**Unit 4**

Introduction

Overview of governance

Privacy and security issues, contribution fromFP7 projects, security

Privacy and trust in IoT data platform forsmart cities

First step toward secure platform

Data aggregation for IoT in smart cities

Security: loopholes and measures

**Introduction**

IoT is broad term, which indicates the concept thatincreasingly pervasive connected devices (embeddedwithin, attached to or related to

“Things”) will supportvarious applications to enhance the awareness andthe capabilities of users.

For example, users will be able to interact with homeautomation systems to remotel control the heatingor the alarm system.

**Why should the Internet of Things (IoT):**

Require special attention when it comes to privacy, securityand governance?

Doesn’the established Internet have these mattersdealt with sufficiently already, given that through justabout every smartphone anywhere there are already awide variety of sensors capturing information whichwe share on the Internet e.g. photos, videos, etc.?

**Why is IoT any different?**

Firstly IoT is different because it will be possible andlikely that objects will autonomously manage theirconnections with the Internet or, this will be doneupon the request of someone or something remotely.When someone shares a video or a photo taken ontheir mobile phone over the Internet they“call theshots”

.

**With IoT potentially someone else is in charge.**

For reasons largely similar to this, the topics ofprivacy, security and governance are very important if not vital to the success of IoT in order toestablish and maintain stakeholder trust andconfidence.Yes, there is a large overlap between IoT and Internetin many areas pertaining to trust however IoT bringsmany new specific dimensions too.The adoption of IoT essentially depends upon trust.Moreover this trust must be established andmaintained with respect to a broad group of stakeholders otherwise IoT will face, to some degreeor other, challenges which may restrict adoptionscope or delay its timing.Security in its broadest definitions includes health andwellbeing as well as other forms of protection.

These aspects need to be viewed from the perspectives ofthe majority if not all the principle stakeholder groups andextended to include the relevant influencing andinfluenced elements of the general environment.

**2.Overview of governance**

The European Research Cluster on the Internet of Things hascreated a number of activity chains to favour close cooperationbetween the projects addressing IoT topics and to form an arenafor exchange of ideas and open dialog on important researchchallenges.

The activity chains are defined as work streams that grouptogether partners or specific participants from partners aroundwell defined technical activities that will result into at least oneoutput or delivery that will be used in addressing the IERCobjectives.

**3.Privacy and security issues**

IERC Activity Chain 05 is a cross-project activityfocused on making a valued contribution to IoTprivacy, security and governance among the ECfunded research projects in the area of Internetof Things.

**Overview of activity chain 05 - governance, privacy & security issues**

Overall, the main objective of the Activity Chain 05 is toidentify research challenges and topics, which could makeIoT more secure for users (i.e. citizen, business andgovernment), to guarantee the privacy of users andsupport the confident, successful and trusted developmentof the IoT market.

**4.Contribution from FP7 projects**

1.FP7 iCore Access Framework (iCore Contribution)

2.IoT@Work Capability Based Access Control System(IoT@Work Contribution)

3.GAMBAS Adaptive Middleware (GAMBASContribution)

4.IoT-A Architecture (IoT-A Contribution)

5.Governance, Security and Privacy in the ButlerProject (Butler Contribution)

1. FP7 ¡Core access framework (iCore contribution)

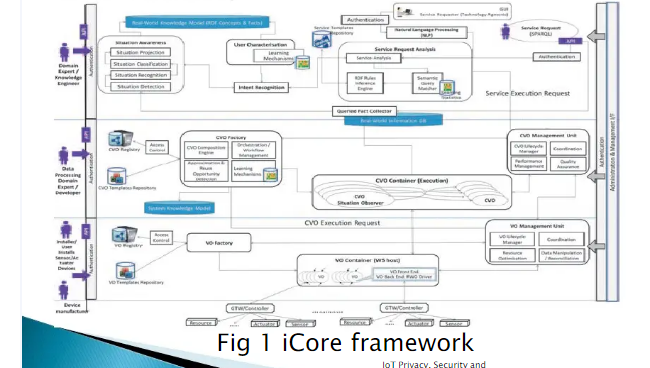
The iCore cognitive framework is based on the principlethat any real world object and any digital object that isavailable, accessible, observable or controllable can have avirtual representation in the“Internet ofThings”,

**which iscalled Virtual Object (VO).**

VOs are primarily targeted to the abstraction oftechnological heterogeneity and include semanticdescription of functionality that enables situation-awareselection and use of objects.Composite virtual objects (CVOs) use the servicesof virtual objects.

A CVO s a cognitive mash-up of semanticallyinteroperable VOs that renders services inaccordance with the user/stakeholderperspectives and the application requirements.

The overall layered approach of the iCore projectis provided in Figure 1.



The first cognitive management layer (VO level cognitiveframework) is responsible for managing the VOsthroughout their lifecycle, ensuring reliability of the link tothe real world object/entity (e.g., sensors, actuators,devices, etc.).

They represent for example, in a logistic related scenario,tracking temperature controlled goods transport,individual goods boxes are represented by VOs thecontainer transported by a truck is a VO as is the truckitself.

The second cognitive management layer(CVOlevel cognitive framework) is responsible forcomposing the VOs in Composite VO. CVOs willbe using the services of VO to compose moresophisticated objects.

In our example, the combination of the truck andthe transported goods is represented in thecognitive framework as a CVO.

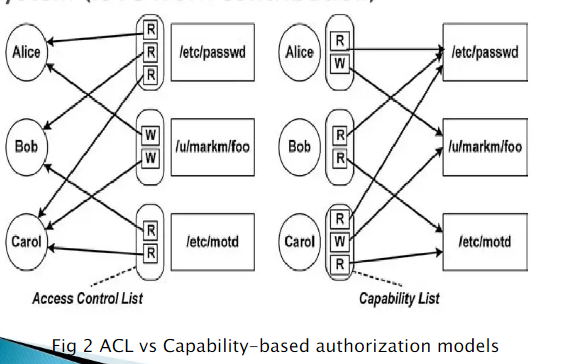
The third level (User level cognitive framework) isresponsible for interaction with User/stakeholders.

The cognitive management frameworks will recordthe users needs and requirements (e.g., humanintentions) by collecting and analyzing the userprofiles, stakeholders contracts (e.g., Service LevelAgreements) and will create/activate relevantVO/CVOs on behalf of the users.

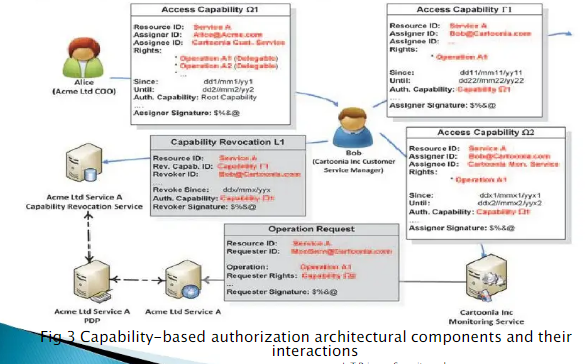
2. IoT@Work capability based access control system (loT@Work contribution)

The Internet of Things (IoT) envisages new security challenges,including in the area of access control that can hardly be met byexisting security solutions.

Indeed, IoT is a more demanding environment in terms ofscalability and manageability due both to the potentiallyunbounded number of things (resources and subjects), theexpected most relevant need to support the orchestration andintegration of different services, the relevance of short-lived,often casual and/ or spontaneous interaction patterns, therelevance of contexts, etc.



As shown in figure 2, a capability based systemreverses the traditional approach being now theuser in charge of presenting his/her/itsauthorization token to the service provider, whilein a traditional ACL or RBAC system it is theservice provider that has to check if the user is,directly or indirectly, authorized to perform therequested operation on the requested resource.

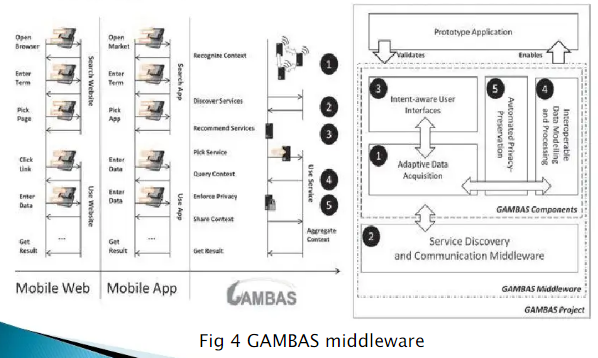


* TheCapBACarchitectural elements can be shortlycharacterized as follows
* The resource object of the capability
* The authorization capability
* The capability revocation
* The service/operation request
* The PDP (Policy Decision Point) is a resource-agnosticservice
* The resource manager
* The revocation service

3.GAMBAS Adaptive Middleware (GAMBAS Contribution)

The GAMBAS project develops an innovative and adaptivemiddleware to enable the privacy-preserving andautomated utilization of behaviour-driven services thatadapt autonomously to the context of users.In contrast to today’s  mobile information access, which isprimarily realized by on-demand searches via mobilebrowsers or via mobile apps, the middleware envisionedby GAMBAS will enable proactive access to the rightinformation at the right point in time.

As a result, the context-aware automationenabled by the GAMBAS middleware willcreate a seamless and less distractiveexperience for its users while reducing thecomplexity of application development.



As indicated in Figure 4, the core innovations realized byGAMBAS are the development of models andinfrastructures to support the interoperable representationand scalable processing of context, the development of ageneric, yet resource-efficient framework to enable themultimodal recognition of the user’s context, protocolsand mechanisms to enforce the user’s privacy as well asuser interface concepts to optimize the interaction withbehaviour-driven services.

* Security and privacy is based on the followingelements.
* Personal acquisition and local storage
* Anonymised data discovery
* Policy-based access control
* Secure distributed query processing

4.IoT-A Architecture (loT-A Contribution)

  Security is an important cornerstone for the Internet of Things(IoT).

This is why, in the IoT-A project, we deemed as very importantto thoroughly address security and privacy issues in variousaspects.

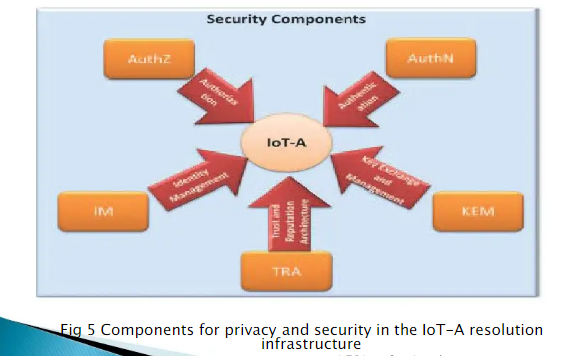
A set of requirements based on the input of external and internalstakeholders was used as a basis for the identification of themechanisms and functionalities that guarantee user data privacyand integrity, user authentication, and trustworthiness of thesystem.

These functionalities were analysed and orchestratedin Functional Groups (FG) and Functional Components(FC) in the frame of WP1.

High-level PS&T specifications were integrated in theframe of the IoT-A Architectural Reference Model(ARM) and then passed to vertical WPs dealing withcommunication protocols (WP3), infrastructureservices (WP4) as well as hardware aspects (WP5).

5.Governance, Security and Privacy in the Butler Project (Butler Contribution)

The goal of the BUTLER project is the creation of anexperimental technical platform to support thedevelopment of the IoT.The main specificity of the BUTLER approach is itstargeted “horizontality”: The vision behind BUTLER isthat of a ubiquitous IoT affecting several domains ofour lives (health, energy, transports, cities, homes,shopping and business) all at once.



The BUTLER platform must therefore be able tosupport different “Smart” domains, by providing themwith communication, location and context awarenessabilities,  while guaranteeing their security and theprivacy of the end users.The issue of security and privacy is therefore centralin the BUTLER project and develops in severalrequirements, the main requirements relate to:

* Standard issues of data security
* The application enabled by the IoT may pose
* additional privacy issues
* However, Privacy and Security do not only referto security of the exchange of data over thenetwork but shall include
* Protection of the accuracy of the data exchanged
* Protection of the server information
* Protection of the usage of the data by explicit
* Selected disclosure of DataThe implementation of“Transparency of data usage”

**SMARTIE**

The Internet of the Future will be an essential part of theknowledge society and will provide new information-basedbusiness.

The usage of the Internet of Things for large-scale,partially mission-critical systems creates the need toaddress trust and security functions adequately.

The usage of the Internet of Things for large-scale,partially mission-critical systems creates the need toaddress trust and security functions adequately.

This framework is envisioned to enable end-to-endsecurity and trust in information delivery fordecision-making purposes following data owner’s privacy requirements.

**New challenges identified for privacy, trust andreliability are:**

Providing trust and quality-of-information inshared information models to enablere-use acrossmany applications.

* Providing secure exchange of data between IoTdevices and consumers of their information.
* Providing protection mechanisms for vulnerabledevices.

SMARTIE will address these challenges withinthe context of Smart Cities.

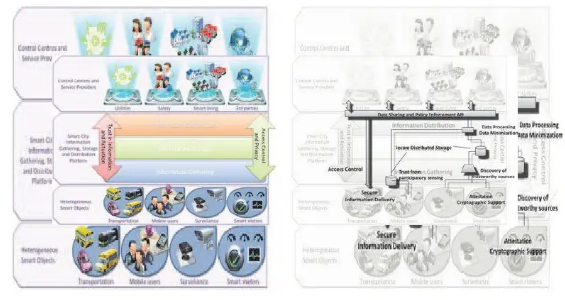
SMARTIE envisions a data-centric paradigm, whichwill offer highly scalable and secure information forsmart city applications.The heart of this paradigm will be the“information management and services” plane as a unifyingumbrella, which will operate above heterogeneousnetwork devices and data sources and will provideadvanced secure information services enablingpowerful higher-layer applications

**5.Security, privacy and trust in IoT- data-platforms for smart cities**

One of the main aims of Smart City technologies is to provide differentoptimization mechanisms for different aspects of data management.Data is gathered from various sources owned by different administrativedomains.

Noteworthy parts are data from public and private transportationproviders, data from mobile users, captured for instance with their smartphones, surveillance data and videos from private and publicorganisations and a vast amount of sensors and meters, attached tomachines and infrastructures, distributed throughout the city

All this information is stored in a variety ofdifferent places, for instance it can remain locallyin the sensors or company internal databases, insocial networks, in data storage located in privatedata centres or even in a public cloud storageservice.



Also actuation decisions can be taken in acoordinated way between multiple controlcentres or data providers.

Hence it is clear that there is a need of aninformation sharing platform in which data flowsfrom various sources and from differentadministrative boundaries need to be treated in asecure and privacy preserving way.

To ensure this, security and privacy need to bepart of the platform by design and may not beadded later on.

Risk to smart city loT platform

We predict that smart city data will eventually be stored inthe cloud and employ cloud computing techniques, due tothe high scalability of resources and computingperformance and reduced cost in maintenance andoperation. In this case, the smart city management system inheritsalso the security and privacy risks of cloud computing, forinstance the compromise of cloud servers or data abuse byinsider attacks.

Additionally the Smart Cities infrastructure is alsointeracting with sensors and actuators in order to gatherdata and control critical infrastructure functions.

This clearly requires to authenticate and authorize theaccess and to provide trusted information in a secure andprivacy-preserving way.

These examples and developments show the importanceof security, privacy and trust in smart city applications.

SMARTIE will focus on challenges that concern privacy,security and trust of the information available in the smartcity.

* Attacker can simultaneously attack on multiple layers:
* Manipulate the sensor measurements to infiltrate the systemwith wrong data, e.g. to cause certain actuations
* Attack the sensors and actuators physically to obtain credentials
* Attack or impersonate network components to act as a man-in-the-middle

**6**. First step towards a secure platform

Past and current projects, such as UbiSec&Sense,SENSEI, WSAN4CIP provide already some solutions onwhich a platform as outlined above can build. We present in this section certain components, whichcan be used as building blocks, but also componentsthat need further development to be suitable for thetype of platform SMARTIE aims for.

Trust and Quality-of-Information in an Open Heterogeneous Network

  In SMARTIE and in other IoT systems, systemsbelonging to different owners need to cooperate.Such a cooperating system can be denoted as asystem of systems (SoS). It is an entity composed of independent systems thatare combined together in order to interact andprovide a given service, which cannot be provided bythe individual systems when not cooperating.

The major properties of SoS especially for applicationfields as those intended in the SMARTIE project aredependability, security and privacy.

Dependability comprises the following attributes:

* Availability
* Reliability
* Safety
* Integrity
* Maintainability

Privacy-preserving Sharing of loT Data

To the large extent, the IoT data may be of personalnature and therefore it is important to protect it fromunauthorised entities accessing it. Privacy is one of the most sensitive subjects in anydiscussion of IoT protection Therefore, data privacy is one of the crucial aspectsof IoT. The amount of data generated by IoT will be huge.

Single pieces of information, i.e., single measurements, inmost cases do not represent a significant threat for theowners of IoT devices (temperature at a location, evenheart rate of a person at a given moment).

However, given that the devices are generating data continuously, it is obvious that unauthorized access to such wealth of data can cause significant problems andcan be used to harm the owners of the data (and possiblyothers, depending on the context of the data).

Therefore, it is of paramount importance to protectaccess to IoT data.On the other hand, the power of IoT lies in the abilityto share data, combine different inputs, process itand create additional value.

Hence, it is equally important to enable access todata generated by other IoT devices, while preventingthe use of data in un-authorized or undesired ways.

The fundamental privacy mechanisms lie in theintelligent data management so that only therequired data is collected.

Detecting the redundancy, data is anonymised at theearliest possible stage and then deleted at theearliest convenience. Furthermore, the processing of collected data willhave to be minimised according to a strict set of rulesso that it cannot be re-used.

7.SMARTIE approach

SMARTIE will design and build a data-centring informationsharing platform in which information will be accessedthrough an information service layer operating aboveheterogeneous network devices and data sources andprovide services to diverse applications in a transparentmanner.

It is crucial for the approach that all the layers involveappropriate mechanisms to protect the data already at theperception layer as well as at the layers on top of it.

These mechanisms shall cooperate in order toprovide a cross-layer holistic approach.SMARTIE will focus on key innovations thatstrengthen security, privacy and trust at differentIoT Layers as below:

* Applications
* Information Services
* Network
* Smart Objects

**Smart transportation:**

 1.**Smart city objectives**

Improving the management of the public transportationnetworks to foster greater use of sustainable transportmodes and to provide time and cost benefits to travellers.

Involving user smartphones in order to include additionalinformation related to their travels.

Improving the management of individual motor car traffic,to reduce travelling time in the town, improve traffic flowand reduce fine dust pollution.

**1.*Smart city objectives***

Extending traffic control systems with mobile trafficcontrol systems to react fast on abnormal situations,planned ones (e.g. road reconstruction) and alsounplanned ones (e.g. accidents).

Exploiting heterogeneous wireless sensor networks placedon public transport vehicles and in the environment(streets etc.) e.g. stationary traffic sensors/actuatorsplaced at cruces of the transportation network.

**2.*Usage***

Public transportation companies monitor the current demand oftravellers for public transportation for certain routes and optimise thenumber of vehicles to match the demand. They also monitor location ofall public vehicles.

Travel plan component located on the cloud infrastructure calculates thebest routing option for the traveller taking into account the travellerlocation, expected arrival times and current traffic conditions.

This information is then forwarded to the associated smartphoneapplication and presented to the traveller.

City traffic authorities monitor the current trafficconditions:

* To optimise the traffic lights in order to achieve bettertraffic
* flow.
* To adapt speed limitation signs.
* To indicate detours in case of road re-construction,accidents
* or other emergency situations.

**Smart campus**

**1.*Smart city objectives***

Monitoring energy efficient in the campusconsidering energy consumption and energygeneration.Evaluating real-time behaviour of systems jointlyacting as a sustainable ecosystem.Providing the user capability to interact with thesystem to facilitate the improvement of the energyefficiency.

**2.*Usage***

Energy Supervisor entity will be able to collect from thedifferent sources: information in real time about buildingconsumption and energy generation from the differententities involved (photovoltaic generators).

Energy Monitoring entity will collect data from the sensorsbeing deployed and also data aggregated and summarizedabout the different energy producers to take decisionsover different actuators involved in the system.

Energy Producer will provide data aggregated to the EntityMonitoring based on the agreement established and willprovide more detail data to the Energy Supervisor as mainregulator.User will provide in certain situations their positions andpresence information to the Energy Monitoring entity bymeans of the sensor within the building or light-streetpathways.

**3.*Security and privacy challenges***

Access to the data of the sensor should be controlledbased on access control and privacy rules. Hence onlycertain services of the entity monitoring could read or actover them especially in the case the monitoring entity is athird party.The exchange will require mechanisms including dataprotection and integrity in the transfer between thedifferent parties.

  Scalable and secure management protocol which lets theverification and authentication of new sensors deployed andensure the extension of the trust domain to new devices in thedeployment environment.

Entities are actually restricted to use the data based on thenational protection data law. They will like to explore how toreuse the data and possible being able to share to third partiesbut also controlling what can be shared based on legislation.