CADI AYYAD UNIVERSITY

Optimization of Advanced Communications Systems, Networking and Security Laboratory (OSCARS)

Access control in The Internet of Things: Big challenges and new opportunities

Anas ABOU ELKALAM

INTERNATIONAL CONFERENCE ON ADVANCED COMMUNICATION SYSTEMS AND INFORMATION SECURITY (ACOSIS'16)

plan

1. • Introduction
2. • IoT security requirements and our OM-AM Model
2. • A proposed taxonomy of access control solutions in IoT
3. • A qualitative evaluation of the main access control solutions proposed in the literature
4. • Open challenges
5. • research directions
6. • FairAccess: our propsed solution to build an adequate access control solution for IOT

Introduction : Access control in IoT

Smart Cities | Smart Environment | Smart Energy | Smart Agriculture | E-Health | Retail | Logistics | Industrial Control

Security and Privacy issues:

- ✓ The more connected devices and data are flowing over networks the more security concerns increase
- ✓ Smart objects may deal with personal and sensible data.

Urgent need to control access to our private data

Main challenges :

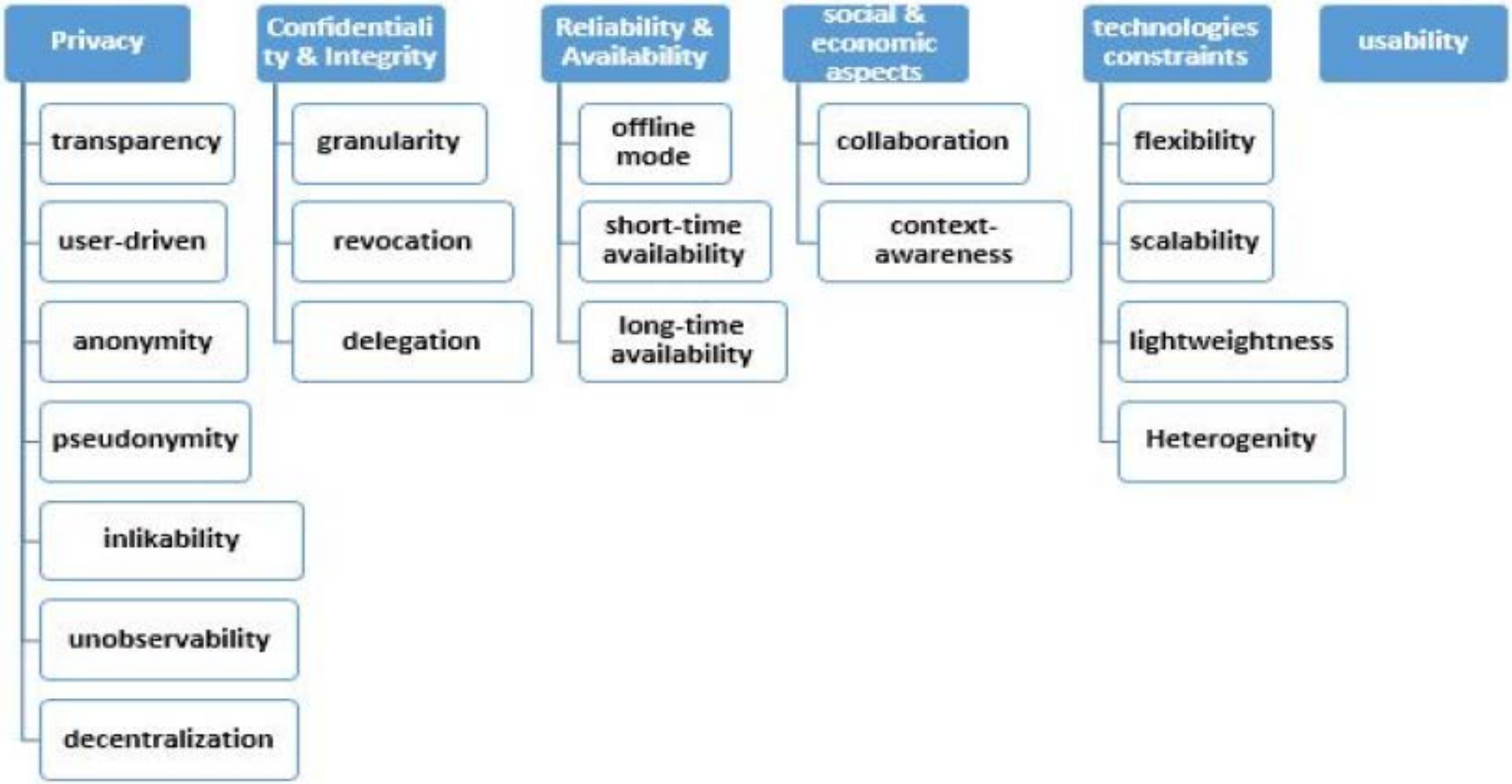
constrained and low power devices

user- driven protocols

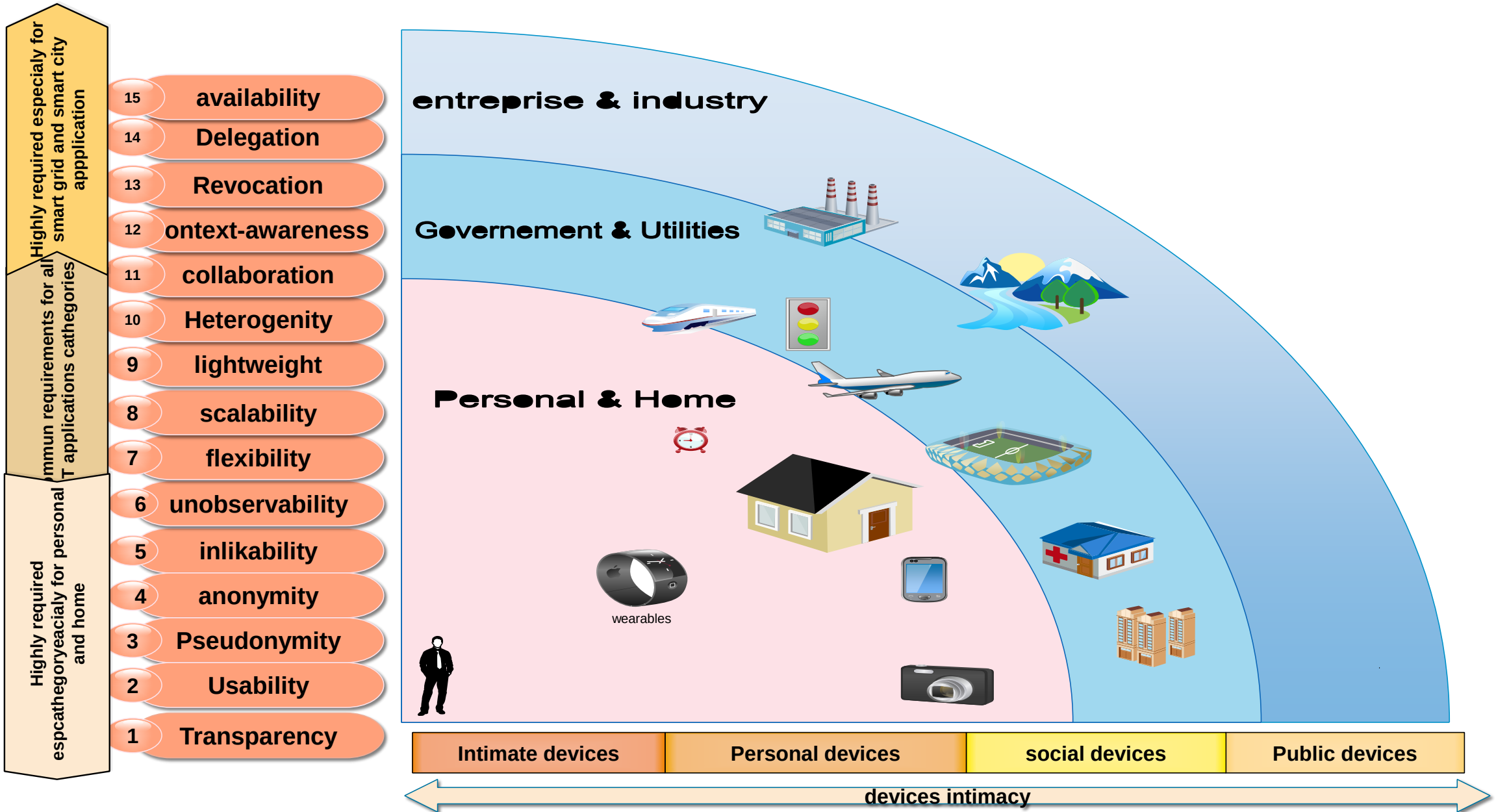
OM-AM Model

Objective	Security Policy, Risk Assessment Octave, EBIOS Methods, ISO/EIC 27002/27005 Standards etc)
Model	Authorization model (e.g. RBAC, ABAC, UCON)
Architecture	Frameworks, protocols (XACML, OAuth, UMA)
Mechanisms	Hardware and software tools : (ACLs, Routers, Encryption, Audit logs, IDS, Antivirus software, Firewalls, Smart cards, Dial-up call-back systems, Alarms and alerts etc)

IoT Security and privacy preserving objectives



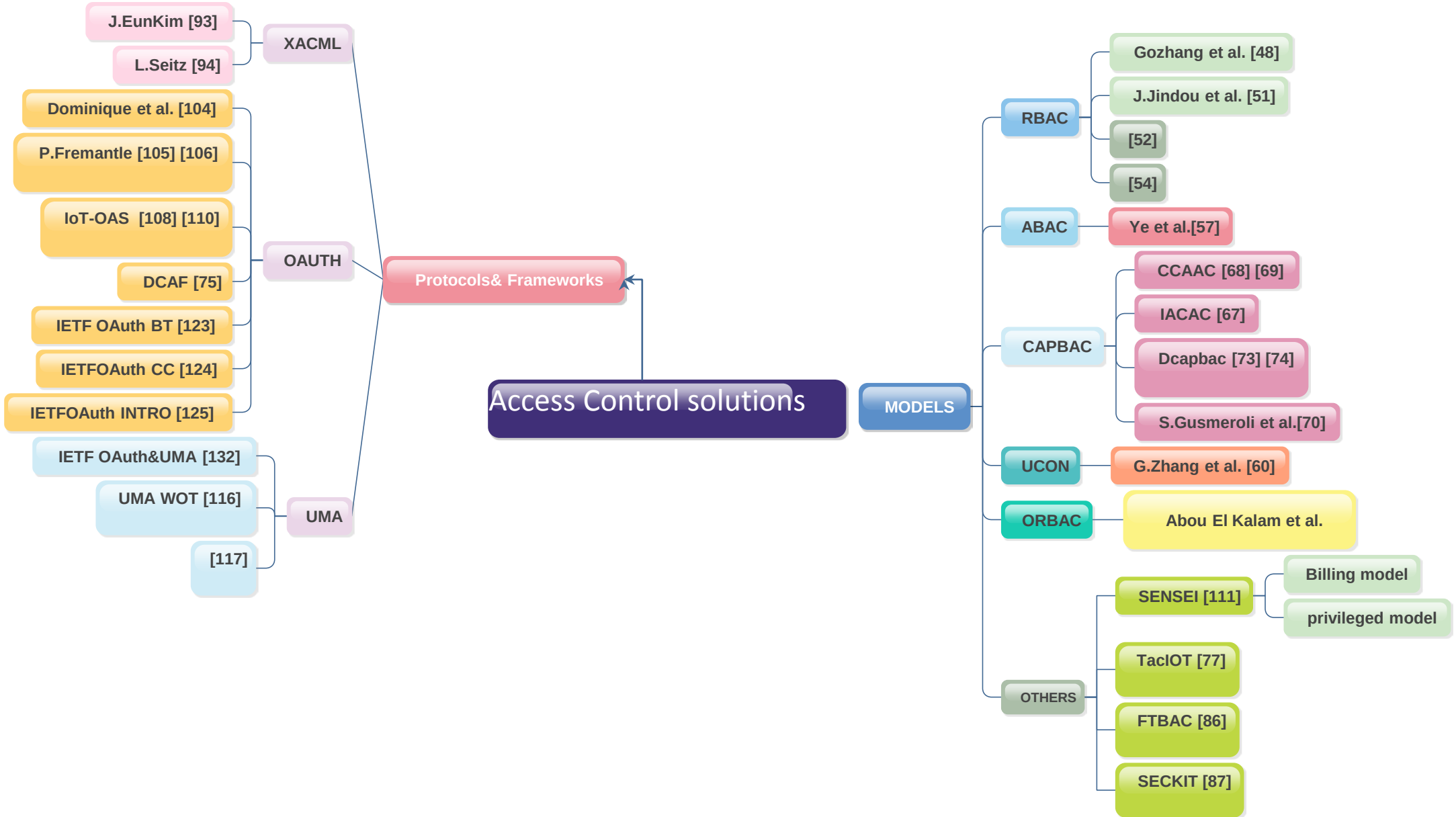
IoT domain application taxonomy and their security requirements.



Security requirements and device taxonomy of IoT applications domains

Domain application		Devices proximity	Reliability& Availability	Confidentiality & Integrity	Usability
Personal and Home	Healthcare	intimate personal	highly required [42]	highly required	highly required
	SmartHome	intimate personal Social	temporal unavailability is tolerated high reliability for (home security and home automation) low reliability for media and entertainment	highly required	highly required
Government and utilities	SmartCity	Personal Social Public	not highly required [43]	not highly required except for user's private data [37] [36]	preferred
Enterprise and industry	SmartGrid	Personal Social Public	highly critical	not highly required except for consumer's private data	preferred

A PROPOSED TAXONOMY OF ACCESS CONTROL SOLUTIONS IN IOT LITERATURE



A qualitative evaluation of the main access control solutions proposed in the literature based on the specified requirements

Access control model	Citation	scalability	Usability	flexibility	interoperability	Context awareness	distribution	Real time	heterogeneity	lightweight	Used-driven	granularity	revocation	delegation	Offline mode
RBAC-	[95]	VL	VL	VL	VL	M	NO	NO	L	NO	VL	H	NO	NO	M
	[98]	L	VH	M	VL	L	NO	NO	L	NO	H	M	NO	NO	NO
	[99]	L	VL	VL	VL	VL	NO	NO	L	NO	VL	L	NO	NO	M
	[100]														
ABAC	[101]	M	L	M	M	H	NO	NO	L	NO	L	H	NO	NO	M
UCON	[102]	M	M	M	VL	H	NO	M	L	NO	VL	H	NO	NO	M
	[79]	M	M	M	H	VH	M	M	H	H	M	VH	NO	NO	M
CAPBAC	[105]	H	M	H	M	VL	M	NO	VL	NO	M	L	VH	VH	M
	[106]	H	M	H	M	L	NO	NO	L	NO	M	VL	VH	VH	M
	[61]	H	M	M	M	L	L	NO	VL	M	M	H	NO	VH	M
	[108]	VH	M	H	H	L	VH	NO	L	H	L	M	VH	VH	M
XACML	|114]	H	H	M	H	H	NO	H	H	NO	H	H	ND	ND	M
	[115]	M	M	M	H	H	M	NO	M	M	M	H	NO	NO	M
TH	[116]	H	H	M	M	L	NO	NO	M	NO	H	L	ND	ND	ND
	[94]	VH	M	H	VL	L	NO	NO	VL	M	M	L	M	ND	NO

[98] M VH M VL NO NO NO NO NO VH M NO NO M

J. Jindou, Q. Xiaofeng, C. Cheng, Access Control Method for Web of Things Based on Role and SNS, in: 2012 IEEE 12th Int. Conf. Comput. Inf. Technol., IEEE, 2012, pp. 316{321.

A quanlitative evaluation through Combos schemes

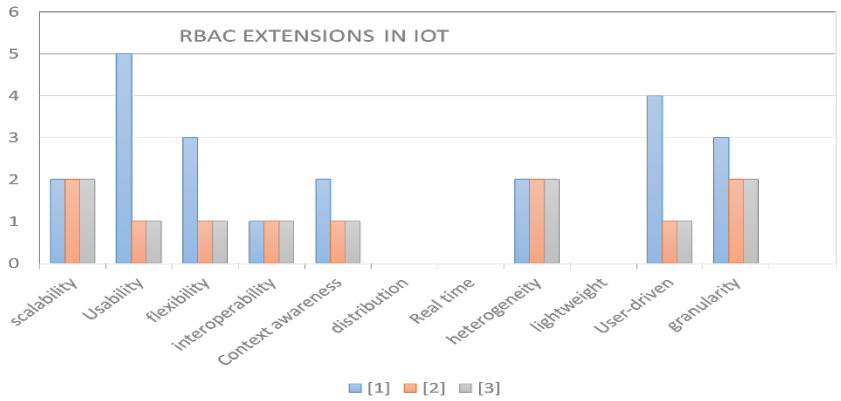


Figure 1: features of access control solution based on RBAC model in IoT

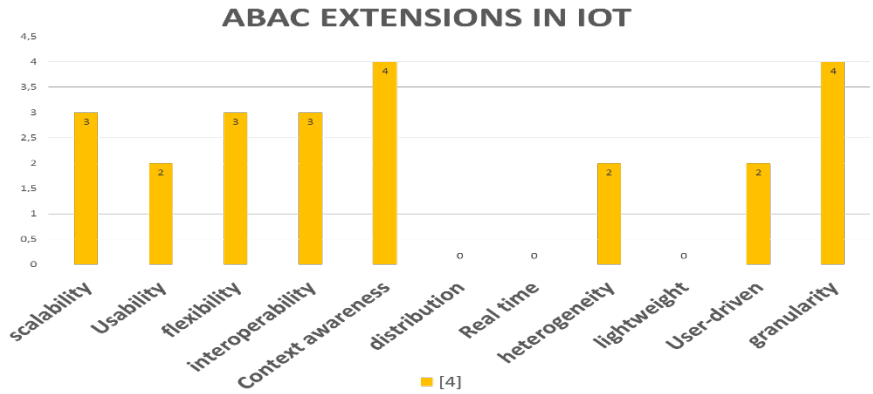


Figure 2: features of access control solution based on ABAC model in IoT

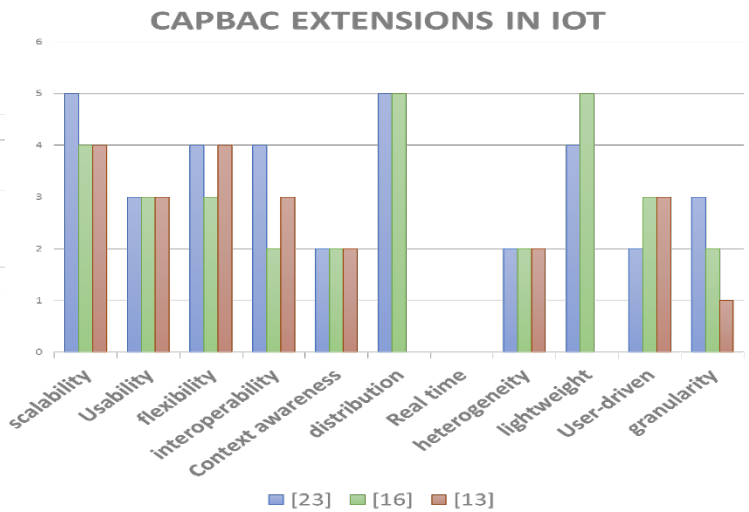


Figure 3: features of access control solution based on CAPBAC model in IoT

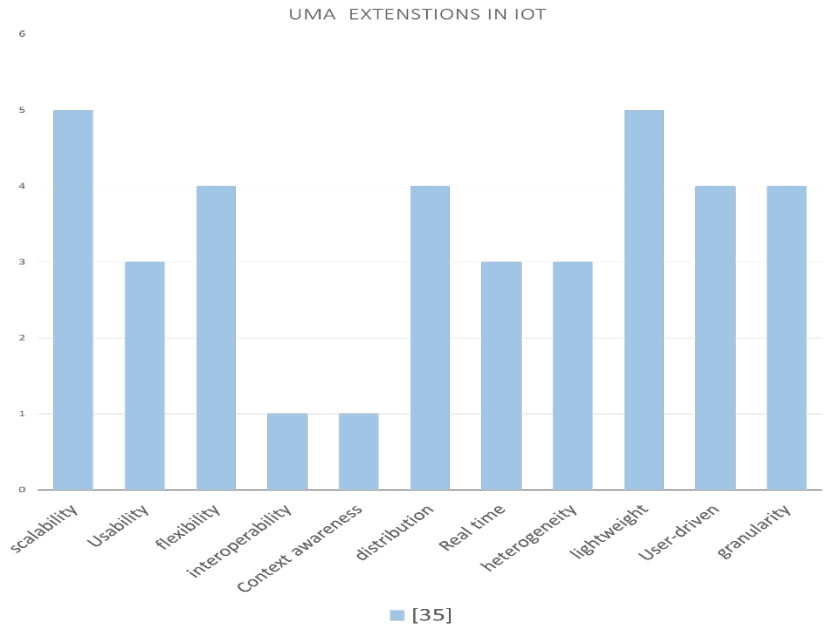
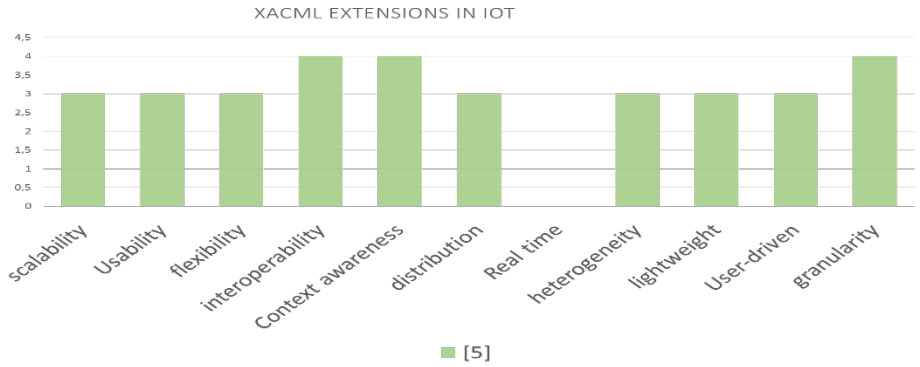
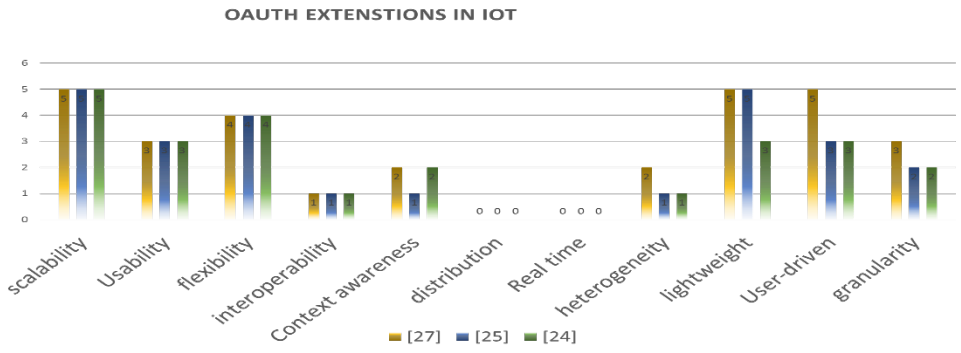
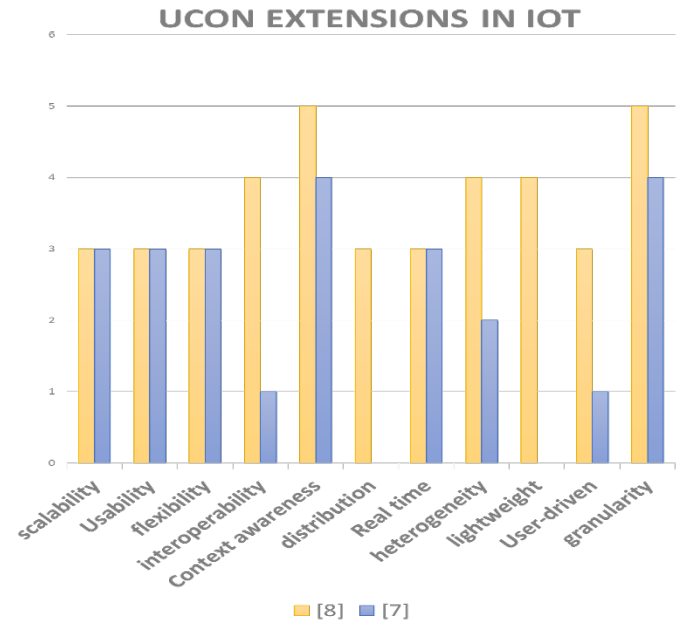


Figure 4: features of access control solution based on UMA in IoT







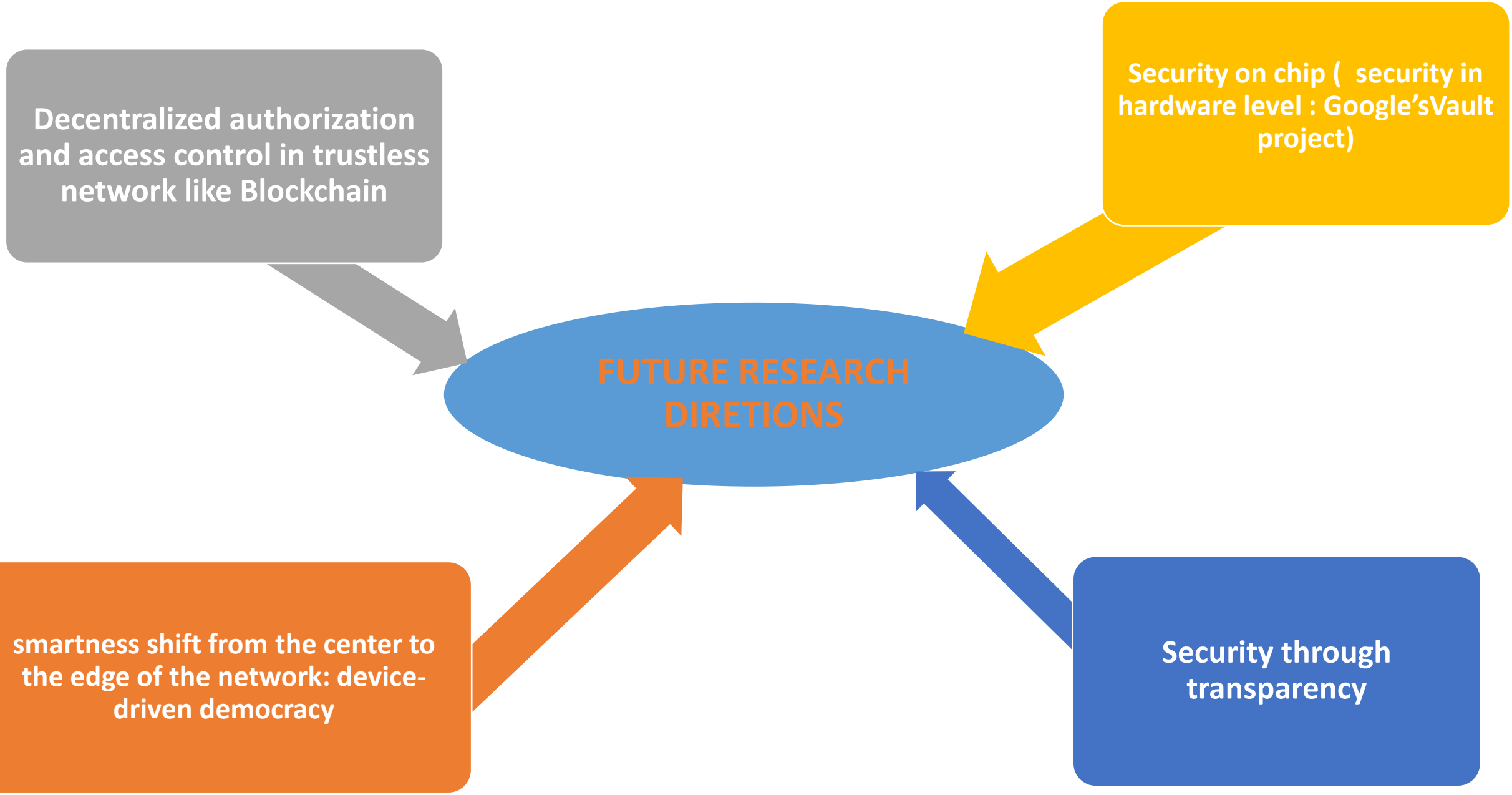
PROS AND CONS OF ACCESS CONTROL STANDARDS FROM AN IOT PERSPECTIVE

UMA	PROS	CONS
	User-driven	New (has not yet a stable version)
	Support claim-based access control	
	Off line mode	
	Externalization of authorization	
	Identity interoperability	Concentrate identity on central hub

Access control challenges in IoT

	Adaptability approach	Reboot approach
Challenge 1: **using existing access control mechanism** **vs** **come up with new ones**	Pros : • Exploit already existing and long experience. • Saving time Cons • Complex solutions • Do not fit with IoT requrirements	Pros: • Fit the new IoT business model • Comply with the principle of privacy by design • Built with IoT requirements in mind Cons: • Need time to be built • Need trust to be investigated, developed and adopted
Challenge 2: **centralized access control management** **VS** **Distributed access control management**	Centralized approach Pros: • Possibility to reuse existing mechanism since the central point is not constrained • Ease to manage access control policies Cons: • End to end security is dropped • Single point of failure • User is not involved in access control over his own data • Trust foreign entities	Distributed approach Pros: • Ensure privacy • Less expensive in cost • Offline mode • No need to trust any third part Cons: • Fine-grained access control logic not supported by constrained devices • Difficulty to manage and update access control policies embedded in device side

Fture research directions



Goal

a balance solution that solves the defined dilemma of :

decentralized approach (possibility to **reuse alredy exsiting access control technologies** with **No need to trust any third**)

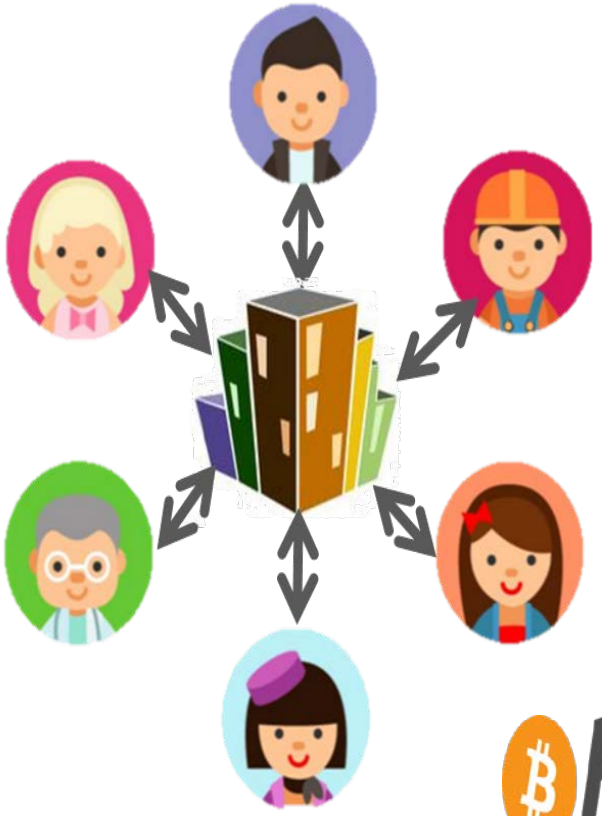
&

centralized approach (**end user transparency and anonimity , contextual access control decisons taken by smart devices)**

FairAccess : using blockchain technology as access control infrastructure

Why	blockchain technology as solution to face access control issues in IoT ?

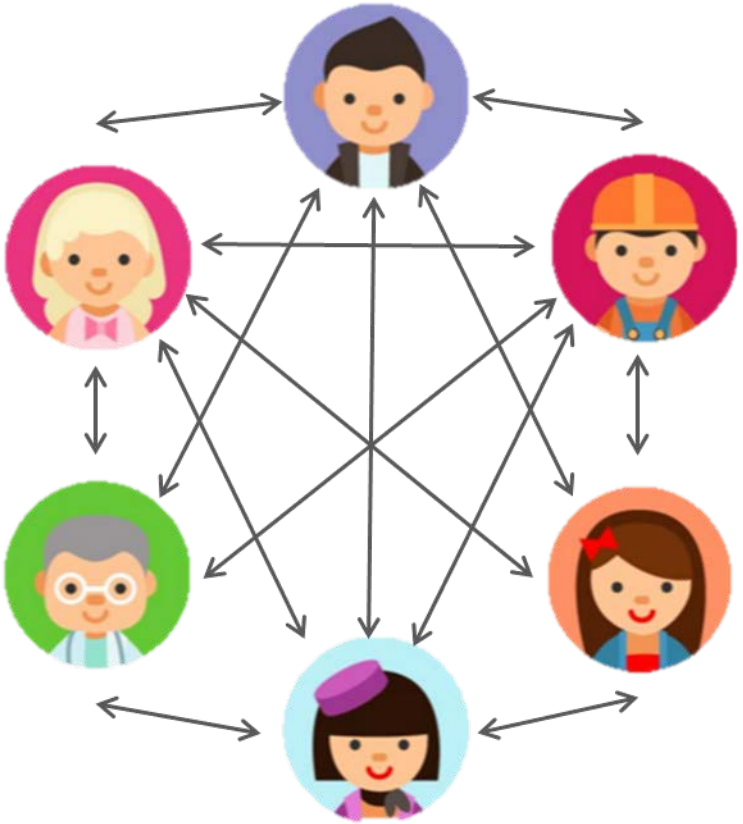
Traditional Trusted Third Party system



BLOCKCHAIN

- Enables parties to directly transfer a digital currency (Bitcoins) without a *TTP* (i.e., banks).!
- Instead, a network of untrusted peers ensures the validity of *all* transactions.!
- All correct transactions are publicly verifiable through a public ledger (the blockchain).!

Decentralised and trustless system



bitcoin

Crypthocurrency 2.0

Voting

Banking

Web Domain

Internet of Things

Healthcare

More are coming

Blockchain in a nutshell

Append-only distributed system of record shared across the network

Shared Ledger

Cryptography

Ensuring secure, authenticated & verifiable transactions

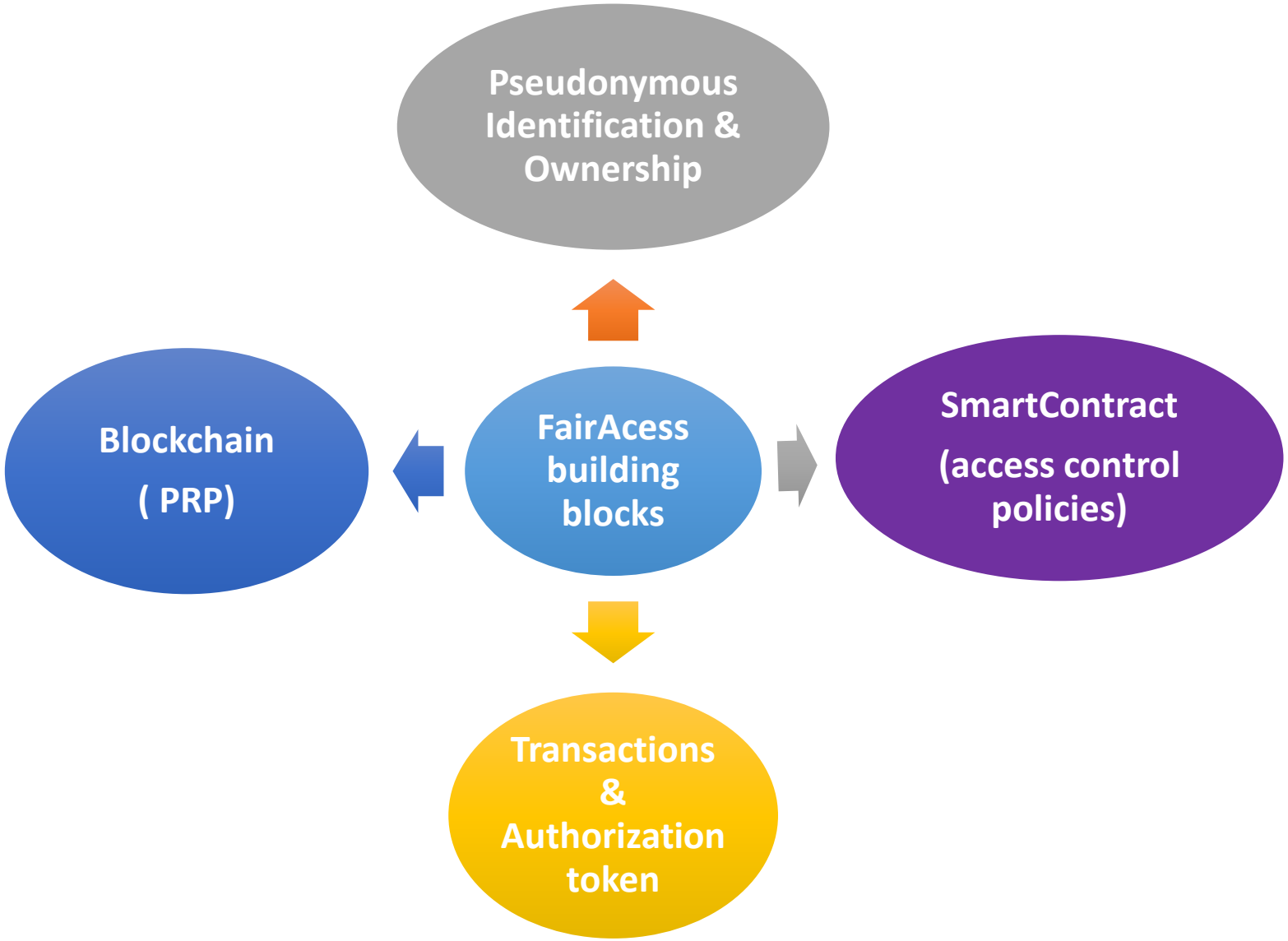
All users in the network can come to collectively agree on the validity of the data recorded

Consensus

Smart Contract

conditions embedded in transaction database & executed with transactions

FairAccess: building blocks



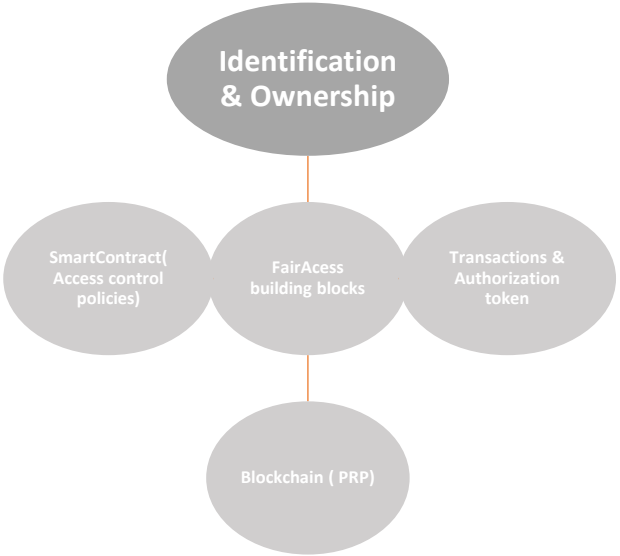
Fairness, user driven, lightweight, trustless

FairAccess: building blocks

- **Ownership and identification** in FairAccess is established through *digital keys*, *bitcoin-like addresses*, and *digital signatures*.

- Keys enable many of the interesting properties of **FairAccess** including**:**

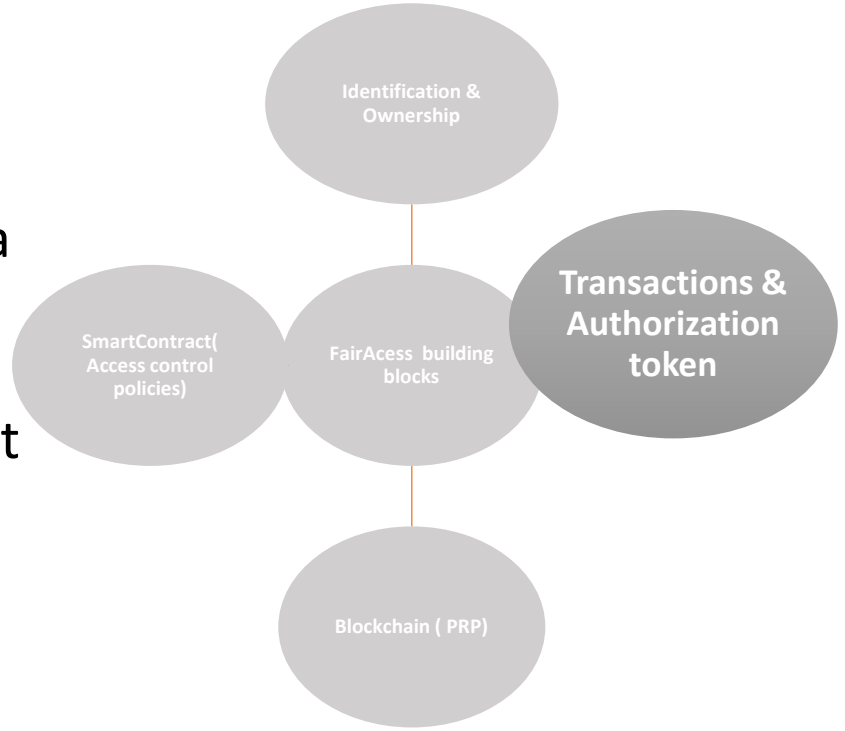
1. **Thing to thing interaction**
2. **Pseudonymity and Unlikability** (no real-world name or identifying information are required)



FairAccess: building blocks

$$Tx=(m,sig_{rs}(m)) \quad where$$
$$m= (IDx,input\ (\ rs),output(rq,\pi x,TKNrs,rq)$$

- IDx The index of the current transaction Tx where x = H (Tx) , H is a hash function
- rs The address of requested resource.
- rq The address of the requester who is the receiver of the current transaction
- πx Locking script (access control policies written in scripting language)
- $TKNrq,rs$ Encrypted "access token associated to couple (rs,rq).

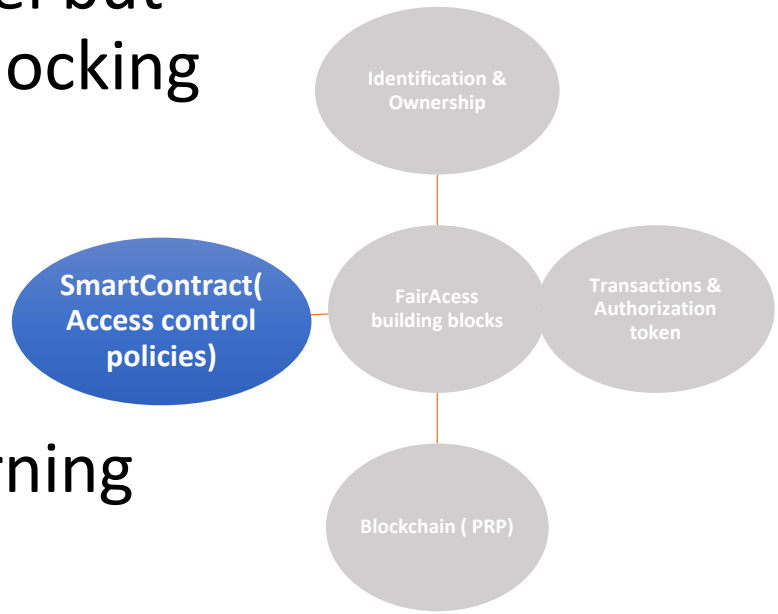


FairAccess: building blocks

Fine grained access control policies :

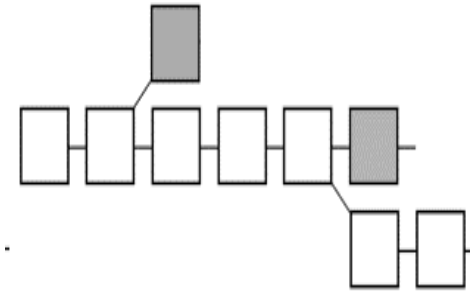
A policy is a set of rules and conditions (based on a specific context or attribute, etc) that a requester entity has to fulfill in order to obtain the Access Token and gets access to the specific resource.

This rules could be expressed by any access control model but must be transformed to a script language considered as locking script placed on the output of a transaction.



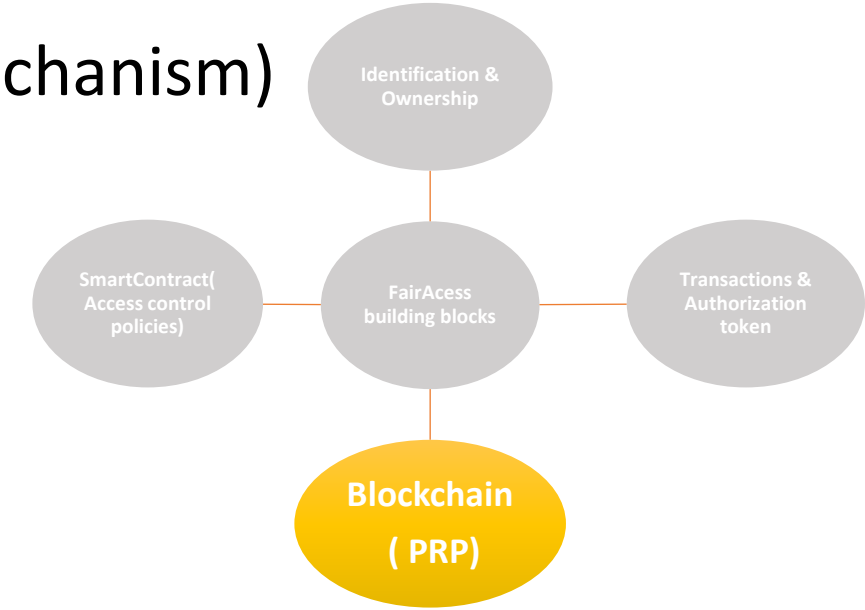
- scripting languages : Multisig, pay to public key
- Smart contract: ethereum programming language (turning complete language)

FairAccess: building blocks



The blockchain :

- Database or policy retrieval point (PRP) (access control policies= SmartContracts).
- logging databases (auditing functions).
- Detecting token reuse (double spending detection mechanism)
- **Lightweight**



Phase 1: reload access control policy in form of smart contract to the blockchain trough: Grant access transaction

1. The RO defines for the couple (Resource, Requester) an access control policy $POLICYrs,rq$

2. The wallet transforms this access control policy to a SmartContract $POLICYrs,rq \rightarrow \pi x$

getting update

3. The wallet generates a GrantAccess Transaction in the following form: $Tx=(m,sigrs(m))$ $where$ $m= (IDx,from\ (\ rs),to(\ \pi x)$

4. Each node verifies the transaction within the transaction validation process.

PDP

PDP

PDP

PDP

PDP

5.broadcasts transcation to the network

RO-Wallet= PEP

Policy management block

<Transaction>
000012DF545
FFF55000012
DF545FFF550
00012DF545F
FF55000012D
F545F

<contract>
</contract>

Access Policy

Token Authorization management block

TKN database

Resource Owner (RO)

6. Reloads policy to the blockchian in form of SmartContract

IF VALID

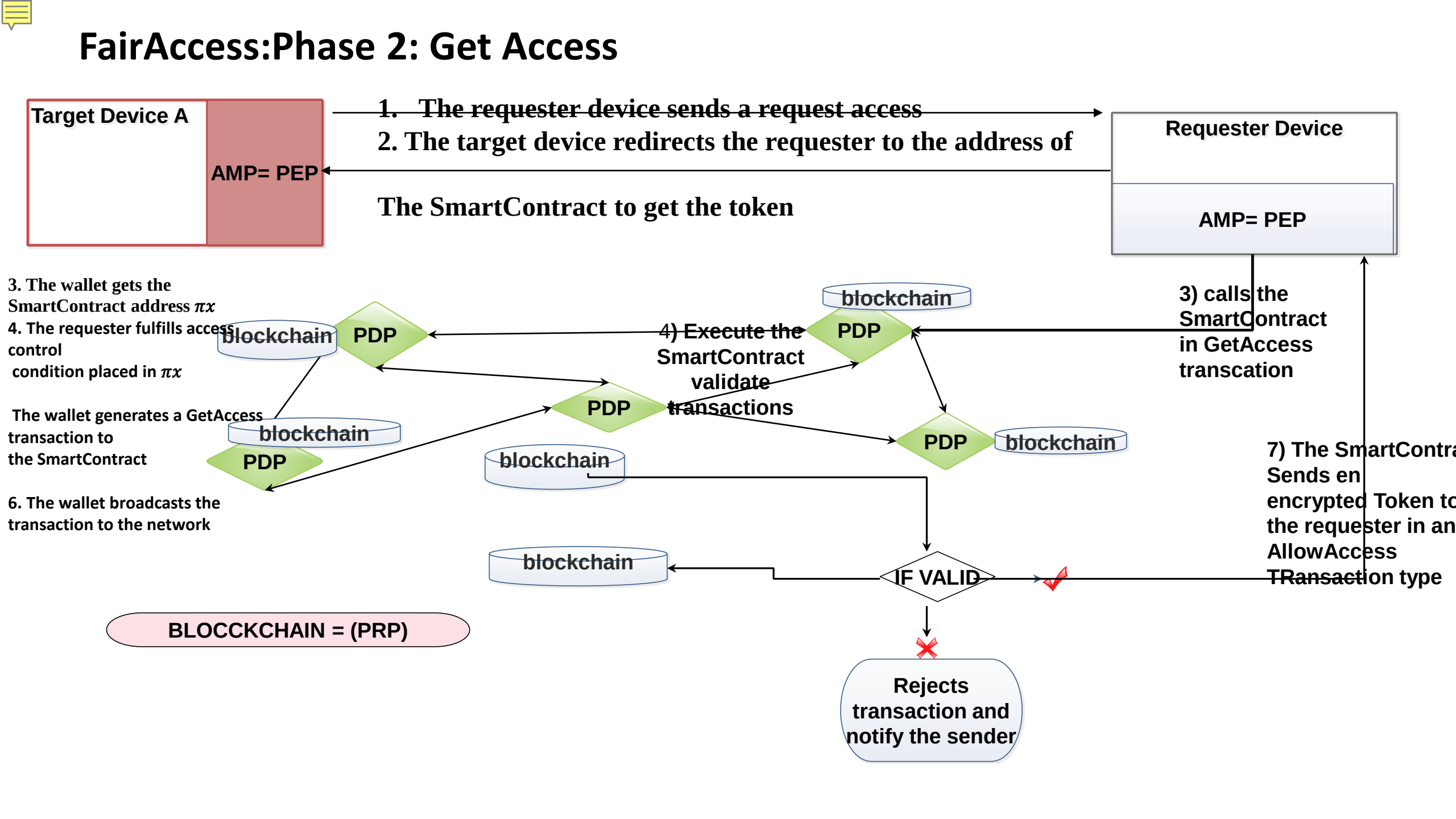
NO

Rejects transaction and notify the sender

YES

BLOCCKCHAIN = (PRP)

FairAccess:Phase 2: Get Access



Blockchain – not for all . . .

Fullfiled items

- **Pseudonymity and Unlikability**
- **Identification enabling thing to thing interaction.**
- **Lightweight**
- **User driven & transparency**
- **Distributed nature and the lack of a central authority**
- **Fine-granularity**

Thank you …

Anas ABOU EL KALAM
aabouelkalam@uca.ac.ma