I·C·S
The Institute for Cyber Security

C·SPECC
Center for Security and Privacy Enhanced Cloud Computing

# The EGRBAC Model for Smart Home IoT Access Control

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**



*World-Leading Research with Real-World Impact!*



UTSA Computer Science

# Introduction & Motivation



- 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.

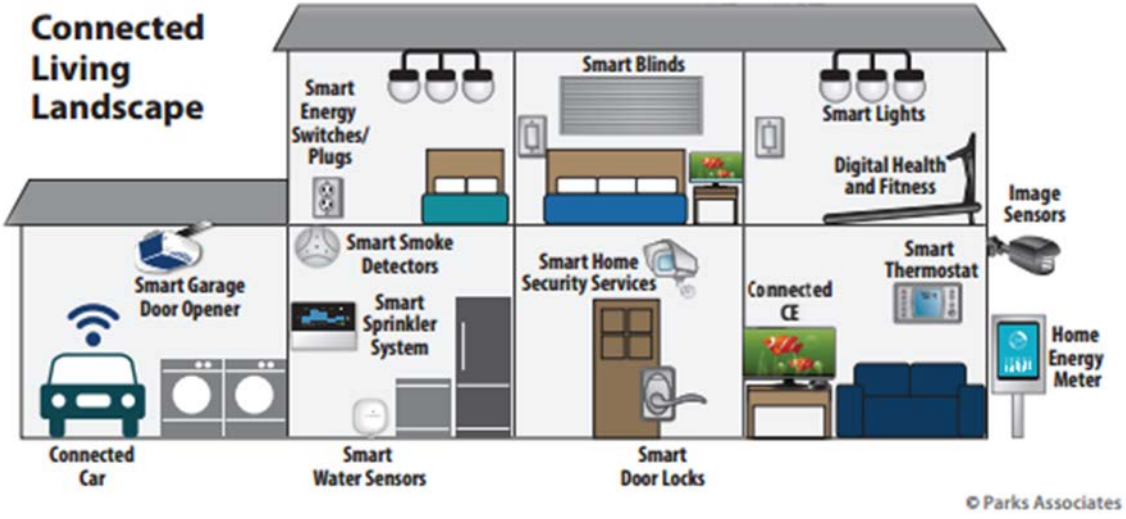
# Introduction & Motivation



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

- Surprisingly, little attention has been paid to access control in home IoT.

- AC issues have been explored extensively for many different domains.



# Introduction & Motivation



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

# Introduction & Motivation



- The characteristics that make IoT distinct from prior computing domains necessitate a rethinking of access control and authentication [1].

- The need arises for a dynamic and fine-grained access control mechanism, where users and resources are constrained [2].

- Why focus on the home rather than general IoT?

  ➢We believe that smart homes provide a rich yet scoped environment where we have limited number of users who want to access limited number of shared constrained smart things with different privileges. Such scoping is necessary to develop an initial set of models. In future these scoped models can be adapted and evolved to address the access control requirements of other IoT domains, such as a smart office, a smart classroom or a smart city.

# 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 smart home devices**.

# 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, 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 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. The insiders who have legitimate digital and physical access to the house, such as family members, guests, and workers.

# Our Threat Model

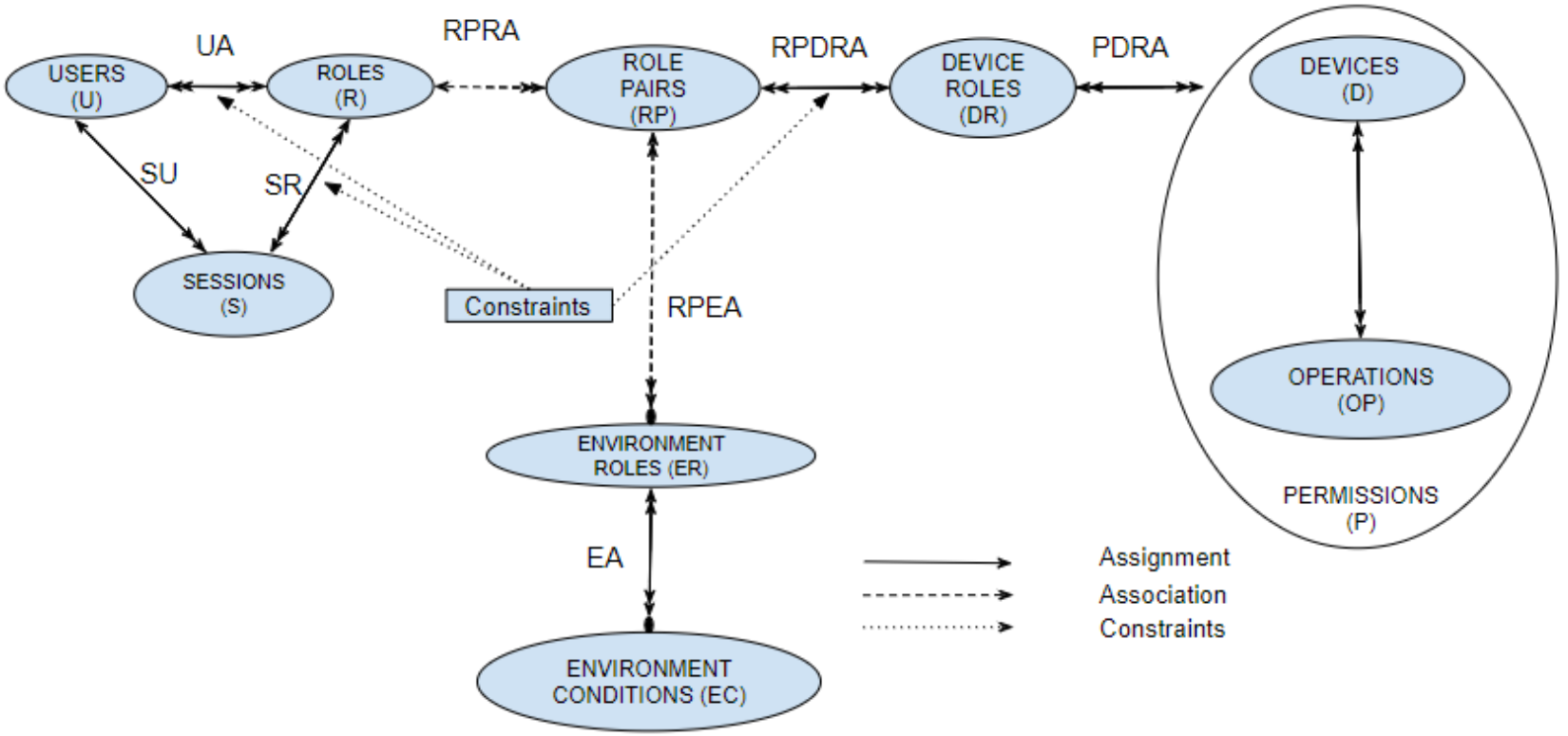


- The intention for legitimate users to break down the access control system of the smart home may vary; some examples may be:
  - Curiosity (a kid playing with the oven setting).
  - Disturbing other family members (a kid locking his brothers outside the house).
  - Disobedience (a kid is trying to watch TV outside the allowed entertainment time).
  - Robbery (a worker getting access to the camera system and adjust it to shutdown at a certain time).

➢ **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.

# The EGRBAC Model





# EGRBAC Model Formalization



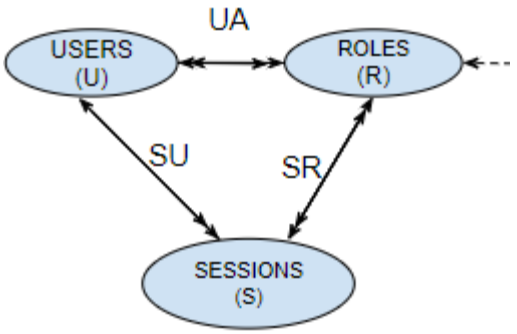
**Users, Roles and Sessions**

– $U, R$ and $S$ are sets of users, roles and sessions respectively

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

– $SU \subseteq S \times U$, many to one sessions to user relation that assigns each session to a single user who controls the session

– $SR \subseteq S \times R$, many to many session to roles relation that assigns each session to a set of roles that can change under user control, where $(s_i, r_j) \in SR \Rightarrow (\exists u_k \in U)[(s_i, u_k) \in SU \wedge (u_k, r_j) \in UA]$; by definition of $SU$, $u_k$ must be unique

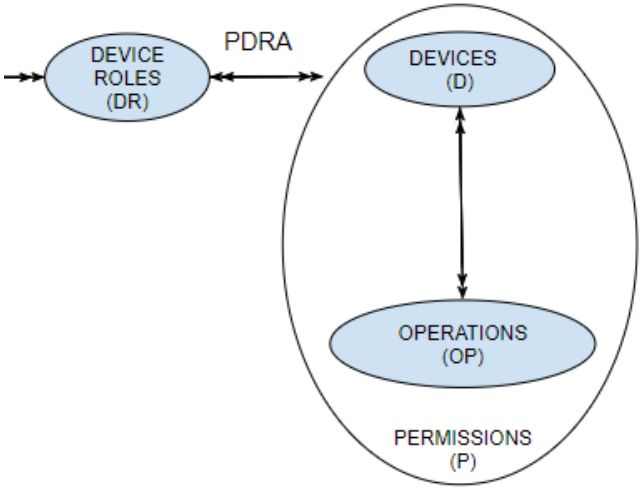



**Devices, Operations, Permissions and Device Roles**

– $D, OP, P$ and $DR$ are sets of devices, operations, permissions and device roles respectively

– $P \subseteq D \times OP$, every permission is a device, operation pair (device manufacturer specified)

– $PDRA \subseteq P \times DR$, a many to many permissions to device roles assignment (home owner specified)



# EGRBAC Model Formalization



**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);

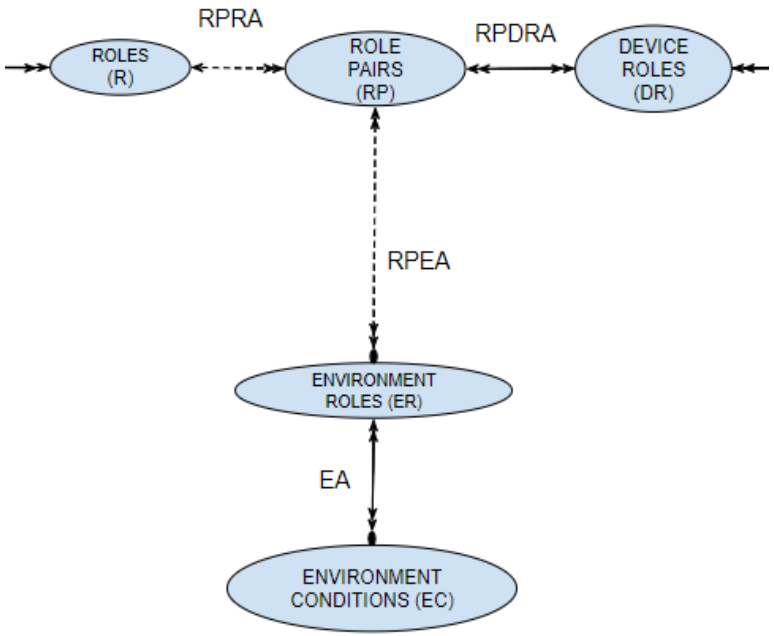
for every $rp = (r_i, ER_j) \in RP$, let $rp.r = r_i$ and $rp.ER = ER_j$

$-RPRA \subseteq RP \times R$, many to one role pairs to role association induced by $RP$, where $RPRA = \{(rp_m, r_n) \mid rp_m \in RP \wedge rp_m.r = r_n\}$

$-RPEA \subseteq RP \times 2^{ER}$, many to one environment roles to role pairs association induced by $RP$, where $RPEA = \{(rp_m, ER_n) \mid rp_m \in RP \wedge ER_n = rp_m.ER\}$

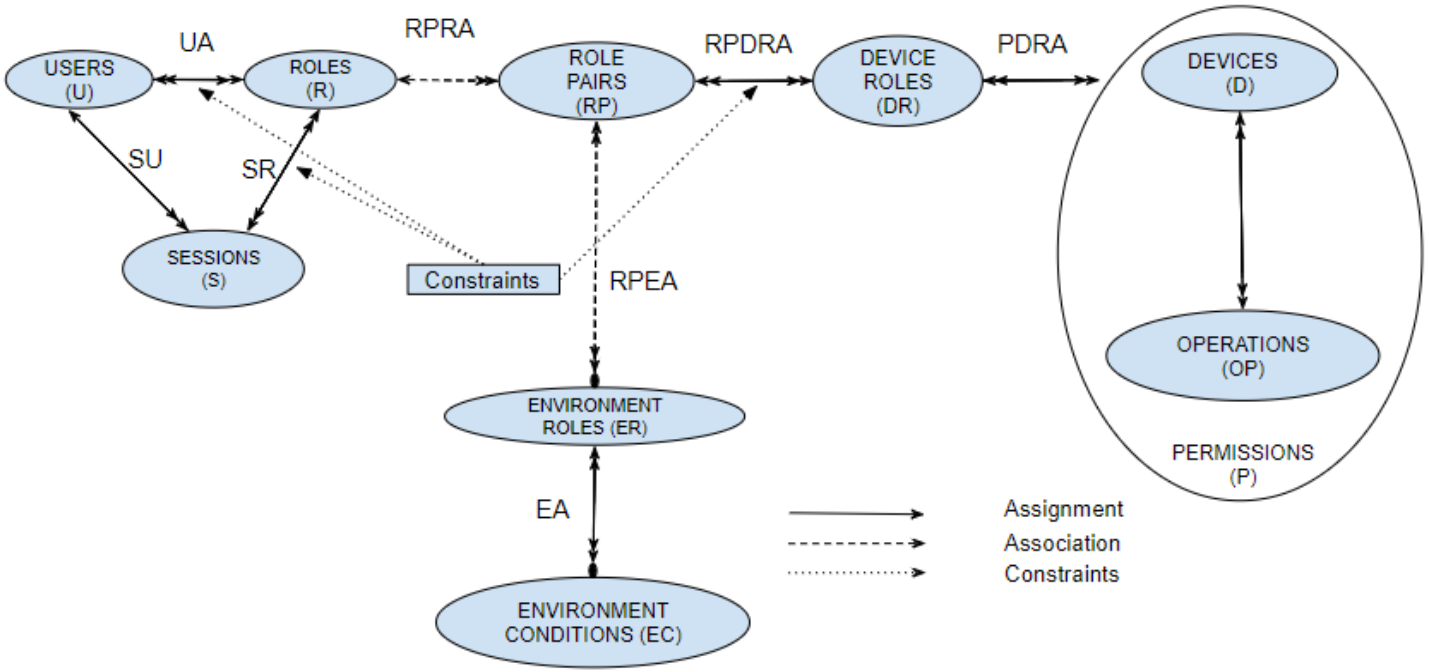
**Role Pair Assignment**

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



# The EGRBAC Model






- The main idea in EGRBAC as a whole is that a user is assigned to a set of roles and according to the current active sessions, and current active environment roles some role pairs will be active, the user will get access to the permissions assigned to the device roles which are assigned to the current active role pairs.

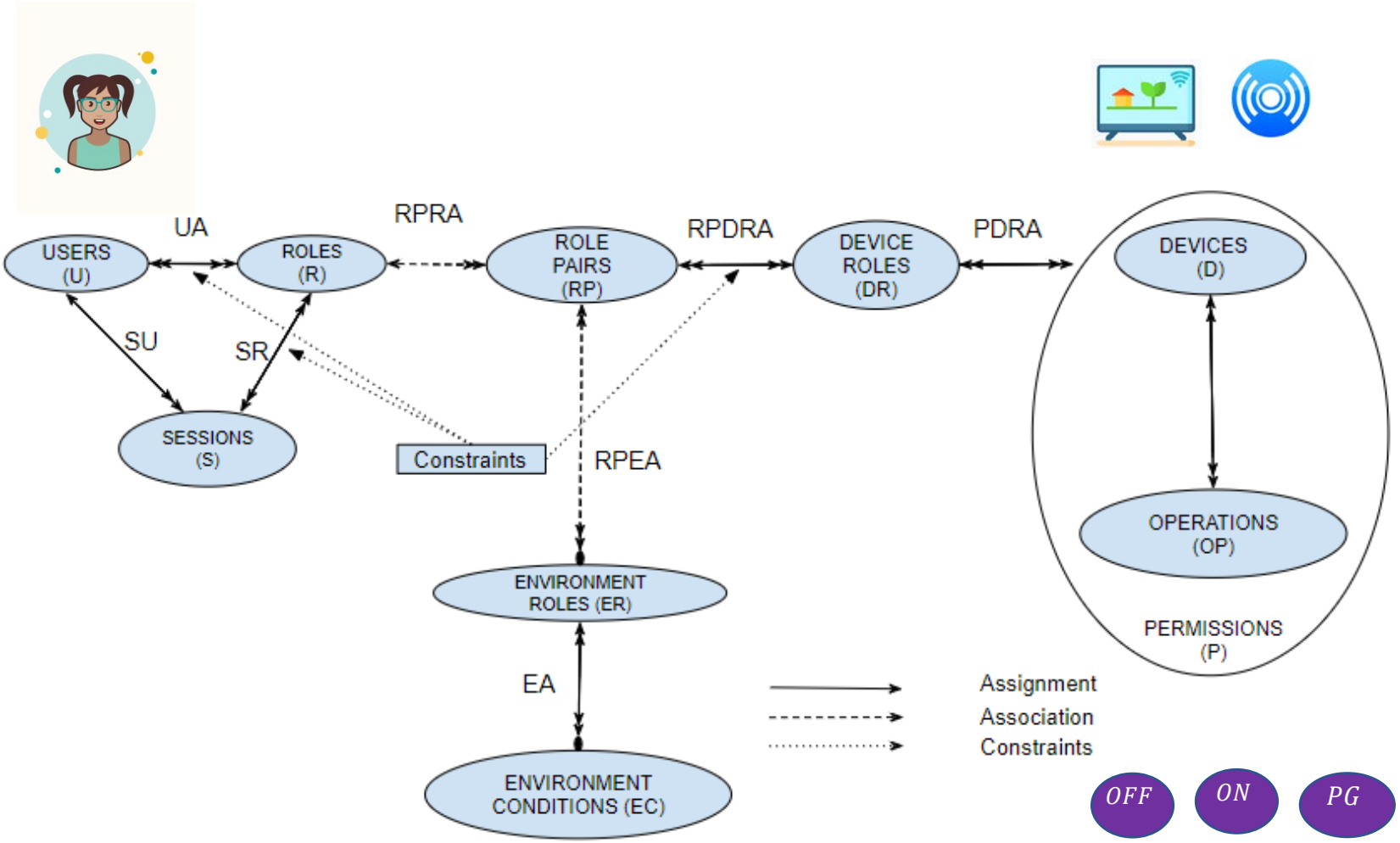
# Use Case



The objective is to allow kids to access a subset of permissions (On, Off, and PG contents) in entertainment devices (TV, DVD) during weekend evenings only.

# Use Case

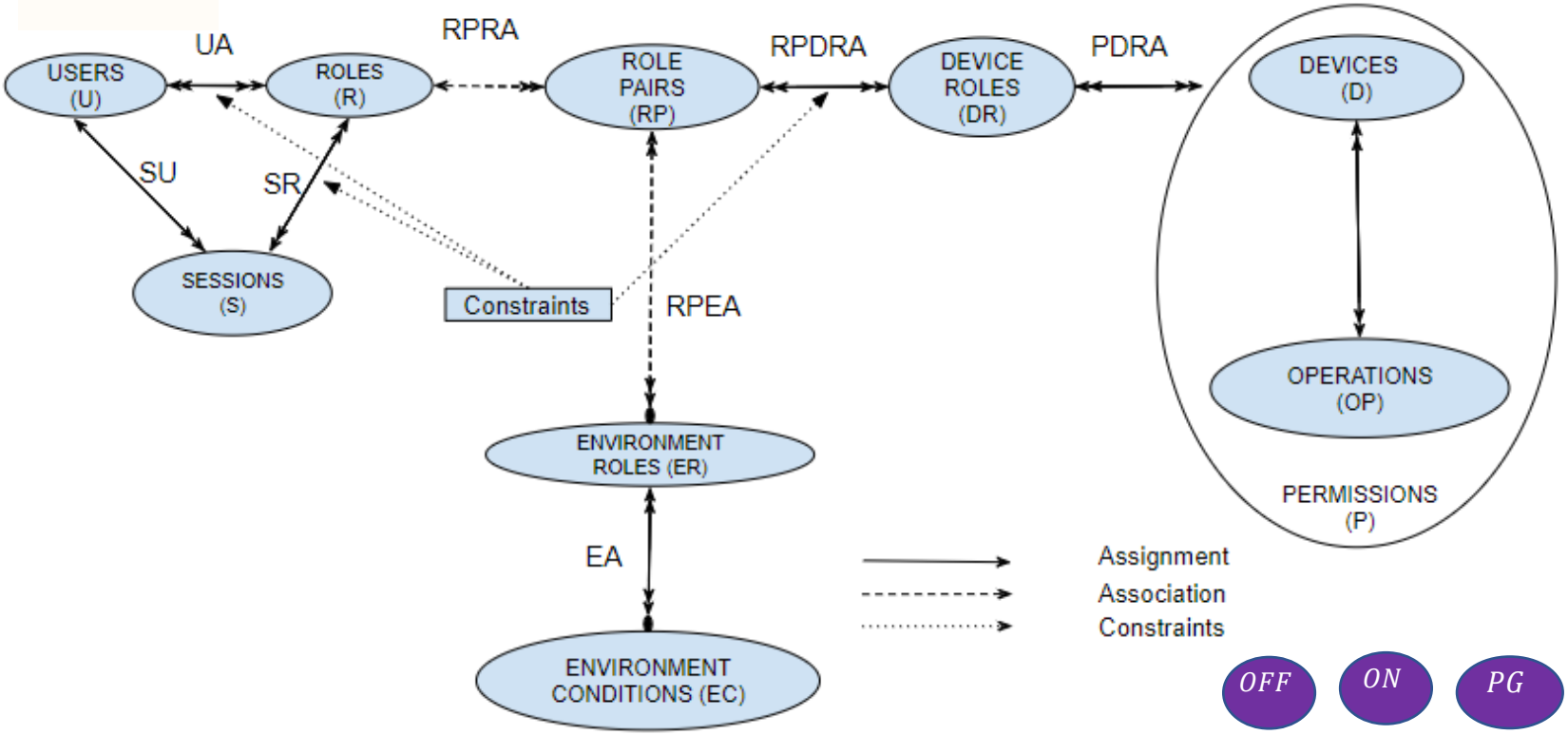




# Use Case

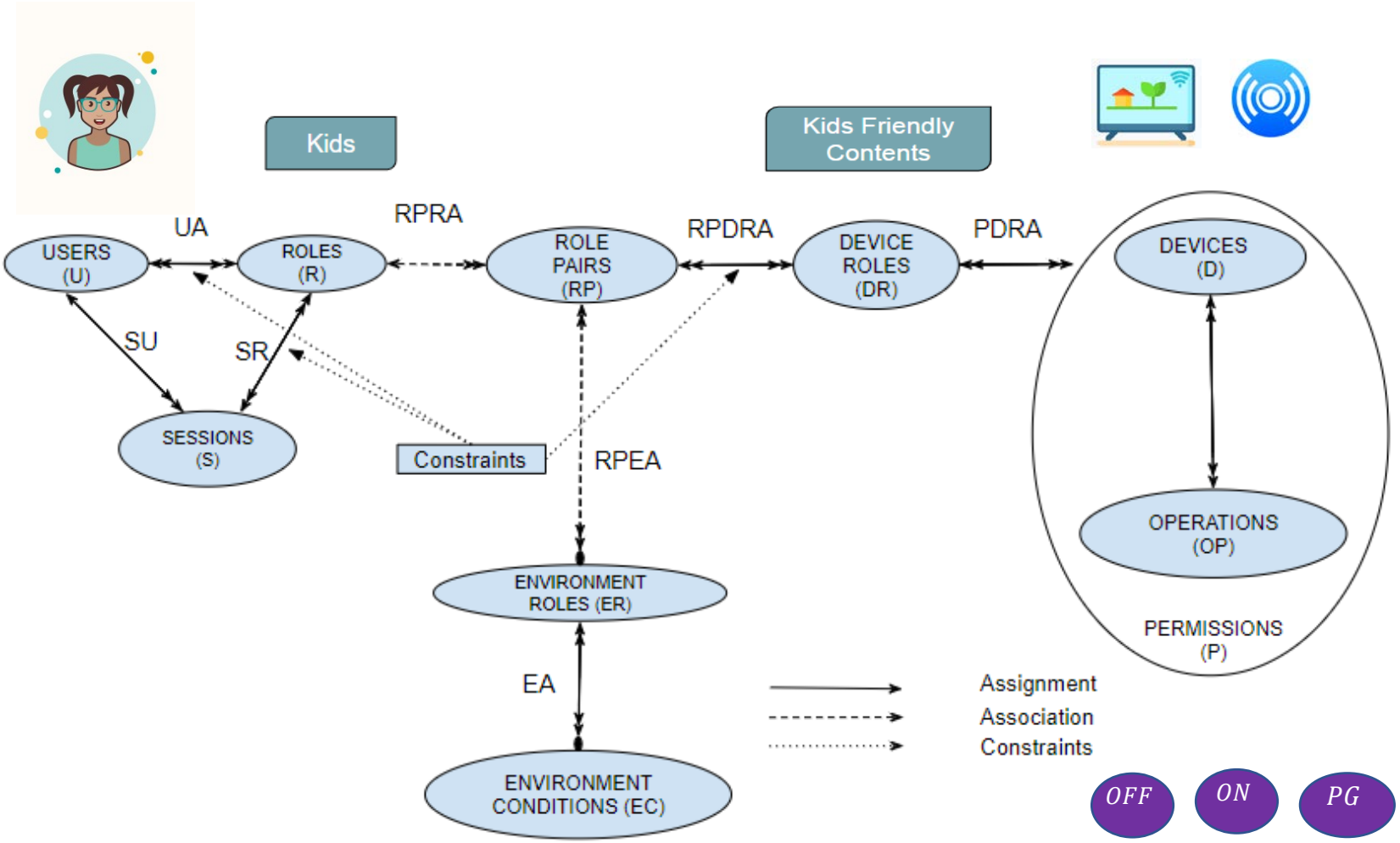


Kids



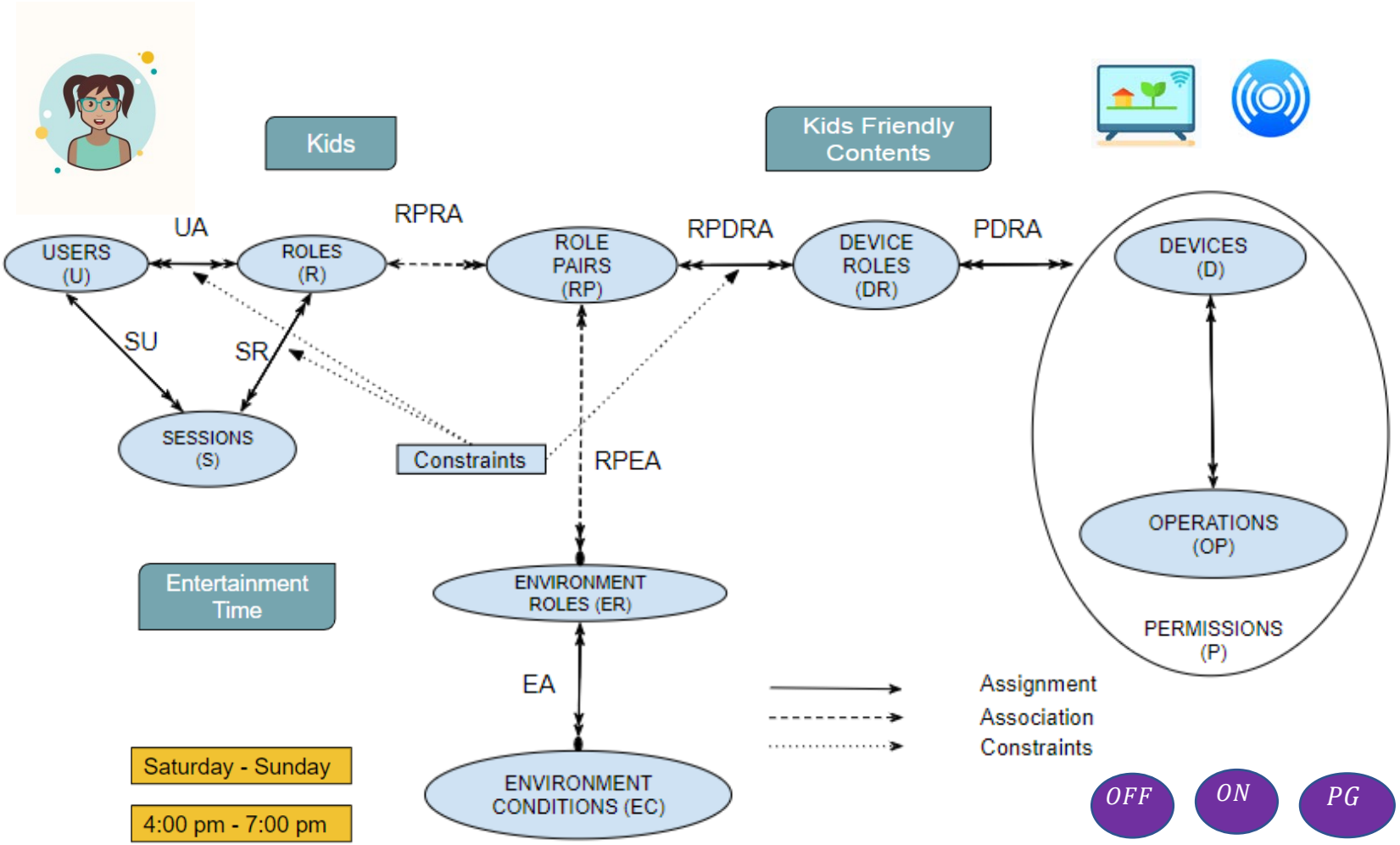
# Use Case





# Use Case

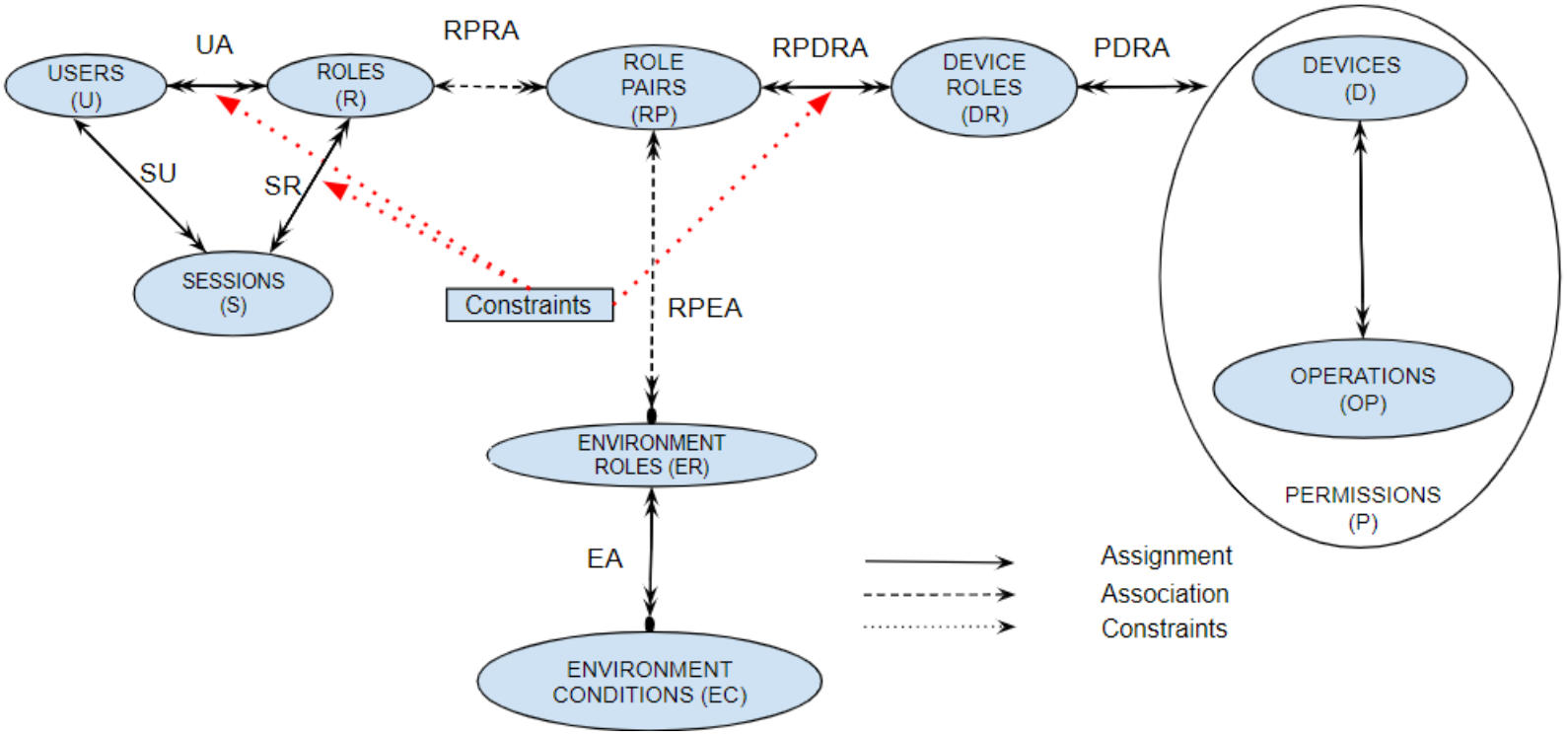




# Constraints



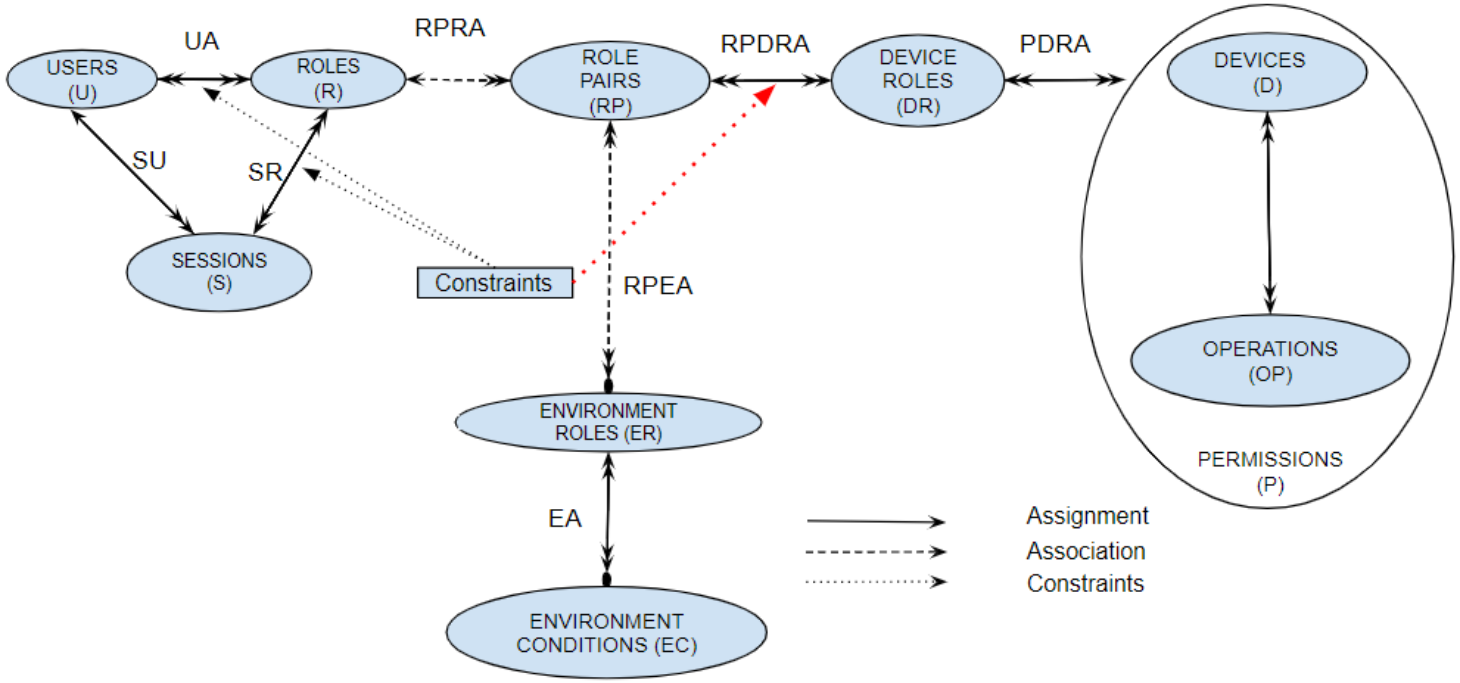
- **A constraint is an invariant that must always be maintained.**



# Constraints



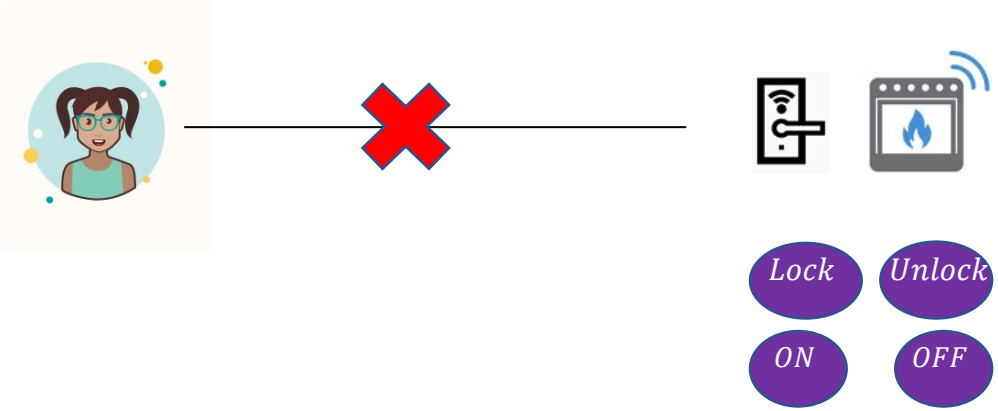
## 1. Permission-role constraint



# Constraints



- These constraints prevent specific roles from getting access to specific permissions.
- For example, what if we want to prevent future assignment of dangerous permissions to the role Kids (which could happen inadvertently by the homeowner)?



# Constraints



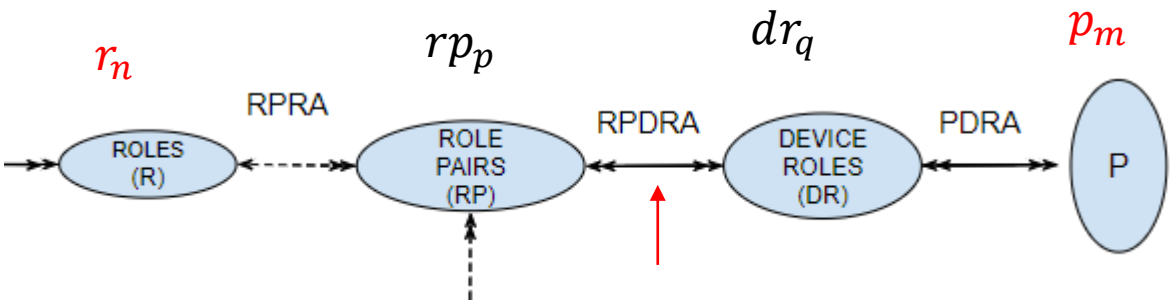
- To prevent such situations, EGRBAC incorporates constraints that forbid such assignment. Formally:

$\boldsymbol{PR\,Constraints} \subseteq \boldsymbol{2^P \times 2^R}$ constitute a many to many subset of permissions to subset of roles relation.

- Each prc $= (P_i, R_j) \in Constraints$ specifies the following invariant:

For every $p_m \in P_i$ and every $r_n \in R_j$ :

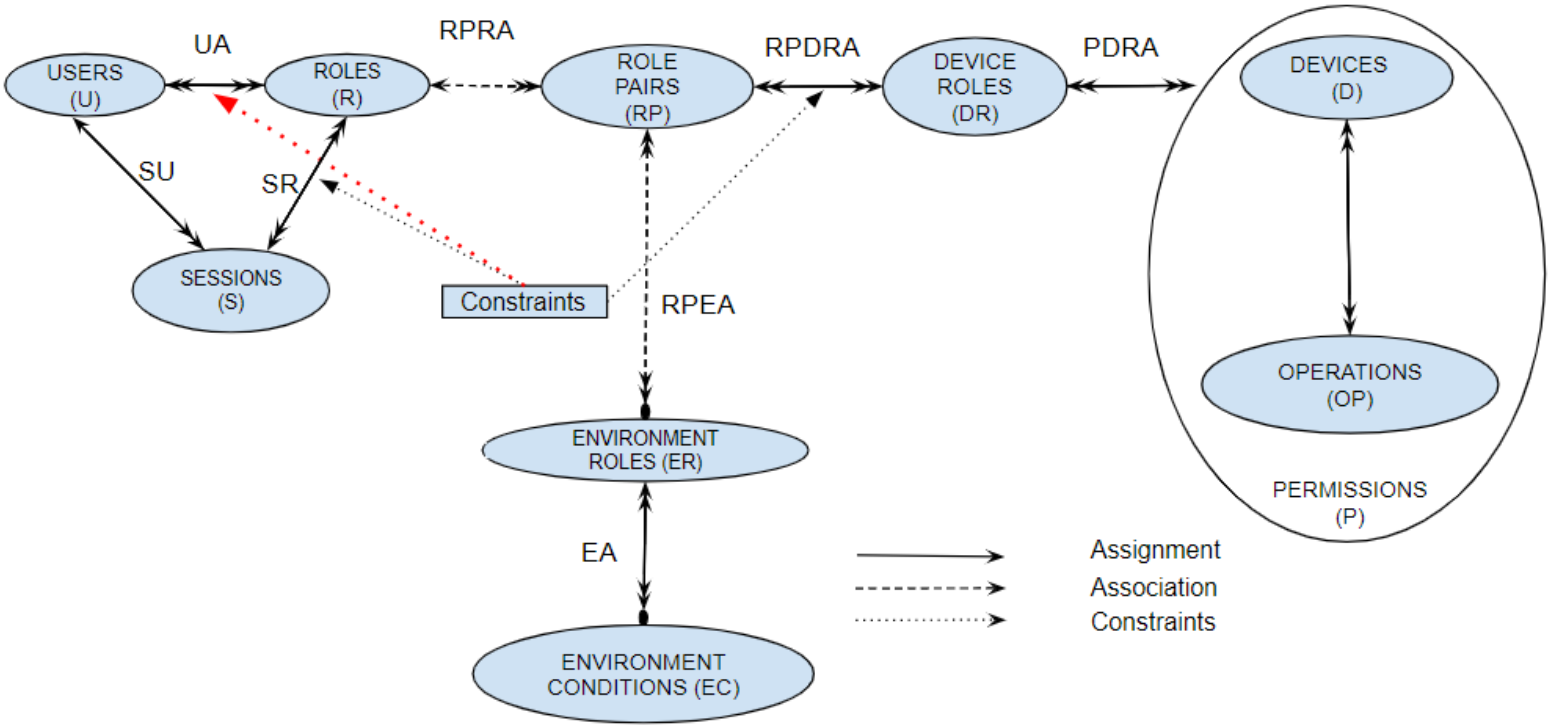
$$\forall_{\boldsymbol{rp_p} \in \boldsymbol{RP},\, \boldsymbol{dr_q} \in \boldsymbol{DR}} \; (\boldsymbol{rp_p}, \boldsymbol{dr_q}) \in \boldsymbol{RPDRA} \quad \Rightarrow \quad (\boldsymbol{p_m}, \boldsymbol{dr_q}) \notin \boldsymbol{PDRA} \quad \vee \quad (\boldsymbol{rp_p}.\boldsymbol{r} \neq \boldsymbol{r_n})$$



# Constraints



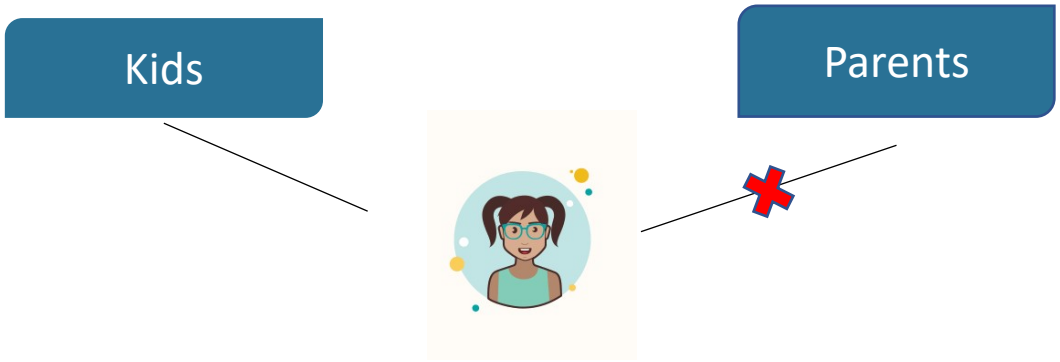
## 2. Static separation of duty:



# Constraints



If a user is authorized as a member of one role, the user is prohibited from being a member of a second conflicting role [16].




$\boldsymbol{SSDConstraints} \subseteq \boldsymbol{R} \times \boldsymbol{2^R}$ constitute a many to many role to a subset of mutually exclusive roles relation.

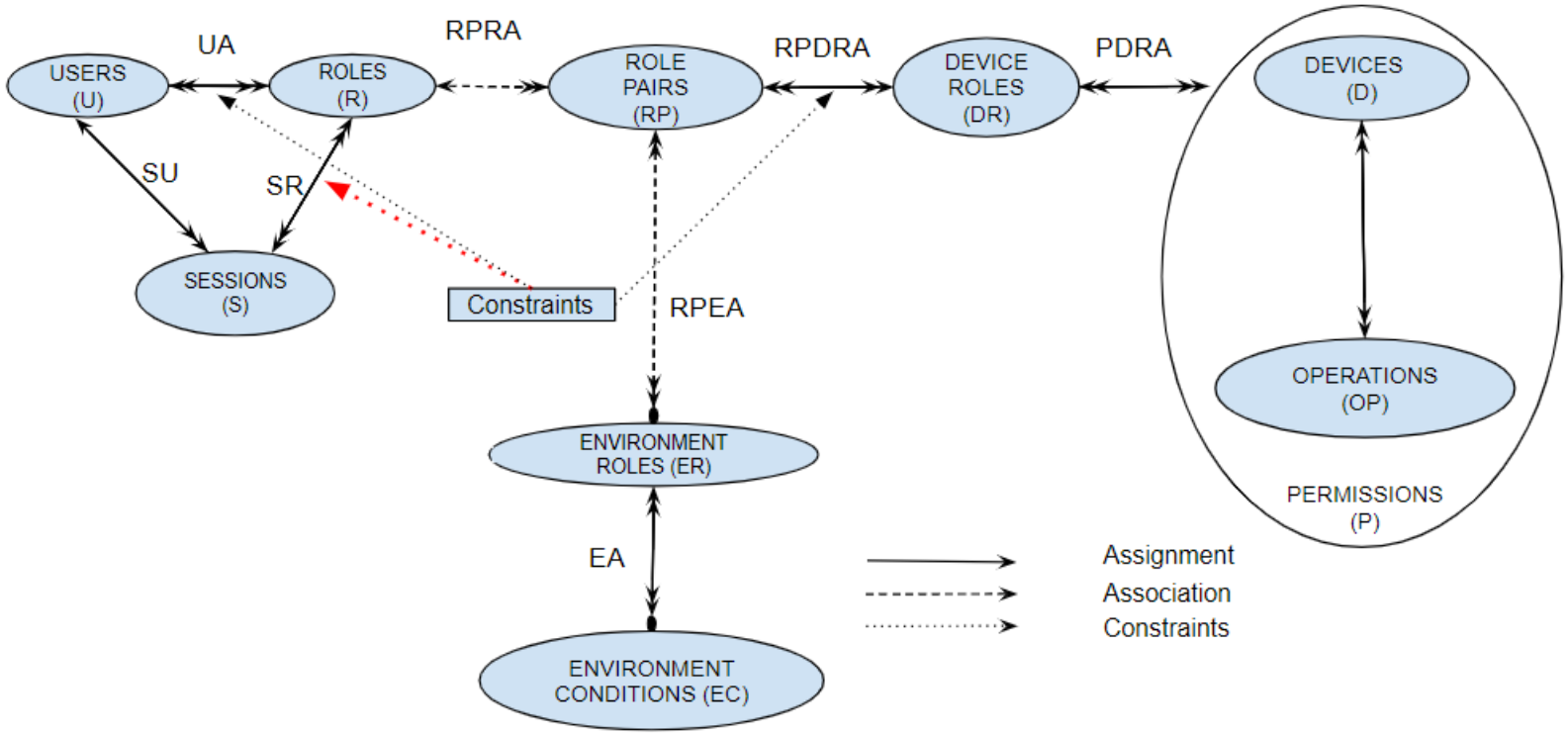
- Each $ssdc = (r_i, R_j) \in SSDConstraints$ specifies the following invariant:

$$(\forall \boldsymbol{u_m} \in \boldsymbol{U})(\forall \boldsymbol{r_n} \in \boldsymbol{R_j})[(\boldsymbol{u_m}, \boldsymbol{r_n}) \in \boldsymbol{UA} \Rightarrow (\boldsymbol{u_m}, \boldsymbol{r_i}) \notin \boldsymbol{UA}]$$

# Constraints



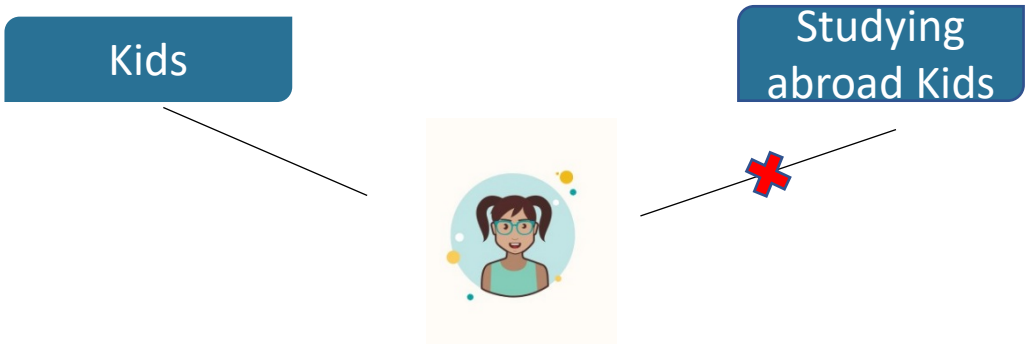
**3. Dynamic separation of duty:**



# Constraints



With DSD it is permissible for a user to be authorized as a member of a set of roles which do not constitute a conflict of interest when acted in independently but produce policy concerns when allowed to be acted simultaneously in the same session [16].



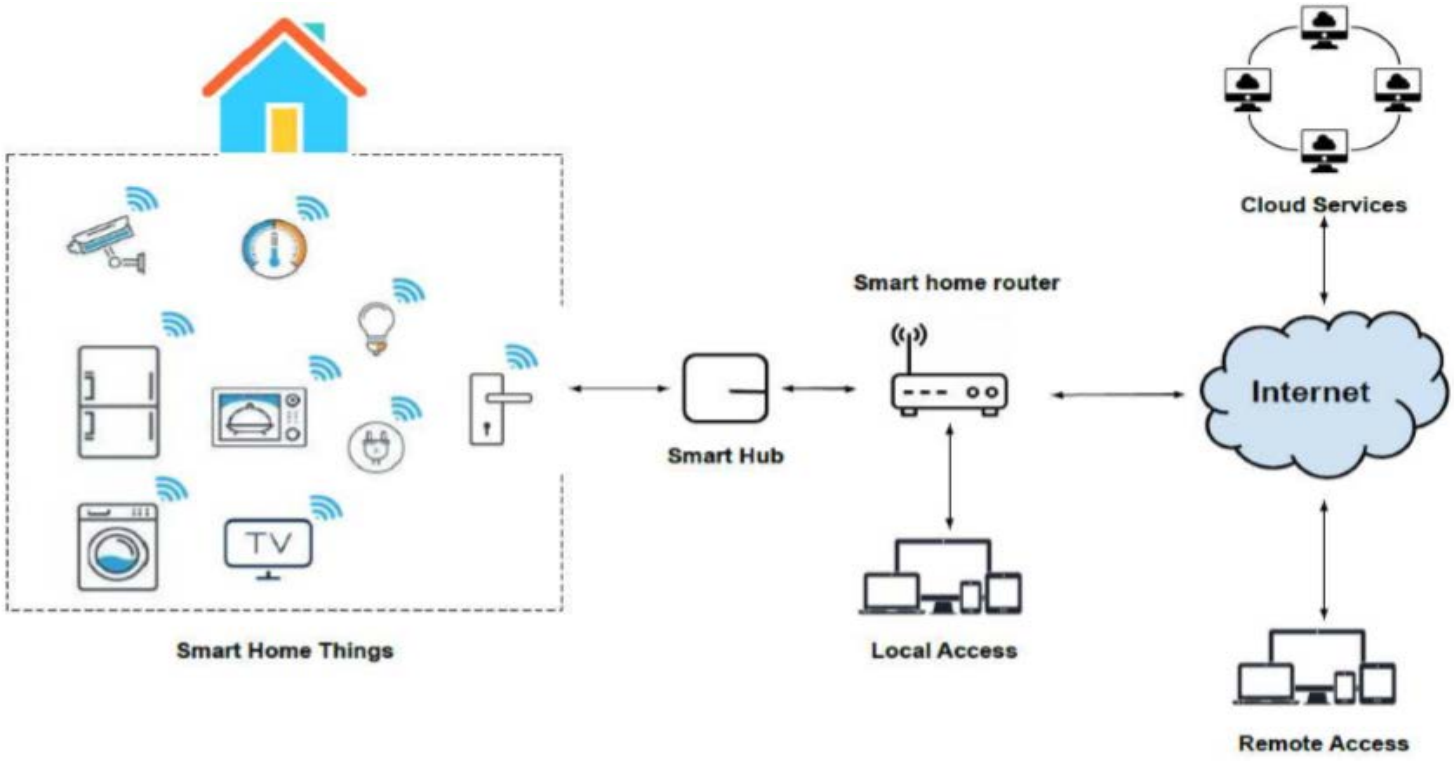

$\boldsymbol{DSDConstraints} \subseteq \boldsymbol{R} \times \boldsymbol{2^R}$ constitute a many to many role to a subset of active mutually exclusive roles relation.

- Each $dsdc = (r_i, R_j) \in DSDConstraints$ specifies the following invariant:

$$(\forall \boldsymbol{s} \in \boldsymbol{S})(\forall \boldsymbol{r_n} \in \boldsymbol{R_j})[(\boldsymbol{s}, \boldsymbol{r_n}) \in \boldsymbol{SR} \Rightarrow (\boldsymbol{s}, \boldsymbol{r_i}) \notin \boldsymbol{SR}]$$

# Enforcement Architecture






- Adapted from [17]
- There are two types of requests: A- Local requests. B- Remote requests.
- We implemented our model using AWS IoT service.

# Performance Analysis



- We conducted a performance test to depict how our system responds in different scenarios with different loads.
- The results show that our model is functional, and applicable.

ONE USER SENDING REQUESTS TO MULTIPLE DEVICES

| Number of Users | Number of devices | Lambda Processing Time in ms. | Total Number of requests |
|---|---|---|---|
| 1 | 1 | 1.029138 | 1000 |
| 1 | 3 | 1.236029 | 3000 (1000 per request) |
| 1 | 5 | 1.202856 | 5000 (1000 per request) |

ONE USER SENDING REQUESTS TO ONE DEVICE

| Number of Users | Number of devices | Lambda Processing Time in ms. | Total Number of requests |
|---|---|---|---|
| 1 | 1 | 1.029138 | 1000 |
| 3 | 3 | 1.796938 | 3000 (1000 per request) |
| 5 | 5 | 2.833097 | 5000 (1000 per request) |

MULTIPLE USERS SENDING REQUESTS TO ONE DEVICE

| Number of Users | Number of devices | Lambda Processing Time in ms. | Total Number of requests |
|---|---|---|---|
| 1 | 1 | 1.029138 | 1000 |
| 3 | 1 | 0.955529 | 3000 (1000 per request) |
| 5 | 1 | 0.956221 | 5000 (1000 per request) |

# Conclusion



- We propose the EGRBAC access control model for smart home IoT.
- Our model's main goal is to ensure that legitimate users are only permitted to use the devices which they are allowed to access under the appropriate conditions.
- It is a dynamic, fine-grained model.
- In the future we are planning, to develop a family (or series) of models ranging from relatively simple and complete to incorporating increasingly sophisticated and comprehensive features.


Q&A

# Thank You

# 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 rolebased access control for securing future applications,” Georgia Institute of Technology, Tech. Rep., 2000.
- [15] R. S. Sandhu, “Role-based access control,” in Advances in computers. Elsevier, 1998, vol. 46, pp. 237–286.
- [16] R. Sandhu, et al. The nist model for role-based access control: towards a unified standard. In ACM workshop on Role-based access control, 2000.
- [17] D. Geneiatakis, et al. Security and privacy issues for an IoT based smart home. In 2017 40th MIPRO. IEEE, 2017