Regulatory model for AAL

J. Pedraza[1], M. A. Patricio[2], A. de Asís[1], J.M. Molina[2]

Abstract In this work, authors define a set of principles that should be contained in context-aware applications (including biometric sensors) to accomplish the legal aspect in Europe and USA. Paper presents the necessity to consider legal aspect, related with pri-vacy or human rights, into the development of the incipient context based services. Clearly, context based services and Ambient Intelligence (and the most promising work area in Europe that is Ambient Assisted Living, ALL) needs a great effort in research new identification procedures.

Keywords: Context-Aware Applications, Ambient Intelligence, Privacy by Design, European Law, Human Rights.

1 Introduction

In Europe, the concept of Ambient Intelligent (AmI) includes the contextual information but expand this concept to the ambient surrounding the people. So, electronic or digital part of the ambience (devices) will often need to act intelligently on behalf of people. It is also associated to a society based on unobtrusive, often invisible interactions amongst people and computer-based services taking place in a global computing environment. Context and context-awareness are central issues to ambient intelligence [40]. AmI has also been recognized as a promising approach to tackle the problems in the domain of Assisted Living [41].

Ambient Assisted Living (AAL) born as an initiative from the European Union to emphasize the importance of addressing the needs of the ageing European population, which is growing every year as [42]. The program intends to extend the time the elderly can live in their home environment by increasing the autonomy of people and assisting them in carrying out their daily activities. Moreover, several prototypes encompass the functionalities mentioned above: Rentto et al. [43], in the Wireless Wellness Monitor project, have developed a prototype of a smart home that integrates the context information from health monitoring devices and the information from the home appliances. Becker et al.

[1] University Carlos III de Madrid, Public Law Department, Avda. Univ. Carlos III, 22, 28270, Colmenarejo, Madrid, Spain. {jpedraza, aeasis}@der-pu.uc3m.es

[2] University Carlos III de Madrid, Computer Science Department, Avda. Univ. Carlos III, 22, 28270, Colmenarejo, Madrid, Spain. mpatrici@inf.uc3m.es, molina@ia.uc3m.es

[44] describe the amiCa project which supports monitoring of daily liquid and food intakes, location tracking and fall detection. The PAUL (Personal Assistant Unit for Living) system from University of Kaiserslautern [45] collects signals from motion detectors, wall switches or body signals, and interprets them to assist the user in his daily life but also to monitor his health condition and to safeguard him. The data is interpreted using fuzzy logic, automata, pattern recognition and neural networks. It is a good example of the application of artificial intelligence to create proactive assistive environments. There are also several approaches with a distributed architecture like AMADE [46] that integrates an alert management system as well as automated identification, location and movement control systems.

All these approaches are promising applications from an engineering point off view, but, no legal aspects are considered in the development. Clearly, an important point is the necessity to identify the users of these systems. Before the inclusion of biometric sensors, identity and location were the main problems of privacy in context applications. Works in the literature have addressed these privacy problems from two different views, the first one centered in the development of frameworks [9] [10] and the second one centered in searching some degree of user anonymity [12] [13] [14].

In [14], these two ideas are combined in a framework with anonymity levels. Authors focus on the privacy aspects of using location information in pervasive computing applications. The tracking of user location generates a high amount of sensitive information. Authors consider privacy of location information as controlling access to this information. The approach is a privacy-protecting framework based on frequently changing pseudonyms, so users avoid being identified by the locations they visit. Agre [8] has advocated an institutional approach that casts privacy as an issue not simply of individual needs and specific technologies, but one that arises from recurrent patterns of social roles and relationships.

The inclusion of biometric technology has legal implications because it has the potential to reveal much more about a person than just their identity. For instance, retina scans, and other methods, can reveal medical conditions. Thus biometric technology can be a potential threaten to privacy [15]. European and American judges [16] have categorized privacy as taking three distinct forms. These includes [17]: a) physical privacy or freedom from contact with other people; b) decisional privacy or the freedom of the individual to make private choices about the personal and intimate matters that affect her without undue government interference and c) informational privacy or freedom of individual to limit access to certain personal information about oneself. Obviously, biometrical technology is related with the a) and c) issues. Biometric identification, of course, is not a new technology. Introduced more than a century ago, fingerprint technology is perhaps the most common biometric identification technique. Thus the social risk [18] associated to this technology is not new. However, technological advances, among other factors

[19], have increased the social risk associated to technique because: a) they have reduced the social tendency to reject its use; b) they have allowed their widespread use [20] and c) they have enabled to obtain more sensitive information on the subject.

The Ontario's Privacy Commissioner, Dr. Ann Cavoukian, in the 90's, addresses the ever-growing and systemic effects of Information and Communication Technologies, creating a new concept "Privacy by Design" [21]. The idea is that privacy cannot be assured solely by compliance with regulatory frameworks; rather, privacy assurance must ideally become an organization's default mode of operation. In ubiquitous computation, the initially concept extends to systems, business practices; and physical design and infrastructure. Principles of Privacy by Design should be applied with special emphasis into sensitive information such as biometric information and in particular medical information. The objectives of Privacy by Design are ensuring privacy and personal control over one's information and it is based on the following foundational principles: proactive not reactive; preventative not remedial; privacy as the default; privacy embedded into design; full functionality; end-to-end lifecycle protection; visibility and transparency; and respect for user privacy. These principles should help to the development of some applications in some scenarios, but they need strong foundations to be applied in any situation. Specified rules, in specific domains, allows faster developments and general principles define these specific rules.

Some results of public consultation by the European Commission, late 2009, on how the current legal framework for data protection could best deal with the challenges of globalisation and technological change, suggest that 'Privacy by Design' will probably be introduced as a new principle – not only relevant for responsible controllers, but also for vendors and developers. Specific areas such as RFID, social networking sites or cloud computing, open the scope for "Privacy by Default" settings.

2 Legal issues in Biometric Identification

Any legal system geared towards fundamental rights protection in the use of biometrics techniques should take account of the following features of this technology as it is drawn up [34]:

- That biometric data are unique and permanent. One of the major problems currently posed by biometrics is that an item of biometric data cannot be revoked when it is compromised, then it's necessary that legislators make provision for cases in which biometric data are usurped, establishing appeal or remedial mechanisms for victims.

- Biometrics is based on probability. This is the reason for the application of a false-rejection rate and a false-acceptance rate. The legal system should include effective appeal procedures for victims of erroneous rejection.

In addition, the regulatory model should neutralise the risks involved in the personalization respect the potential breaches of the fundamental rights (inter alia, non discrimination, due legal process). In Europe, this problem has been analysed, case by case [35] in the light of the Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data, and it's possible conclude that the legal solution to this problem is based in the following principles:

- Special protection to particular categories of data: data which are capable by their nature of infringing fundamental freedoms or privacy should not be processed unless the data subject gives his explicit consent; whereas, however, derogations from this prohibition must be explicitly provided for in respect of specific needs, in particular where the processing of these data is carried out for certain health-related purposes by persons subject to a legal obligation of professional secrecy or in the course of legitimate activities by certain associations or foundations the purpose of which is to permit the exercise of fundamental freedoms (Recitals 33 and 34 of the Directive)
- Automated individual decisions- The data subject shall have the right not to be subject to a decision which produces legal effects concerning him or her or significantly affects him or her and which is based solely on automated processing of data intended to evaluate certain personal aspects relating to him or her, such as his or her performance at work, reliability or conduct, unless the decision is expressly authorised pursuant to national or Community legislation or, if necessary, by the European Data Protection Supervisor. In either case, measures to safeguard the data subject's legitimate interests, such as arrangements allowing him or her to put his or her point of view, must be taken. (Article 19 of the Regulation (EC) No 45/2001 of the European Parliament and of the Council of 18 December 2000 on the protection of individuals with regard to the processing of personal data by the Community institutions and bodies and on the free movement of such data).
- Accountability: mean that a responsible organization should be able to demonstrate compliance with its data protection obligations. This would stimulate the use of Privacy Impact Assessments and Privacy Audits.

3 Principles of a regulatory model

Society as a whole needs to be aware of the obligations and rights that are applicable in relation to the use of context-aware applications with biometric sensors. Therefore it makes sense to create a regulatory model for the collection, use and dissemination of biometric information. In that regard, there're several options like laissez faire approach, self-regulation, public regulation [36][37][38]. Under a laissez faire regime, no authority requires businesses to disclose their biometric policies to consumers. Therefore, it would be difficult for customers to comprehensively weigh the alternatives. The self regulation is not sufficient because entails one big drawback: the lack of enforcement. The last alternative deals with binding legislation with effective, proportionate and dissuasive sanctions for infringements. This model should duly take into account:

- Central axiological elements: The protection of human dignity, fundamental rights and in particular the protection of personal data, are the key issues of regulatory model.
- Principles: This regulatory model and a range of implementing measures needs to be adopted to complete the legal framework, should duly take into account some general principles.

From our point of view, the general principles that should be taken into account could resume in the following ones:

- Public objective driven vs. technology driven: the legal treatment for context-aware applications should not be 'technology-driven', in the sense that the almost limitless opportunities offered by new technologies should always be checked against relevant human rights protection principles and used only insofar as they comply with those principles [39].
- Proportionality: requires that measures implemented should be appropriate for attaining the objective pursued and must not go beyond what is necessary to achieve it. The use of biometrics should not in principle be chosen if the objective can also be reached using other, less radical means.
- Reasonability: reasonableness of a measure is therefore to be adjudged in the light of the nature and legal consequences of the relevant remedy and of the relevant rights and interests of all the persons concerned
- Data governance: is a useful principle that covers all legal, technical and organizational means by which organizations ensure full responsibility over the way in which data are handled, such as planning and control, use of sound technology, adequate training of staff, compliance audits, etc. [39]
- Human rights protection by design: human rights protection requirements should be an integral part of all system development and should not just be seen as a necessary condition for the legality of a system [39].
- Best Available Techniques: shall mean the most effective and advanced stage in the development of activities and their methods of operation which indicate the practical suitability of particular techniques for providing in principle the basis for ITS applications and systems to be compliant with Human rights protection requirements [39].

- Precautionary: where there is scientific uncertainty as to the existence or extent of risks to human rights, the institutions may take protective measures without having to wait until the reality and seriousness of those risks become fully apparent.
- Technology neutrality: regulatory framework must be flexible enough to cover all techniques that may be used to provide context-aware applications.

These principles should be considered in context aware applications to include legal requirements in analysis and design phases of software development, and, at the same time, national and international regulations should consider the new capacities of technology applied in this kind of systems.

4 Regulatory model for AAL Developments

Several AAL developments have been carried out in our laboratory, a complete description could be consulted in [47][48][49]. In these applications, the provisioning of the services occurs automatically in the Context Engine as the right context is found to each user: Role, Zone, Location, etc…

In [48], elders can specify personal activities they would like the house to automate (temperature control, light control, music control, etc.). For a grandfather sitting in a wheelchair with an RFID-tag, who usually takes his medications between 10am and 11am, the following rule is discovered by the system:

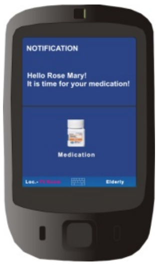
ScenarioI: Taking Medication + Elderly

Event part: *When the wheelchair (it is supposed to be the elderly person) with RFID-tag is detected in the TV room,*

Condition part: *(and) it is the first time between 5 am and 6 am,*

Action part: *(then) turn on the TV room light,(and) turn on the TV and display the morning news, (and) displays the MEDICATION'S ALERT on the PDA screen*

```
Taking_medication is true
  ( IF  Role_Taking_Medication is true
    ( IF ELDERLY is true
       AND (Zones_TV_Room is true)
       AND (time is >5:00 and time <6:00)
          ))
```



Hello Rose Mary!
It is time for your medication!

Figure 3 – Services offered to adult users in the kitchen

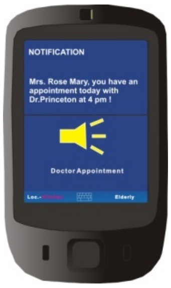
Scenario II: Routine Doctor Appointment + Elderly+ Blind

Event part: *When Mrs. Rose Mary is getting close to the kitchen its PDA is located,*

Condition part: *(and) it is about to be the 15th day of the current month*

Action part: *(then) turn on the PDA and the VoIP functionality will alert through a voice message "Mrs Rose Mary you have an appointment today with Dr. Princeton at 4pm"*

```
Notification_Doctor_Appointment is true
  ( IF  Role_Notification_Dr_Appointment is true
    ( IF ELDERLY is true
       AND (Blind.Profile.Elderly is true)
       AND (Zones_kitchen is true)
       AND (day.date is =15)
          ))
```



Mrs. Rose Mary, you have an appointment today with Dr.Princeton at 4 pm !

Figure 4 – Services offered to adult users in the kitchen

As an illustrative example, the rule of scenario I is evaluated in order to offer the appropriate services to the elderly woman who is in the TV room. The intelligent home is able to know the location of each person at home (using cameras or wifi), identify each one (using cameras or wifi), correspond each mobile device with people who carry out, and apply context-rules to inform each user. In this simple example, some legal consideration should be done, following the principles of the proposed regulatory model:

- Public objective driven vs. technology driven: the device could offer higher level functionalities in an automatic way but considering public goal and "the principle of the independence of will", the device should be configured in order to capture the information defined by the user.
- Proportionality: the identification system does not need a personal recognition based on cameras only the identification of the device is necessary.
- Reasonability: in this application the message send to the user could be turn off (other applications need to be always turn on, for example, in a hospital the message should send to medical assistance to be considered in any case).
- Data governance: the whole system is under personal data privacy law.
- Human rights protection by design: user should be able to configure the way in which the alarm is showed in order to avoid the publicity of the personal situation to other people at home.
- Best Available Techniques: the designed devices should consider the minimum effort from the user and a low cost.
- Precautionary: the technology involved should be tested to avoid healthy problems as to interfere with medical devices.

- Technology neutrality: the functionalities should be open to any device with similar technology.

These legal principles define the deployment of the system and technology and devices to be used, they impose several requirements on software development and they bring a new way to define AAL applications.

5 Conclusions

In this paper, we present the necessity to consider legal aspect, related with privacy or human rights, into the development of the incipient context based services. Clearly, context based services and Ambient Intelligence (and the most promising work area in Europe that is Ambient Assisted Living, ALL) needs a great effort in research new identification procedures. These new procedures should be non-intrusive, non-cooperative, in order to the user be immersed in an Intelligent Environment that knows who is, where is and his/her preferences. These new paradigms should be development accomplished the legal issues to allow users be citizen maintaining their legal rights.

References

1. Dey, A.K., Saber, D., Abowd, G.D.: A conceptual Framework and a Toolkit for Supporting the Rapid Prototyping of Context-Aware Applications. Human-Computer Interaction (HCI) Journal 16 (2001) 97-166.
2. Chen, Guanling, Kotz, David, Context Aggregation and Dissemination in Ubiquitous Computing Systems, Proceedings of the Fourth IEEE Workshop on Mobile Computing Systems and Applications, p.105, June 20-21, 2002
3. Hong, J.: The context fabric: An infrastructure for context-aware computing. In Minneapolis, A.P., ed.: Extended Abstracts of ACM Conference on Human Factors in Computing Systems (CHI 2002). ACM Press: Minneapolis, MN. (2002) 554{555.
4. Burke, R., Hammond, K., Young, B.: Knowledge-based navigation of complex information spaces. In: PROCEEDINGS OF THE NATIONAL CONFERENCE ON ARTIFICIAL INTELLIGENCE. (1996) 462:468.
5. Abowd, G., Atkeson, C., Hong, J., Long, S., Kooper, R., Pinkerton, M.: Cyber-guide: A mobile context-aware tour guide. Wireless Networks 3(5) (1997) 421:433
6. Sanchez-Pi, N., Fuentes, V., Carbo, J., Molina, J.: Knowledge-based system to define context in commercial applications. In: Proceedings of 8th International Conference on Software Engineering, Artificial Intelligence, Networking, and Paraallel/Distributed Computing (SNPD), Qingdao, China. (2007).
7. Victoria Bellotti, Abigail Sellen, "Design for privacy in ubiquitous computing environments",Proceedings of the third conference on European Conference on Computer-Supported Cooperative Work, Milan, Italy, 77-92, 1993.
8. Agre, P. 2001. "Changing Places: Contexts of Awareness in Computing". Human-Computer Interaction, 16(2-4), 177-192.
9. Jason I-An Hong. An Architecture for Privacy-Sensitive Ubiquitous Computing, PhD. Thesis, University of California, Berkeley, 2005.
10. Weiser, M., R. Gold, and J.S. Brown, The Origins of Ubiquitous Computing Research at PARC in the Late 1980s. IBM Systems Journal, 1999. 38(4): pp. 693-696.

11. M. Langheinrich, “A Privacy Awareness System for Ubiquitous Computing Environments,” Proc. Ubicomp, LNCS 2498, Springer-Verlag, 2002, pp. 237–245.

12. Scott Lederer, Jennifer Mankoff, Anind K. Dey, “Who wants to know what when? privacy preference determinants in ubiquitous computing”. Conference on Human Factors in Computing Systems. Extended abstracts on Human factors in computing systems. 724 – 725, 2003.

13. Leysia Palen, Paul Dourish, “Unpacking "privacy" for a networked world”. Conference on Human Factors in Computing Systems, Florida, USA, 129 – 136, 2003.

14. Beresford, A.R.; Stajano, F., “Location privacy in pervasive computing”. Pervasive Computing, IEEE, 2-1, 46-55, Jan-Mar 2003

15. That right is enshrined in Article 12 of Universal Declaration of Human Rights, Article 7 the Charter of Fundamental Rights of the European Union (2000/C 364/01) and implicity in Fourth Amendment.

16. See. European Court of Human Rights, López Ostra v. Spain - 16798/90 [1994] ECHR 46 (9 December 1994). Katz v. United States, 389 U.S 347 (1967) Skinner v. Railway Labor Executives’ Ass’n, 489 U.S. 602 (1989). To see differences between legal systems: Kirtley: Is implementing the EU Data Protection Directive in the United States irreconcilable with the First Amendment?. In: Government Information Quaterly, vol. 16, nº. 2 p. 87-91. (2001).

17. Woodward. Jhon: Biometric scanning, law & policy: identifying the concerns-drafting the biometric blueprint. In: U. Pitt. L. Rev nº 59, p. 97-155. (1997-1998).

18. Beck, Ulrich: La sociedad del riesgo: hacia una nueva modernidad.(1998).

19. Lin; Liou; Wu: Opportunities and challenges created by terrorism. In: Technological Forecasting and Social Change Volume 74, Issue 2, February 2007, Pages 148-164 , p. 158.

20. Kennedy, Gwen: Thumbs up for biometric authentication. In: Computer Law Review & Tech Nº. 8, p. 379-407, (2003-2004).

21. http://www.privacybydesign.ca/. Peter Hustinx (European Data Protection Supervisor) “Privacy by Design: The Definitive Workshop” Madrid, 2 November 2009

22. A.K.Jain, R.M.Bolle and S.Pankanti, Biometrics: Personal Identification in a Net-worked Society ,Norwell,MA: Kluwer,1999. ISBN:0792383451.

23. J.Daugman, Biometric Decision Landscape,Technique Report No. TR482, University of Cambridge Computer Laboratory, 1999.

24. See Regulation (EC) No 444/2009 of the European Parliament and of the Council of 28 May 2009 amending Council Regulation (EC) No 2252/2004 on standards for security features and biometrics in passports and travel documents issued by Member States. OJ L 142, 06.06.2009, p. 1–4.

25. B. Schouten, B. Jacobs. “Biometrics and their use in e-passports”, Image and Vision Computing 27 (2009) 305-312.

26. Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data OJ L 281, 23.11.1995, p. 31–50 and Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector OJ L 201, 31.7.2002, p. 37–47.

27. David Wrighta, Serge Gutwirthb, Michael Friedewaldc, Paul De Hertb, Marc Langheinrichd, Anna Moscibrodab. Privacy, trust and policy-making: Challenges and responses. Computer law & security review 25 (2009) 69–83.

28. Jan Grijpink. Privacy Law. Biometrics and Privacy. Computer Law & Security Report Vol. 17 no. 3 2001.

29. Parejo Alfonso, Luciano: Seguridad pública y policía administrativa de seguridad. Valencia, (2008).

30. To see examples http://www.biometrics.gov/Documents/FAQ.pdf (040809).

31. hat rights are enshrined in Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data OJ L 281, 23.11.1995, p. 31–50 and Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the

processing of personal data and the protection of privacy in the electronic communications sector OJ L 201, 31.7.2002, p. 37–47. In the United States doesn't exist general regulation for data protection. Kuner, C: An international legal framework for data protection: issues and prospects. In: Computer Law & Security Review nº. 25, p. 307-317. (2009).

32. Haas, Eric: Back to the future? The use of biometrics, its impact on airport security, and how this technology should be governed. In: Journal of Air Law and Commerce, No. 69, p. 459 y ss. (spring 2004).
33. Rodríguez de Santiago, J.Mª. La ponderación de bienes e intereses en el Derecho Administrativo. Madrid (2000).
34. Peter Hustinx. European Data Protection Supervisor. Third Joint Parliamentary Meeting on Security: "Which technologies and for what security? The new instruments of internal and civil security".Maison de la Chimie, Paris, 23 March 2010
35. See, EDPS Video-surveillance Guidelines, 17 March 2010, Guidelines concerning the processing of health data in the workplace by Community institutions and bodies, 28 September 2009.
36. Kennedy. Note 20.
37. Star, Greg: Airport security technology: is the use of biometric identification technology valid under the Fourth Amendment?: Law & Technology Journal No. 251, (2001-2002).
38. Luther, Jörg: Razonabilidad y dignidad humana. In: Revista de derecho constitucional europeo, Nº. 7, ps. 295-326, (2007).
39. Opinion of the European Data Protection Supervisor on the Communication from the Commission to the European Parliament and the Council on an area of freedom, security and justice serving the citizen (2009/C 276/02) OJC 276/8 17.11.2009.
40. Schmidt, A.: Interactive context-aware systems interacting with ambient intelligence. IOS Press, Amsterdam (2005)
41. Emiliani, P., Stephanidis, C.: Universal access to ambient intelligence environments: Opportunities and challenges for people with disabilities. IBM SystemsJournal 44(3), 605–619 (2005)
42. World population prospects: The 2006 revision and world urbanization prospects: The, revision. Technical report, Population Division of the Department of Economic and Social Affairs of the United Nations Secretariat (last access: Saturday, February 28, 2009; 12:01:46 AM)
43. Rentto, K., Korhonen, I., Vaatanen, A., Pekkarinen, L., Tuomisto, T., Cluitmans,L., Lappalainen, R.: Users' preferences for ubiquitous computing applications at home. In: First European Symposium on Ambient Intelligence 2003, Veldhoven, The Netherlands (2003)
44. Becker, M., Werkman, E., Anastasopoulos, M., Kleinberger, T.: Approaching ambient intelligent home care system. In: Pervasive Health Conference andWorkshops 2006, pp. 1–10 (2006)
45. Floeck, M., Litz, L.: Integration of home automation technology into an assisted living concept. Assisted Living Systems-Models, Architectures and Engineering Approaches (2007)
46. Fraile, J., Bajo, J., Corchado, J.: Amade: Developing a multi-agent architecture for home care environments. In: 7th Ibero-American Workshop in Multi-Agent Systems (2008)
47. R. Cilla, M. A. Patricio, A. Berlanga, J. García, J. M. Molina, "Non-supervised Discovering of User Activities in Visual Sensor Networks for Ambient Intelligence applications". Special session Challenges in Ubiquitous Personal Healthcare and Ambient Assisted Living, ISABEL 2009.
48. N. Sánchez, J.M. Molina, "A Smart Solution for Elders in Ambient Assisted Living". In "Methods and Models in Artificial and Natural Computation", Ed. J. Mira et al. Lecture Notes in Computer Science 5602, pp. 95-103 (part II), Springer-Verlag, 2009. Proceedings of Third International Work-Conference on the Interplay Between Natural and Artificial Computation, Special session "The role of knowledge based system on supporting Elderly Care at Home", IWINAC 2009. Santiago, Spain, June 23-26, 2009.
49. N. Sánchez, J.M. Molina, "A Centralized Approach to an Ambient Assisted Living Application: An Intelligent Home". In "Distributed Computing, Artificial Intelligence, Bioinformatics, Soft Computing and Ambient Assisted Living", Ed. S. Omatu et al. Lecture Notes in Computer Science 5518, pp. 706-709, Springer-Verlag, 2009. Proceedings of International Workshop on Ambient Assisted Living (IWAAL 2009)".