A systemic and cognitive approach for IoT security

Arbia Riahi, Enrico Natalizio, Yacine Challal, Nathalie Mitton, Antonio Iera

A systemic and cognitive approach for IoT security

Arbia Riahi*, Enrico Natalizio†, Yacine Challal†, Nathalie Mitton‡, Antonio Iera§
* VRIT Lab - Military Academy of Tunisia, Nabeul, Tunisia. e-mail: arbia.rahi@ati.tn
† Lab. Heudiasyc, UMR CNRS 7253, UTC, France. e-mail: *name.lastname*@hds.utc.fr
‡ Inria Lille - Nord Europe, France. e-mail: nathalie.mitton@inria.fr
§ Universitá "Mediterranea" di Reggio Calabria, Italy. e-mail: antonio.iera@unirc.it

***Abstract*—The Internet of Things (IoT) will enable objects to become active participants of everyday activities. Introducing objects into the control processes of complex systems makes IoT security very difficult to address. Indeed, the Internet of Things is a complex paradigm in which people interact with the technological ecosystem based on smart objects through complex processes. The interactions of these four IoT components, *person, intelligent object, technological ecosystem,* and *process*, highlight a systemic and cognitive dimension within security of the IoT. The interaction of people with the technological ecosystem requires the protection of their privacy. Similarly, their interaction with control processes requires the guarantee of their safety. Processes must ensure their reliability and realize the objectives for which they are designed. We believe that the move towards a greater autonomy for objects will bring the security of technologies and processes and the privacy of individuals into sharper focus. Furthermore, in parallel with the increasing autonomy of objects to perceive and act on the environment, IoT security should move towards a greater autonomy in perceiving threats and reacting to attacks, based on a cognitive and systemic approach. In this work, we will analyze the role of each of the mentioned actors in IoT security and their relationships, in order to highlight the research challenges and present our approach to these issues based on a holistic vision of IoT security.**

I. Introduction

Incorporating IoT into our lives introduces many benefits into several domains such as health-care, transportation, safety and business. With the uninterrupted evolution of technology, new opportunities have been created to set up new experiences and practices in our everyday life. Information and intelligence became distributed and passive entities are turning out to be active participants of our lives when connected to the Internet. In this new context, it became possible for objects, services and applications to make decisions and to react according to a given situation in their environment.

As the IoT deals with a huge number of *things* and their relevant data, many security challenges have to be addressed. This is true especially when things need to interact with each other across other set of things, through many security techniques and according to different policy requirements [1]. For example, many attacks can occur such as message modification, traffic analysis, Denial of Service, eavesdropping, Sybil attack and so on. In order to avoid these threats and to permit authorized use only, current research efforts have been focusing on the following areas [4]: protocol and network security, data and privacy, identity management, trust and governance, fault tolerance, dynamic trust, security, and privacy management.

As a possible holistic methodology to include all these aspects in a coherent framework, we propose a systemic and cognitive approach for IoT security. Compared to the analytic approach, our vision may lack theoretical rigor, but a more flexible approach can be required in decision making when accomplishing a given action or reaction. In fact, we believe that a particular attention should be paid to the interactions among the different system elements and the effects of these interactions on the global perception. In fact, rather than focusing on the analysis of each single subsystem of things, the focus of the research should be on the practical results of the system behavior and on the validation of the developed models through a direct comparison with the real systems. For all the mentioned reasons, and due to the large number of interactions between things, a systemic and cognitive approach seems to be an appropriate choice for IoT security.

In this trend, former research activities were performed to propose a systemic approach for security in organizational framework. The authors in [2] state that a two-dimensional model made up of people, process, and technology is not feasible for organizational context. To become fully secure, they propose a three-dimensional pyramid-shaped model, where *process*, *people*, *technology* and *organization* are at the vertexes. We include in our approach also a *cognitive* dimension in order to give the flexibility to the system to be able to analyze different situations and perform the most suitable measures to guarantee reliability and security. In our systemic and cognitive vision, the interactions among nodes are dynamic and complex. Thus, they are called *tensions* and they require a special attention when detailed. In [3], we proposed a 2D vision of our systemic approach for IoT security, based on [2]. In this work, we will extend our former proposal [3] towards a 3D system highlighting new functional plans of security.

In Section II of this paper, we will detail the proposed approach including overall structure, components and relationship among elements. In section III, we will define each node of the system. Section IV is intended to show the dynamic relationships between different nodes, known as *tensions*, and to present possible research issues for each tension. In Section V, we will discuss open research issues and future trends for IoT security framework to conclude the paper.

*This work has been carried out in the framework of the Labex MS2T, which is funded by the French Government, through the program "Investments for the future", managed by the National Agency for Research (Reference ANR-11-IDEX-0004-02).

II. Our Vision of security in IoT

The systemic and cognitive approach for IoT security, illustrated in Fig. 1 is made up of four nodes, namely *person*, *people*, *technology*, and *intelligent object*. To guarantee conformity in conception and implementation of secure applications, all these nodes must cooperate. The inclusion of the *intelligent objects* into such a complex system is a delicate issue for many reasons. First, this inclusion increases the complexity of the control process considerably. Second, the interaction between objects and people is difficult to address due to the increasing number of connected objects per person, the different levels of data sensitivity and security requirements. Finally, omnipresent objects lead modern technology to new applications and new services. Consequently, the resulting computing environment may involve humans, computers, sensors, RFID tags, network equipments and protocols, system software, and applications.

The connections among the nodes are dynamic and complex because they follow the environment characteristics. We refer to these connections as *tensions*. Tensions emphasize their roles of cooperation/conflict between the nodes. By modelling each tension and once the main actors of a security issues are identified, it will be easier to define the adequate solution by using our approach. Special interest must be given to understand these tensions and their security requirements. We name seven tensions between nodes: *identification*, *trust*, *privacy*, *reliability*, *responsibility*, *safety* and *self-immunity*.

To explain the difference between node and tension, we present an example of IoT application in a smart environment to ensuring comfortable services. We consider a scenario that involves a home owner, who plays the role of **people**, sensors and actuators within the house perform the role of **intelligent objects**, communication means and protocols depict the **technological ecosystem** and remote monitoring of heater represents the **process**. In this scenario, the home owner needs to **identify** the right sensor or actuator to adapt the ambient temperature to her preferences. The actuator has to **trust** the originator of the command to react correctly. Also, in order to avoid irresponsible people's mistakes, **responsibility** must be attributed to the right people. This process should not involve anyone else, then, **privacy** must be guaranteed. **Safety** of people and equipment when performing this action must be a priority to protect people's health. Finally, the smart object must ensure its **immunity** against physical or logical intrusion.

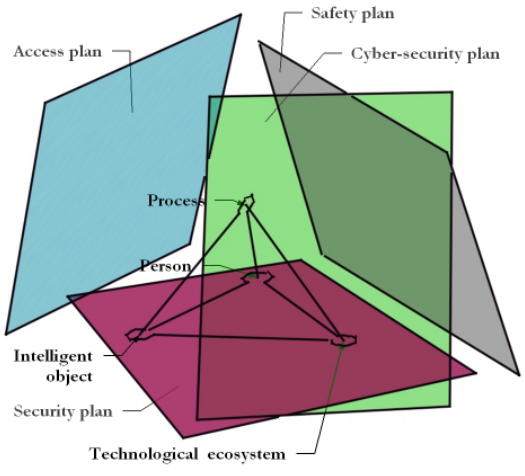


Figure 1. The proposed approach and its main elements.

In Fig. 1 we present also the four planes within which the interactions among the nodes take place through the tensions that are visible in Fig. 2, where we give a 2D perspective of each group of nodes. These planes are specified according to the relationships among the different triads of nodes.

The *Safety* plane (Fig. 2(a)) concerns process, person and technological ecosystem and involves the following tensions: privacy, safety and reliability. In this plane, the *technological* choice made by a *person* to perform a given *process* like analyzing, storing or distributing data must be done in a *safe* and *reliable* manner. The use of this approach during operations as process design, process change, operation and maintenance practices, incident reaction/response planes, etc. must respect *privacy* constraints in the overall IoT environment.

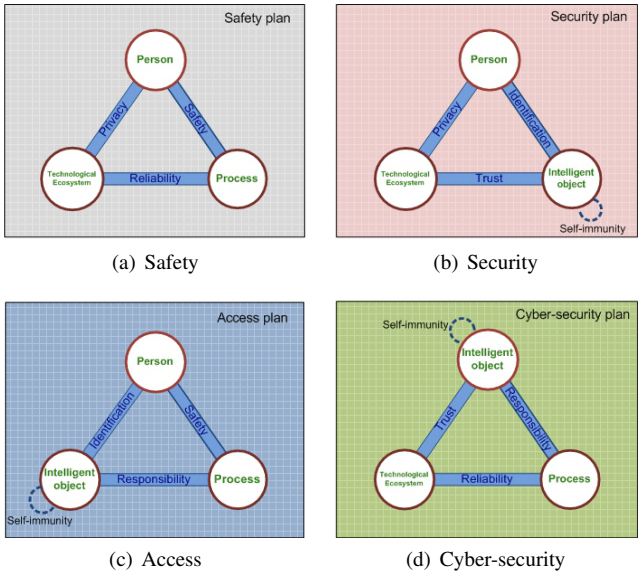
The *Security* plane (Fig. 2(b)) includes person, technological ecosystem and intelligent object and details related tensions namely: trust, privacy and identification. In the IoT, all kinds of *objects* and equipment are connected together through different *technologies* and networks. Then, *users* can profit to develop and benefit from new services and applications. However, it is imperative to *identify* various intervening entities rigorously, meet *privacy* requirements of users and data, and establish robust mechanisms of *trust management* to avoid access right violation and other privilege-related attacks.

The *Access* plane (Fig. 2(c)) contains process, person and intelligent object and implies their connected tensions: identification, safety and responsibility. The *intelligent objects* are able to interact with other networked entities (objects and/or *persons*) and store information related to a specific *process*. This interaction must be developed in a fluent manner that (i) *identifies* correctly the intelligent objects, (ii) respects *safety* rules of humans and equipment and (iii) precises convenient access rules and *responsibilities* for each entity. This is of great importance especially in ubiquitous environment where the presence of objects and humans can not be controlled.

The *Cyber-security* (Fig. 2(d)) plane includes process, technological ecosystem and intelligent object. The tensions considered for this plane are responsibility, trust and reliability. The objective is to produce an effort to ensure security properties of the IoT cyber environment against security risks. For example, testing the *process* operation and *technology* necessary to deploy security procedures during *intelligent objects* interaction is a serious task. The *reliability* of the equipment and communication means must be guaranteed, *trust management* techniques between intelligent objects must be implemented and *responsibility* states must be attributed.

III. Nodes

In this Section we show the main features of the actors involved in our model, namely: person, process, technological ecosystem and intelligent object, and we highlight the role of each actor in our vision.



(a) Safety (b) Security

(c) Access (d) Cyber-security

Figure 2. Projections of the 3D-pyramid on each of the planes.

A. Person

Security concerns are always depending on people's interest and intentional/unintentional behavior. The human resource is always involved in all the processes as a cause and/or an effect. Then, it is considered as the most basic node in the model. However, it is very difficult to control and to deal with people having different expectations, behaviors and technical knowledge. In fact, they must be conscious of the necessity of having security background including objectives, risks, practices, choices, loyalties and skills.

Concretely, humans must accomplish the tasks related to security rules management, which consists of:

- Addressing security practices and rules to develop an efficient *security policy* documentation.
- Auditing security practices and rules effectiveness including personnel, documentation and technical control procedures.
- Implementing practices and rules in operational mode.

B. Process

The process node is about a mean or a way to perform tasks in the IoT environment according to specific security conditions. Process must be in accordance with effective security policies to guarantee a sufficient level of security at different IoT architecture layers. Also, we agree that security practices are awkward to put into effect due to the sophistication of the model and the presence of various constraints that originate from the process node. In this trend, the Federal Financial Institutions Examination Council's (FFIEC) has defined a set of standard areas to consider when performing a secure process[1]:

- Information Security Risk Assessment.
- Information Security Strategy.
- Security Controls Implementation.
- Security Monitoring.
- Security Process Monitoring and Updating.

Practically, a secure process must widely fit the requirements of policies, standards, strategies, procedures and other specific documentation or regulation. A convenient compromise has to be set up between complexity of the processes and intended security conditions.

To explain the previous idea, let us consider the example of a smart home context. Requirements may vary from a simple network to a complex structure. In a family's home, objects such as windows, doors and electrical equipment may have simple sensor or RFID tag that communicate with other devices for commanding and controlling the whole house. On the other hand, this command and control device can interact with other devices, through a simple network or a complex architecture, to allow the family members to access and control their objects remotely. Consequently, process complexity is different from the first case to the second.

C. Technological ecosystem

The third node is about the technological alternatives taken to guarantee acceptable IoT security level. In [2], authors describe five categories of information security elements:

- Security Design and Configuration;
- Identification and Authorization;
- Enclave internal;
- Enclave boundary;
- Physical and environmental.

Decision made about the above elements may concern communications infrastructures and protocols, system architecture, implemented algorithms, access control methods, etc. Obviously, a compromise between security conditions, technical constraints and technology advancements should be held to ensure an adequate level of security and an acceptable performance of IoT system.

The large number of possible IoT applications needs a software development framework that permits joining applications, command, control processing, routing processing and security. An extensive, reusable and accessible ecosystem is highly recommended, and represents the key success factor to permit the development of IoT nodes and applications. In the same vision, a special interest need to be granted to communication choices since data and commands may be remotely generated and handled. According to (i) data format (data unit structure: frame, cell, packet or segment), (ii) data content (user data, control data, etc.), (iii) application requirements (priority, error tolerance, real-time constraints, etc.) (iv) physical infrastructure (topologies, transmission media, etc.), (v) technological choices (WiFi, ZigBee, etc.) and many other conditions, convenient selection needs to be made.

D. Intelligent object

The intelligent object is quite a new node that refers to an object like a sensing node (camera, X-ray machine, etc.), an RFID reader or tag (detecting the presence of a person, an animal or an object) involved in a given application. This object is enhanced by electronic features to interact with other objects. It becomes able to collaborate, share and exchange

[1] http://www.ffiec.gov

information about its environment, and react to specific events by performing adequate functioning. It is worth to mention that security practices conception of these objects has necessarily to consider their pervasive character to address the adequate security levels.

These nodes will have a unique ID and can be controlled separately. A practical case may include a smart-phone with RFID and GPS features that can interact with RFID/GPS enabled objects in a vehicle or a building, to locate themselves within the environment. As a result, RFID and GPS terminal will be registered, commanded or controlled in a remote location of the IoT.

IV. Tensions

In this Section we give a detailed definition of each tension and the related open research issues.

A. Privacy

1) Definition: Privacy represents the tension induced by the interaction between person and technological ecosystem. Data to be protected are necessarily related to human beings, thus their privacy is a mandatory objective of the IoT, due to the omnipresence of intelligent objects. Also, the misuse of technology is a cause of privacy violation. In practice, many research activities have been led in the field of privacy management techniques and mechanisms. In [5], authors distinguished three main axes of research activities in data privacy, namely:

a) Privacy in data collection: IoT is a global vision rather than a specific technology. In data collection operation, IoT involves various technologies with different characteristics of energy, connectivity, capability and so on. Specifically, in IoT, data are collected from different components including RFID tags and readers, Wireless Sensor Networks, mobiles phones with 3G and WiFi connectivity, GPS terminals, etc. This openness may lead a direct effect on data privacy and may imply inevitable risks.

b) Privacy in data sharing and management: Obviously, a large amount of data is exchanged over the network between IoT components. These information are frequently human-centric and need to be correctly protected. From a practical point of view, infrastructures conveying these data may be shared between many entities or networks with different security policies and practices. Also, the frequent use of wireless communications and other diffusion-based networks may lead to data disclosure if adequate precautions have not been taken.

c) Data security issues: In the IoT, data may be stored and processed in the collection nodes. Lasting for a variable time in pipelines may lead to data integrity and confidentiality problems. Hence, adequate mechanisms need to be addressed to avoid these threats.

2) Open research issues: It is important to implement applications that respect the data minimization principle and give priority to data control rather then data collection. Then, there is a need of developing IoT standard to meet a sufficient level of security and privacy in practice. Finally, security mechanisms must be elaborated to allow users protecting their private data instead of expecting implemented mechanisms in IoT systems to respect their privacy. Many data anonymization techniques have been proposed in the literature. However, those technique are known to be extremely demanding in terms of CPU, energy and memory resources. Their implementation in the context of the IoT would be even more complicated. Therefore, new lightweight techniques are required to ensure data anonymization.

B. Trust

1) Definition: Trust, the second tension that we consider in our model, links the intelligent object with the technological ecosystem. In the literature, many definitions of trust have been proposed. The first definition focuses on reliability trust and describes it as "the subjective probability by which an individual, A, expects that another individual, B, performs a given action on which its welfare depends" [11]. Here, we notice the presence of two main concepts: dependency and degree of trust (probability). The major drawback of this definition is the fact that trusting in a person is not enough to assume complete dependency on that person. The second definition is interested in decision trust and stipulates that "Trust is the extent to which someone is willing to depend on something or somebody in a given situation with a feeling of relative security, even though negative consequences are possible" [12]. Here four concepts are involved, namely: dependency, reliability, utility and risk. The third definition talks about trust management and precises it as "an approach to making decisions about interacting with something or someone we do not completely know, establishing whether we should proceed with the interaction or not" [13]. This last two definitions give an adequate framework to study (i) security parameters like policies and credentials and (ii) trust relationships. Different models for trust management can be considered such as rule-based (access control in compliance with to security policy, and using a verification system like digital certificates), reputation and/or recommendation-based (depending on node reputation and experience) and social-networks based (privacy, friendship, honesty, and social reputation or recommendation).

In the IoT context, we notice severe resource constraints, and difficult technological choices. Special interest must be granted to trust management definition and operations including establishing, updating, and revoking credentials, keys and certificates. Also, we notice that current technological ecosystems guarantee the trust relationship between person and intelligent object. This is due to the fact that the IoT is an ubiquitous, changing and pervasive environment and it possibly implies the participation of non-human entities. Obviously, adequate trust relationship must be established between involved human and/or non-human entities to contribute to the success of system operation. This preoccupation has a inevitable effect on related technologies, practices, conceptions and applications.

2) Open research issues: Although many research activities have been performed in relation with trust management and IoT, some other issues can be explored. First, we can address foundational aspects: (i) solving the lack of general theory concerning trust in heterogeneous networks of humans and intelligent objects, and (ii) approaching the precise link between computational and behavioral trust in the IoT. Second,

it is convenient to put in operation trust mechanisms in cloud computing in order to manage relationship between entities. Third, it is useful to conceive reputation mechanisms, able to maintain protected services within a changing infrastructure. Fourth, we propose to encourage cooperation of humans and intelligent objects through self-reinforcing trust mechanisms. Close coupling of intelligent objects to humans should be profitable to better asses trust relationships through extrapolating existing human relationships (in a social network for instance) to trust relationships in the IoT.

C. Identification

1) Definition: The IoT envisions a huge number of devices (sensors, actuators, network equipment and so on), temporarily or permanently interconnected. In such conditions, identification and localization of a given object is a fundamental subject that concerns the general system operation including architecture, components, access rights, etc. In the literature, three main areas of research can be found. The first area is interested in multiple vs. unique identifiers: whether it is possible to use global unique scheme like IPv6 logical address or multiple identifier spaces. The former can offer a high flexibility of governance models but suffers from limited and critical Internet resources. The latter depends tightly on the interoperability of the used naming spaces. The second area is about identifiers vs. network addresses. The identifier represents the unique reference to the object, whereas the network address can change according to the physical situation of the entity, its affiliation to a given network or its actual function. The third area focuses on resolution and discovery mechanisms, such as Object Naming Service (ONS) and Object Directory Service (ODS).

2) Open research issues: When examining the amount of research activities achieved in this context, we get the impression that an adequate job has been done. However, there are still other issues to investigate. First, we can focus on collision problems of unique addresses in a global scheme and supporting dynamic networks, where devices can randomly appear and disappear from the network, or privacy constraints suggest to hide/reveal its identity. Second, since industries adopt proprietary identification schemes, a global identification system is required and needs to consider a large number of identification schemes. Third, network performance issues must be handled when localizing a given object among millions of devices. Fourth, the use of a hierarchical naming system (URL/URI) is not necessarily convenient for IoT frameworks where entities are often mobile. Fifth, automated discovery procedures are required for communication in changing network and topologies of the IoT. Finally, object owner identification through biometrics can be interesting means to avoid spoofing attacks.

D. Reliability

1) Definition: According to ANSI, software reliability is defined as "the probability of failure-free software operation for a specified period of time in a specified environment" [14]. In the IoT context, this tension can be considered when handling unique and reliable entities addresses, managing data over the network or in case of effective use of device(s) for specific applications.

2) Open research issues: Unlike previous tensions, research efforts are needed in this topic. In the soft reliability case, the compliance checking between preventive and reactive approaches, and prediction techniques need to be developed. Other issues that should be investigated concern the way to implement a reliable data processing on local devices, and the way woth which privacy can be guaranteed. Also, we can focus on analyzing and visualizing remote entity usage data and data management in different situations and over time [6].

E. Safety

1) Definition: In real life, autonomous systems became more widespread. Their control software can be the cause of a random or unpredictable behavior. A similar situation must be controlled to avoid disastrous consequences for the whole system and the physical environment. Furthermore, sensors are widely used to feed databases with important informations and signals. People may refuse participating in collective activities due to the privacy and safety concerns. Thus, safety seems to be a very important tension to avoid unexpected problems.

2) Open research issues: A number of research issues can be detailed here. We can elaborate an integrated safety knowledge base where we store safety constraints in a uniform layout. Also, we must define adequate mechanisms for collecting, extracting and interpreting safety data and develop a runtime safety constraints enforcement mechanism. Finally, IoT can be used to monitor environmental safety, building physical security and protection of products against counterfeit.

F. Responsibility

1) Definition: Responsibility is closely related to access rights or authorization privileges. For example, if a given IoT object is configured by one entity, it must be able to handle connections from other objects and distinguish their different access rights. Then, it grants authorizations according to these devices' access rights.

2) Open research issues: The research activities related to responsibility in IoT are considerable and consistent. After examining the main projects in this field, we can suggest the following future work. In relation with the IACAC (Identity Authentication and Capability Based Access Control) project [7], it would be possible to integrate the proposed protocol with an RFID middleware architecture in order to manage entities' identities in the IoT. Also, it is useful to specify and evaluate capability based access control propagation and revocation from a security point of view. Finally, interoperability seems an open issue that should be further investigated.

G. Self-immunity

1) Definition: Frequently, nodes are used in distant and/or hostile areas. They became unprotected and exposed to physical attacks due to the site constraints such as unreliability of available wireless communication links, resource limitations, insufficient physical protection of nodes, absence of a robust trust management system, etc. The potential risks can be related to privacy (inventorying or rogue scanning, backward/forward tracing or tracking) or to security (replay attack, tag counterfeiting or cloning, relay attack, man-in-the-middle attack, denial of service, reverse engineer of tags, etc).

Also, under a severe electromagnetic disturbance, the node may lose information packets, or may stop working [9].

Thus, defense mechanisms must be addressed. An example is the use of Intrusion Detection Systems (IDS)/Intrusion Prevention Systems (IPS). The standard operation in an IDS is the comparison between the current behavior of the system with its behavior in the absence of intrusions [8].

2) Open research issues: Self-immunity is a tension that needs more research efforts. First, it is interesting to develop efficient models for secure precision feedback. Second, we can think of a new intrusion detection system for heterogeneous networks like IoT. Third, we can imagine a mission-oriented IDS for IoT applications.

V. Discussion and conclusion

IoT is a novel concept, that involves different technologies, human and non-human entities. Some recent efforts have been made in the direction of designing and deploying unifying architectures. However, none of these attempts specifically aimed at proposing a holistic vision of IoT security. Also, practical solutions, if they exist, are intended to fulfill precise application needs (RFID, WSN, etc.). In the future, when attempting to realize a wide range of applications and services, it will become impossible to use a unique reference architecture model for real achievements. This openness and diversity require serious reflections concerning security issues. Our systemic and cognitive approach for IoT security remains still applicable even in the presence of the previously mentioned constraints and limitations of the IoT paradigm.

In the previous sections, we presented the open issues related to the tensions between the constituting components of our scheme. In the following, we group some of the mentioned issues according to their importance for future IoT systems along with other relevant and unmentioned issues.

Solving the *lack of standardization* and modeling foundations represent an a priori issue. Technical and interoperation details of the intended model need to be provided for architecture composition, available interfaces, communication protocols and algorithms. More precisely, additional efforts must be done to solve the limitation problem of *identification* standards. In the same direction, robust and lightweight mechanisms of objects and persons *authentication* must be developed in compliance with IoT characteristics. From an access control point of view, we can focus on *security policies management* like access rights definition, modification and execution. Conflicting problems between security rules and practices have to be solved in a complicated and evolving IoT environment. Also, applications using computational or behavioral *trust* according to a lightweight access control model are of great importance. Concerning the *privacy*, we can consider aspects like secure storage and privacy protection of massive and distributed data. Other issues may concern schemes development of privacy preserving techniques taking into consideration data sensitivity and context's constraints. Finally, it is of interest to focus on IDS operations as a possible realization of *self-immunity* concept. This may include secure precision feedback techniques, mission-oriented IDS and IDS for heterogeneous networks [10].

To conclude, in this work, we proposed a systemic and cognitive approach for IoT security which can be represented by a triangular pyramid, whose vertexes are: person, technological ecosystem, process and intelligent object. We used four planes to distinguish the interactions between every triad of nodes of the system. First, we gave the definition of the different planes, and explained the role of the nodes. Then, we detailed the objective of each tension of the model and the possible research issues in its context. We concluded the work with a brief discussion summarizing the research challenges.

References

[1] H. Sundmaeker, P. Guillemin, P. Friess, S. Woelfflé, "Vision and Challenges for Realising the Internet of Things", CERP-IoT - Cluster of European Research Projects on the Internet of Things, 2010.

[2] L. Kiely, T. Benzel, "Systemic Security Management: A new conceptual framework for understanding the issues, inviting dialogue and debate, and identifying future research needs", Institute for Critical Information Infrastructure Protection (ICIIP), 2008.

[3] A. Riahi, Y. Challal, E. Natalizio, Z. Chtourou, A. Bouabdallah, "A Systemic Approach for IoT Security," , 2013 IEEE International Conference on Distributed Computing in Sensor Systems (DCOSS), pp.351,355, doi: 10.1109/DCOSS.2013.78IoTIP, Boston, USA, May 2013.

[4] R. Roman, P. Najera, J. Lopez, "Securing the Internet of Things", IEEE Computer, vol. 44, no. 9, pp. 51-58, DOI: 10.1109/MC.2011.291, September 2011.

[5] C. C. Aggarwal, P. S. Yu, "Privacy-preserving data mining: models and algorithms", ISBN 978-0-387-70992-5, Springer, 2008.

[6] M. Funk, "Model-driven Design of Self-observing Products", PhD dissertation, ISBN: 978-90-386-2427-3, 2011.

[7] P. N. Mahalle, B. Anggorojati, N. R. Prasad and R. Prasad, "Identity Authentication and Capability Based Access Control (IACAC) for the Internet of Things", Journal of Cyber Security and Mobility, Vol. 1, 309Ű348, 2013.

[8] C. Liu, J. Yang, Y. Zhang, "Research on Immunity-based Intrusion Detection Technology for the Internet of Things", Seventh International Conference on Natural Computation, DOI 10.1109/ICNC.2011.6022060, 2011.

[9] R. Acharya, K. Asha, "Data integrity and intrusion detection in wireless sensor networks", Proceedings of the IEEE ICON, 2008.

[10] D. Chen and G. Chang, "A Survey on Security Issues of M2M Communications in Cyber-Physical Systems", DOI: 10.3837/tiis.2012.01.002, KSII Transactions on Internet and Information Systems, vol.6, no. 1, January 2012.

[11] A. Jøsang, R. Ismail, C. Boyd, "A survey of trust and reputation systems for online service provision", Decision Support Systems 43(2), pp. 618Ű644, 2007.

[12] D. McKnight, N. Chervany, "The Meanings of Trust". Technical Report MISRC 96-04, Management Information Systems Research Center, University of Minnesota, 1996

[13] S. Etalle, J.I. den Hartog, and S. Marsh, "Trust and Punishment", Proceedings of the 1st International Conference on Autonomic Computing and Communication Systems, Autonomics, Rome, Italy, 2007.

[14] ANSI/IEEE, "Standard Glossary of Software Engineering Terminology", STD-729-1991, ANSI/IEEE, 1991.