_{DVD} \cup OP_{Playstation} \cup \ldots$$
$$DR = \{Entertainment\_Devices, \ldots\}$$
$$DRA = \{(TV, Entertainment\_Devices), (DVD, Entertainment\_Devices), (Playstation, Entertainment\_Devices), \ldots\}$$

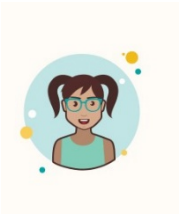
$$EC = \{weekends, evenings, TRUE, \ldots\}$$
$$ER = \{Entertainment\_Time, Any\_Time, \ldots\}$$
$$EA = \{(\{weekends, evenings\}, Entertainment\_Time), (TRUE, Any\_Time), \ldots\}$$

$$RP = \{(kids, \{Entertainment\_Time\}), (parents, \{Any\_Time\}), \ldots\}$$
$$RPDRA = \{((kids, \{Entertainment\_Time\}), Entertainment\_Devices), ((parents, \{Any\_Time\}), Entertainment\_Devices), \ldots\}$$

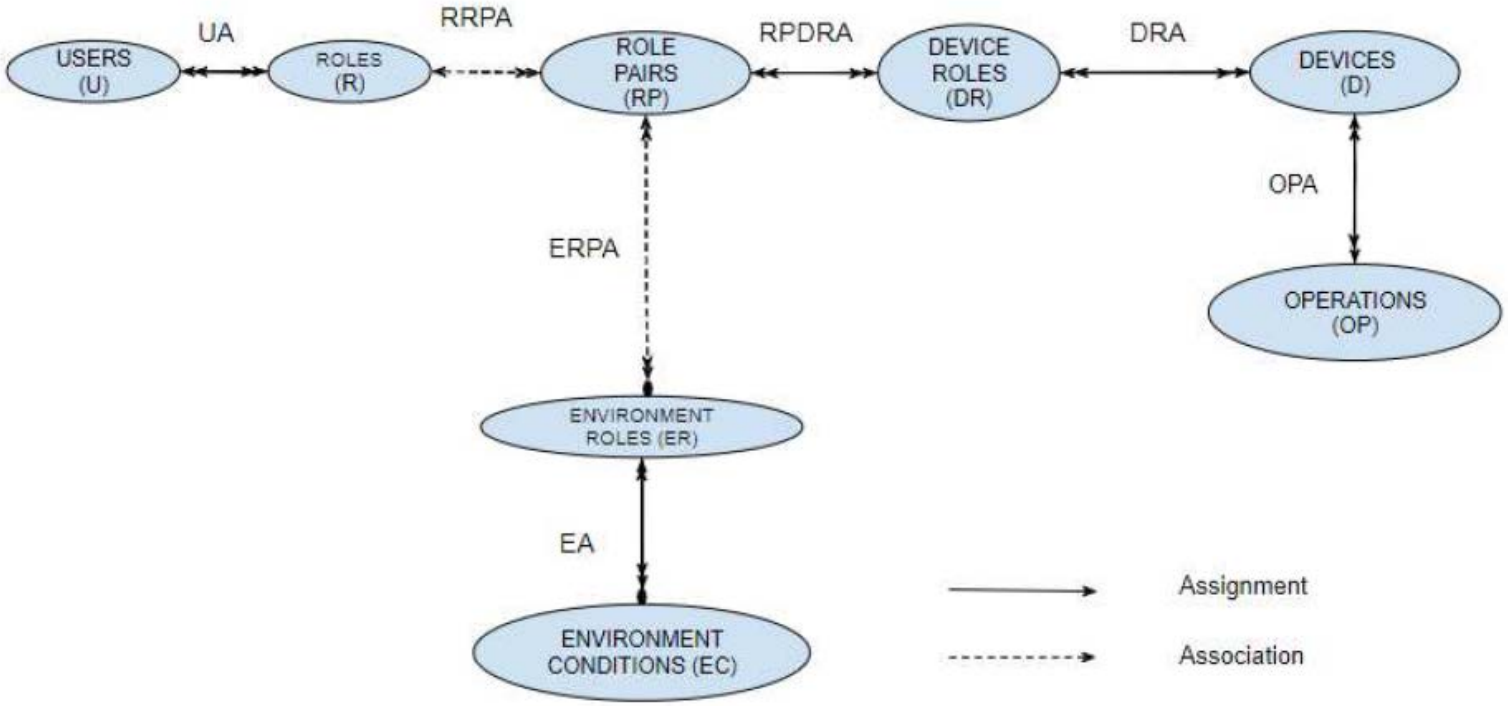
Use Case 1.A



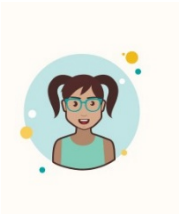
Use Case 1.A



Kids

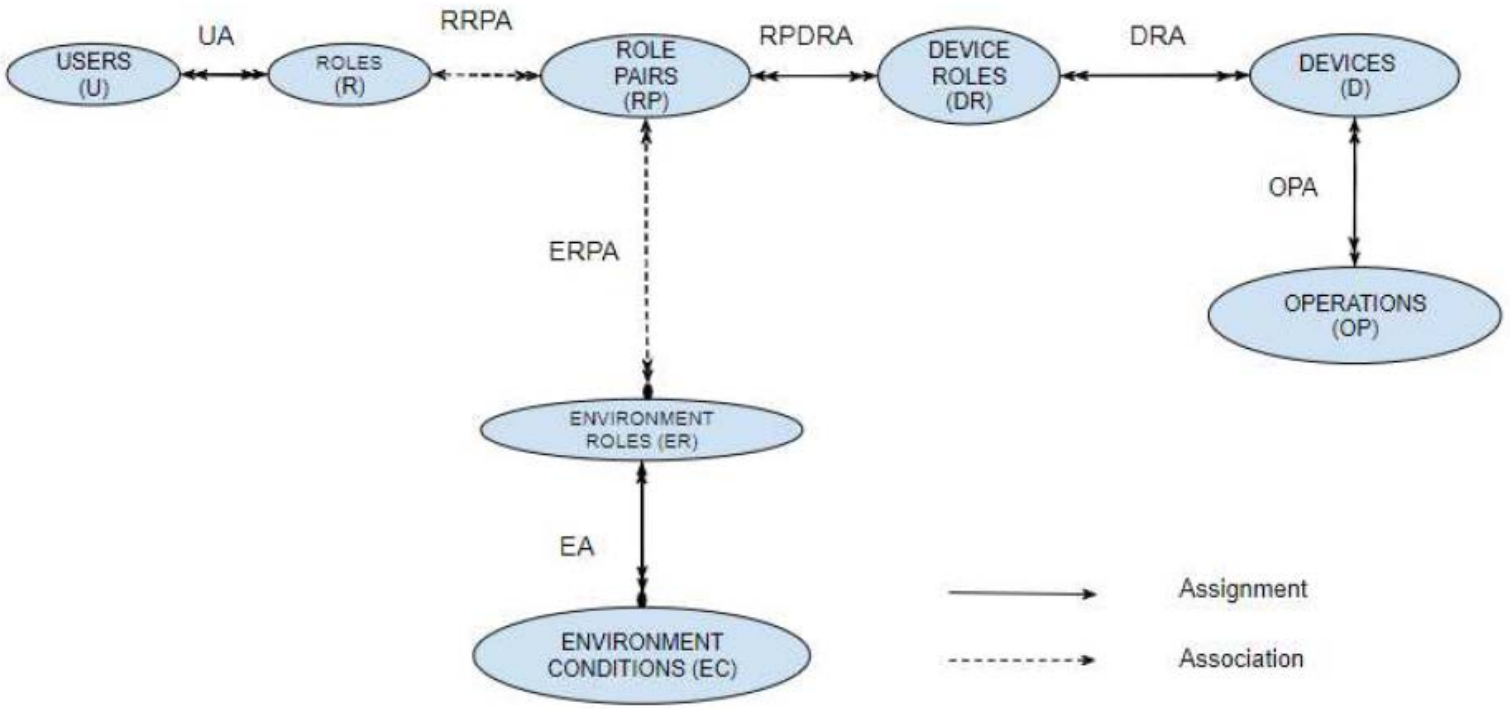


Use Case 1.A

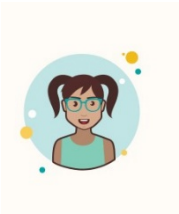


Kids

Entertainment Devices

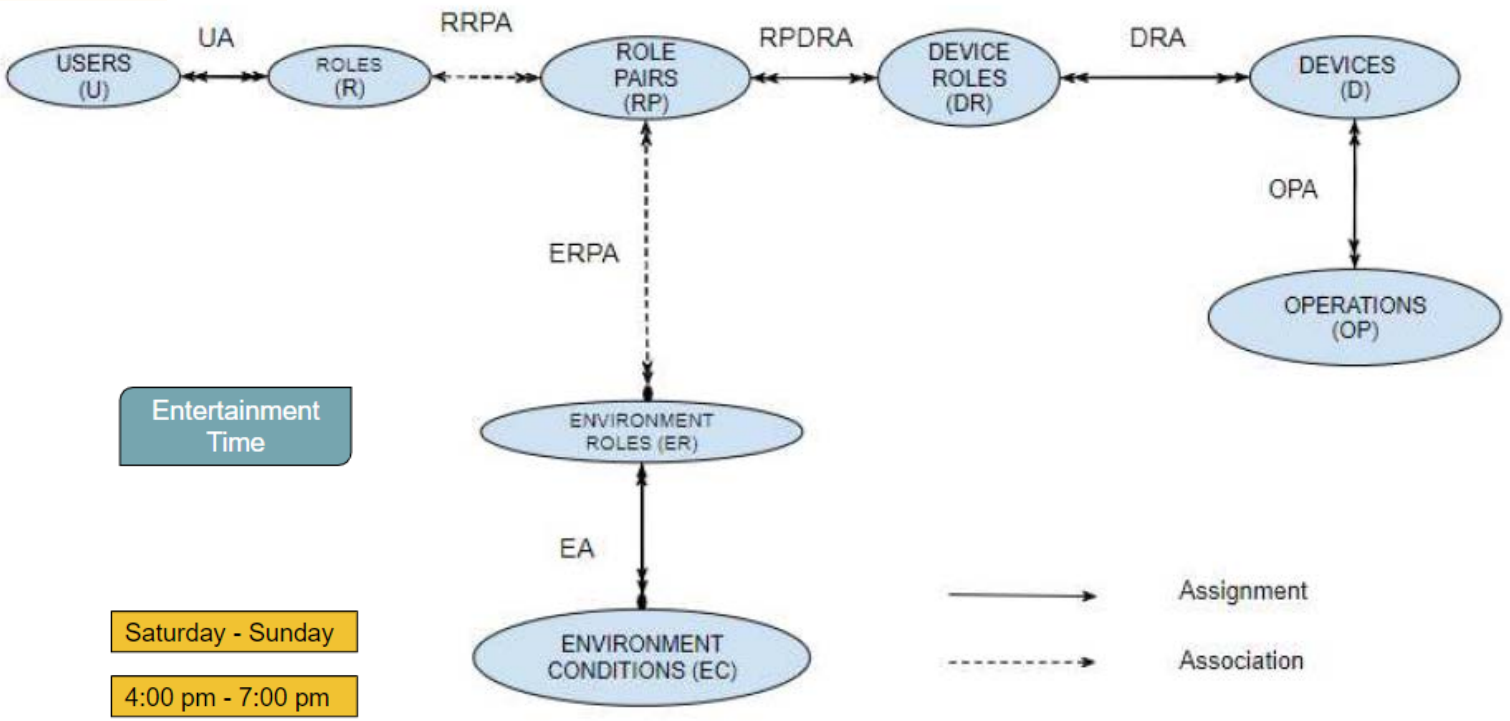


Use Case 1.A



Kids

Entertainment Devices

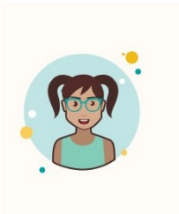


Entertainment Time

Saturday - Sunday

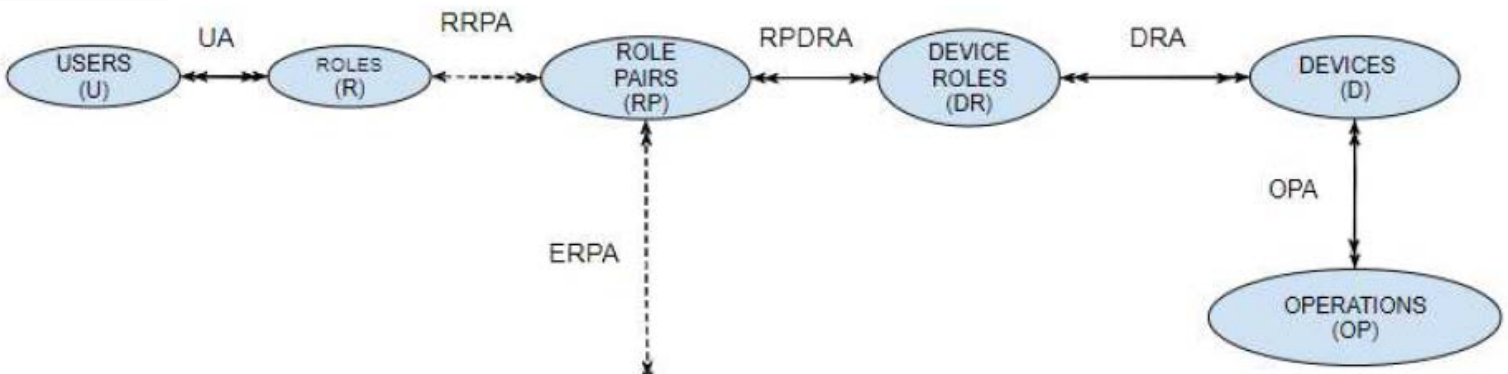
4:00 pm - 7:00 pm

Use Case 1.A



Kids

Entertainment Devices



Entertainment Time

Saturday - Sunday

4:00 pm - 7:00 pm

World-Leading Research with Real-World Impact!

References

- [1] W. He, M. Golla, R. Padhi, J. Ofek, M. D¨urmuth, E. Fernandes, and B. Ur, “Rethinking access control and authentication for the home internet of things (IoT),” in 27th USENIX Security Symposium (USENIX Security 18), 2018, pp. 255–272.
- [2] A.Ouaddah,H.Mousannif,A.A.Elkalam,andA.A.Ouahman,“Access control in the internet of things: Big challenges and new opportunities,” Computer Networks, vol. 112, pp. 237–262, 2017.
- [3] M. J. Covington, M. J. Moyer, and M. Ahamad, “Generalized role based access control for securing future applications,” Georgia Institute of Technology, Tech. Rep., 2000.
- [4] G. Zhang and J. Tian, “An extended role based access control model for the internet of things,” in 2010 International Conference on Information, Networking and Automation (ICINA), vol. 1. IEEE, 2010, pp. V1–319.
- [5] E. Barka, S. S. Mathew, and Y. Atif, “Securing the web of things with role-based access control,” in International Conference on Codes, Cryptology, and Information Security. Springer, 2015, pp. 14–26.

References

- [6] J. Jindou, Q. Xiaofeng, and C. Cheng, "Access control method for web of things based on role and sns," in 2012 IEEE 12th International Conference on Computer and Information Technology. IEEE, 2012, pp. 316–321.
- [7] S. Kaiwen and Y. Lihua, "Attribute-role-based hybrid access control in the internet of things," in Asia-Pacific Web Conference. Springer, 2014, pp. 333–343.
- [8] J. Liu, Y. Xiao, and C. P. Chen, "Authentication and access control in the internet of things," in 2012 32nd International Conference on Distributed Computing Systems Workshops. IEEE, 2012, pp. 588–592.
- [9] N. Ye, Y. Zhu, R.-c. Wang, R. Malekian, and L. Qiao-Min, "An efficient authentication and access control scheme for perception layer of internet of things," Applied Mathematics & Information Sciences, vol. 8, no. 4, p. 1617, 2014.
- [10] S. Bandara, T. Yashiro, N. Koshizuka, and K. Sakamura, "Access control framework for api-enabled devices in smart buildings," in 2016 22nd Asia-Pacific Conference on Communications (APCC). IEEE, 2016, pp. 210–217.

References

- [11] A. Mutsvangwa, B. Nleya, and B. Nleya, "Secured access control architecture consideration for smart grids," in 2016 IEEE PES PowerAfrica. IEEE, 2016, pp. 228–233.
- [12] Y. Xie, H. Wen, J. Wu, Y. Jiang, J. Meng, X. Guo, A. Xu, and Z. Guan, "Three-layerssecureaccesscontrolforcloud-basedsmartgrids,"in2015 IEEE 82nd Vehicular Technology Conference (VTC2015-Fall). IEEE, 2015, pp. 1–5.
- [13] F. Martinelli, C. Michailidou, P. Mori, and A. Saracino, "Too long, did not enforce: a qualitative hierarchical risk-aware data usage control model for complex policies in distributed environments," in Proceedings of the 4th ACM Workshop on Cyber-Physical System Security. ACM, 2018, pp. 27–37.
- [14] M. J. Covington, W. Long, S. Srinivasan, A. K. Dev, M. Ahamad, and G. D. Abowd, "Securing context-aware applications using environment roles," in Proceedings of the sixth ACM symposium on Access control models and technologies. ACM, 2001, pp. 10–20.
- [15] R. S. Sandhu, "Role-based access control," in Advances in computers. Elsevier, 1998, vol. 46, pp. 237–286.