IOSR Journal of Computer Engineering (IOSR-JCE)
e-ISSN: 2278-0661,p-ISSN: 2278-8727, Volume 18, Issue 1, Ver. III (Jan – Feb. 2016), PP 80-85www.iosrjournals.org

A Survey of the Internet of Things

Sumita Dey[1], Dr. S. D.Joshi[2], Shruti Patil[3], Dr. Barun Kumar[4], Dr. Vishwal Ajit Kagi[5]

[1]*M-Tech Student,Department of Computer Science, Bharati Vidyapeeth Engineering college, Pune, Maharashtra, INDIA.*
[2]*Professor, Department of Computer Science, Bharati Vidyapeeth Engineering college, Pune, Maharashtra, INDIA.*
[3]*Assistant Professor, Department of Computer Science, Symbiosis Institute of Technology, Pune, Maharashtra, INDIA*
[4]*Assistant Professor,Department of Oral & Maxillofacial Surgery, Bharati Vidyapeeth Dental College & Hospital, Sangli, Maharashtra, INDIA.*
[5]*Assistant Professor Department of Orthodontic, Bharati Vidyapeeth Dental College & Hospital, Sangli, Maharashtra, INDIA*

Abstract: *This paper studies the state-of-art of Internet of Things (IoT). By enabling new forms of communication between people and things, and between things themselves, IoT would add a new dimension to the world of information and communication just as Internet once did. In this paper, IoT definitions from different perspective in academic communities are described and compared. The main enabling technologies in IoT are summarized such like RFID systems, sensor networks, and intelligence in smart objects, etc. The effects of their potential applications are reviewed. Finally the major research issues remaining open for academic communities are analyzed.*

Keywords*: Internet of Things, RFID, sensor networks, survey*

I. Introduction

During the past several years, in the area of wireless telecommunications a novel paradigm named "the Internet of Things" (IoT), which was first used by Kevin Ashton in a presentation in 1998, has gained more and more attention in academia and industry (1). By embedding short-range mobile transceivers into a wide array of additional gadgets and everyday items, enabling new forms of communication between people and things, and between things themselves, IoT would add a new dimension to the world of information and communication.

IoT would radically transform our corporations, communities, and personal spheres. In the 20th Tyrrhenian Workshop on Digital Communications, the basic idea of IoT has been summarized as the pervasive presence around us of a variety of "things" or "objects", such like Radio Frequency Identification (RFID) tags, sensors, actuators, mobile phones, which, through unique addressing schemes, are able to interact with each other and cooperate with their neighboring "smart" components to reach common goals (2). The internet of things refers to uniquely addressable objects and their virtual representations in an internet- like structure. Such objects may link to information about them, or may transmit real- time sensor data about their state or other useful properties associated with the objects.

Realization of IoT paradigm depends on integration of RFID systems (tracing and addressing items non-contact and automatically[3]), Wireless Sensor Networks(integrating distributed information collection, transmission and processing (4), intelligent technologies (using knowledge to solve certain problems and mainly covering

Artificial Intelligence, Machine-to-Machine systems and intelligent signal processing (5) and nanometer technologies (concentrating on the characteristic and application of materials of size between 0.1 and 100 nm). Since research of IoT is still in the beginning phase, there exists no common IoT architecture.

Nowadays the EPCglobal network architecture supported by Auto-ID Labs together with EPCglobal (6), and the Unique/Universal/Ubiquitous Identifier (UID) architecture in Japan (7) are the most representative among others. The basic idea underlying EPCglobal network is to design a system covering every object in the world, by use of RFID and wireless communication technologies on the basis of traditional Internet. Each object would be assigned a unique Electronic Product Code (EPC) and managed by RFID information system. **A**round the globe, many countries, regional organizations and research institutions have paid enormous attention to the Research and Development of IoT.

In US in 2009, IBM’s CEO S. Palmisano proposed the concept of "Smart Planet": by embedding and equipping sensors into everyday items (power grid, railways, etc.) and other applications, and through intelligent processing, Smart State should be achieved (8). In Europe the European

Commission (EC) had made efforts to tackle regulatory issues of IoT since 2006. In 2008, EC published a StaffWorking Document to discuss policy issues in governance of IoT, on which several concerned stakeholders have commented (9).

In 2009, EC expressed that the governance of the IoT should be carried out in a coherent manner with all public policy activities related to Internet governance (10).

In China in 2009, the concept of "Sensing China" is proposed and the sensor networks
center is built in Wuxi, Jiangsu province, as one of the major science and technology projects in the country. Now the total investment is about 11.1 billion RMB and applications are provided on a small scale. Australia, Singapore, France, Germany and other developed countriesare also speeding up the deployment of infrastructure of next generation network.

The remainder of this paper is organized as follows: in Section 2 definitions of IoT from various perspectives are introduced and compared. The applications of IoT already available are summarized in Section 3. This follows Section 4 which states the issues remaining open and possible solutions. Finally Section 5 gives the conclusion.

II. Definition Of Iot

In research communities definition of IoT is studied from various perspectives, thus there exist manifold definitions. According to (5), definitions oriented from perspective of Things, Internet and semantics are summarized.

2.1. Perspective of Things

In this perspective it focuses on how to integrate generic "objects" or "Things" into a common framework, and the "Things" under investigation are RFID tags. In (3), a literature review of academic research into RFID is presented. According to (3,11), RFID still stands at the forefront of the technologies driving the IoT vision, mainly due to its maturity and low cost, and consequently its strong support from the business community. Item traceability and addressability technologies, such as RFID systems and sensor networks, play a special role within the IoT paradigm.

However, IoT is beyond a global EPC system where the only objects are RFID tags. The idea of item identification is only part of IoT paradigm. This also applies to the alternative UID architecture (7). Besides that, UN has also proposed that the perspective of "Things" of IoT goes beyond RFID. It is stated in a UN report that a new era of ubiquity is coming where the users of the Internet will be counted in billions, and where humans may become the minority as generators and receivers of traffic. Changes brought about by Internet will be dwarfed by those prompted by the networking of everyday objects (12).

The consortium CASAGRAS proposes that an IoT vision statement goes well beyond a mere "RFID centric" approach as well. Its members focus on”a world where things can automatically communicate to computers and each other, providing services to the benefit of the human kind" (13). It not only proposes IoT would connect both virtual and physical generic objects as a global infrastructure, but also emphasizes the importance of incorporating the traditional Internet related technologies and infrastructures in the development of IoT.

Similarly, other relevant institutions have stressed the concept that IoT has pri-marily focused on the "Things" and that the road to its full deployment has to start from the augmentation in the Things’ intelligence (5). This concept has found some real-world implementations in one sort of smart sensor. Besides usual wireless communication, memory, and elaboration capabilities, this sort of sensor is also equipped with new potentials and capabilities such like autonomous and proactive behavior, context awareness, collaborative communications and elaboration. It will act as one of atomic components in the deployment of IoT. Apart from this, more and more devices, networks and service technologies enter as components that will eventually build up IoT. Technologies such as Near Field Communications (NFC) and Wireless Sensor and Actuator Networks (WSAN) together with RFID systems will provide all the necessary atomic components that will link the real world with the digital world (11).

Perspective of "Things" leads to the International Telecommunication Union (ITU) definition of the IoT: "from anytime, any place connectivity for anyone, we will now have connectivity for anything"(14). In (15), the European Commission gives a similar definition. It relates to "things having identities and virtual personalities operating in smart spaces using intelligent interfaces to connect and communicate within social, environmental, and user contexts".

2.2. Perspective of Internet

While the perspective of "Things" focuses on integrating generic "objects" into a common framework, the perspective of "Internet" pushes towards a network oriented definition. The IP for Smart Objects (IPSO) Alliance promotes the Internet Protocol as the network technology for connecting Smart Objects around the world (16).

According to IPSO, the IP stack is a lightweight protocol that already connects a huge amount of communicating devices and runs on tiny and battery operated embedded devices. This guarantees that IP has all the qualities to make IoT a reality. By reading IPSO whitepapers, it seems that through a wise IP adaptation and by incorporating IEEE 802.15.4 into the IP architecture, the full deployment of the IoT paradigm will be automatically enabled [16]. In some forums this is looked at as the wisest way to move from the Internet of Devices to the Internet of Things. To summarize, the IoT will be deployed by means of a sort of simplification of the current IP to adapt it to any object and make those objects addressable and reachable from any location.

2.3. Perspective of semantics

This perspective indicates "a worldwide network of interconnected objects uniquely addressable, based on standard communication protocols" [15]. The underlying idea in this perspective is that the number of items involved in the future Internet is destined to become extremely high. A huge number of (heterogeneous) objects will be involved in IoT scenario. Various physical world objects would be allowed to be connected to IT infrastructure. Industrial automation such like automated monitoring, control, maintenance planning, etc., of industrial resources and processes will be possible [5]. Such development will also necessarily create demand for a much wider integration with various external resources, such as data storages, information services, and algorithms, which can be found in other units of the same organization, in other organizations, or on the Internet. Therefore, issues of representing, storing, searching, and interconnecting information generated in IoT will become very challenging.

Under such circumstances, semantic technologies could play a key role in modeling 1) things description, 2) reasoning over data generated by IoT, 3) semantic execution environments and architectures that accommodate IoT requirements, and 4) scalable storing and communication in-frastructure [17]. They are claimed to be a qualitatively stronger approach to interoperability than contemporary standardsbased approaches [18]. They should not only be applied to facilitate the discovery of heterogeneous components and data integration, but also for the behavioral control and coordination of those components.

III. Applications Of Iot

Enabling the objects in our everyday working or living environment to possibly communicate with each other and elaborate the information collected from the surroundings will make a lot of applications possible [5]. The applications of IoT technologies, which are either directly applicable or closer to our current living habitudes, might be grouped into the following 4 domains.

3.1. Supply chain management

With lower cost and lower power requirement, real-time information processing technology based on RFID and NFC in IoT will be widely used in supply chain. Accordingly, accurate and real-time information relating to inventory of finished goods, work-in-progress, and in-transit stages with reliable due dates would be obtained. As a result, the demand forecast would be more accurate and extra buffers would be unnecessary. Automatic replenishment of out-of-stock goods and reduction of inventory would be possible.

For example, a manufacturer of soft drinks can identify with the click of a button how many containers of its soda cans are likely to reach their expiration date in the next few days and where they are located at various grocery outlets. Using this information, it might modify its future production and distribution plans, possibly resulting in significant cost savings [19]. As a result of applications, the reaction time of traditional enterprises is 120 days from orders of customers to the supply of commodities while Wal-Mart applying these technologies only needs few days and can basically work with zero safety stock [20].

3.2. Transportation

Cars, buses and taxis as well as roads intersections are becoming more instrumented with sensors, actuators, and processing power [5]. Important information could be collected to realize traffic control and guidance, help in the management of the depots, and provide tourists with appropriate transportation information. One of the successful applications of IoT in transportation is the Traffic Information Grid (TIG) implemented on ShanghaiGrid [21].

TIG shields all the complexities in information collection, storage, aggregation and analysis. It utilizes Grid technology to ingrate traffic information collected by sensors and actuators, share traffic data and traffic resources, provide better traffic services to traffic participators, and help to remove traffic bottlenecks and resolve traffic problems [21]. The TIG portal provides users with various information services and can be accessed by Web browsers, mobile phones, PDAs and other public infrastructure. Services provided in TIG included road status information, least-time travel scheme selection, least cost travel scheme selection, map operation and information query.

3.3. Healthcare

The IoT technologies such as RFID,WSN, etc., could provide many benefits in the healthcare domain. For example, a person’s health status could be inferred from the RFID tags on clothes or from discovering a wearable medical device. And the applications in hospital could be categorized into: tracking of hospital staff and patients, identification and authentication of people, automatic data collection and sensing [22], and remote healthcare [4].

In the remote healthcare system in [4], everyday a human's blood oxygen concentration, blood glucose level and blood pressure are collected automatically by sensor nodes, transmitted wirelessly to base-station, and displayed against time on the LCD screen. Furthermore, by connecting the base-station with a networked home PC, the data can be transferred to the remote server. Doctors may check the data to see if the result is normal or not. The data can also be transmitted to doctor's mobile device through the GSM short messages from the home basestation. This system is able to bring benefits to remote healthcare at home or in the hospitals.

3.4. Disaster alerting & recovery

Recently, natural disasters (flood, landslide, forest fire, etc.) and accidental disasters (coal mine accident, etc.) are taking place more and more frequently. Technologies in IoT, such like RFID and WSN could play a crucial role in disaster alerting before it happens, and disaster recovery after it ends.

In order to lessen the effects of natural disasters such like flood, landslide or forest fire, it is necessary to anticipate its occurrence and to alert in time. The timely access to relevant information on hazardous environmental conditions gives residents in the nearing area time to apply preparedness procedures, alleviating the damage and reducing the number of casualties derived from the event. WSN enables the acquisition, processing and transmission of environmental data from the location where disasters originate to potentially threatened cities. Then this information could be used for authorities to rapidly assess critical situations and to organize resources [23]. As to accident disaster recovery, for example, after a coal mine accident occurs, instant tracking and positioning of trapped workers using RFID technologies could provide timely rescue and lessen casualties and economic loss to the largest extent. Knowing trapped workers' geographic distribution and comparatively accurate position, the rescue action would be more targeting thus is time-efficient.

Apart from the above applications, many others could be described as futuristic since they rely on some (communications, sensing, material and industrial processes) technologies that are still to come or whose implementation is still too complex [5]. The most appealing futuristic applications included robot taxi, city information model and enhanced game room.

We refer to [2] for more details.

IV. Open Issues

4.1. Standardization

Although considerable efforts have been made to standardize the IoT paradigm by scientific communities, European Standards Organizations (ETSI, CEN, CENELEC, etc.), Standardization Institutions (ISO, ITU) and global Interest Groups and Alliances (IETF, EPCglobal, etc.), they are not integrated in a comprehensive framework.

Efforts towards standardization have focused on several principal areas: RFID frequency, protocols of communication between readers and tags, and data formats placed on tags and labels [8]. EPCglobal, European Commission and ISO are major standardization bodies dealing with RFID systems. EPCglobal mainly aims at supporting the global adoption of a EPC for each tag and related industry driven standards [6]. European Commission has made coordinated efforts aiming at defining RFID technologies and supporting the transition from localized RFID applications to the IoT [25]. Differently from these, ISO deals with how to modulate, utilize frequencies and prevent collision technically [26].

The European Telecommunications Standards Institute (ETSI) has launched the Machine-to Machine (M2M) Technical Committee to conduct standardization activities relevant to M2M systems and define cost-effective solutions for M2M communications. Due to lack of standardization of this leading paradigm towards IoT, standard Internet, Cellular and Web technologies have been used for the solution of standards. Therefore, the ETSI M2M committee aims to develop and maintain an end-to-end architecture for M2M (with end-to-end IP philosophy behind it), and strengthen the standardization efforts on M2M [27].

Within the Internet Engineering Task Force (IETF), there are two working groups 6LoWPAN and ROLL dealing with integrating sensor nodes into IPv6 networks. 6LoWPAN is to define a set of protocols to make the IPv6 protocol compatible with low capacity devices. Core protocols have been already specified [28]. While ROLL recently produced the RPL (pronounced "ripple") draft for routing over low power and lossy networks including 6LoWPAN [5]. Lots of contributions are needed to reach a full solution.

4.2. Security And Privacy

Authentication and data integrity mainly concern security. Due to lack of proper infrastructures and servers to exchange messages among nodes, authentication is particularly difficult in IoT scenarios. Furthermore, things have scarcer resources comparing to PCs, PDAs, cell phones, etc., to carry out complex computing. In [29], some solutions about authentication have been proposed, but they all have serious problems and can't help solve the man-in-the-middle attack problem [5].

Data integrity solutions require that an adversary cannot modify data in the transaction without the system detecting the change. In traditional information area, the problem of data integrity has been widely studied. When RFID systems and sensor networks are integrated in the Internet there would be new problems. Sensor nodes or RFID tags are spread in a wide area and spend most of the time unattended. Data can be modified by adversaries while it is stored in the node or when it traverses the network [30]. To protect data against the first type of attack, memory is protected in most tag technologies and solutions have been proposed for wireless sensor networks as well [31]. To protect data against the second type of attack, messages may be protected according to the Keyed-Hash Message Authentication Code (HMAC) scheme [32]. Referto [5] for more details. In [33] some cryptographic methodologies are proposed to support security use. Such solutions cannot be completely applied to the IoT, given that they will include IoT components such like RFID tags and sensor nodes that are limited in energy, communications, and computation capabilities. It follows that new solutions are required to be able to balance between security level and resource scarcity.

The right to privacy can be considered as a personal right or possession [33]. In IoT people's privacy problem mainly relates to data collection (which of their personal data is being collected, who is collecting such data, and when this is happening), the use of collected data (only for authorized services by authorized service providers) and recently begun data forgetting (the collected data should be stored only until it is strictly needed) [5].

In RFID systems, there are two problems concerning data collection. In fact, on the one hand usually RFID tags are passive and reply to readers queries regardless of the desire of their proprietary [29]. Thereby, individuals' data could be collected without them even knowing about it [33]. On the other hand an attacker can eavesdrop the reply from a tag to another authorized reader.

As been mentioned above, authentication of authorized readers can not solve the first type of problems. A new system based on preferences set by the user has been proposed in [34] to negotiate privacy on the individual's behalf. The privacy decisions taken by the above system can be enforced by creating collisions in the wireless channel with the replies transmitted by the RFID tags, which should not be read [35]. Using encryption to protect communication from eavesdropping still allow malicious readers to detect the presence of RFID tags by scanning. As for this problem, there is a new family of solutions where the signal transmitted by the reader has the form of a pseudo-noise. Such noisy signal is modulated by the RFID tags and therefore, its transmission cannot be detected by malicious readers [36].

To fix the problem of un-authorized use of personal data collected, solutions have been proposed that usually rely on a system called privacy broker [37]. The proxy interacts with the user on the one side and with the services on the other, which guarantees the provider obtains only the strictly needed information about the user. The user can set the preferences of the proxy. However, such solutions based on privacy proxies suffer from scalability problems [5]. And the policy adopted by privacy brokers could not be influenced by individuals.

As an important issue recognized recently, digital forgetting is still studied at the beginning phase [38]. In fact, as the cost of storage decreases, the amount of recordable data increases dramatically. Accordingly, once information is generated, it will most probably be retained indefinitely [5]. Accordingly there is the need to create solutions that periodically delete information of no use for the purpose it was generated. The full deployment of IoT should support such forgetting functionalities, requiring further research effort.

4.3. Governance

The questions of "thin" legitimacy and lack of sufficient transparency and accountability arise in the IoT environment just as in present Internet [39]. Since IoT is not only a mere extension of today's Internet, but rather a networking of independent but interoperable systems, the Internet Governance concepts are no longer suitable to identically be applied.

Learning from the regulation of the Internet, the concept of "multi-stakeholder in governance" should be perceived as the new way forward in favor of the inclusion of the whole society [39]. Such a development challenges the traditional legaland political understanding of legitimacy and makes it necessary to tackle the general question of who could be a legitimate stakeholder. Consequently, architectural principles are to be developed and compiled in an international legal framework. Representation only has a legitimizing effect, if the outcome reflects the represented stakeholders' values. Besides equal bargaining powers and fair proceedings ,this concept requires transparency, accountability and inclusion of public opinion in IoT governance.

V. Conclusion

In this paper, we survey the state-of-art on the IoT, including the manifold definitions, enabling technologies, already or soon available applications and open research issues with efforts been. However, it is not this paper's main purpose to provide a comprehensive review of the details of the relevant technologies. It is believed that in the near future the achievement of the vision of "from anytime, anyplace connectivity for anyone, we will now have connectivity for anything" should depend on cross-discipline and cooperative efforts in related fields.

References

[1]. G. Santucci, From Internet of Data to Internet of Things, Paper for the International Conference on Future Trends of the Internet, 2009.

[2]. D. Giusto, A. Iera, G. Morabito and L. Atzori, editors. The Internet of Things, Springer, 2010

[3]. E. Ngai, K. Moon, F. Riggins and C. Yi, RFID research: An academic literature review (1995-2005)

[4]. and future research directions, International Journal of Production Economics, 112:510–520, 2008.

[5]. L. Ni, C. Li, L. Qiong, N. Hoilun and Z. Ze, "Status of the CAS/HKUST joint project BLOSSOMS",

[6]. Proc. Of the 11th IEEE International Conference on Embedded and Real-Time Computing Systems and Applications, pp. 469–474, August, Hongkong (China), 2005.

[7]. L. Atzori, A. Iera and G. Morabito, The Internet of Things: A survey, Computer Networks, doi:10.1016/j.comnet.2010.05.010, 2010.

[8]. The EPCglobal Architecture Framework, EPCglobal Final Version 1.3, Approved 19 March 2009,<www.epcglobalinc.org>.

[9]. K. Sakamura, "Challenges in the age of ubiquitous computing: a case study of T-engine – an open development platform for embedded systems", Proc. Of the 28th International Conference on Software Engineering, pp. 713–720, May, Shanghai (China), 2006. http://www.ibm.com/smarterplanet

[10]. Commission Staff Working Document, Future Networks and the Internet - Early Challenges regarding the "Internetof Things".

[11]. Commission of the European Communities,"Internet of Things-An actionplan for Europe", COM(2009) 278final.

[12]. M. Presser and A. Gluhak, The Internet of Things: Connecting the Real World with the Digital World, EURESCOM message-The Magazine for Telecom Insiders, 2, 2009.

[13]. M. Botterman, Internet of Things: An Early Reality of the Future Internet, Report of the Internet of Things Workshop, Prague, Czech Republic, May 2009.

[14]. A. Dunkels and J. Vasseur, IPfor Smart Objects, Internet Protocol for Smart Objects (IPSO)

[15]. Alliance, White Paper #1, September 2008, <http://www.ipso-alliance.org>.

[16]. ITU Internet Reports, The Internet of Things, November 2005.

[17]. INFSO D.4 Networked Enterprise & RFID INFSO G.2 Micro & Nanosystems, in: Co operation with the Working Group RFID of the ETP EPOSS, Internet of Things in 2020, Roadmap for the

[18]. Future, Version 1.1, 27 May 2008.

[19]. J. Hui, D. Culler and S. Chakrabarti, 6LoWPAN: Incorporating IEEE 802.15.4 Into the IP

[20]. Architecture- Internet Protocol for Smart Objects (IPSO) Alliance, White Paper #3, January 2009.

[21]. I. Toma, E. Simperl and G. Hench, "A joint roadmap for semantic technologies and the internet of things", Proc. Of the 3rd STI Roadmapping Workshop, June, Crete (Greece), 2009.

[22]. W. Wahlster, Web 3.0: Semantic Technologies for the Internet of Services and of Things, Lecture at the 2008 Dresden Future Forum, June 2008.

[23]. I. Bose and R. Pal, Auto-ID: Managing anything, anywhere, anytime in the supply chain, Communications of the ACM. 48:100–106, 2005.

[24]. R. Yuan, L. Shumin and Y. Baogang, Value Chain Oriented RFID System Framework and Enterprise Application, Science Press, Beijing, 2007.

[25]. M. Li, M. Wu, Y. Li, J. Cao, L. Huang, Q. Deng, X. Lin, C. Jiang, W. Tong, Y. Gui, A. Zhou, X. Wu and S. Jiang, ShanghaiGrid: an information service grid, Concurrency and Computation: Practice and Experiment. 18:111–135, 2006.

[26]. A. Vilamovska, E. Hattziandreu, R. Schindler, C. Van Oranje, H. De Vries and J. Krapelse, RFID

[27]. Application in Healthcare-Scoping and Identifying Areas for RFID Deployment in Healthcare Delivery, RAND Europe, Febru-ary 2009.

[28]. M. Castillo-Effen, D. Quintela, R. Jordan, W. Weshoff and W. Moreno, "Wireless sensor networks for flashflood alerting", Proc. Of the 5th IEEE International Caracas Conference on Devices, Circuits and Systems, November, Dominican Republic, 2004.

[29]. SENSEI FP7 Project, Scenario Portfolio, User and Context Requirements, Deliverable 1.

[30]. Commission of the European Communities, Early Challenges Regarding the "Internet of Things",2008. http://www.iso.org.

[31]. Z. Shelby, ETSI M2M Standardization, March 16, 2009, <http://zachshelby.org>.

[32]. N. Kushalnagar, G. Montenegro and C. Schumacher, IPv6 Over Low- Power Wireless Personal

[33]. Area Networks (6LoWPANs): Overview, Assumptions, Problem Statement, and Goals, IETF RFC 4919, August 2007.

[34]. A. Jules, RFID security and privacy: a research survey, IEEE Journal on Selected Areas in Communications, 24:381–394, 2006.

[35]. T. Karygiannis, B. Eydt, G. Barber, L. Bunn and T. Phillips, Guidelines for Securing Radio

[36]. Frequency Identification (RFID) Systems, NIST Special Publication 800-98, April 2007.

[37]. R. Kumar, E. Kohler and M. Srivastava, "Harbor: software-based memory protection for sensor nodes", Proc. Of International Conference on Information Processing in Sensor Networkss, pp.340-349, Cambridge, MA, USA, April 2007.

[38]. H. Krawczyk, M. Bellare and R. Canetti, HMAC: Keyed-Hashing for Message Authentication, IETF RFC 2104, February 1997.

[39]. R. Weber, Internet of Things-New security and privacy challenges, Computer Law & Security Review, 26:23– 30, 2010.

[40]. C. Medaglia and A. Serbanati, "An overview of privacy and security issues in the internet of things", Proc. Of 20th Tyrrhenian International Workshop on Digital Communications, pp. 389 395, Pula (Italy), September 2009.

[41]. O. Savry and F. Vacherand, "Security and privacy protection of contactless devices", Proc. Of 20th

[42]. Tyrrhenian International Workshop on Digital Communications, pp. 409-419, Pula (Italy), September 2009.

[43]. O. Savry, F. Pebay-Peyroula, F. Dehmas, G. Robert and J. Reverdy, "RFID noisy reader: how to prevent from eavesdropping on the communication?" Proc. Of Workshop on Cryptographic Hardware and Embedded Systems 2007, pp. 334-345, Vienna (Austria), September 2007.

[44]. G. Lioudakis, E. Koutsoloukas, N. Dellas, S. Kapellaki, G. Prezerakos, D. Kaklamani and I.

[45]. Venieris, "A proxy for privacy: the discreet box", in: EUROCON 2007, pp. 966-973, Warsaw (Poland), September 2007.

[46]. V. Mayer-Schoberger, Delete: The Virtue of Forgetting in the Digital Age, Princeton University Press, 2009.

[47]. R. Weber, Internet of things-Need for a new legal environment? Computer Law & Security Review, 25:522–527, 2009.