I·C·S
The Institute for Cyber Security

C·SPECC
Center for Security and Privacy Enhanced Cloud Computing

# User-To-Device Access Control Models for Cloud-Enabled IoT With Smart Home Case Study

**Ph.D. Dissertation Defense**
**Safwa Ameer**
Institute for Cyber Security,
Department of Computer Science
The University of Texas at San Antonio

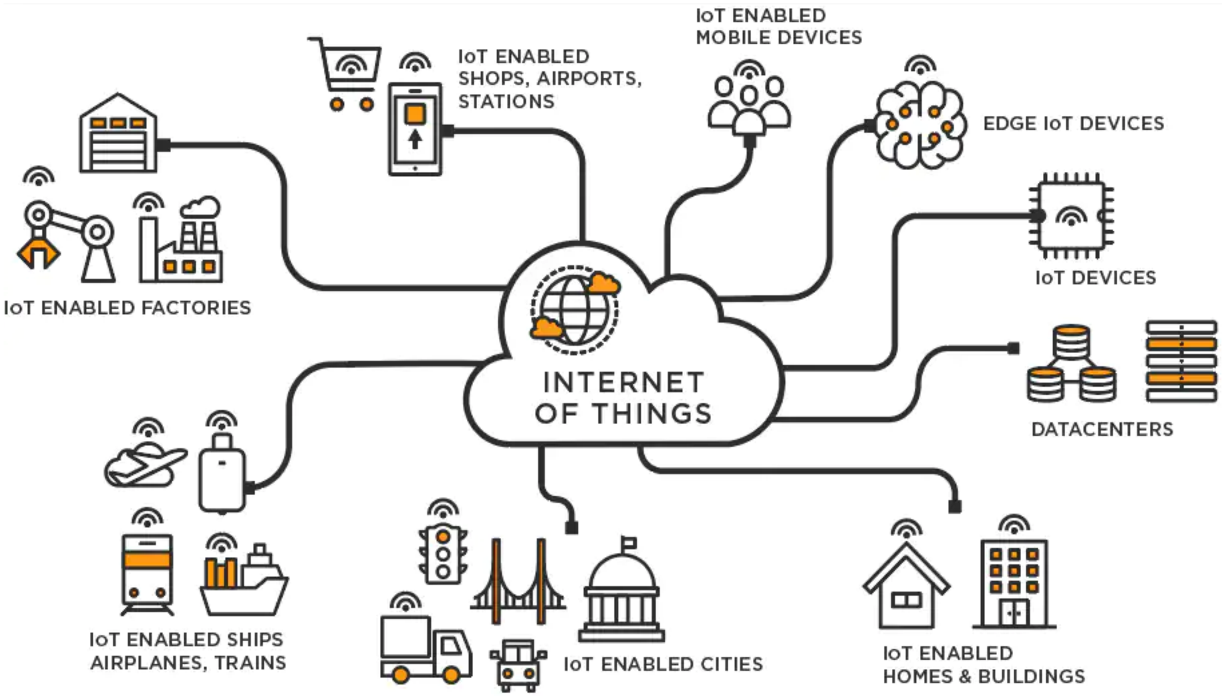
**Committee:**
Dr. Ravi Sandhu (Advisor and Chair)
Dr. Jianwei Niu
Dr. Ram Krishnan
Dr. Weining Zhang
Dr. Xiaoyin Wang

**July 2021**

# Internet of Things

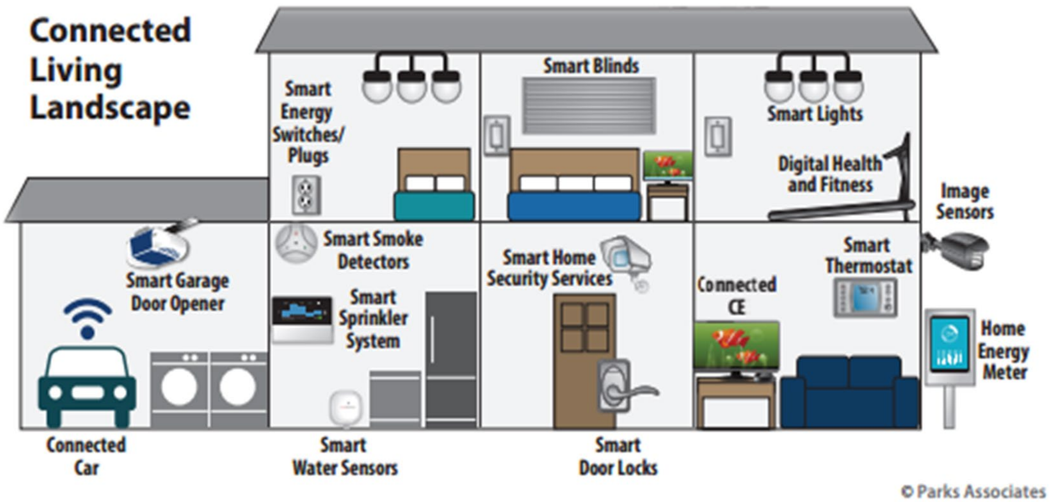


- The Internet of Things (IoT) is a new technology paradigm envisioned as a global network of physical objects (things) that are embedded with sensors, software, and other technologies for the purpose of connecting and exchanging data with other devices and systems over the Internet.



# Smart Home IoT

- Surprisingly, little attention has been paid to access control in home IoT.
- AC issues have been explored extensively for many different domains.
- The characteristics that make IoT distinct from prior computing domains necessitate a rethinking of access control and authentication.
- The need arises for a dynamic and fine-grained access control mechanism, where users and resources are constrained.



# Problem Statement

- In the literature, several access control models have been proposed for IoT in general.
- Most of them are built on ABAC or RBAC.
- Some researchers argue that RBAC is more suitable for IoT since it is simpler in management and review, while ABAC is complex.
- Others argue that ABAC models are more scalable and dynamic, since they can capture different devices and environment contextual information.
- Hence, when it comes to smart homes, at this point it is not fully clear what is the benefit of ABAC over RBAC, and vice versa.
- Our intuitive insight is that a hybrid model will better capture smart home IoT access control requirements.

# Thesis Statement



*The established paradigms of role-based and attribute-based access control can be utilized, adapted, and extended to provide fine grained and dynamic authorization approaches for user to device access in smart home IoT. A detailed analysis of these approaches, their formal models, and implementation can ultimately be utilized to develop hybrid access control models that combine role-based and attribute-base access control features to meet smart home IoT challenges.*

# Summary of Contributions

## USER-TO-DEVICE ACCESS CONTROL MODELS FOR CLOUD-ENABLED IOT WITH SMART HOME CASE STUDY

### Analyze literature IoT Access Control Models

1- Criteria for Home IoT Access Control Models.
2- Analyze literature IoT access control models against the proposed criteria.

### RBAC for Home IoT AC

***EGRBAC***

### ABAC for Home IoT AC

***HABAC***

1- Constructing *EGRBAC* from *HABAC*
2- Constructing *HABAC* from *EGRBAC*
3- Compare the theoretical expressive power of *EGRBAC* and *HABAC*

### Combined Models for Home IoT AC

$HyBAC_{RC}$ | $HyBAC_{AC}$

1- Constructing $HyBAC_{RC}$ from $HyBAC_{AC}$
2- Constructing $HyBAC_{AC}$ from $HyBAC_{RC}$
3- Compare the theoretical expressive power of $HyBAC_{RC}$ and $HyBAC_{AC}$

# Summary of Contributions



## USER-TO-DEVICE ACCESS CONTROL MODELS FOR CLOUD-ENABLED IOT WITH SMART HOME CASE STUDY

### Analyze literature IoT Access Control Models

1- Criteria for Home IoT Access Control Models.
2- Analyze literature IoT access control models against the proposed criteria.

### RBAC for Home IoT AC

***EGRBAC***

### ABAC for Home IoT AC

***HABAC***

1- Constructing *EGRBAC* from *HABAC*
2- Constructing *HABAC* from *EGRBAC*
3- Compare the theoretical expressive power of *EGRBAC* and *HABAC*

### Combined Models for Home IoT AC

$HyBAC_{RC}$ | $HyBAC_{AC}$

1- Constructing $HyBAC_{RC}$ from $HyBAC_{AC}$
2- Constructing $HyBAC_{AC}$ from $HyBAC_{RC}$
3- Compare the theoretical expressive power of $HyBAC_{RC}$ and $HyBAC_{AC}$

# Criteria for Smart Home IoT Access Control Models

# 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**. Smart things in homes are usually limited in term of computational power, and storage. Furthermore, 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, 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.

# Summary of Contributions



## USER-TO-DEVICE ACCESS CONTROL MODELS FOR CLOUD-ENABLED IOT WITH SMART HOME CASE STUDY

### Analyze literature IoT Access Control Models

1- Criteria for Home IoT Access Control Models.
2- Analyze literature IoT access control models against the proposed criteria.

### RBAC for Home IoT AC

**EGRBAC**

### ABAC for Home IoT AC

**HABAC**

1- Constructing *EGRBAC* from *HABAC*
2- Constructing *HABAC* from *EGRBAC*
3- Compare the theoretical expressive power of *EGRBAC* and *HABAC*

### Combined Models for Home IoT AC

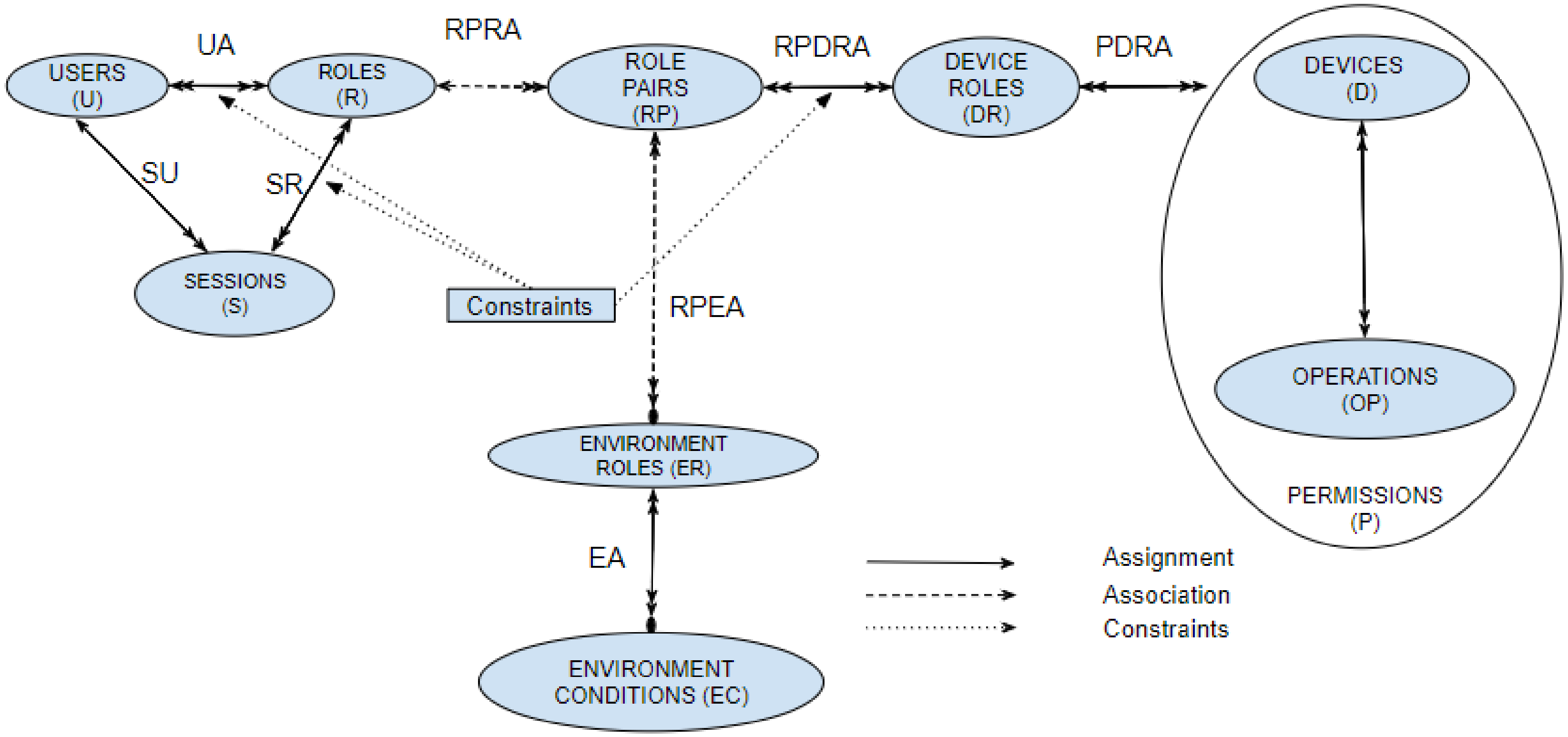
**$HyBAC_{RC}$** | **$HyBAC_{AC}$**

1- Constructing $HyBAC_{RC}$ from $HyBAC_{AC}$
2- Constructing $HyBAC_{AC}$ from $HyBAC_{RC}$
3- Compare the theoretical expressive power of $HyBAC_{RC}$ and $HyBAC_{AC}$

# Role-Based Access Control Model for Smart Home IoT (EGRBAC)

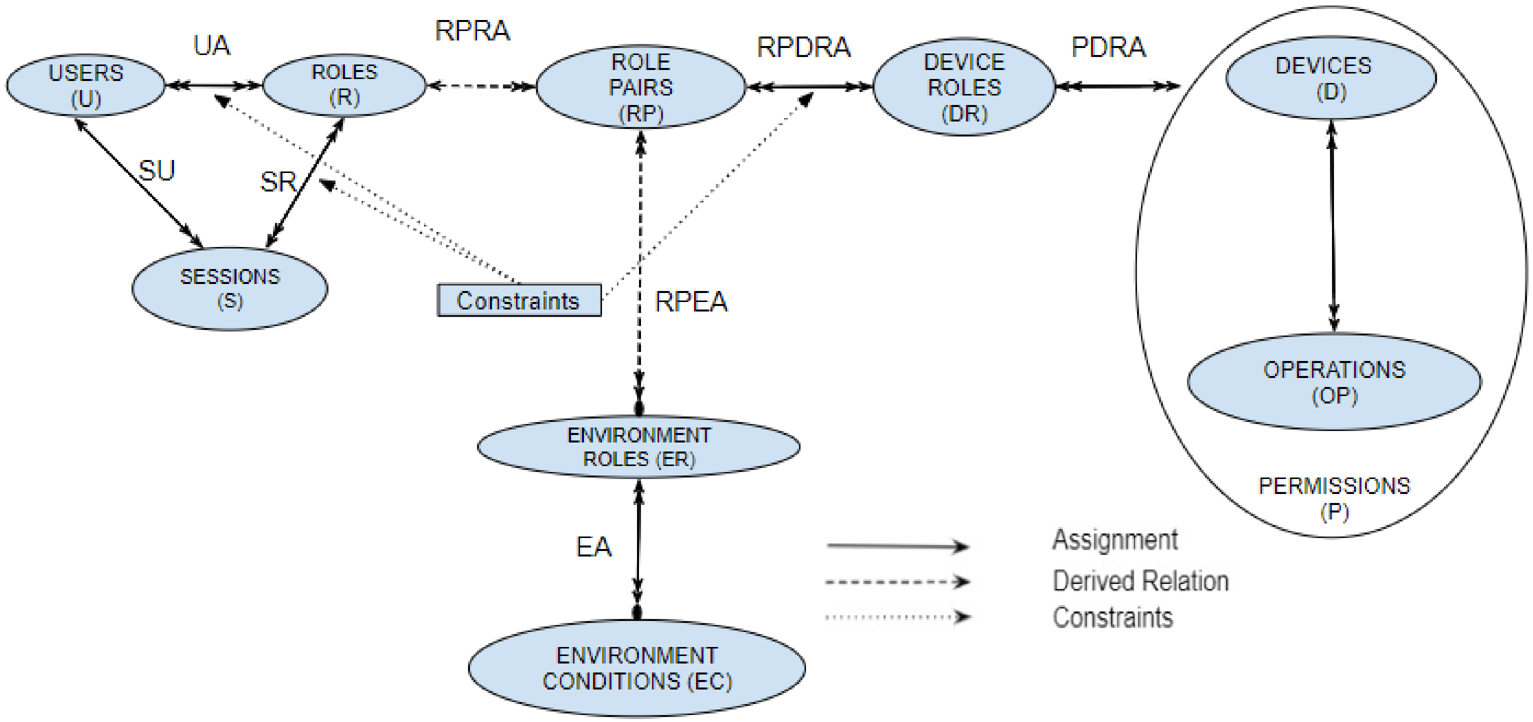
# The EGRBAC Model





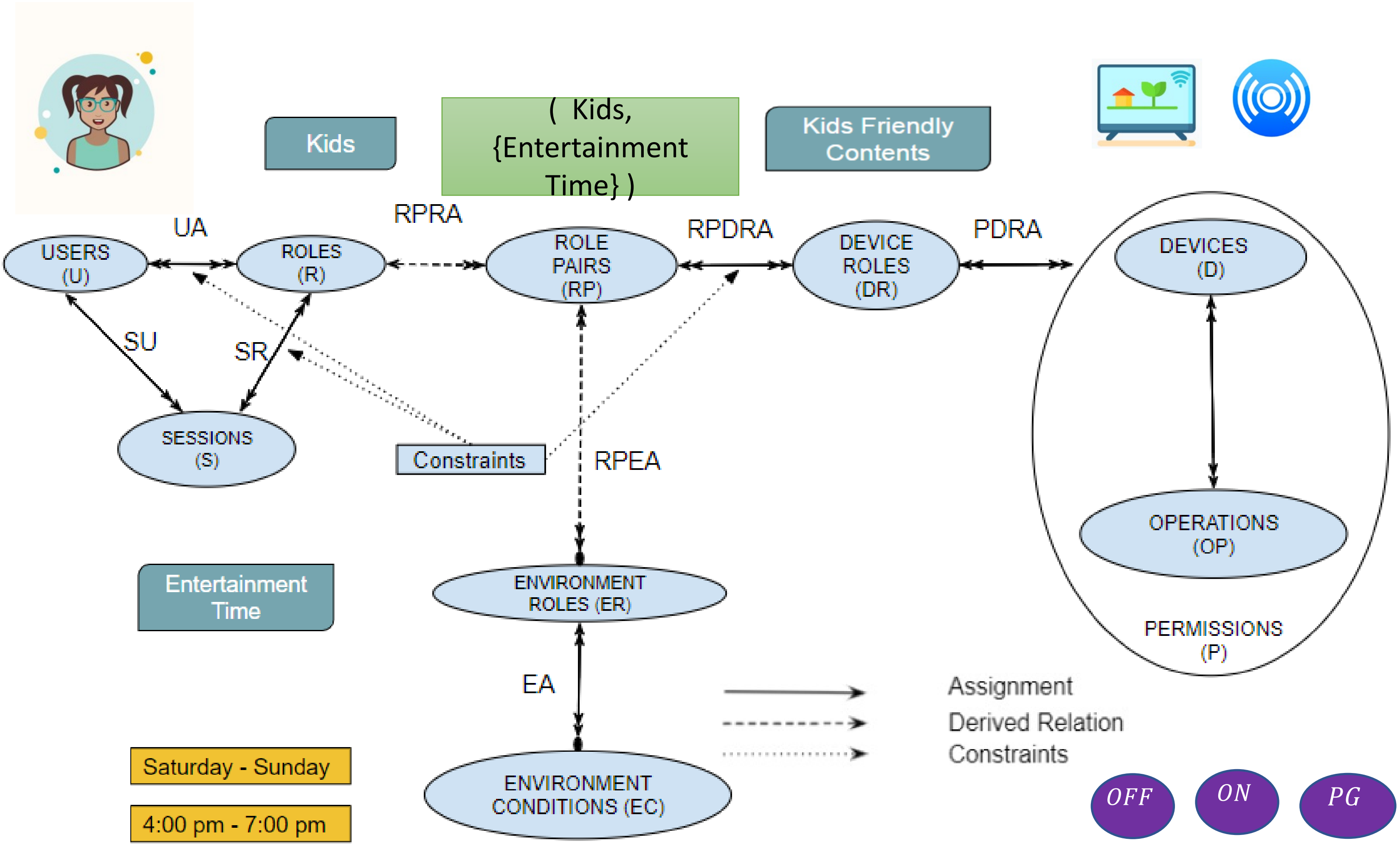
# The EGRBAC Model






- 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.

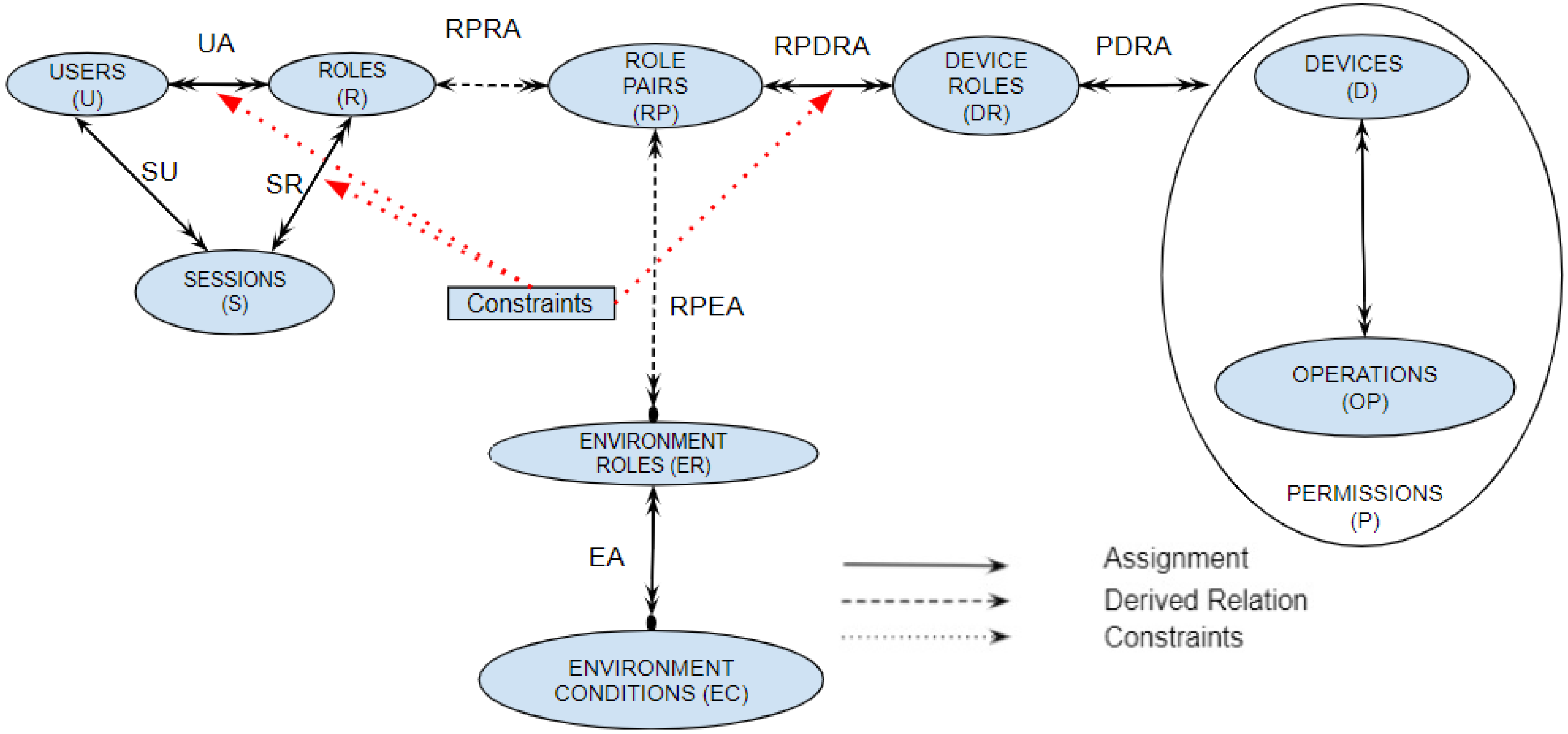
# Use Case


Kids
( Kids, {Entertainment Time} )
Kids Friendly Contents
UA
RPRA
RPDRA
PDRA
USERS (U)
ROLES (R)
ROLE PAIRS (RP)
DEVICE ROLES (DR)
DEVICES (D)
SU
SR
SESSIONS (S)
Constraints
RPEA
OPERATIONS (OP)
PERMISSIONS (P)
Entertainment Time
ENVIRONMENT ROLES (ER)
EA
Assignment
Derived Relation
Constraints
Saturday - Sunday
4:00 pm - 7:00 pm
ENVIRONMENT CONDITIONS (EC)
OFF
ON
PG

# Constraints



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

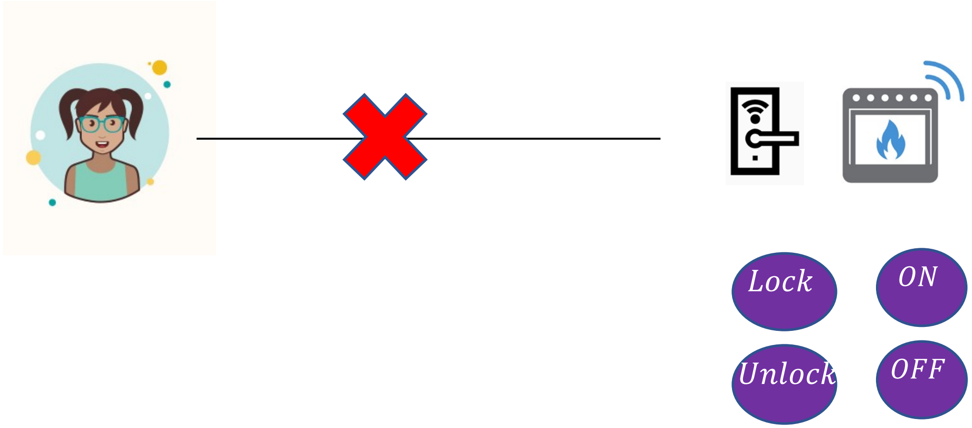


# Constraints

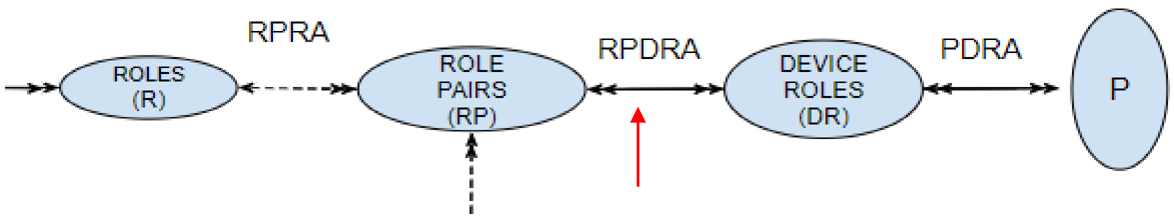


1. **Permission-role constraint:** these constraints prevent specific roles from getting access to specific permissions.

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




$(\{\ (DoorLock, Lock), (DoorLock, Unlock), (Oven, On), (Oven, OFF)\ \}, \{\ Kids\ \})$

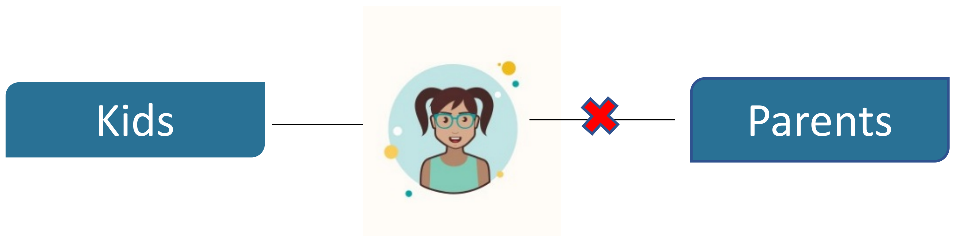


# Constraints

**2- Static separation of duty:**

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

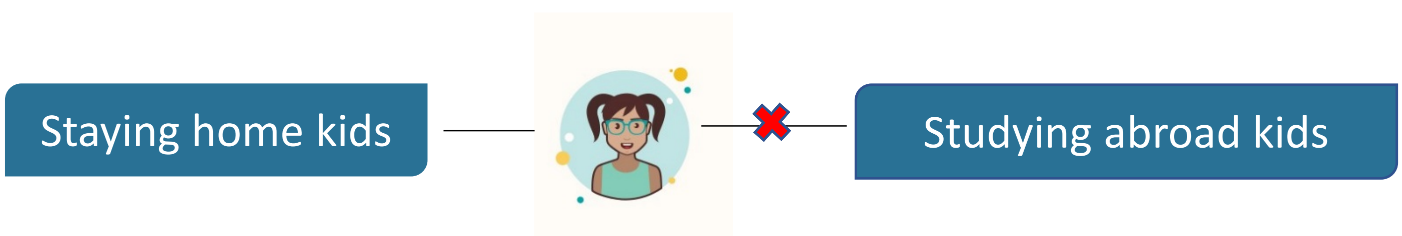
$$(Kids, \{Parents\}\ \ )$$



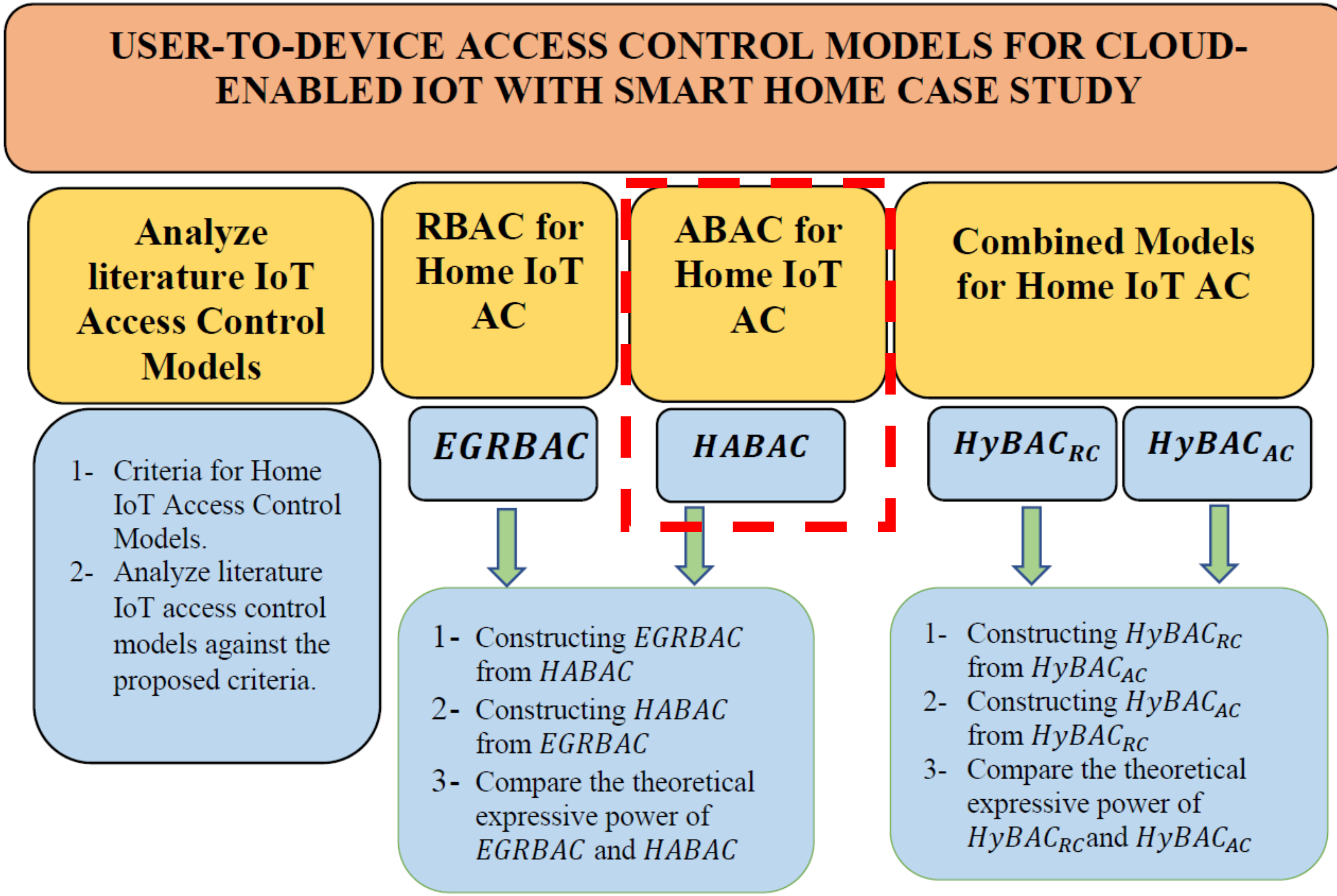

**3. Dynamic separation of duty:**

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

$$(Staying\ home\ kids, \{Studying\ abroad\ Kids\}\ \ )$$



# Summary of Contributions

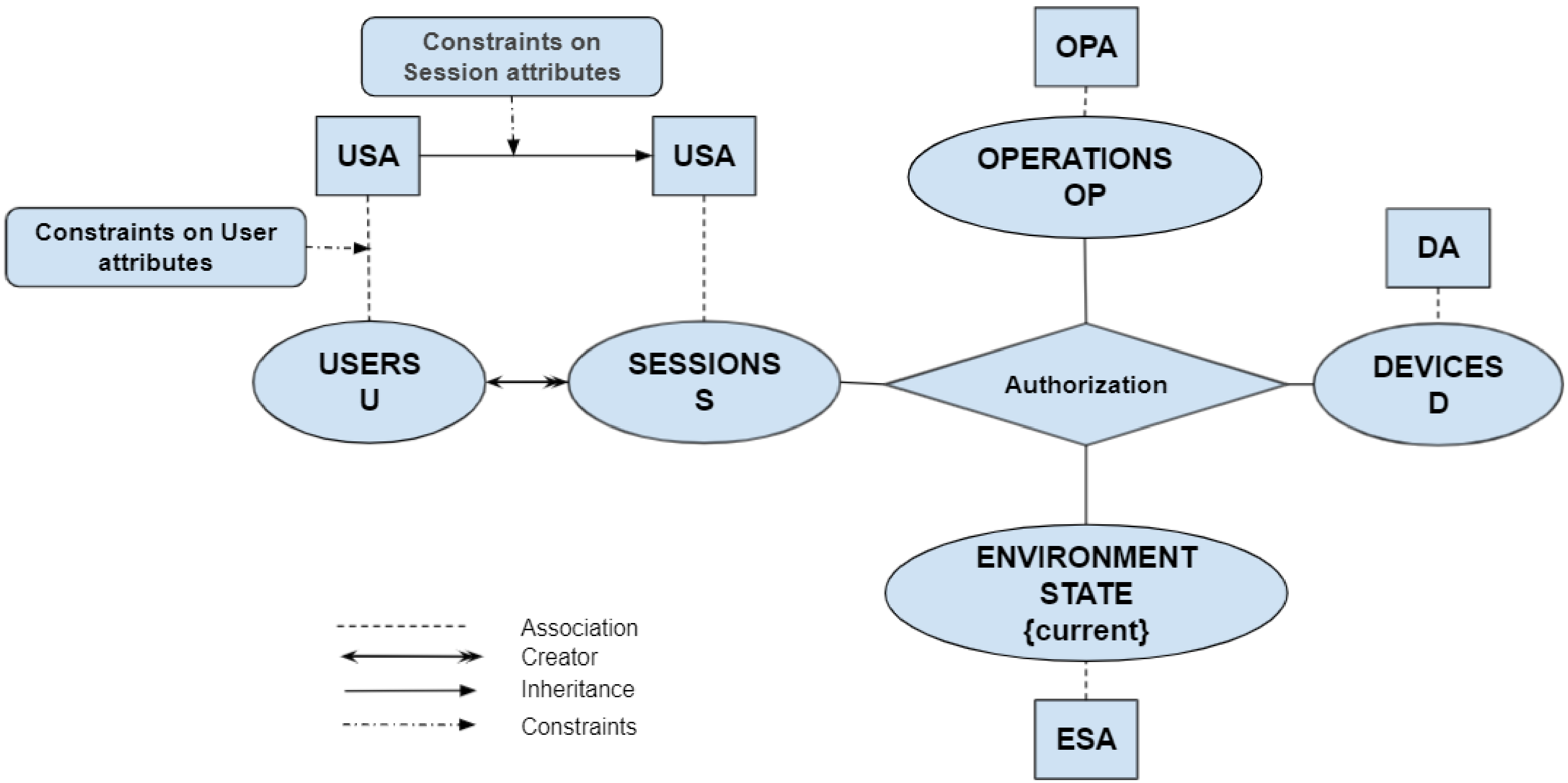


# Attribute-Based Access Control Model for Smart Home IoT (HABAC)

I·C·S
The Institute for Cyber Security

# The HABAC Model

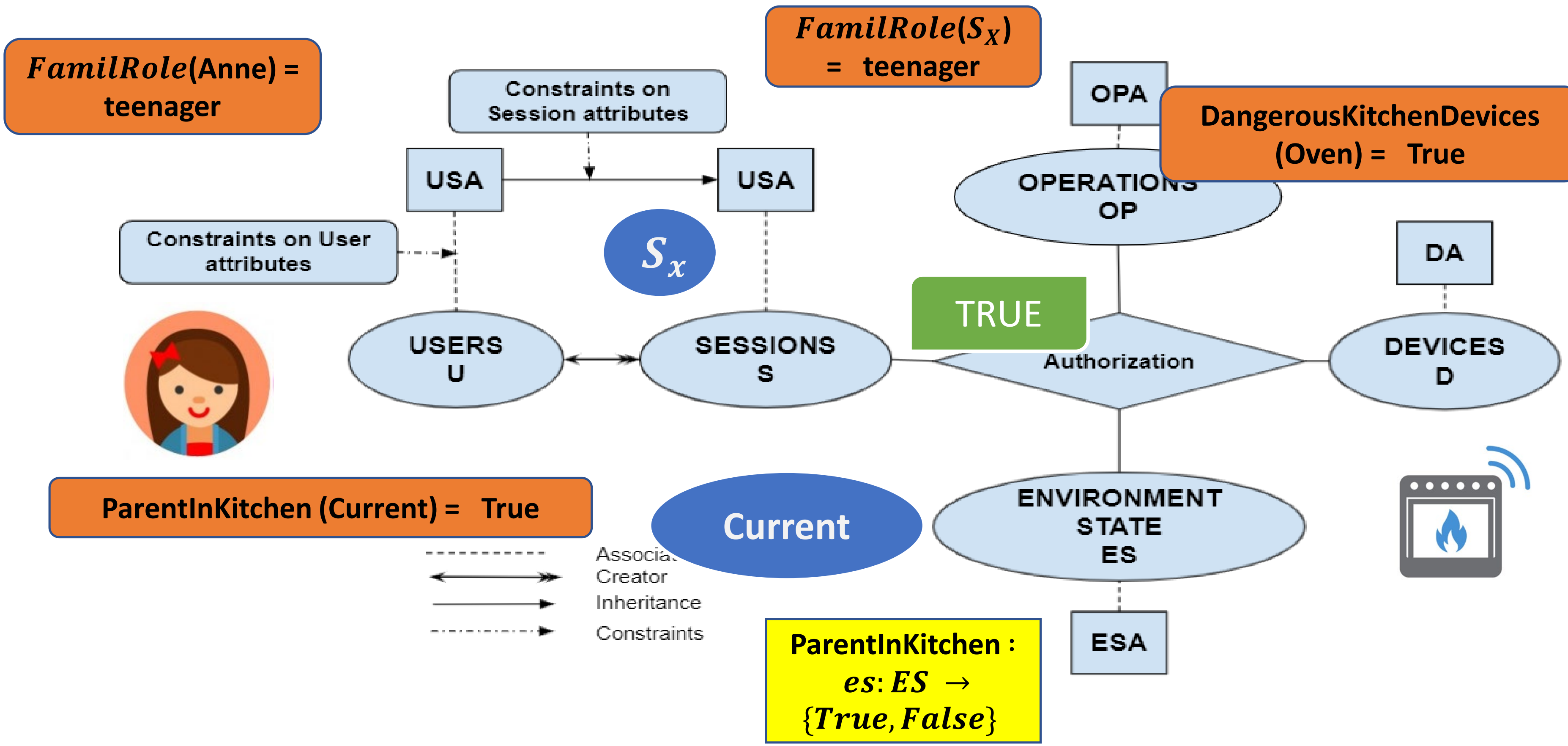
C·SPECC
Center for Security and Privacy Enhanced Cloud Computing



# Use Case

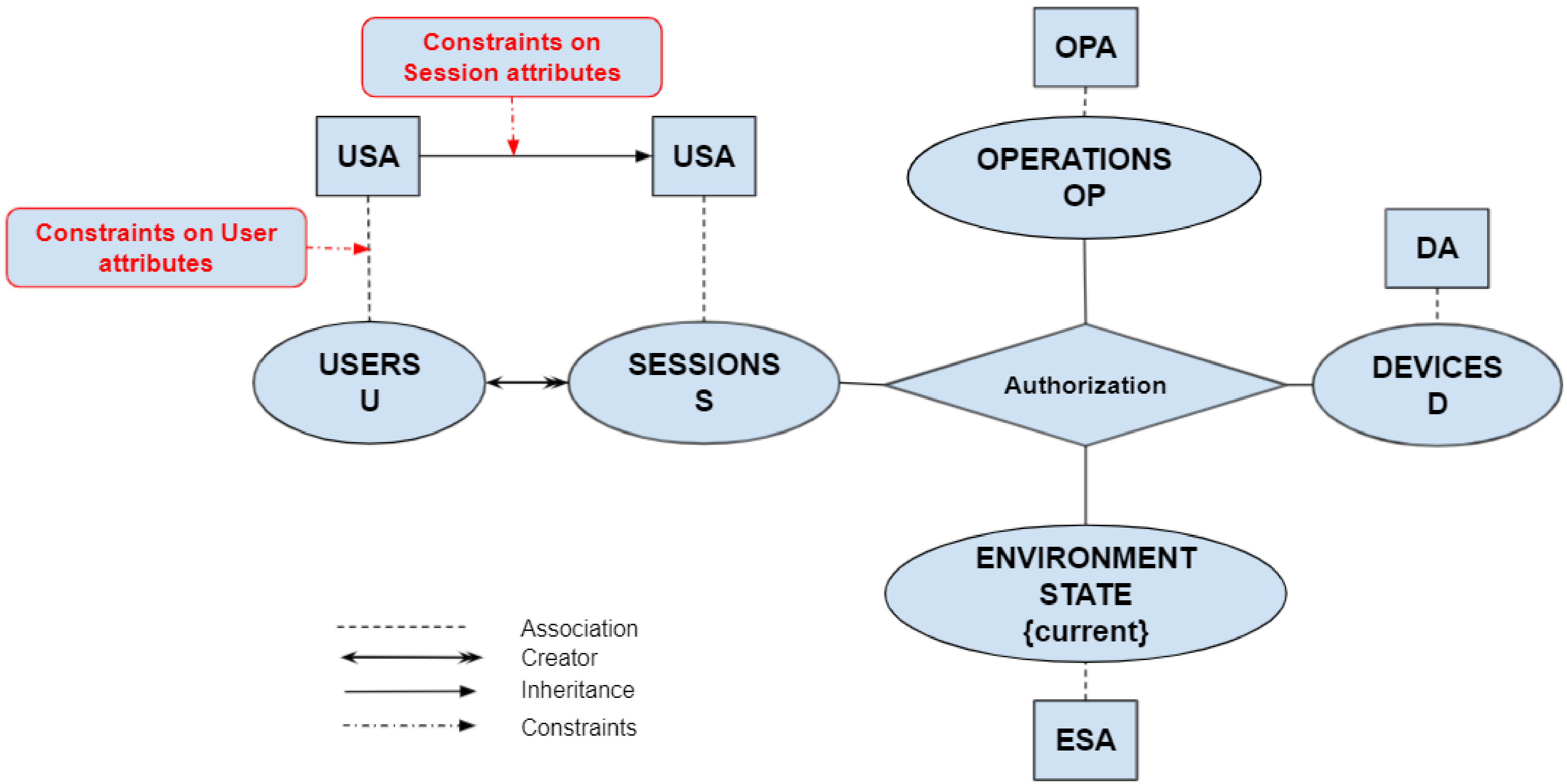


$FamilRole(s) = teenager$ ∧ DangerousKitchen Devices (d) = True ∧ ParentInKitchen (Current) = True



# The HABAC Model





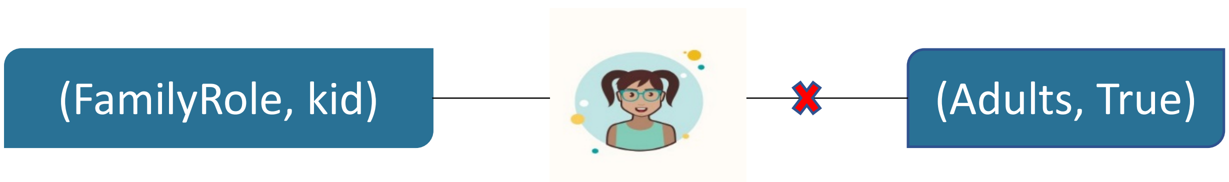
# The HABAC Model
## Constraints



1- Constraints on user attributes: these constraints enforce restrictions on user attributes.

- $\boldsymbol{UAConstraints} \subseteq \boldsymbol{UAP} \times \boldsymbol{2^{UAP}}$ . Constitute a many to many user/session attribute pair to a subset of mutually exclusive user/session attribute pairs.

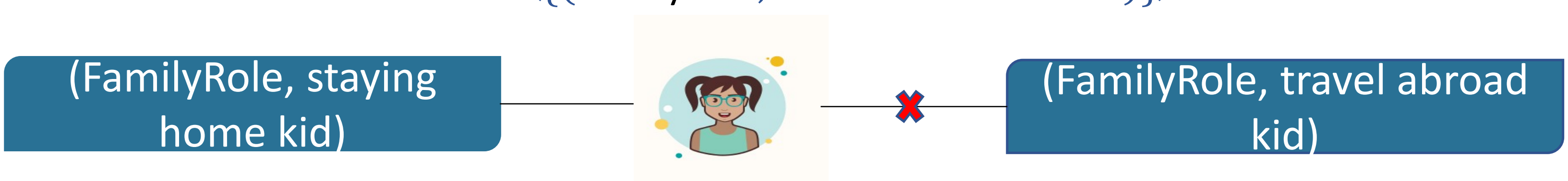
$$uac = \left((\text{FamilyRole}, kid),\ \{(\text{Adults}, True)\}\right)$$




2- Constraints on session attributes: these constraints enforce restrictions on session attributes.

- $\boldsymbol{SAConstraints} \subseteq \boldsymbol{UAP} \times \boldsymbol{2^{UAP}}$ . Constitute a many to many user/session attribute pair to a subset of mutually exclusive user/session attribute pairs.

$$sac = \begin{pmatrix} (\text{FamilyRole}, staying\ home\ kid), \\ \{(\text{FamilyRole}, travel\ abroad\ kid)\} \end{pmatrix}$$



# Summary of Contributions



## USER-TO-DEVICE ACCESS CONTROL MODELS FOR CLOUD-ENABLED IOT WITH SMART HOME CASE STUDY

### Analyze literature IoT Access Control Models

1- Criteria for Home IoT Access Control Models.
2- Analyze literature IoT access control models against the proposed criteria.

### RBAC for Home IoT AC

***EGRBAC***

### ABAC for Home IoT AC

***HABAC***

1- Constructing *EGRBAC* from *HABAC*
2- Constructing *HABAC* from *EGRBAC*
3- Compare the theoretical expressive power of *EGRBAC* and *HABAC*

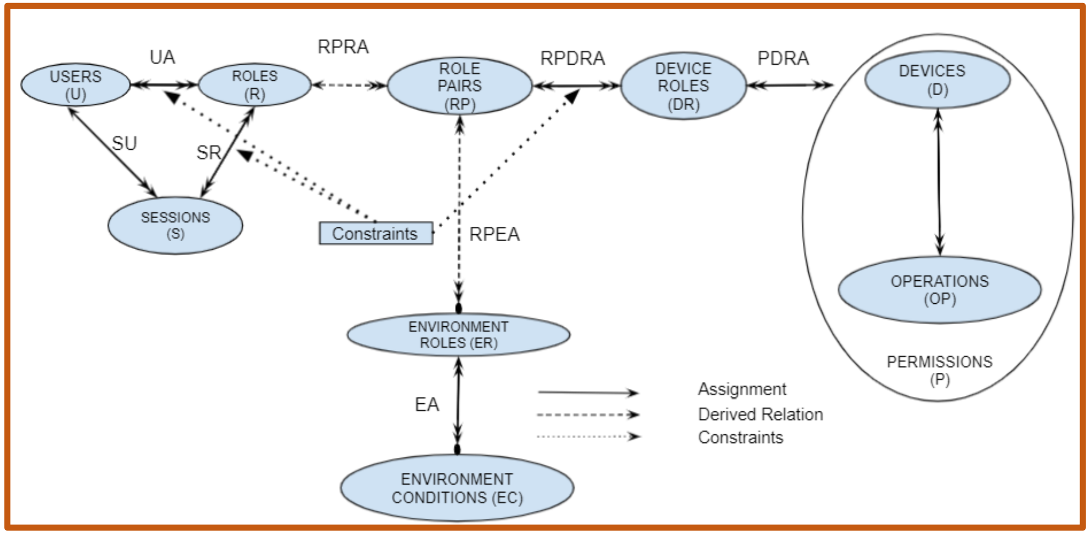
### Combined Models for Home IoT AC

$HyBAC_{RC}$ | $HyBAC_{AC}$

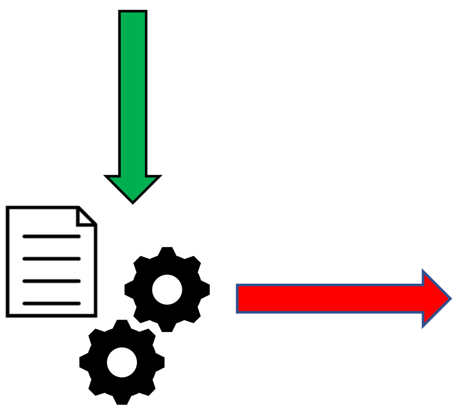
1- Constructing $HyBAC_{RC}$ from $HyBAC_{AC}$
2- Constructing $HyBAC_{AC}$ from $HyBAC_{RC}$
3- Compare the theoretical expressive power of $HyBAC_{RC}$ and $HyBAC_{AC}$

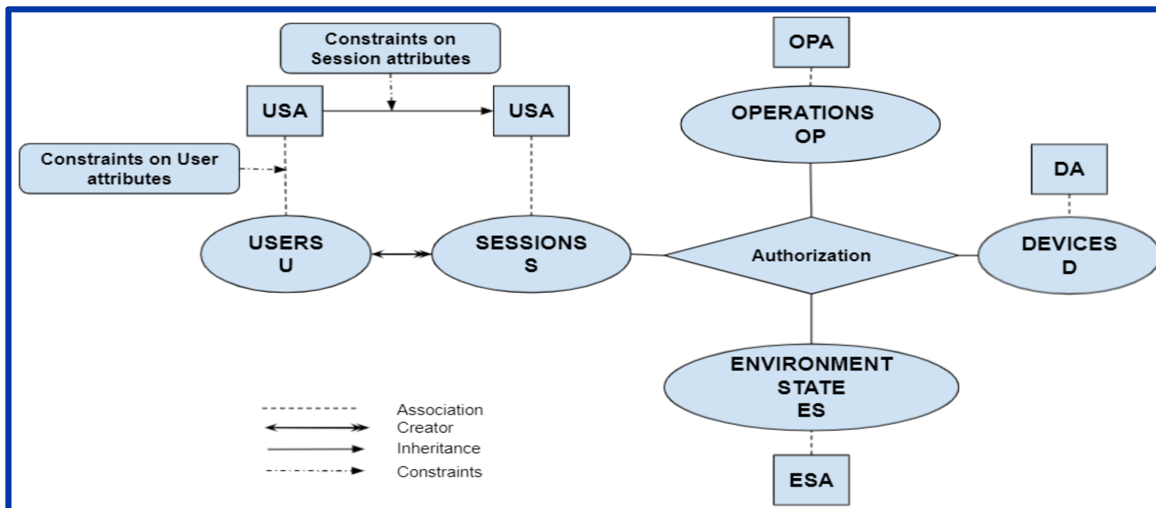
# From HABAC to EGRBAC and Vice Versa

# Constructing HABAC From EGRBAC

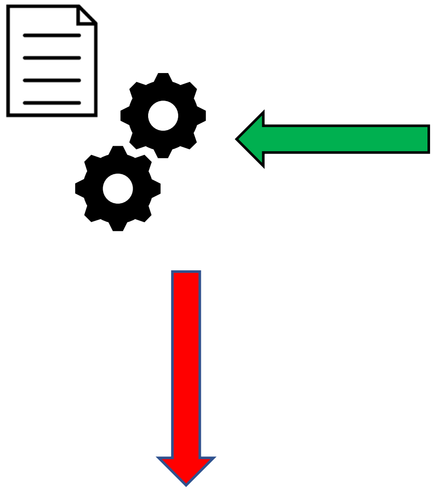


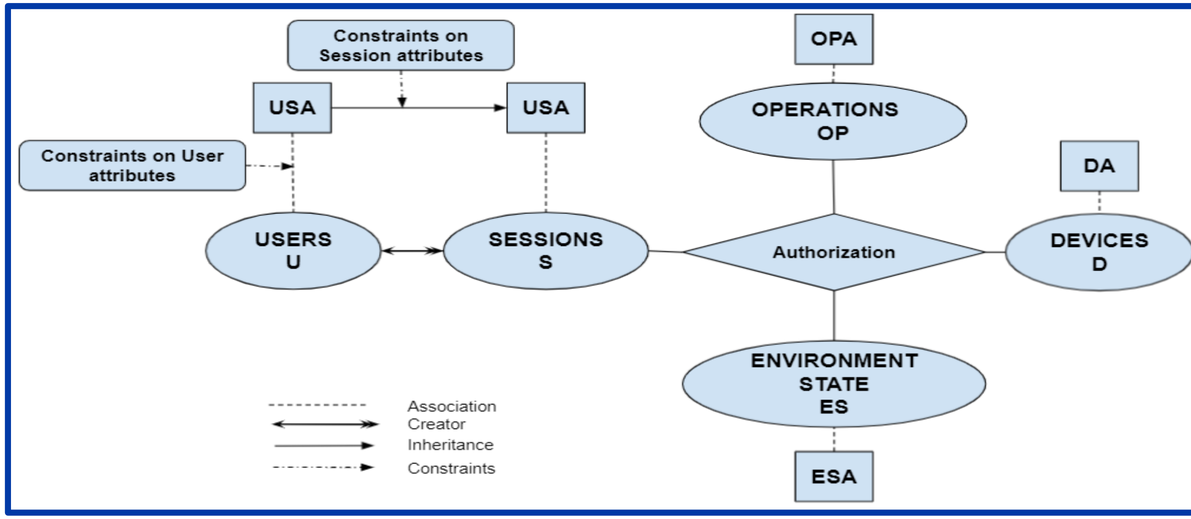

The goal is to construct HABAC elements (U, UA, SA, ES, ESA, D, DA, OP, OPA) and the authorization policy function from EGRBAC policy in such a way that the authorizations are the same as those under EGRBAC.

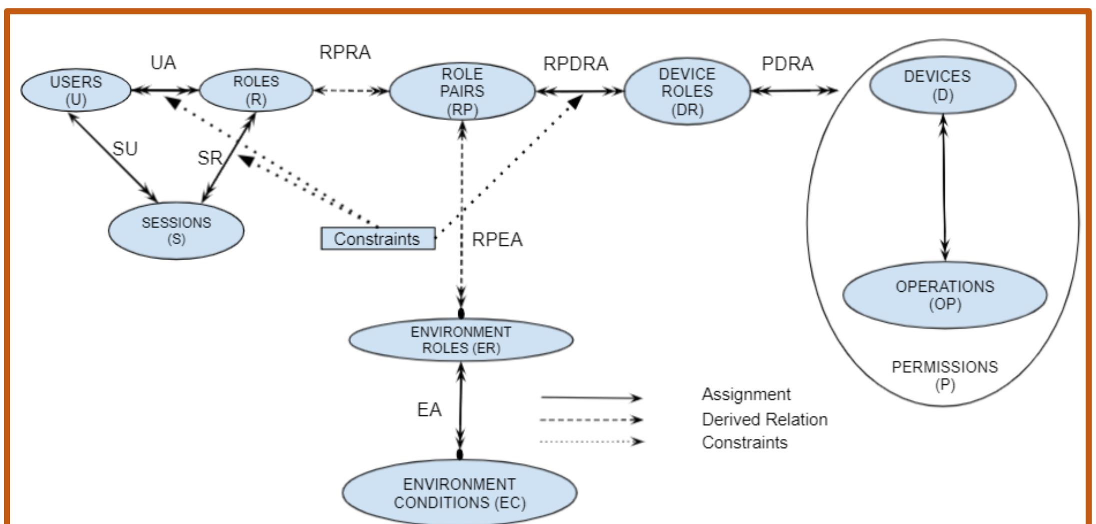




# Constructing EGRBAC From HABAC



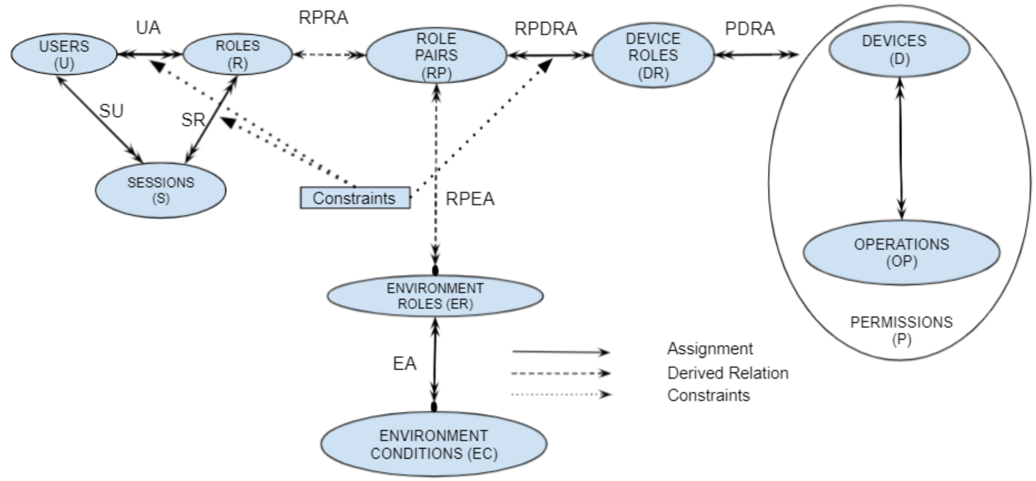


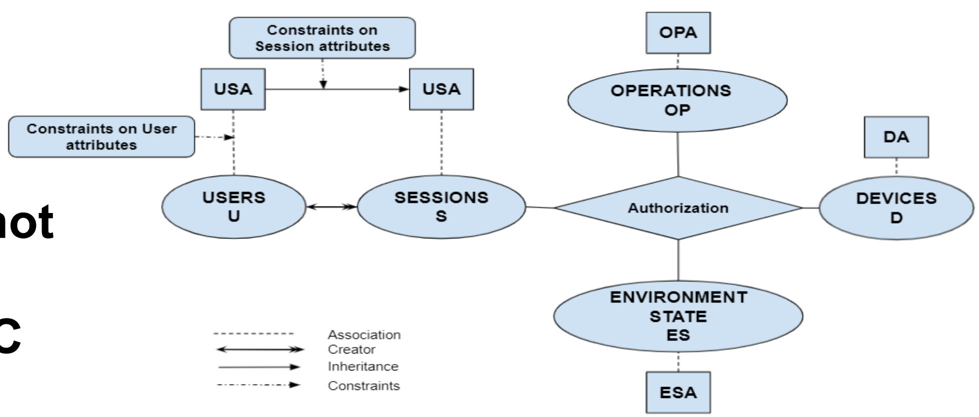




The goal is to construct EGRBAC elements (U, R, EC, ER, RP, D, OP, P, DR), assignments (UA, EA, PDRA, RPDRA), and associations (RPRA, RPEA) from HABAC policies in such a way that the authorizations are the same as those under HABAC.

# HABAC Vs EGRBAC





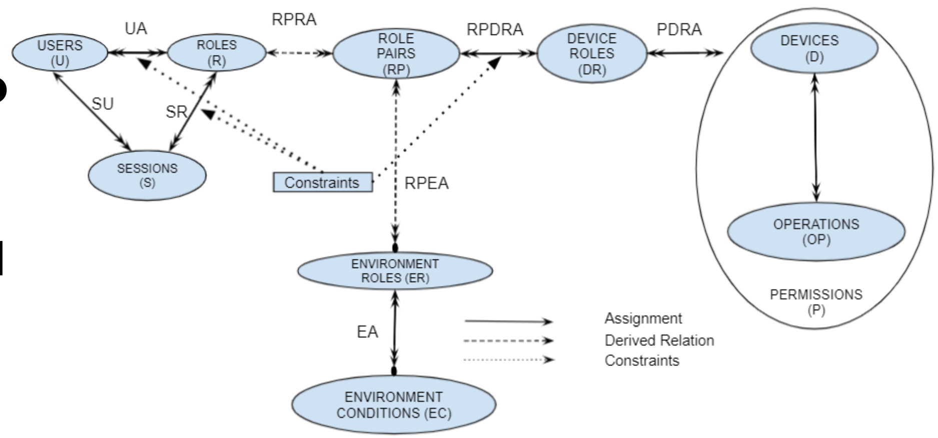




**1- In HABAC we can not create something equivalent to EGRBAC PRConstraints.**

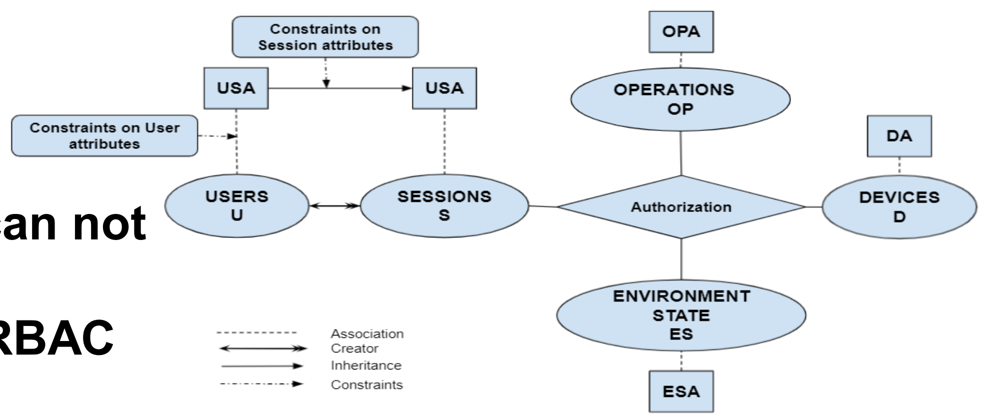
# HABAC Vs EGRBAC



**2- In EGRBAC it is easy to define who has what permissions, and who is not allowed to have a future access to specific permissions.**



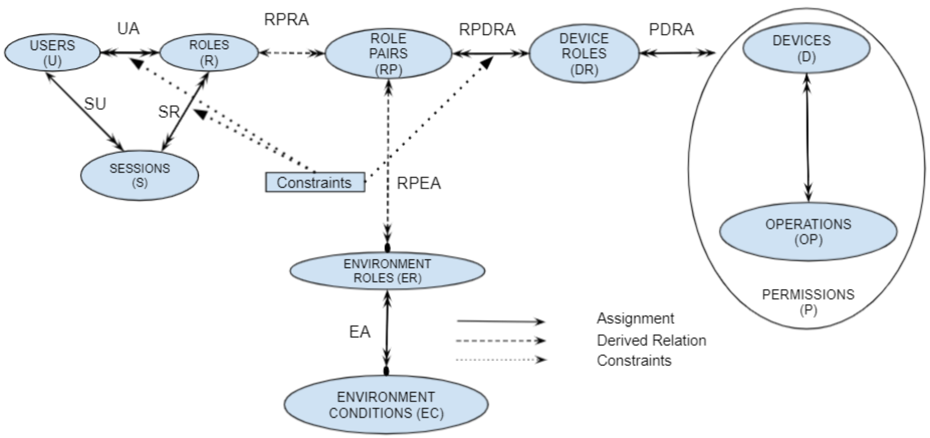

**1- In HABAC we can not create something equivalent to EGRBAC PRConstraints.**



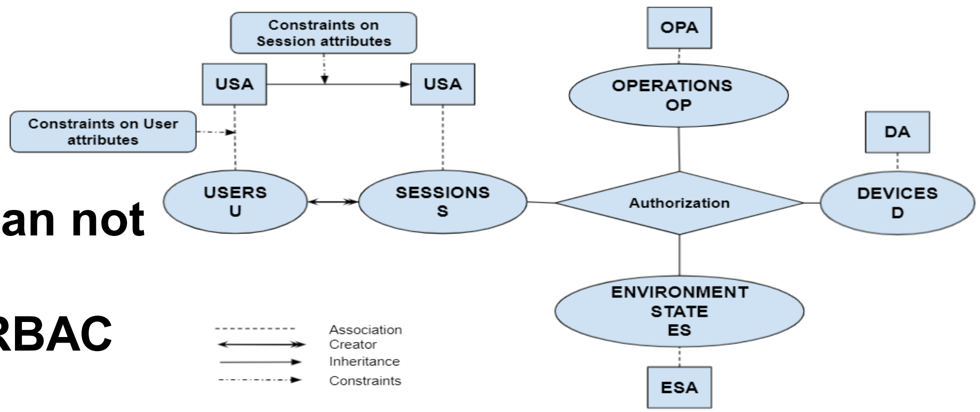
# HABAC Vs EGRBAC



**2- In EGRBAC it is easy to define who has what permissions, and who is not allowed to have a future access to specific permissions.**




**3- in EGRBAC, we can't handle HABAC policies that involve users, devices and operations dynamic attributes. Such handling may lead to role explosion in EGRBAC.**




**1- In HABAC we can not create something equivalent to EGRBAC PRConstraints.**

# Summary of Contributions



## USER-TO-DEVICE ACCESS CONTROL MODELS FOR CLOUD-ENABLED IOT WITH SMART HOME CASE STUDY

**Analyze literature IoT Access Control Models**

1- Criteria for Home IoT Access Control Models.
2- Analyze literature IoT access control models against the proposed criteria.

**RBAC for Home IoT AC**

***EGRBAC***

**ABAC for Home IoT AC**

***HABAC***

1- Constructing *EGRBAC* from *HABAC*
2- Constructing *HABAC* from *EGRBAC*
3- Compare the theoretical expressive power of *EGRBAC* and *HABAC*

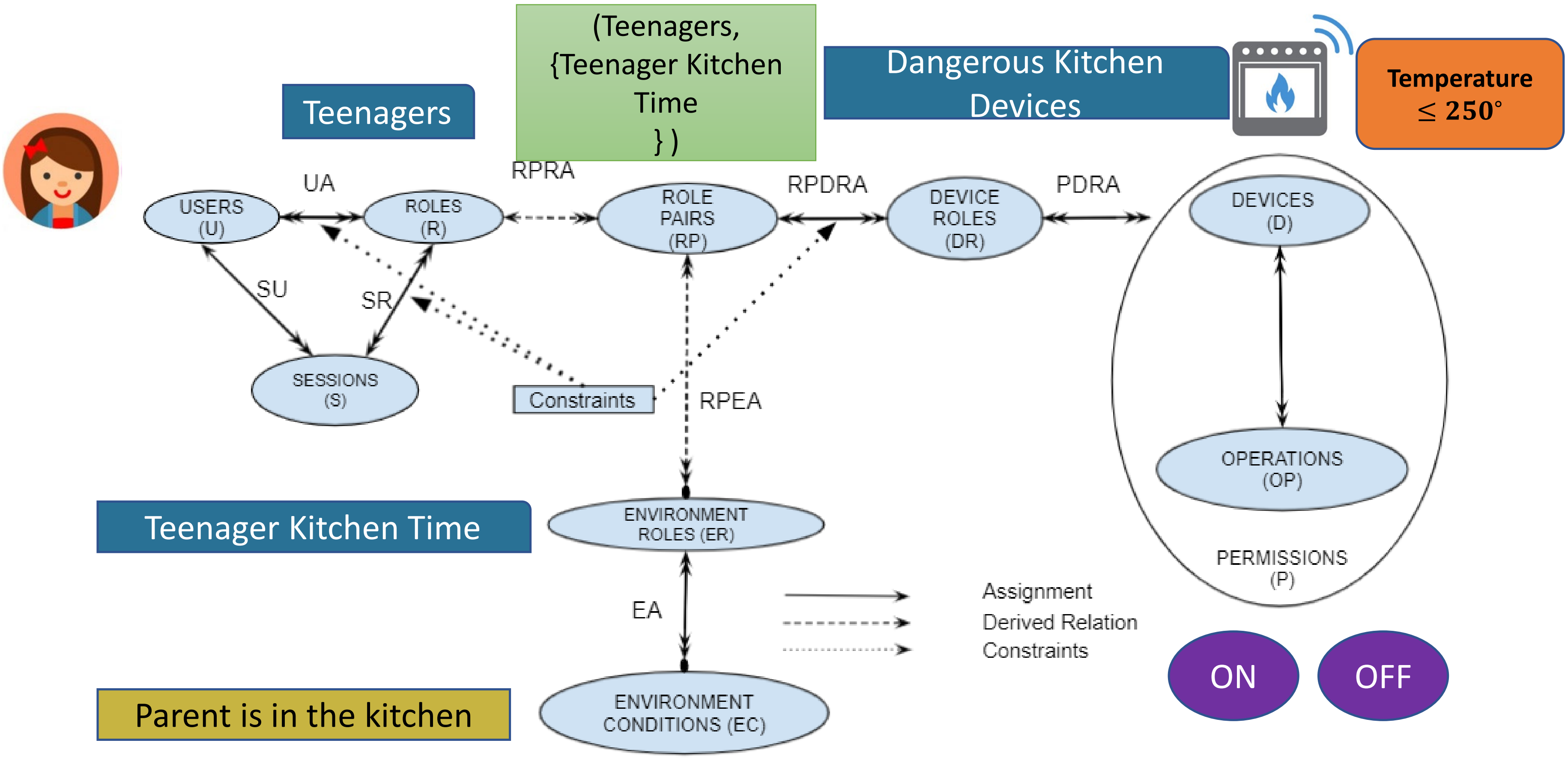
**Combined Models for Home IoT AC**

***$HyBAC_{RC}$*** ***$HyBAC_{AC}$***

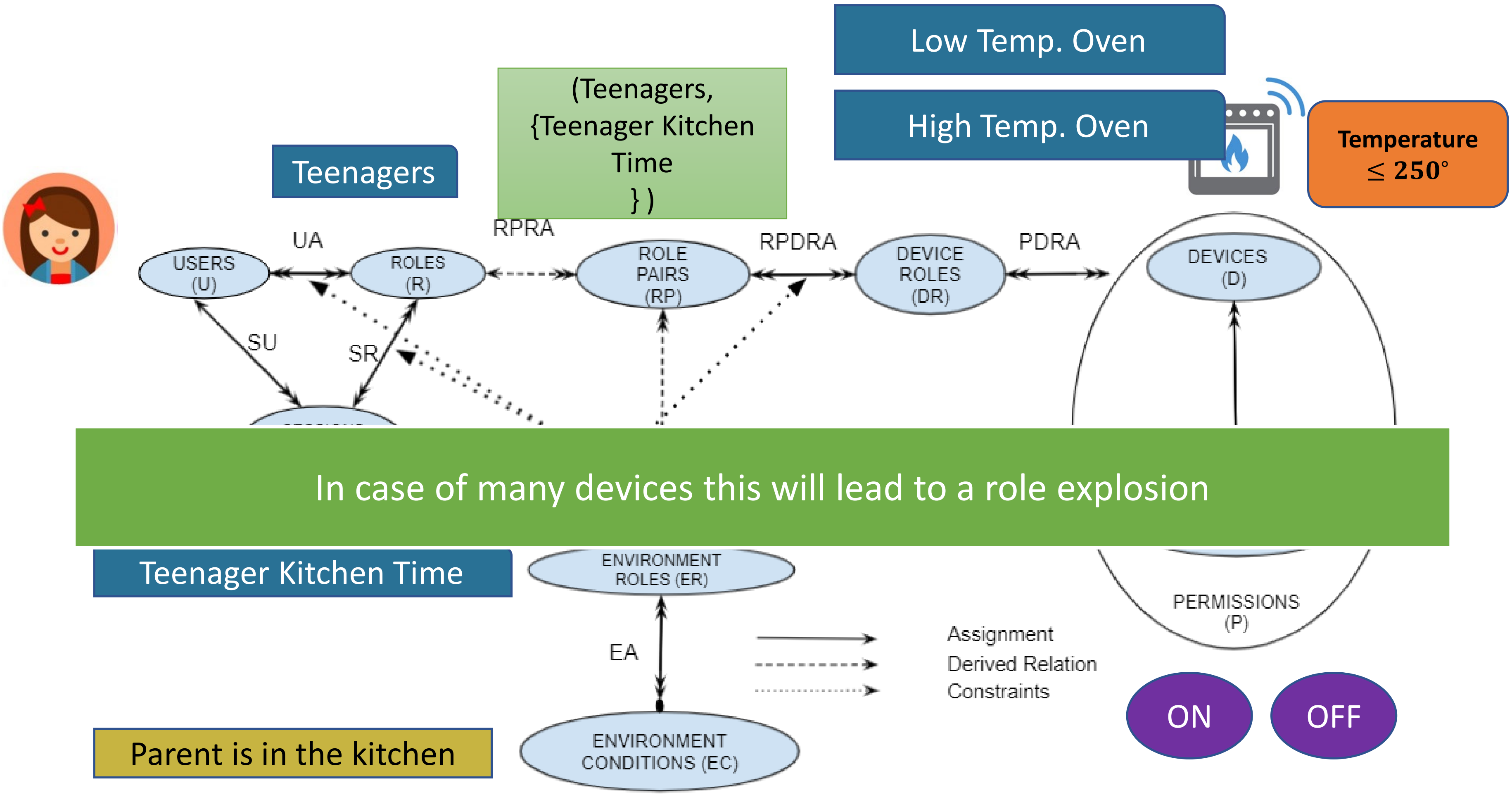
1- Constructing $HyBAC_{RC}$ from $HyBAC_{AC}$
2- Constructing $HyBAC_{AC}$ from $HyBAC_{RC}$
3- Compare the theoretical expressive power of $HyBAC_{RC}$ and $HyBAC_{AC}$

# Hybrid Role-Centric Access Control Model for Smart Home IoT ($HyBAC_{RC}$)

# Motivation


Teenagers
(Teenagers, {Teenager Kitchen Time } )
Dangerous Kitchen Devices
Temperature ≤ 250°
USERS (U)
UA
ROLES (R)
RPRA
ROLE PAIRS (RP)
RPDRA
DEVICE ROLES (DR)
PDRA
DEVICES (D)
SU
SR
SESSIONS (S)
Constraints
RPEA
OPERATIONS (OP)
PERMISSIONS (P)
Teenager Kitchen Time
ENVIRONMENT ROLES (ER)
EA
Assignment
Derived Relation
Constraints
ON
OFF
Parent is in the kitchen
ENVIRONMENT CONDITIONS (EC)

# Motivation


Low Temp. Oven
High Temp. Oven
(Teenagers, {Teenager Kitchen Time } )
Teenagers
Temperature ≤ 250°
UA
RPRA
RPDRA
PDRA
USERS (U)
ROLES (R)
ROLE PAIRS (RP)
DEVICE ROLES (DR)
DEVICES (D)
SU
SR
In case of many devices this will lead to a role explosion
Teenager Kitchen Time
ENVIRONMENT ROLES (ER)
PERMISSIONS (P)
EA
Assignment
Derived Relation
Constraints
ON
OFF
Parent is in the kitchen
ENVIRONMENT CONDITIONS (EC)

# Motivation

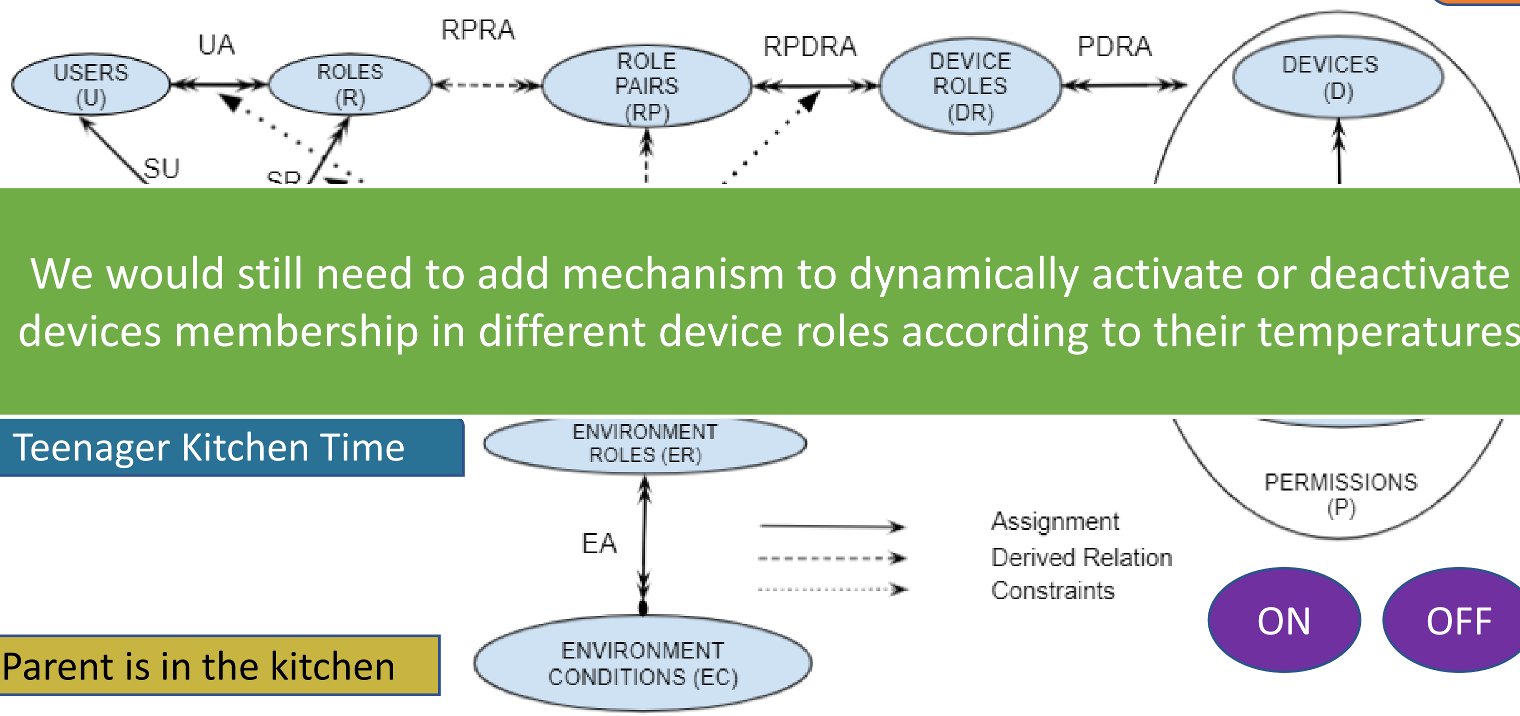


Low Temp. Dangerous Kitchen Devices

High Temp. Dangerous Kitchen Devices

Teenagers

Temperature ≤ 250°




We would still need to add mechanism to dynamically activate or deactivate devices membership in different device roles according to their temperatures

Teenager Kitchen Time

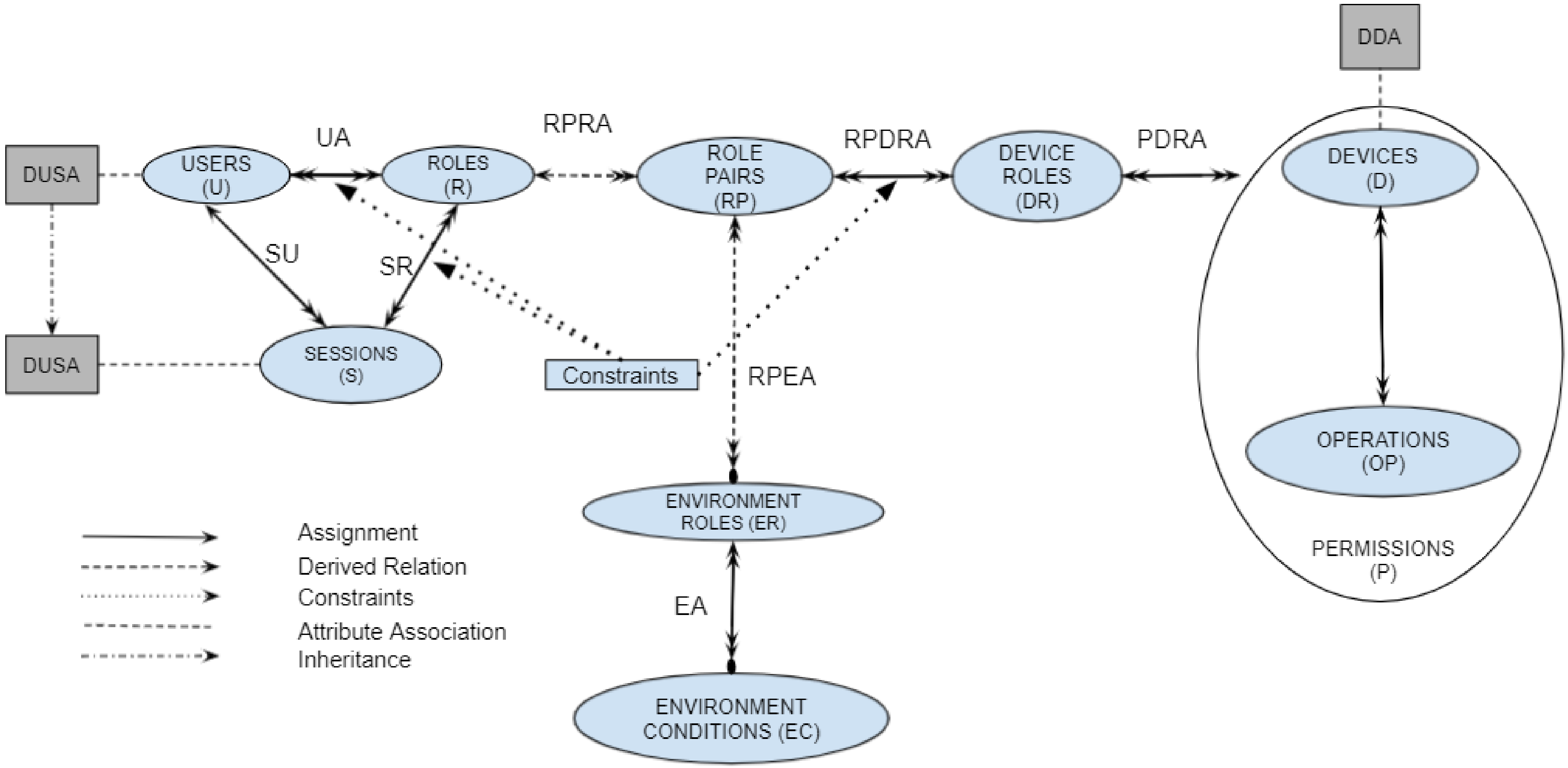
Parent is in the kitchen

ON

OFF

# $HyBAC_{RC}$




DDA
RPRA
UA
RPDRA
PDRA
DUSA
USERS
(U)
ROLES
(R)
ROLE
PAIRS
(RP)
DEVICE
ROLES
(DR)
DEVICES
(D)
SU
SR
DUSA
SESSIONS
(S)
Constraints
RPEA
OPERATIONS
(OP)
ENVIRONMENT
ROLES (ER)
Assignment
Derived Relation
Constraints
Attribute Association
Inheritance
EA
PERMISSIONS
(P)
ENVIRONMENT
CONDITIONS (EC)

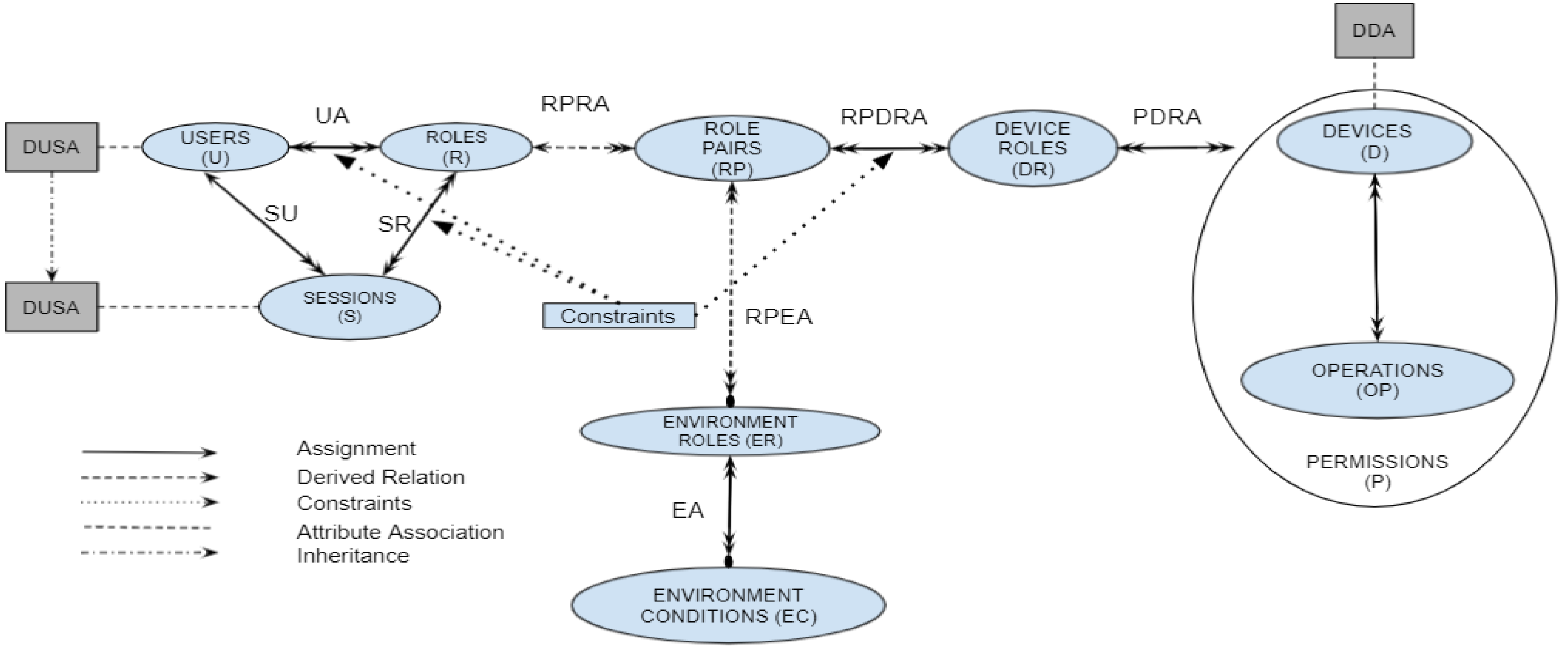
# $HyBAC_{RC}$



The check access predicate will evaluate to True if and only if:

a. The requirements of role membership and role activation specified by EGRBAC are true.

b. The authorization function evaluates to True.



I·C·S The Institute for Cyber Security

# Summary of Contributions

C·SPECC Center for Security and Privacy Enhanced Cloud Computing

## USER-TO-DEVICE ACCESS CONTROL MODELS FOR CLOUD-ENABLED IOT WITH SMART HOME CASE STUDY

### Analyze literature IoT Access Control Models

1- Criteria for Home IoT Access Control Models.
2- Analyze literature IoT access control models against the proposed criteria.

### RBAC for Home IoT AC

***EGRBAC***

### ABAC for Home IoT AC

***HABAC***

1- Constructing *EGRBAC* from *HABAC*
2- Constructing *HABAC* from *EGRBAC*
3- Compare the theoretical expressive power of *EGRBAC* and *HABAC*

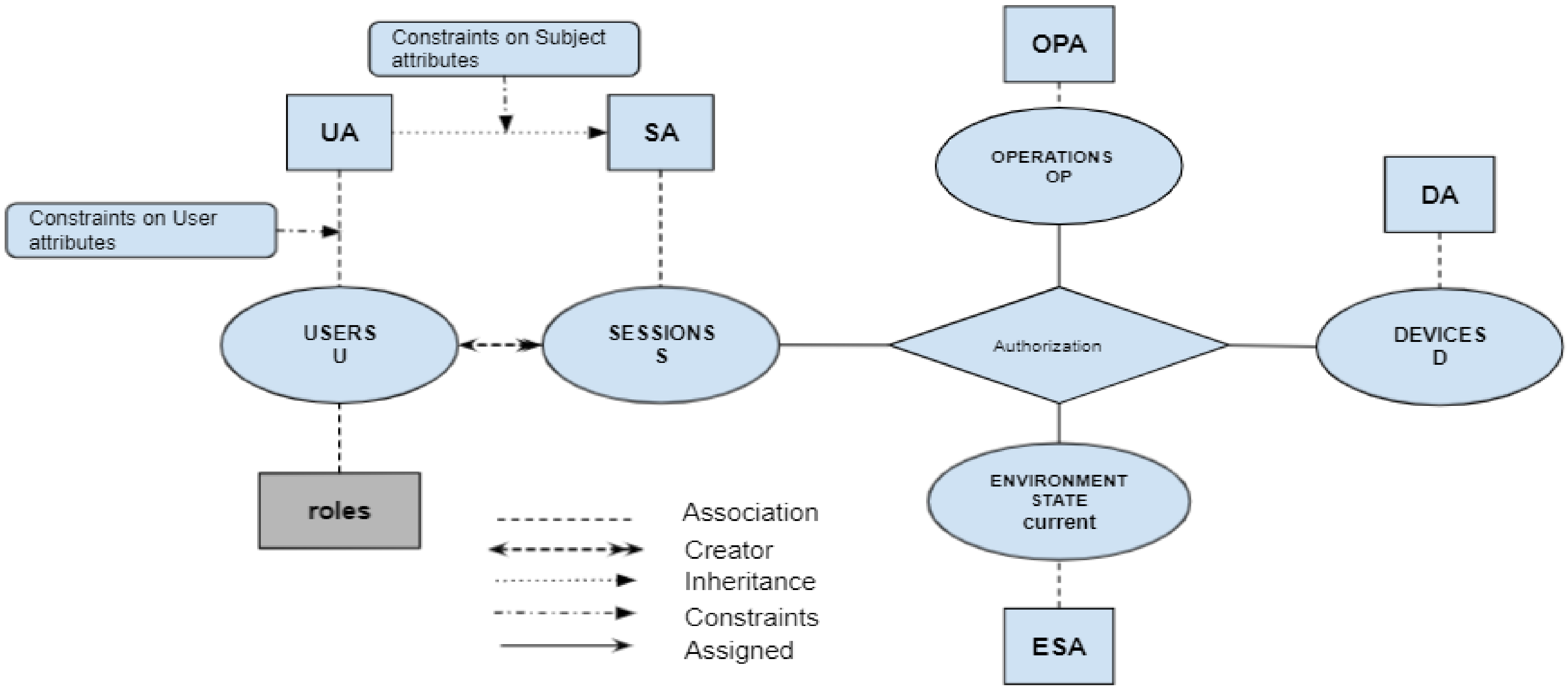
### Combined Models for Home IoT AC

$HyBAC_{RC}$ | $HyBAC_{AC}$

1- Constructing $HyBAC_{RC}$ from $HyBAC_{AC}$
2- Constructing $HyBAC_{AC}$ from $HyBAC_{RC}$
3- Compare the theoretical expressive power of $HyBAC_{RC}$ and $HyBAC_{AC}$

# Hybrid Attribute-Centric Access Control Model for Smart Home IoT ($HyBAC_{AC}$)

# $HyBAC_{AC}$




- The function **roles** (aka anti-roles) maps each user to a subset of roles.
- $\boldsymbol{PR\ Constraints} \subseteq 2^{P} \times 2^{R}$ constitute a many to many subset of permissions to subset of roles relation.

# $HyBAC_{AC}$

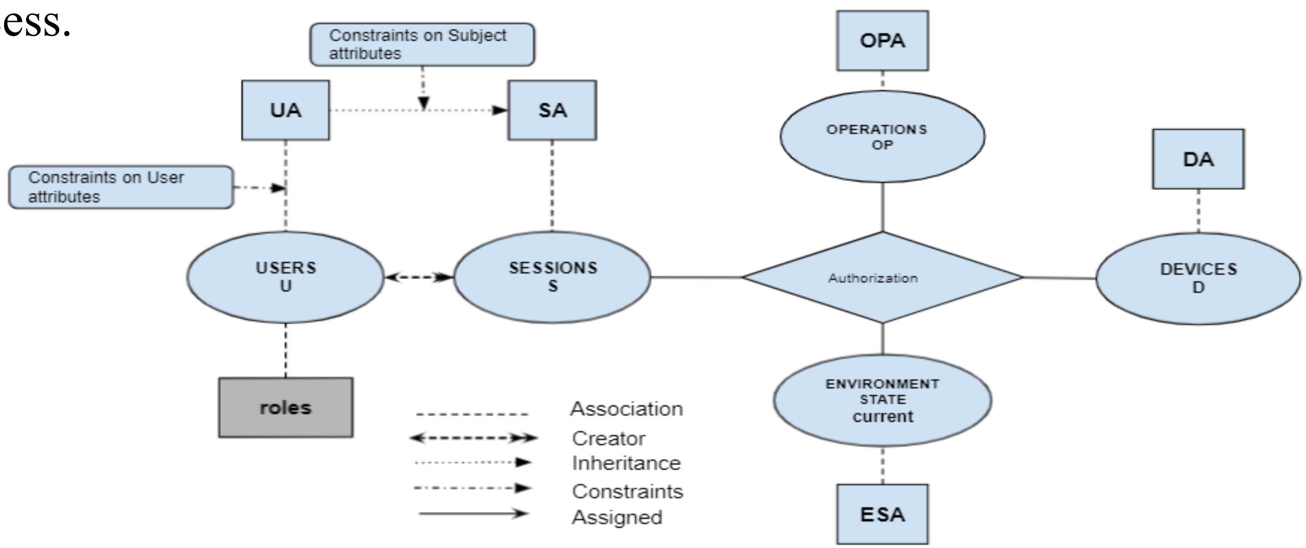


The check access predicate will evaluate to True if and only if:

a. The requested operation is assigned to the requested device by the device manufacturer.

b. The authorization function evaluates to True.

c. There is no permission role constraint in the set of permission role constraints that prevent this access.



# Summary of Contributions



## USER-TO-DEVICE ACCESS CONTROL MODELS FOR CLOUD-ENABLED IOT WITH SMART HOME CASE STUDY

### Analyze literature IoT Access Control Models

1- Criteria for Home IoT Access Control Models.
2- Analyze literature IoT access control models against the proposed criteria.

### RBAC for Home IoT AC

***EGRBAC***

### ABAC for Home IoT AC

***HABAC***

1- Constructing *EGRBAC* from *HABAC*
2- Constructing *HABAC* from *EGRBAC*
3- Compare the theoretical expressive power of *EGRBAC* and *HABAC*

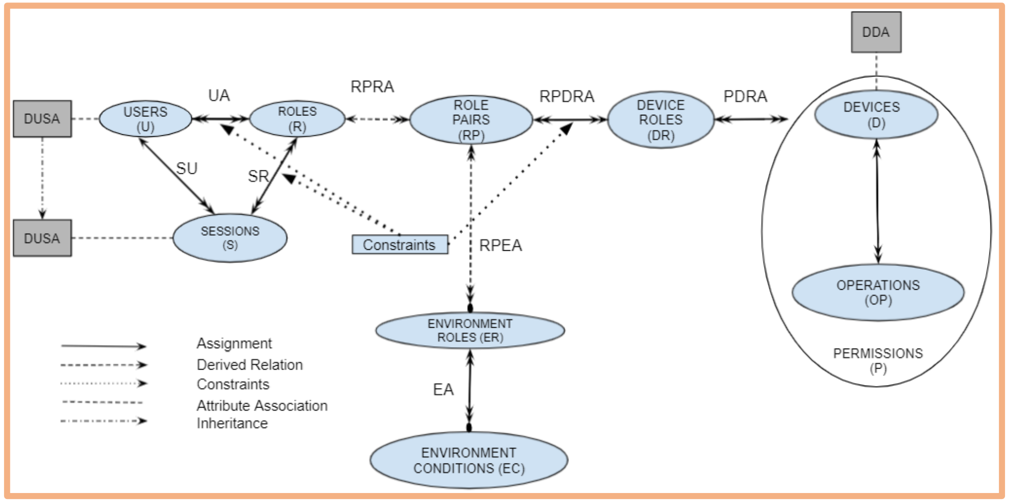
### Combined Models for Home IoT AC

$HyBAC_{RC}$ $HyBAC_{AC}$

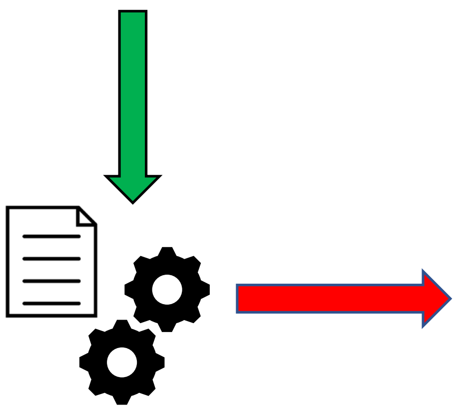
1- Constructing $HyBAC_{RC}$ from $HyBAC_{AC}$
2- Constructing $HyBAC_{AC}$ from $HyBAC_{RC}$
3- Compare the theoretical expressive power of $HyBAC_{RC}$ and $HyBAC_{AC}$

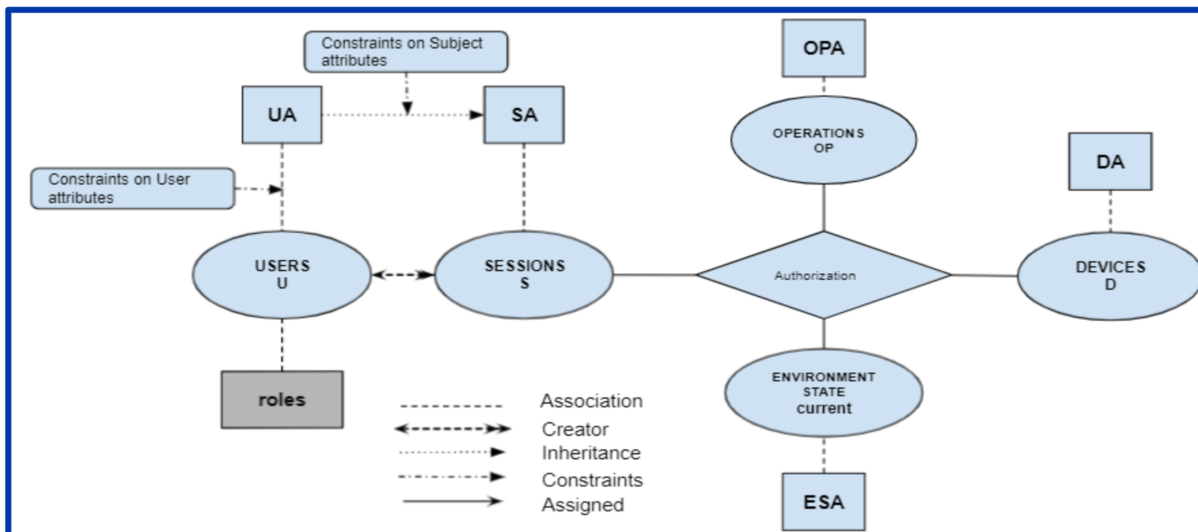
# From $HyBAC_{RC}$ to $HyBAC_{AC}$ and Vice Versa

# Constructing $HyBAC_{AC}$ From $HyBAC_{RC}$

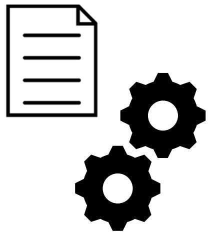


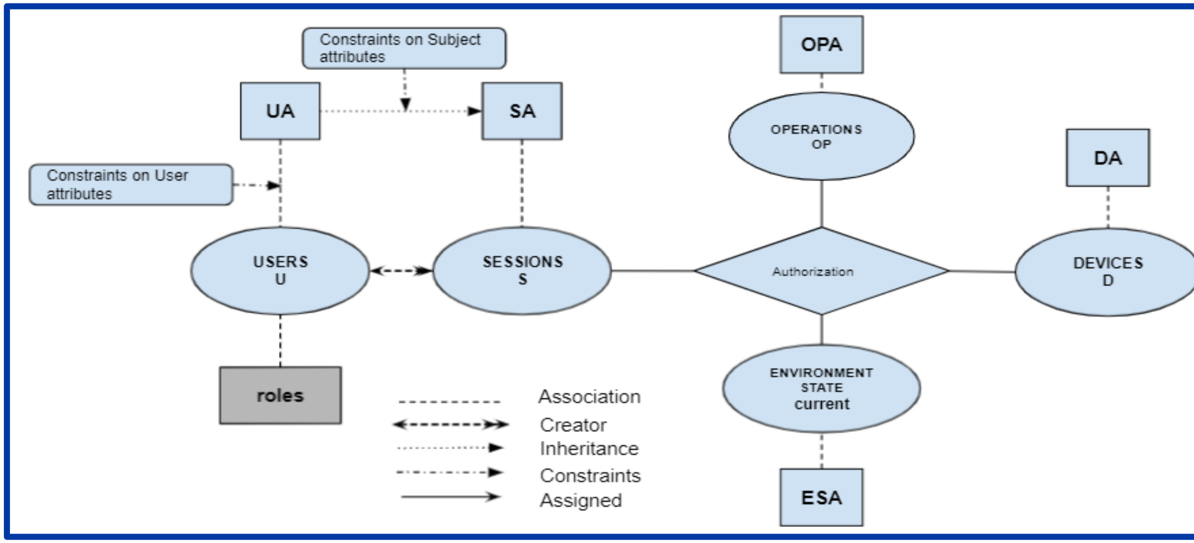

The goal is to construct $HyBAC_{AC}$ elements and the attribute authorization function configuration from $HyBAC_{RC}$ configuration in such a way that the authorizations are the same as those under $HyBAC_{RC}$.

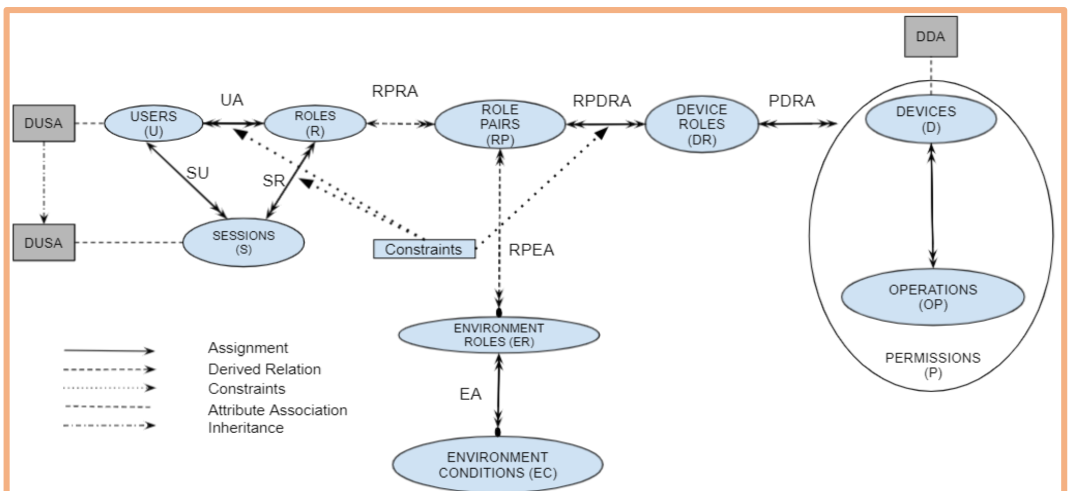




# Constructing $HyBAC_{RC}$ From $HyBAC_{AC}$






The goal is to construct $HyBAC_{RC}$ elements and the attribute authorization function configuration from $HyBAC_{AC}$ configuration in such a way that the authorizations are the same as those under $HyBAC_{AC}$.

# $HyBAC_{\mathrm{RC}}$ Vs $HyBAC_{AC}$



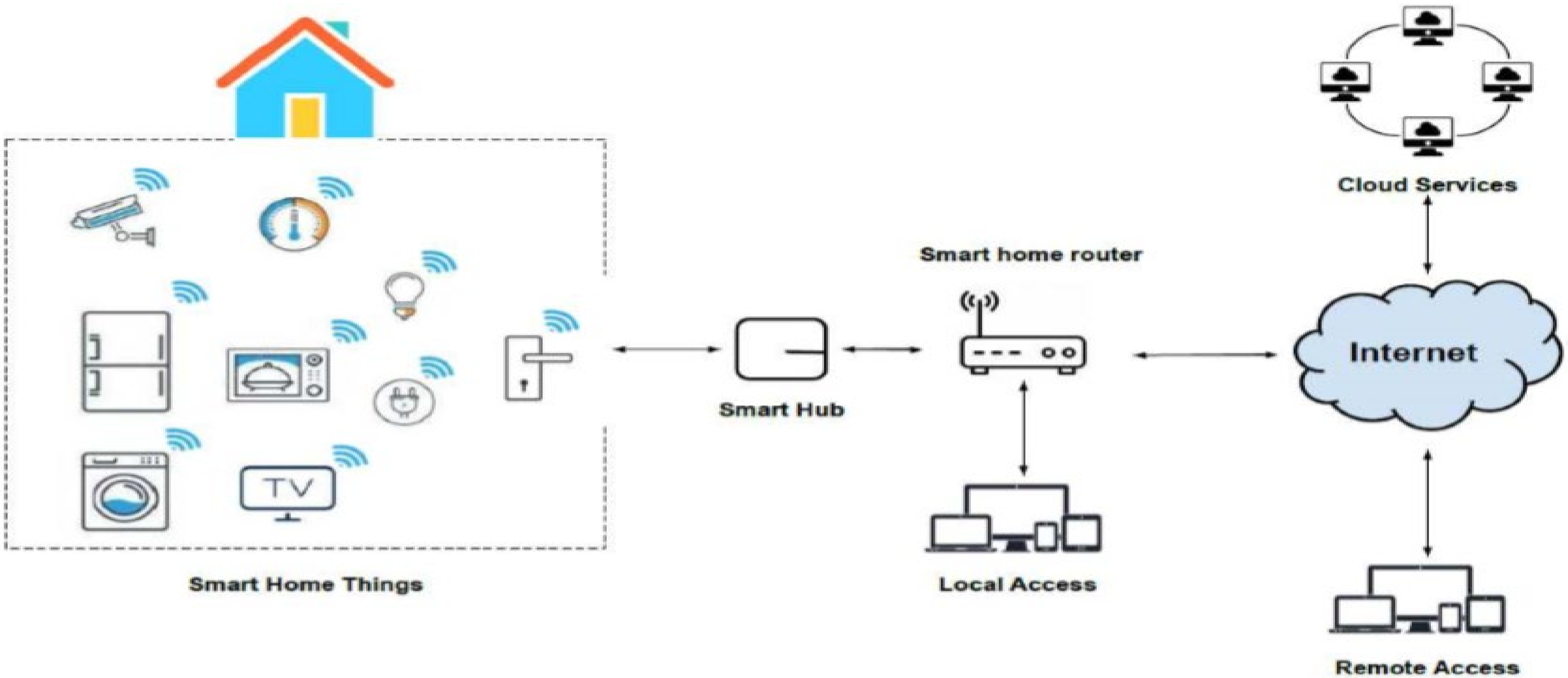
- $HyBAC_{\mathrm{RC}}$ and $HyBAC_{AC}$ are both capable of capturing different static and dynamic characteristics.

- $HyBAC_{\mathrm{RC}}$ and $HyBAC_{AC}$ are both capable of expressing different constraints. However, $HyBAC_{\mathrm{RC}}$ enforces permission-role constraints during configuration time, while $HyBAC_{AC}$ can only enforce it during execution time.

# Implementation

# Enforcement Architecture

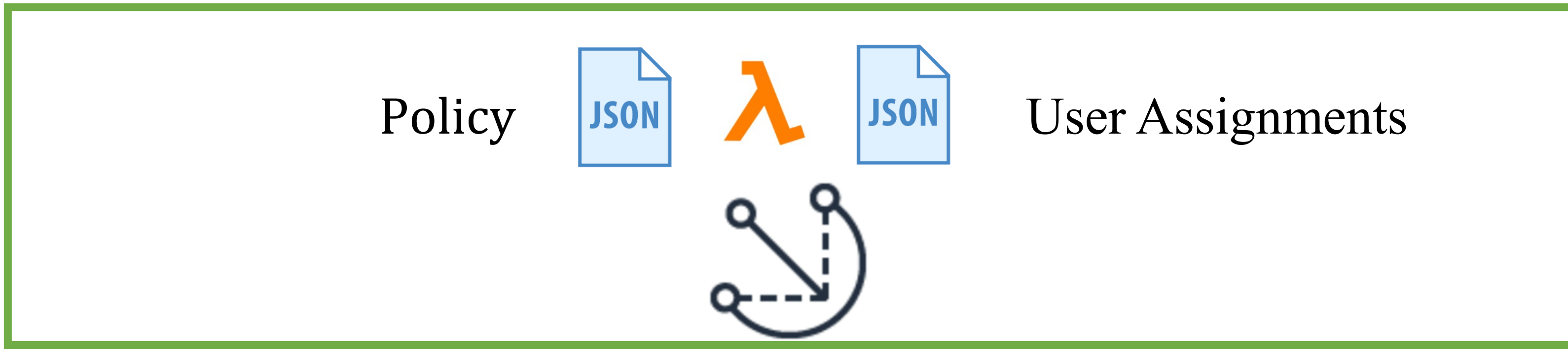


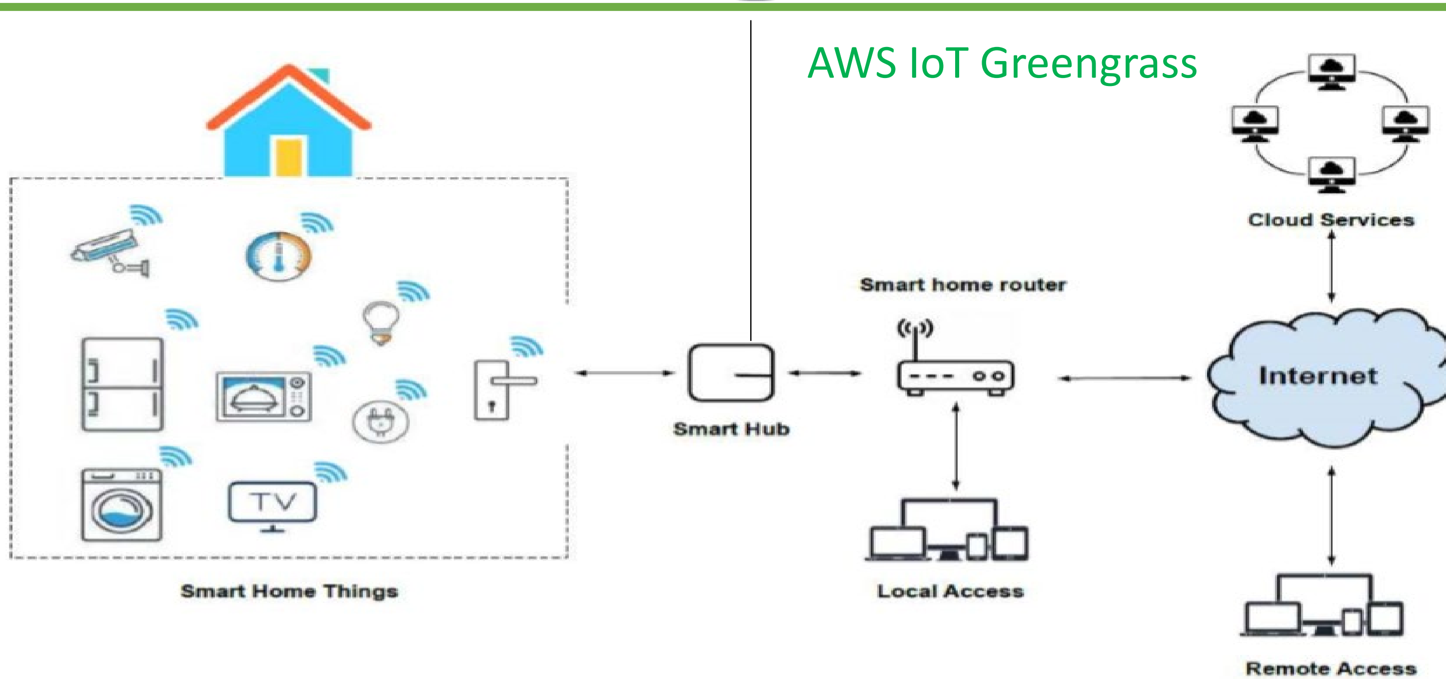



- Adapted from [1]
- There are two types of requests: A- Local requests. B- Remote requests.
- We implemented our model using AWS IoT service.

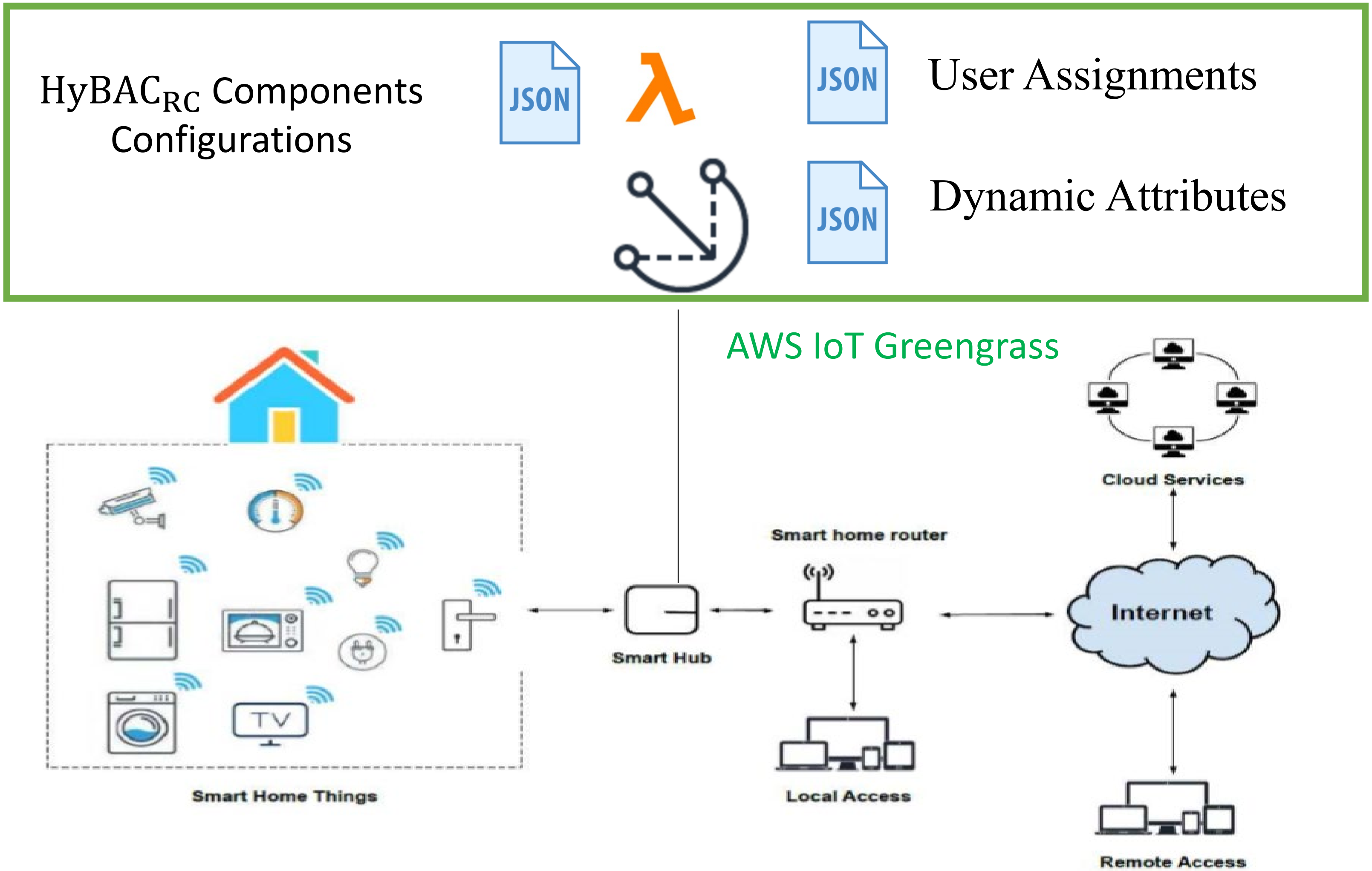
# EGRBAC Enforcement





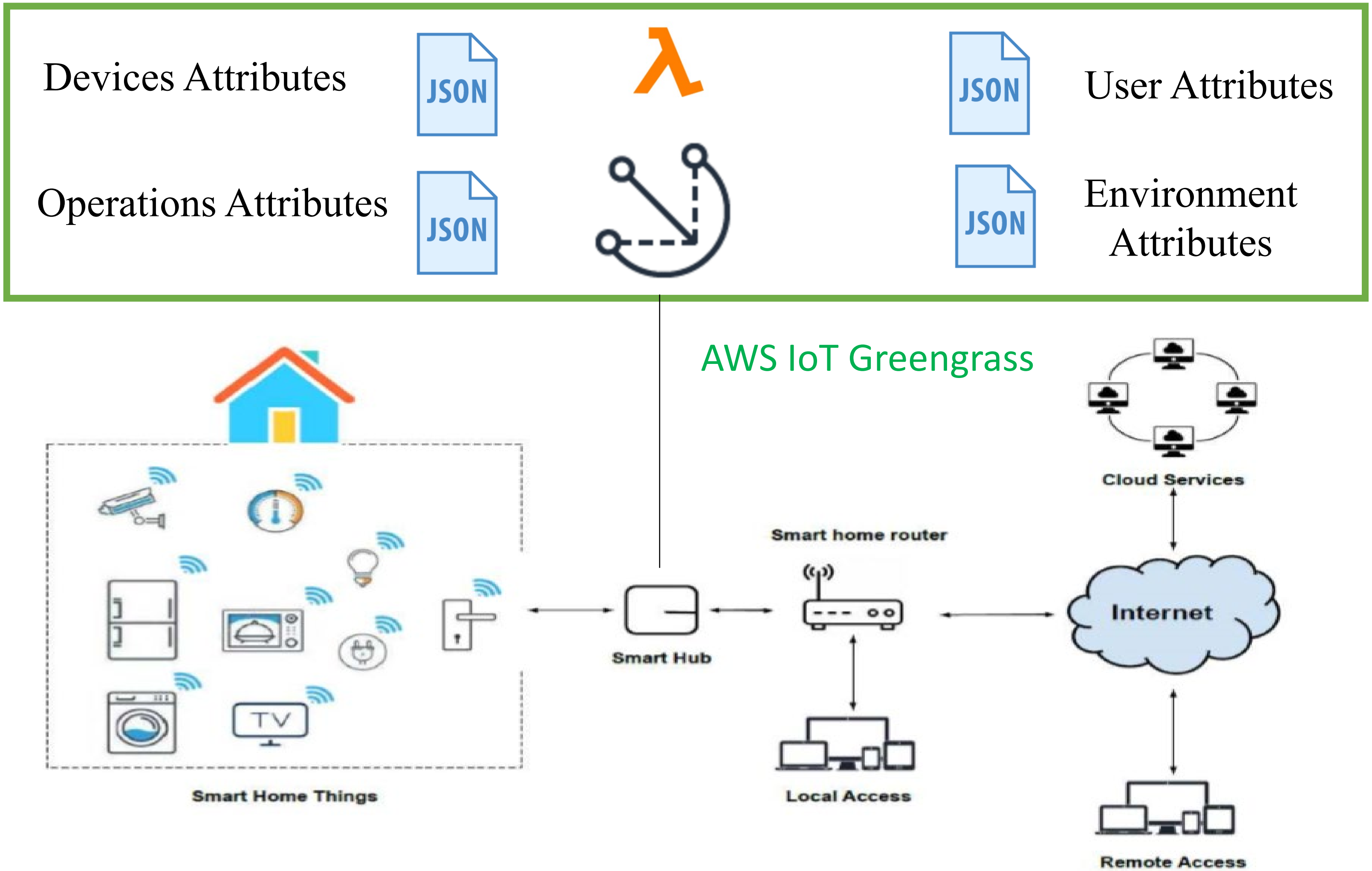



# $HyBAC_{RC}$ Enforcement

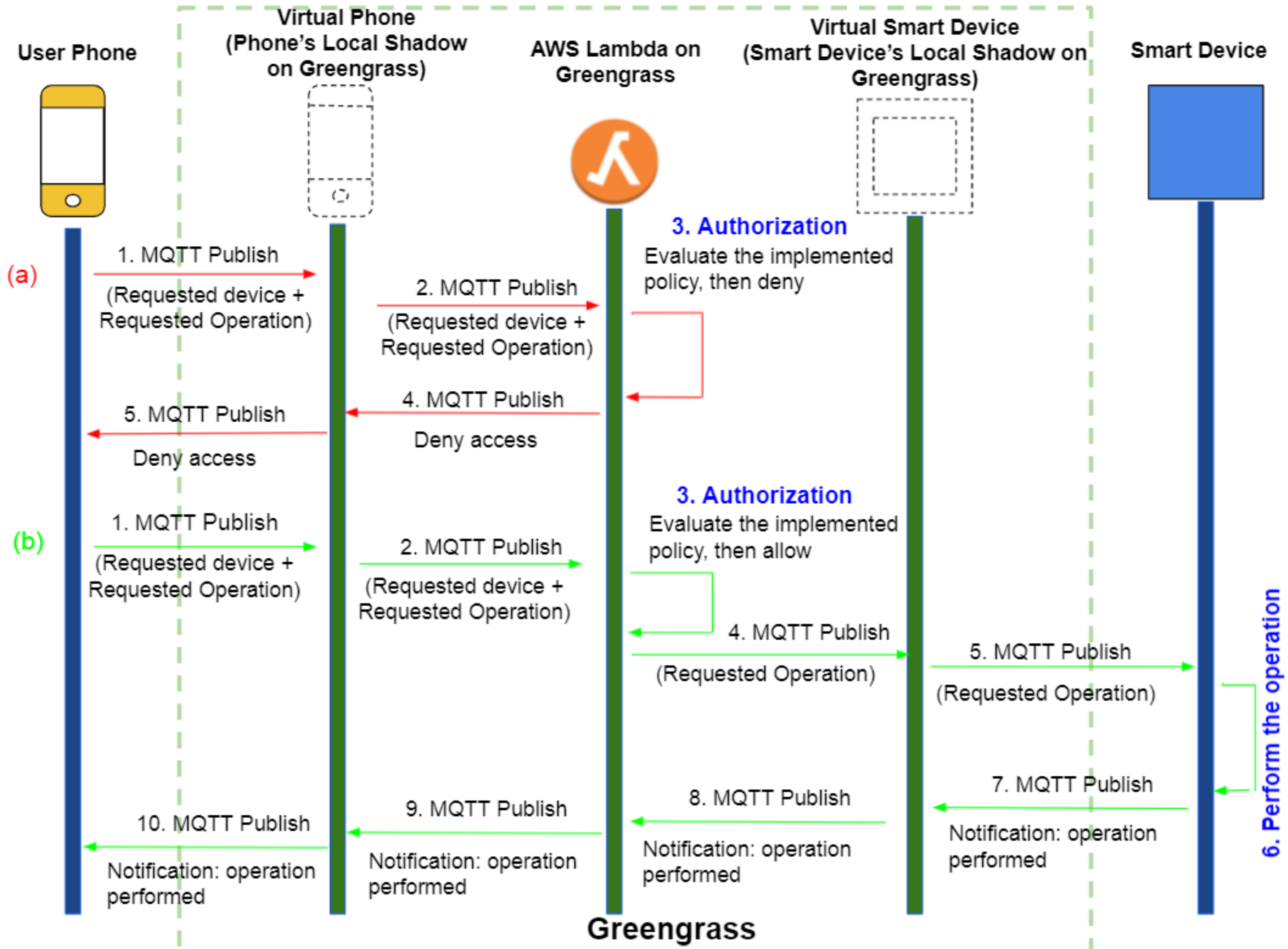


# $HyBAC_{AC}$ Enforcement





# Sequence Diagram



# EGRBAC 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) |

# $HyBAC_{RC}$ and $HyBAC_{AC}$ Performance Analysis

One User Sending Requests to Multiple Devices

| Users | Devices | $HyBAC_{RC}$ L.P.T | $HyBAC_{AC}$ L.P.T | N.R |
|---|---|---|---|---|
| 1 | 1 | 1.8343 | 1.2661 | 10 |
| 1 | 3 | 1.7408 | 1.3118 | 30 |
| 1 | 5 | 1.76588 | 1.3503 | 50 |

Multiple Concurrent Instances of One User Sending Request to One Device.

| Users | Devices | $HyBAC_{RC}$ L.P.T | $HyBAC_{AC}$ L.P.T | N.R |
|---|---|---|---|---|
| 1 | 1 | 1.8343 | 1.2661 | 10 |
| 3 | 3 | 1.8385 | 1.3803 | 30 |
| 5 | 5 | 2.01128 | 1.3247 | 50 |

Multiple Users Sending Requests to One Device

| Users | Devices | $HyBAC_{RC}$ L.P.T | $HyBAC_{AC}$ L.P.T | N.R |
|---|---|---|---|---|
| 1 | 1 | 1.8343 | 1.2661 | 10 |
| 3 | 1 | 1.73177 | 1.2818 | 30 |
| 5 | 1 | 1.8771 | 1.2654 | 50 |

L.P.T ≡ Lambda function processing time in ms.
N.R ≡ Total number of requests (10 per unique request)

# Theoretical Comparison

# A Comprehensive Comparison
# 1- Basic and Main Criteria



- This Criteria is adapted from [2]

| Criteria | $EGRBAC$ | $HABAC$ | $HyBAC_{RC}$ | $HyBAC_{AC}$ |
|---|---|---|---|---|
| **1. Constraints** | | | | |
| a. Static separation of duty | Yes | Yes | yes | Yes |
| b. Dynamic separation of duty | Yes | yes | yes | yes |
| c. P-R constraints | Yes | No | yes | yes |
| **2. Attributed based specifications** | | | | |
| a. Static | Yes | Yes | yes | Yes |
| b. Dynamic | No | yes | yes | yes |
| **3. Least privilege principle** | Yes | yes | yes | yes |
| **4. Authentication** | Positive(Close) | Positive(Close) | Positive(Close) | Positive(Close) |

# A Comprehensive Comparison
## 1- Basic and Main Criteria



| Criteria | $EGRBAC$ | $HABAC$ | $HyBAC_{RC}$ | $HyBAC_{AC}$ |
|---|---|---|---|---|
| **5. Access administration** | | | | |
| a. User provisioning | Easy | Complicated | Easy | Complicated |
| b. Policy provisioning | Complicated | Easy | Complicated | Easy |
| c. Configuration effort | 1- Define and set initial users, devices, and operations static characteristics ( user roles, and device roles)<br>2- Define environment conditions, environment roles, and environment activations<br>3- Setting up initial role structure and assignments | 1- Define and set initial users, devices, and operations static characteristics ( user roles, and device roles)<br>2- Define and set initial users, and devices dynamic characteristics (Dynamic attributes)<br>3- Define environment states, and environment state attributes<br>4- Specify access policies | 1- Define and set initial users, devices, and operations static characteristics ( attributes)<br>2- Define and set initial users, and devices dynamic characteristics (Dynamic attributes)<br>3- Define environment conditions, environment roles, and environment activations<br>4- Setting up initial role structure and assignments<br>5- Specify access policies | 1- Define and set initial users, devices, and operations static characteristics ( attributes)<br>2- Define and set initial users, and devices dynamic characteristics (Dynamic attributes)<br>3- Define environment states, and environment state attributes<br>4- Specify access policies |
| **6. Access review** | Easy | Complicated | Easy | Complicated |
| **7. Administrative policies** | Centralized | Centralized | Centralized | Centralized |

# A Comprehensive Comparison
## 2- Quality Criteria



1- Expressiveness and meaningfulness:

- Formally defined.
- Support different constraints.
- Captures different types of static and dynamic attributes.
- $HyBAC_{RC}$ and $HyBAC_{AC}$ are more expressive and meaningful than $HABAC$ and $EGRBAC$.

2- Flexibility:

- The model should be flexible enough to meet smart Home IoT requirements.
- Should support delegation.
- The flexibility of provisioning new users or policies.
- $HyBAC_{RC}$ and $HyBAC_{AC}$ are more flexible than $HABAC$ and $EGRBAC$.

3- Efficiency level and scalability:

Can it be expanded easily?

Does the model development effect its efficiency level?

# Conclusion



## USER-TO-DEVICE ACCESS CONTROL MODELS FOR CLOUD-ENABLED IOT WITH SMART HOME CASE STUDY

### Analyze literature IoT Access Control Models

1- Criteria for Home IoT Access Control Models.
2- Analyze literature IoT access control models against the proposed criteria.

### RBAC for Home IoT AC

***EGRBAC***

### ABAC for Home IoT AC

***HABAC***

1- Constructing *EGRBAC* from *HABAC*
2- Constructing *HABAC* from *EGRBAC*
3- Compare the theoretical expressive power of *EGRBAC* and *HABAC*

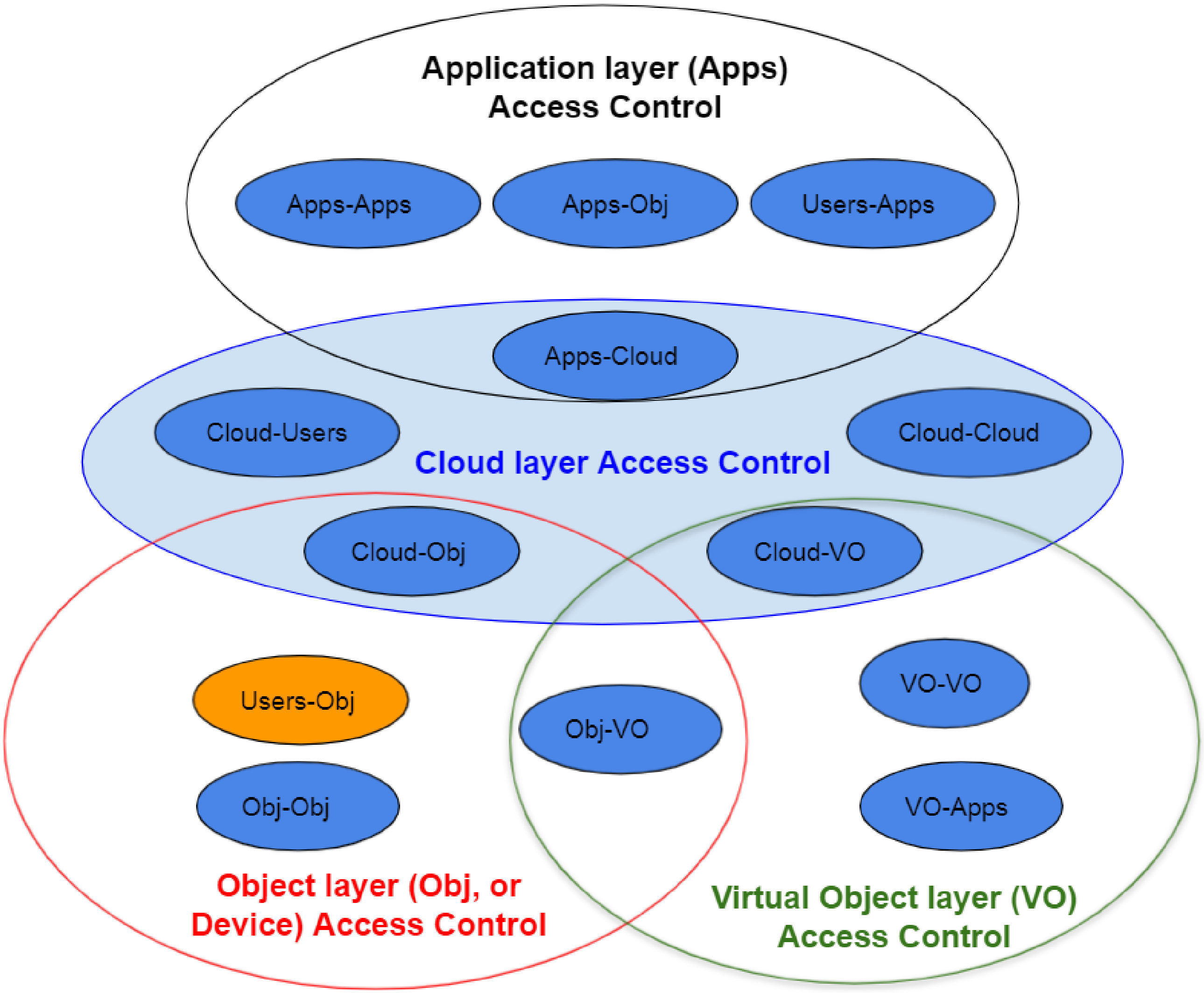
### Combined Models for Home IoT AC

$HyBAC_{RC}$ | $HyBAC_{AC}$

1- Constructing $HyBAC_{RC}$ from $HyBAC_{AC}$
2- Constructing $HyBAC_{AC}$ from $HyBAC_{RC}$
3- Compare the theoretical expressive power of $HyBAC_{RC}$ and $HyBAC_{AC}$

# Some Future Directions





# Dissertation Publications



## Conference papers:

1. Ameer, Safwa, James Benson, and Ravi Sandhu. "The EGRBAC Model for Smart Home IoT." In 2020 IEEE 21st International Conference on Information Reuse and Integration for Data Science (IRI), pp. 457-462. IEEE, 2020. **(Published)**
2. Ameer, Safwa, and Ravi Sandhu. "The HABAC Model for Smart Home IoT and Comparison to EGRBAC". In the Proceedings of the ACM Workshop on Secure and Trustworthy Cyber-Physical Systems (SaT-CPS 2021). **(Published)**

## Journal papers:

1. Ameer, Safwa, James Benson, and Ravi Sandhu. "Hybrid Approaches (ABAC and RBAC) Toward Secure Access Control in Smart Home IoT". To be submitted to IEEE Trans. on Dependable and Secure Computing.
2. Ameer, Safwa, and Ravi Sandhu. " An ABAC Approach toward secure Access Control in Smart Home IoT". Got invitation to be submitted to Special Issue "Secure and Trustworthy Cyber–Physical Systems" in Information.

# Refrences



[1] Dimitris Geneiatakis, Ioannis Kounelis, Ricardo Neisse, Igor Nai-Fovino, Gary Steri, and Gianmarco Baldini. Security and privacy issues for an IoT based smart home. In 2017 40th MIPRO. IEEE, 2017.

[2] Shabnam Mohammad Hasani and Nasser Modiri. Criteria specifications for the comparison and evaluation of access control models. International Journal of Computer Network and Information Security, 2013.

# Thank you!
# Questions?