1st International Electronic Conference on Sensors and Applications

Automatic system for providing security services in the Internet of Things applications over Wireless Sensor Networks

Authors:

J.A. Sánchez Alcón: jose.asanchez-alcon@.upm.es

Lourdes López: lourdes.lopez@upm.es

José-Fernán Martínez: jf.martinez@upm.es

Pedro Castillejo: pedro.castillejo@upm.es

INDEX

1.- Our team

2.- The problem

3.- Objectives

4.- Proposal

5.- The key elements

6.- Expert System Functional Blocks

7.- Testing scenario

8.- Results

9.- The next steps

Our team

POLITÉCNICA "Ingeniamos el futuro"
CAMPUS DE EXCELENCIA INTERNACIONAL

citSem POLITÉCNICA Centro de Investigación en Tecnologías del Software y Sistemas Multimedia para la Sostenibilidad

GRyS
Group of Next-Generation Networks and Services

Our job

THE PROPOSAL:

Automatic system for providing security services in the IoT applications over WSN

CONCEPTS ARE TESTING OVER AWARE ENVIRONMENT, AND THEY ARE WORKING TOGETHER

AWARE PROJECT

BOLETÍN OFICIAL DEL ESTADO
Núm. 23 Viernes 27 de enero de 2012 Sec. III. Pág. 7931

Partiality funded: TEC2011-28397: AWARE
ACCESSIBLE WEARABLE DEVICE PLATFORM FOR SMART ENVIRONMENTS

GOBIERNO DE ESPAÑA MINISTERIO DE ECONOMÍA Y COMPETITIVIDAD

The problem

Security and privacy can be a problem for market and society.

New IoT Service. It should to consider:

- The appropriates security solutions for privacy.
- Resources limitations
  - Battery
  - Memory
  - Processing
  - …..
- Great diversity of legislative frameworks all around the world.
- *Changes in use cases may alter the legislative framework too*.

DIVERSIY OF APPLICATIONS WITH THE SAME PRODUCT

Different uses cases → **Different impacts on data protection**

Dairy facilities

Horse race

THE SAME PRODUCT

Monitoring Belt

Supervise the health for firemen activity

Soccer team

Objectives

Avoiding the user's **negative perception** with the IoTs technologies about security and their privacy.

To do an automatically determination process.

- About security services and privacy protections
- For products and services on the Internet of Things
- For products and services over Wireless Sensor Network

Proposal

To go beyond for the art state over this topic.

To find the best solutions based on an Expert System.

It is based on the knowledge generated by the involved areas

- Skilled persons with knowledge on Business area
- Skilled persons with knowledge on Juridical area.
- Skilled persons with knowledge on Technological area.
- All these knowledge working together to give the best solutions for people.

The key elements

- "Utility Matrix" as a main concept to link all interests of stakeholders regarding their security needs.
- The expert system has been divided in three parts.
- All of these interacting each other by interchanged information.
- Each part processes its own knowledge to give answers.
- To obtaining (based on “Utility Matrix”) the legal imperatives and dataset to protect.
- To collect the security mechanisms available in the last state of art.
- To select the most efficient solutions as a security policy.
- This proposal will connect the Industrial, Judicial and Technological areas working together.

Expert System Functional Blocks

Automatic system for providing security services process stages				
Stage	**Functional Blocks**	**INPUT**	**KNOWLEDGE DATABASE**	**OUTPUT**
1º	**Business (BES)**	Services Requirements	Business Knowledge structure	Utility matrix Personal data involved
2º	**Legal (LES)**	Utility matrix + personal data involved	Laws, standards	Legal Imperatives Sensitive information
3º	**Technological (TES)**	Legal Imperatives over sensitive information	Attacks, security services, mechanisms, …	Security services & mechanisms over information pieces.
4º	**Business BES)**	Security services & mechanisms over information pieces.	Business Knowledge structure	Final decision over security strategy to apply over network elements
5º	**Legal (LES)**	Final decision	Validity check	Legal certification is emitted to BES. One message is sent to TES for register.

Testing scenario

- The Expert System provides security policy.
- A middleware service oriented platform (AWARE) to configure security services over WSN.
  - AWARE middleware architecture is based on the *nSOM*, composed by three abstraction layers named:
    - Wireless Sensor Node Platform
    - Service-Oriented Software Platform (SOS)
    - Service Composition Platform (SCP)
  - The security system was deployed as a service inside the SOS layer.
  - The security service can be used by the upper layer (SCP) to compose new secured services.
- Sensors for monitoring human health status.

Results

1. Data identity and measures must be hidden.
2. Data have to be unknown by non-authorized people.
3. System nodes have to always be controlled and known (no intruders).
4. Non-authorized people and non-authorized systems must not access personal data.
5. Transmission data must not to be done in broadcast.
6. Historical data and results have to be protected. (Encrypted, or split data in DB).
7. Data must be protected in standalone mode. In memory overflow, Alarm/Alert data must be preserved.
8. During standalone mode, visual or audible alarm/alert must be generated.
9. If one node leaves the system, data must be discharged before and erased.

Imperatives for personal data LOPD in Spain.

SERVICES		
Nº	**Service**	**Information**
1	Confidentiality	All data
2	Confidentiality	Personal Identity
3	Authentication	Access Control List (ACL)
4	Authorization	Access privileges
5	Authentication	Node identities.
6	Confidentiality	Database in server
7	Integrity	Measures, health alarms and alerts
8	Availability	
9	Confidentiality	

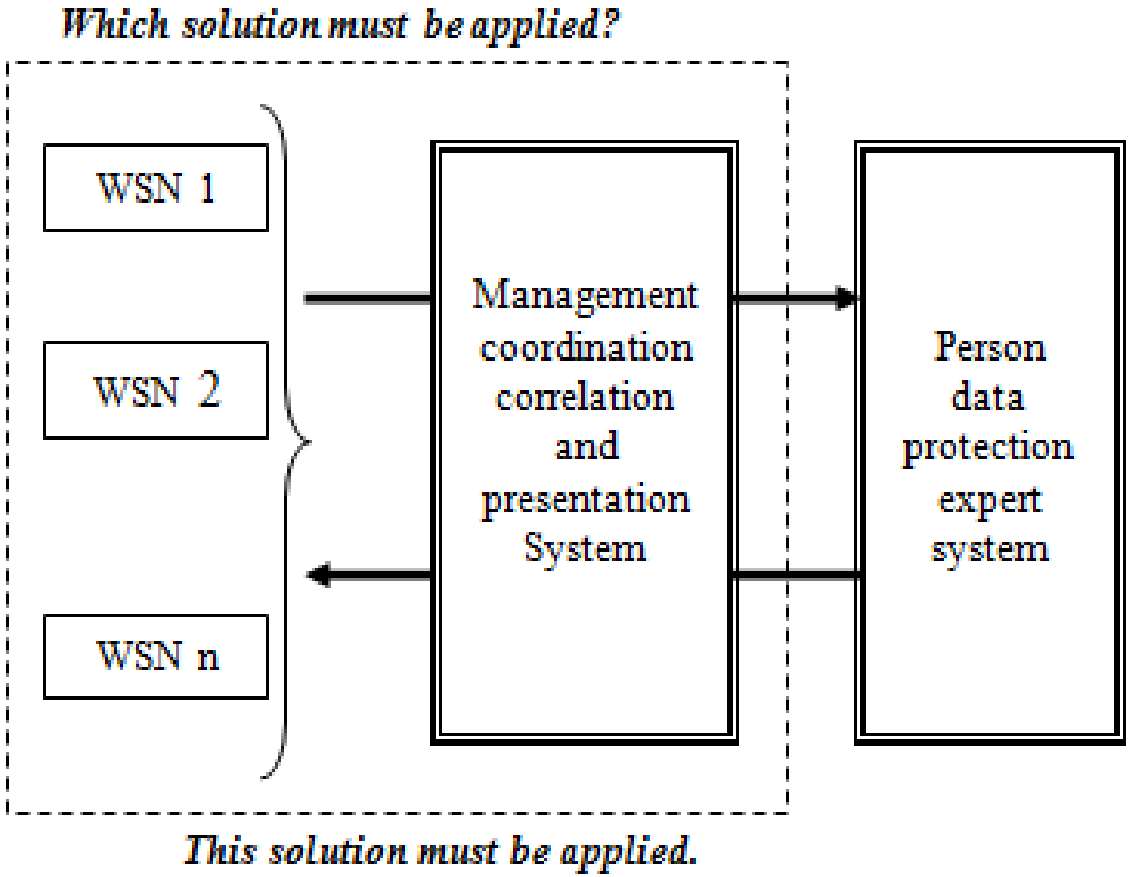
USES CASES				
Security requirements	**Cow milk farm**	**Horse races**	**Soccer team**	**Firemen**
Options chosen	4	3; 4	2; 3; 4; 5; 6; 9	2; 3; 4; 6; 7; 8; 9

Information involved

- About Services Requirements:
  - Environment information: country, service type, ….
  - Service structure: Data collecting areas, aggregation, resources limitation, ...
  - Monitored data: Collected information.
  - Service data: Management data for service.
  - Stakeholders requirements
  - Other service requirements: Continuity ….
- Important information for LES is sent inside Utility Matrix.
- All these information along with the Knowledge bases should be enough for processing.

Security and Privacy Management

In a large IoT environment, the intelligence for security and privacy management could be insert on the Network Operation Centre (NOC).



The next steps

Promoting ways of collaboration with Phd students and their thesis directors.

- Judicial area.
- Company area.
- Some other security experts

Next year we will perform some test over real services being developed.

Thanks for your attention