Internet of Things – A Paradigm Shift of Future Internet Applications

Sarita Agrawal, Manik Lal Das

Abstract— **Internet has emerged as a medium to connect people across the world for emailing, conferencing, on-line trading, gaming and so on.** *Internet of Things (IoT)* **is aimed at making daily lives more sophisticated, flexible and highly reachable to any objects across the world. In IoT, physical objects such as home appliances, vehicles, supply chain items, containers etc. will have digital identities and they will be context aware to sense the environment around them and interact with each other. The objects will be able to respond with the information useful for real-time decision making such as safely changing the lane while driving, automatically switching off the lights in a room when no one is around and so on. Effective monitoring of the environmental conditions to control issues such as pollution, disaster and global warming is another important objective of IoT. For IoT, objects are required to be made** *smart* **by embedding intelligence into them using technologies such as Wireless Sensor Networks (WSN) and Radio Frequency IDentification (RFID). In addition to mobile communication technology, Internet will be the primary backbone of the communication channel of IoT. As Internet is a public (and insecure) channel, security is an important concern in IoT infrastructure to communicate the voluminous information across the globe in a secure and timely manner. In this paper, we discuss the potential scope of IoT, the major technologies involved in IoT infrastructure and some important application domains for IoT. We also discuss the security and privacy issues of two important technologies of IoT, namely, WSN and RFID.**

Index Terms- **Internet of Things, Privacy, Radio Frequency IDentification, Security, Wireless Sensor Networks.**

I. INTRODUCTION

INTERNET has changed our lives drastically-the way we think, we work, we live - by providing anytime, anywhere connectivity with anyone. With the advancement in technology, the cost of sensors, processors and transmitters is becoming less and less, allowing putting them into any object of our day-to-day life -the food, the clothes, the medicines and so on. The technological advances also enhance this connectivity by adding one more dimension to it -connecting anything. Today's Internet is now moving towards Internet of Things (IoT) -*The Internet where the existing network of computer systems will connect to the real world objects such as home appliance, vehicles and environment. Smart objects will be able to sense objects around them and will be able to communicate and interact with each other without the intervention of humans. These smart objects will make their own independent social networks where each object can be tracked through its unique digital identity.* For IoT to take the desired shape of global connectivity, each and every small object/thing in the world needs to be connected in sensory and intelligent manner. The first requirement is that of unique identification of the millions of *things*. Radio Frequency IDentification (RFID) technology provides the platform towards this objective, wherein an RFID tag with unique identification number can be attached to each object in the IoT. To manage the unique identification for trillions of objects expected to be connected in the IoT, 128-bit IPv6 addressing scheme has been adopted which can accommodate about 340 trillion trillion trillion addresses [1]. With this new addressing scheme, the threat of address exhaustion, with 32-bit IPV4 addressing *scheme* in present Internet, is not a matter of concern any more. The smart objects in the IoT would be having the capabilities of sensing the physical objects and environment. The Wireless Sensor Networks (WSN) will play a vital role here, wherein the sensor nodes will collaborate with each other to provide the required information about the surroundings. A tremendously large amount of information would be flowing across the globe and therefore very high speeds of communication will be required. The advanced mobile communication technologies such as 3G and 4G will, therefore, be an inevitable aspect of IoT technologies. Combining these three major technologies of RFID, WSN and mobile communication along with conventional LAN/WAN, the IoT infrastructure will be able to connect anyone, any-where, anytime to anything in this world.

A. Key Challenges

Standards: For mass deployment of IoT globally and making it accepted by the people all over, the standardization is very much required.

Privacy: One of the major challenges in global acceptance of this ubiquitous connectivity through IoT is the privacy of trillions of objects [2].

Identification and Authentication: The objects in the IoT will be tagged for the purpose of identification and tracking. This identification has to be protected from tracking by unauthorized elements in the network. The users must be provided with the adequate control over the privacy of their personal information.

Security: Communication between the objects through IoT poses security threats which need to be addressed pro actively and appropriate measures must be implemented well before the full-fledge implementation of IoT.

Trust and Ownership: Relying on the information captured

978-1-4577-2168-7/11/$26.00 ©2011 IEEE

and communicated within this global network is also a concern. Trust implies the authenticity and integrity of the communicating parties such as accurate sensing of the data by correctly functioning sensors and valid reader interaction with tags [3].

Integration: In the current scenario, the world of Internet and the physical world seem to be two different worlds. The main challenge with IoT is to integrate these two worlds effectively. The factors such as cost, durability, communication speed, information capacity, and security need to be considered in order to link many heterogeneous devices and independent networks together [4].

Coordination: When we visualize the globally connected objects which can facilitate sharing of data, we need collaboration and cooperation of people, programs, processes and services, which are (and will be) integrated in IoT [5].

Regulation: Regulation can be carried out in three different ways: traditional government regulations, international agreements and self regulations. Traditional government regulations being limited to their territorial boundaries do not suit the global structure of IoT. Self regulation is cost effective and efficient but only few motivated and principled *Things* may take part in it. As for international agreements, either a new trusted body can be established or the existing body such as WTO can work as an international legislator [6].

B. Opportunities

Insure & not Secure: As security is a service, vendors and service providers in IoT will find an opportunity to buy security services as per requirement. However, the claimed security services in IoT (and its applications) should be liable to protect collaborating companies' asset and customers as well. Security through trust is a successful negotiation, but IoT infrastructure needs a bit more, something like *security through trust and insurance* together. That would possibly help acquiring business interest if something wrong happens due to cyber attacks or intentional interest of a participating member of IoT infrastructure.

Reachability: As IoT promises to connect the physical world with the digital world, each and every *Thing* around us will be having a unique identification. Assigning an IPv6 address to each IoT element will make it possible to reach them from any other node of the network. Applications developed locally could reach global market once the standardization protocols are in place. e.g. remote patient monitoring systems based on RFID tags and sensors.

Efficiency: With the availability of IoT technologies, various applications could be developed sharing some costly common infrastructure such as data center, financial switch etc. Another way to provide efficiency is through reachability. For example, in supply chain management, it could provide efficiency in material handling and general logistics, warehousing and product tracking, data management, reducing production and handling costs etc. The connected smart things will have immediate access to information about the physical world and the objects in it.

Cost effectiveness: With IoT, the things as small as dust particle will have the ability to interact and connect with the Internet. The miniaturization and nano-technology advancement is resulting in low cost of these smart things. Efficiency in various aspects of life, due to IoT, such as smart homes, remote medical care, end-to-end supply chain management etc. would also have impact on the cost factor in an effective manner.

AAA Connectivity: Here AAA means AnyTime-AnyThing-AnyPlace. One of the objectives of IoT is to enable connectivity of two objects located at two different places. We have mobile banking, tele-conferencing, etc. where services are being achieved while traveling or staying at home. The IoT infrastructure aims to connect all real-world objects through conventional computing system, RFID, WSN and mobile technologies, and Internet will act as the primary backbone of the communication channel. Through this collaborating and integrated approach, one would be able to get AAA required service from IoT for all applications that we may use in our daily lives.

This paper aims to give a broader perspective of IoT - challenges and opportunities. The key challenges that arise in IoT are primarily -standards, integration, cooperation, trust and ownership and security of applications, middle-ware, operating system, embedded devices etc. In addition to the conventional computing infrastructure, IoT is aimed at using two main resource-constrained environments such as Wireless Sensor Networks (WSN) and Radio Frequency IDentification (RFID). We discuss important characteristics of WSN and RFID in the context of IoT. Finally, a few important application areas have been highlighted, where IoT could play a significant role in the coming years.

The remainder of the paper is organized as follows. Section II mentions about the importance of IoT. Section III discusses some technological advancement with respect to IoT. Section IV discusses security and privacy issues of two major technologies namely WSN and RFID with respect to IoT. Section V highlights some important application areas of IoT. We conclude the paper with Section VI.

II. The Internet-Of-Things (IoT)

In 1999, Kevin Ashton used the term *Internet of Things* (IoT) in one of his presentations at Proctor and Gamble while introducing the idea of using RFID in their supply chain. At that time, even Internet was also not as popular, as it became in last decade. With present capabilities of Internet, we could collect data available on the web; however, it is dependent on human intervention. Importantly, our society and economy is not just based on data and information, but on the things around us. IoT aims to empower the computers to interact directly with the things by seeing, hearing and smelling the things without intervention of humans, to make the real use of the connectivity and information flow we obtain through the use

of Internet [7]. When used in the context of IoT, the *Things* is defined as *a real/physical or digital/virtual entity that exists and moves in space and time and is capable of being identified* [8]. Identification numbers, names and/or locations can be used to identify the Things. *Things* include not only the material things but also the virtual things and the events connected to them. IoT extends the communication between human and applications to integrate *Things* within it. These things will interact and communicate among themselves as well as with their environment (by sensing the environment) and the data and information can be exchanged. They can also react independently to the events happening in the real world. Even without directly involving the humans, the things can run processes to trigger certain actions or create services. *Things* will thus be active participants in business, information and social processes. The term *Things*, however, will be perceived differently in different contexts and will depend on the application domain. IoT will thus make not just human-to-human, human-to-things communication possible, but also things-to-things communication will become a reality with IoT. A new dimension with things [2] is depicted in Fig.1.

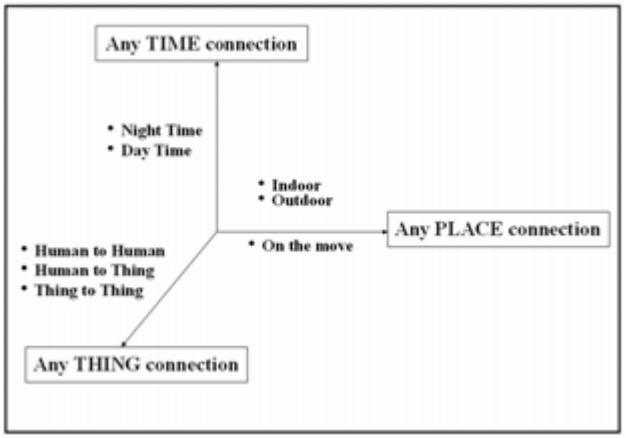

Fig. 1. New Dimension with *Things*

IoT can also be considered as a *Global network which allows the communication between anything in the world by providing a unique digital identity to each and every object. The things communicating may actually exist in the real world of physical objects or may be a virtual object. These communicating objects will be smart enough to independently configure themselves and operate without human intervention. The fast wireless medium will support the network infrastructure without any limitation of distance and location of the communicating entities.*

The demands of people are increasing in all areas of life especially for better health, and medical treatment and services. So far, information and communication (ICT) technologies have helped the society in providing better services with the use of Internet, mobile communication etc. and therefore, it is believed that ICT can solve the problems of social and economic development and also help people enhance their standards of living [9].

III. Driving Forces that Reduce Gap between Physical Objects and Virtual Objects

The major technologies that would dominate IoT applications are WSN, RFID and Mobile communications along with the existing LAN/WAN. To cater for the unique digital identification of various heterogeneous objects in IoT, the things, the people and the places, IPV6 with 128-bit unique addressing scheme and RFID are considered as promising approaches. To connect these uniquely identifiable *Things* across the globe, we need to provide senses to them, so that they can work even without the human intervention. The sensor nodes will be utilized for this purpose. The wireless network of sensor nodes would help sense the environment and objects around and communicate to the other *Things*. Wireless Sensor Network technology is, thus, one more essential pillar for the giant edifice of IoT. Most of the *Things* connected to this huge network including people and vehicle will be moving from one place to other. Advanced mobile communication technology (3G and 4G) will make uninterrupted high-speed communication possible, even while on move to keep the things connected endlessly. The Fig.2 shows a high-level view of IoT infrastructure as far as major technologies are concerned.

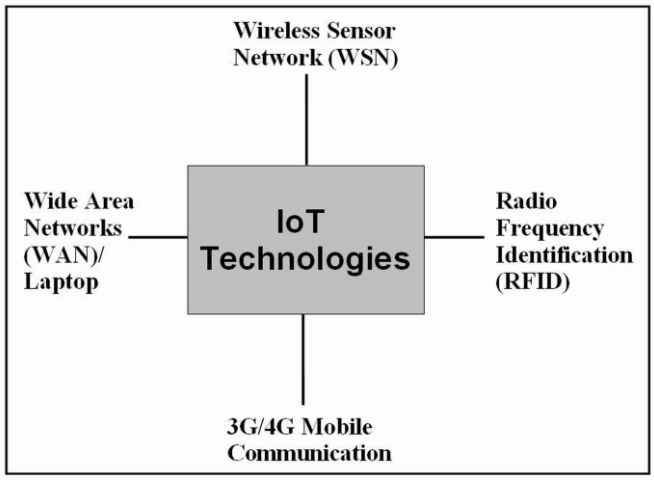

Fig. 2. Major Technologies involved in IoT

A. Radio Frequency Identification (RFID)

Radio Frequency Identification (RFID) is a technology that connects the objects over-the-air so that the objects can be tracked and the data about them can be shared by individuals and organizations. The technology consists of tags/transponders, a reader and a back-end computer system. The tag has a unique identifier (ID) and an antenna for transmitting/receiving radio waves from reader in vicinity. The reader forwards information received from tags to the back-end server for validation and the back-end system runs the applications based on the data received from reader. RFID tags can be active or passive. Active tags have on-board power supply and have long read range with beacon

rate, typically, of 1 to 15 seconds. On the other hand, passive tags are cheap and small with short read range. A passive tag does not have a power supply of its own and absorbs energy from the electromagnetic field created by the antenna of the reader. There are also *semi-passive* and *semi-active* tags [10]. RFID system has been widely used for tracking objects, people and animals. One of the crucial factors of IoT infrastructure is identification of trillions of objects. And, RFID provides an important technological support for this requirement.

B. Wireless Sensor Networks

Wireless Sensor Networks (WSN) consist of a large number of tiny sensor nodes capable of sensing the objects and environment in physical world and communicate to the digital world of computer systems for making informed decisions e.g. in building monitoring and controlling vehicle movement *etc.* Sensor nodes collect and forward the data to base station to cooperatively monitor the physical objects or environmental conditions such as temperature, vibrations, pressure and motion. In WSN, there are usually one or more base stations and several sensor nodes. The base-station acts as the central trusted authority and also serves as the data sink/processor which connects the sensor network to the external world. WSN technologies are now recognized widely for applications ranging from military services, traffic monitoring and agriculture. However, the present forms of WSN's usage are mostly working in isolation serving a specific application area. But WSN can be designed as cluster-based, hierarchical, or group-based. Enabling sensors to various objects and making communication through Internet would provide a virtual sensing layer to IoT infrastructure [11].

C. Mobile Communications Technology

The mobile communication technology used with Internet is effectively shifting the wireless communication from voice-centric to data centric. The challenge of accessing rich multi-modal information on *things* connected through wireless medium will be met by transmitting data/video contents over wireless platform using the advanced mobile communication technology. In present scenario, two dominating mobile technologies are Global System for Mobile Communications (GSM) and Code Division Multiple Access (CDMA) [12]. Third generation (3G) mobile and wireless networks have further increased the enhanced multimedia and streaming video capabilities. 3G systems are also capable of providing universal access and portability across different device types (Telephones, PDA's, etc.). 3G systems are IP - based network, which serves two main purposes as follows. For communication between mobile terminal and application host, user-level IP address is used, whereas, transport-Level IP address is used for communication among network entities. With IoT, even the physical objects used for everyday life such as clothes, food will be connected via network, resulting in lots of information flow. The upload and download speeds on network can restrict our daily life and therefore, with a speed of up to 1 gigabit per second on wireless medium, 3G/4G is inevitably a part of IoT revolution giving easy and fast access, portability and reliability.

IV. Security and Privacy Issues for IoT Infrastructure

IoT aims to integrate several real-world standalone applications to communicate with each and every object associated in the applications. Naturally, IoT needs a tighter security measures than application's own security strength. For example, WSN is being successful for room temperature control, container tracking and health care. On the other hand, hand-held device with Internet, say Mobile banking, can provide on-line trading service. Each of these applications has its own security measure and risk according to its requirement. However, when IoT enables a bridge between WSN's health care and 3G's Mobile banking, individual application's security will not be sufficient, as there could be potential proxy agents who could possibly dilute applications' security strength. Moreover, more channels are to be opened for getting access to objects, which in turn, allows good or bad entities to compromise object's privacy. Therefore, IoT considers security as one important factor in addition to other key challenges. Below we discuss security aspects of two important technologies, namely RFID and WSN, which are going to become essential components of IoT. At present the items which possess communication capabilities are designed with some specific purpose to work in a specific scenario such as RFID tags in-built into keys for auto-mobiles and buildings, motion and fire detectors reporting to a specific network address. In IoT, we can expect the *things* to have wireless communication capabilities and having less specific purpose. They will no longer be restricted to operate in a limited environment, but the *things* will be a part of a global network and they might need to work in different contexts at different times. It may happen that some of the contexts are not visualized at the time of design and therefore unexpected side effects may occur causing security issues. With more and more objects getting attached to the network, privacy problems will be emerging as another major concern with IoT [13]. In RFID systems, any reader in the vicinity can read the data from the tag and the tag reading does not require line-of-sight. RFID tags are attached to items to avoid creating forged items and prevent counterfeiting. Because of resource-constrained tags, RFID system, at present, supports lightweight security solution for authentication and authorization. Based on application's requirement, RFID tags perform only XOR or random number generation operation. For tight security services (say, strong authentication, confidentiality, non-repudiation) symmetric key encryption and message authentication code or public key encryption and signature are needed. Also, security solutions which can resist physical memory analysis and having low-computational complexity

are required [14]. In case the tag or a set of tags is attached to a person and the tag(s) come in the reader's field at a given place, it will disclose the location of the person, tracing the locations of person through a longer period of time may result in the disclosure of lots of information about the person's movements. To avoid this, either the tags have to identify the illegitimate readers and remain silent when such readers interrogate or tags should randomly update their IDs [15]. Some of the potential threats in RFID system are replay, synchronization, RF eavesdropping, data alteration, etc. In the context of IoT, more security requirements are expected from RFID system like mutual authentication, key establishment for data confidentiality, anonymity, etc. It is also expected that in near future, RFID tags would become self sufficient to support strong cryptographic operation using symmetric and public key cryptography.

Security aspects of WSN have been evolving with greater pace. Now WSN nodes (e.g. IRIS [16], SunSPOT [17]) are capable enough to perform symmetric and asymmetric cryptographic operations. In present scenario, the base-station acts as a powerful entity in WSN, which has large computational resource in comparison to sensor nodes. The base-station ensures the secure connectivity of WSN with the rest of the Internet. However, in the scenarios, where sensor nodes may require to directly communicating with the entities outside the WSN, there are many issues that need to be addressed. To integrate WSN application in IoT infrastructure, security of that application has to be ensured, i.e., ensuring authentication of nodes and data, confidentiality and integrity of information transmitted between nodes, data freshness and availability of the information are important factors, which requires further attention.

V. Applications of Internet Of Things

The possible applications of IoT can be divided into three application domains: Society, Industry and Environment [8]. Each domain has specific set of activities. However, these domains cannot be isolated from each other and therefore applications and services used at inter-domain and intra-domain levels must be thought of. For example, the implications of production and supply of medicines is not restricted to pharmaceutical industry, but it has environmental (from what and how the medicines are prepared) as well social impact (on patients).

Climate monitoring: Due to the low cost of sensor nodes, a large number of nodes are deployed that can sufficiently represent the variability in the environment. Sensor nodes are used to detect water level, rain fall and weather condition and thus predict the flood conditions. Similarly, by sensing the humidity, temperature and pressure in the air, sensor networks help foreseeing earth quakes, tsunami, forest fires and other natural calamities. Until now, such WSN have been working independently for a limited geographical area. With IoT, such independent networks could work in collaboration and could virtually cover larger geographical area in the sense that the critical information can be quickly disseminated to farther distances.

Transport and road safety: Different technologies of IoT can work together for providing efficient transport services and ensure road safety. For example, RFID tags maintaining the history can be attached to the parts of vehicle/aircraft to avoid counterfeiting of parts. Tags attached to the passenger's luggage/cargo for easy identification during transport thus saving time. Monitoring of fuel level, tyre pressure, acceleration level, brake condition etc. could help in vehicles to guard against sudden breakdown and accidents. A vehicle can communicate with other vehicle to keep track of its distance to avoid any accident. A vehicle can communicate itself to the emergency services giving its location, vehicles in vicinity, parts required etc. for getting the help in case of break down. Cars having RFID - based toll-collection tags are already in use. In some countries, sensors have been deployed on the roadside that can detect the flow of cars having such tags. Drivers can be instructed about traffic information with the help of sensors.

Home automation and Building monitoring: The smart home can be simply thought of as an integration of all household installations, being controlled from one control panel in a room, remotely via a control unit, the computer or the Internet. Sensing devices, which are the core of IoT, are deployed to sense the things and environment around them, such as temperature, and conveyed through wireless network to the control units. The comfort level at home can be automatically adjusted with the use of sensors which sense the surrounding temperature and humidity. The refrigerator can keep track of the items stored in it, raise an alert in case a food item is about to expire, order for replenishing the items required. Human activities can be monitored and support can be provided especially to disabled or elderly people, for example, switching on the light, opening the door or pulling the curtains. Buildings can be monitored by installing sensors at crucial places in the building to sense water leaks, gas leakage, vibrations and fire. RFID Tags can be associated with the persons authorized to enter the building and thus prevent unauthorized entry and vandalism.

Health care: IoT would play a very crucial role in health care segment. Sensors can be put on the patient's body to monitor the blood pressure, heart beat and other health parameters. As these sensors will be the part of sensor network, the sensed parameters can be monitored remotely and timely and appropriate treatment can be given. It will be especially useful in the case of emergency and mass casualty. Patient's complete medical history can be recorded and attached to the patient itself for easy retrieval and use. Once such sensor networks get connected to the Internet, it would be possible for the medical practitioners from different parts of the world to discuss about critical health cases and decide

on the best possible treatment in real time.

Supply Chain: RFID tags came into existence as the replacement of bar codes and have been used effectively for supply chain management. However, their usage has been restricted within the individual organizations or in limited geographical spreads. RFID technology is continuously advancing and has become one of the most required technologies for realization of IoT. The new sophisticated RFID tags assigned to product can contain information having complete history of the item from production till disposal. The manufacturer details, production date, expiry date (if applicable), warranty period, after sale service details, all these can be tracked. As the RFID enabled systems become part of IoT, real-time and efficient supply chain management would be possible. On-shelf stock can be monitored and replenishment done in real time can save from over-stocking and even over production.

Agriculture and Rural Development: Sensor networks can be deployed for monitoring the soil, finding the water levels on the fields and prediction of rain falls. Timely and accurate information on these parameters would help farmers plan their field work effectively. Vaccination of plants/crops can help the farmers get better yields and also tracking of the harvest from farms to market will provide them with better return on investment. Keeping track of animals in the herd by providing identification through RFID tags serves in easy and efficient care of animals.

Border Security and Military Application: For enhancing the border security, the border space surveillance can be done by deploying the sensor networks e.g. using sensors to raise alarm in case of any unusual enemy movement at borders. RFID systems can be used for tracking of assets, infrastructure, and people. In military applications, it is very crucial to get the information quickly. For example, if enemy movement is seen at a particular location then immediate replenishment of the arms and logistics, attention to causalities and so on. When sensor networks and RFID system gets connected securely using the Internet, the information could be quickly passed on to the head quarters and immediate decisions could be taken in any alarming situation, thus saving the lives and infrastructure. The application areas of IoT can be extended to other domains also by which every real-world *things* would be able to communicate to others using the Internet.

VI. CONCLUSION

In this paper, we have discussed the technology, security and applications of IoT. Undoubtedly, IoT's scope shows tremendous potential in real-world applications. It is the aspiration that IoT is going to penetrate into each and every aspect of our life, the security of the communication at this global level and privacy of the people and "things" involved is one of the most important requirements of IoT. We discussed the security and privacy issues in WSN and RFID systems, which are two important existing infrastructures that will play significant roles in IoT. Due to heterogeneous devices involved in IoT, we anticipate the *interoperability* issues such as capability mismatch, difference in communication and processing bandwidth and different security solution requirements. This also requires standardization of semantics of data apart from protocol and data frames. Furthermore, the acceptance of IoT depends on users' and service providers' trust on the system and control over their information being shared on the network. With IoT, where all the objects would have digital identities, the ownership of the objects as well as data is also an important concern to make IoT infrastructure robust and scalable.

Acknowledgement. This work is supported in part by Department of Science and Technology, Ministry of Science & Technology, Government of India through DST/INT/SPAIN/P-6/2009 Indo-Spanish Joint Programme of Cooperation in Science and Technology.

VII. REFERENCES

[1] "The IPv6 Challenge Part 1, A Service Provider guide to the Basics, Transition Strategies, and Implementation Issues". A white paper by Incognito Software, January, 2011.

[2] "ITU Internet Reports 2005:The Internet of Things". http://www.itu.int/osg/spu/publications/internetofthings/. (as on 19 Sep 2011)

[3] J. Newmarch and P. Tam. "Issues in Ownership of Internet Objects". *International Conference on Electronic Commerce Research*, 2002.

[4] "CERP-IoT: Cluster of European Research Projects on the Internet of Things". *Integration in CERP–IoT Cluster Description for cluster Book.doc*

[5] C. Petrie. "The Future of the Internet is Coordination*". Future Enterprise Systems Workshop*, 2010.

[6] R. Weber, R. Weber. "Internet of things: legal perspectives". *Springer*. June 2010.

[7] K. Ashton. "That 'Internet of Things' Thing". http://www.rfidjournal.com/article/view/4986. (as on 19 Sep 2011)

[8] "Internet of Things -Strategic Research Roadmap". *Developed by European Research Projects on the Internet of Things (CERP-IoT),* 2009.

[9] X. Xing, J. Wang, M. Li. "Services and Key Technologies of the Internet of Things". *ZTE Communications* No. 2, 2010

[10] C. Huang. "An Overview of RFID Technology, Application, and Security/Privacy Threats and Solutions". *George Mason University, Scholarly paper*, 2009.

[11] C. Alcaraz, P. Najera, J. Lopez and R. Roman. "Wireless Sensor Networks and the Internet of Things: Do We Need a Complete Integration?". *International Workshop on the Security of The Internet of Things* (SecIoT), 2010.

[12] R. Jehadeesan and J. Rajan. "Mobile communication Technologies". library.igcar.gov.in/readit-2005/conpro/info mgt/s2-7.pdf (as on 19 Sep 2011)

[13] S. Radomirovic. "Towards a model for security and privacy in the Internet of things". *International Workshop on the Security of the Internet of Things* (SecIoT'10). 2010.

[14] S. A. Weis, S. Sarma, R. Rivest, and D. Engels. "Security and privacy aspects of low-cost radio frequency identification systems". *First International Conference on Security in Pervasive Computing*, LNCS 2802, pp.201–212. 2003.

[15] M. Langheinrich. "A survey of RFID privacy approaches". *Personal Ubiquitous Computing*, Vol 13, Issue 6, pp. 413–421, 2009.

[16] "IRIS Datasheet". http://www.memsic.com/products/wireless-sensor-networks/wireless-modules.html (as on 19 Sep 2011)

[17] "SunSPOT sensor nodes". https://www.sunspotworld.com/ (as on 19 Sep

2011)