Internet of Things: Challenges and Opportunities

S. C. Mukhopadhyay and N. K. Suryadevara

Abstract The term Internet of things (IoT) is used to describe embedded devices (things) with Internet connectivitsy, allowing them to interact with each other, services, and people on a global scale. This level of connectivity can increase reliability, sustainability, and efficiency by improved access to information. Environmental monitoring, home and building automation and smart grids could be interconnected, allowing information to be shared between systems that affect each other. Giving these systems better awareness can improve their efficiency, reliability and sustainability. Due to the large number of applications the IoT has the potential to replace people as the largest consumer and producer of information on the Internet. Low powered wireless embedded devices are cost effective and require little infrastructure, however the Internet and its protocols are unsuitable for such devices due to a lack of resources. IPv6 over low-power wireless area networks (6LoWPAN) was created for this purpose by the Internet Engineering Task Force (IETF). The IETF created the standards the Internet operates on. 6LowPAN allows low powered wireless devices to behave like any other Internet connected device with some restrictions. This chapter will give an introduction of the status of IoT along with the challenges and opportunities of making the IoT.

1 Introduction and Literature Review

The use of internet is increasing steadily over the years. As per the statistics [1], the number of internet users at the end of 2011 exceeded 2.2 billion and the details of the users based on geographical distribution as shown in Fig. 1. Providing internet facility is a financially costly resources and it may be extremely valuable proposition to think

S. C. Mukhopadhyay (✉) · N. K. Suryadevara
School of Engineering and Advanced Technology, Massey University,
Palmerston North, New Zealand
e-mail: S.C.Mukhopadhyay@massey.ac.nz

S. C. Mukhopadhyay (ed.), *Internet of Things*, Smart Sensors,
Measurement and Instrumentation 9, DOI: 10.1007/978-3-319-04223-7_1,

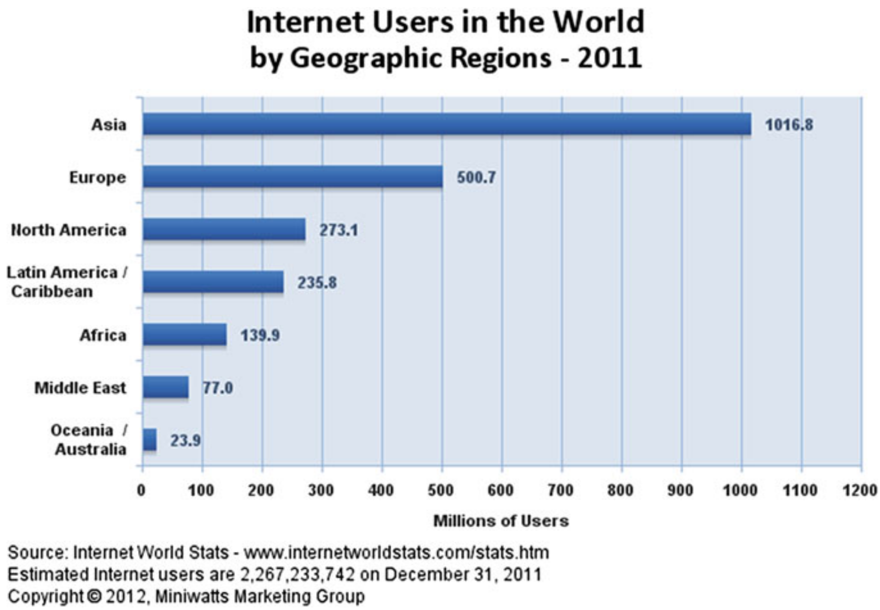

Fig. 1 The internet users in the world by geographic regions [1]

of internet for other applications. The internet can be used to transmit the sensing data collected from widely distributed regions such as measurement of environmental parameters.

The percentage of internet users based on the geographic regions is shown in Fig. 2. From Fig. 2 it is seen that a huge percentage of populations in many countries are still not enjoying the internet and there is a strong possibility of growth of internet in near future.

In recent times an enormous amount of research and development works are carried out in different parts of the world to make Internet of Things to be feasible. Every THING in this world will be connected to each other via INTERNET so that we can know anything we want to know.

Though the term "Internet of Things" was proposed by Kevin Ashton [2, 3] in 1999 but 'The Internet of Things' is a concept originally coined and introduced by MIT, Auto-ID Center and intimately linked to RFID and electronic product code (EPC) [4, 3]. The IoT literally means, "… all about physical items talking to each other..". Machine-to-machine communications and person-to-computer communications will be extended to things. Technologies that will drive the future Internet of Things: Sensor technologies including RFID, smart things, nanotechnology and miniaturization. The concept of the Internet of Things is now being influenced strongly by developments in computing and network ubiquity and developments in the next generation Internet—and considered at all levels including United Nations [5].

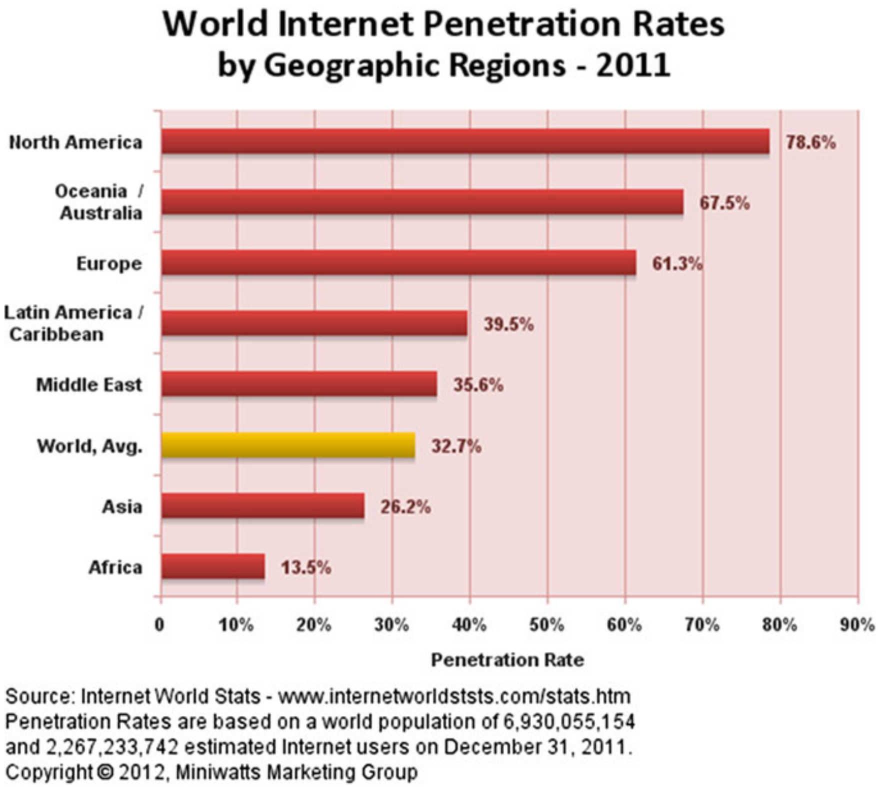

Fig. 2 The percentage internet users in the world by geographic regions [1]

"We are heading into a new era of ubiquity, 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 the Internet will be dwarfed by those prompted by the networking of everyday objects" [3]. The importance of IoT in future can be perfectly visualized with the help of Fig. 3 [6]. It shows that there will be many times connected devices that the population in another few years' time. In future, it will use the Internet as a scaffold to support and transmit its sensations. It may consist of millions of embedded electronic measuring devices: thermostats, pressure gauges, pollution detectors, cameras, microphones, glucose sensors, ECGs, electroencephalographs. These will probe and monitor cities and endangered species, the atmosphere, our ships, highways and fleets of trucks, our conversations, our bodies-even our dreams.

A significant amount of research papers, both in journal and conferences are reported in the last few years. A special issue has recently been published by IEEE Sensors journal, Vol. 13. No. 10, October 2013 in which 35 papers have reported different works on IoT architecture, protocols, services and different applications [7].

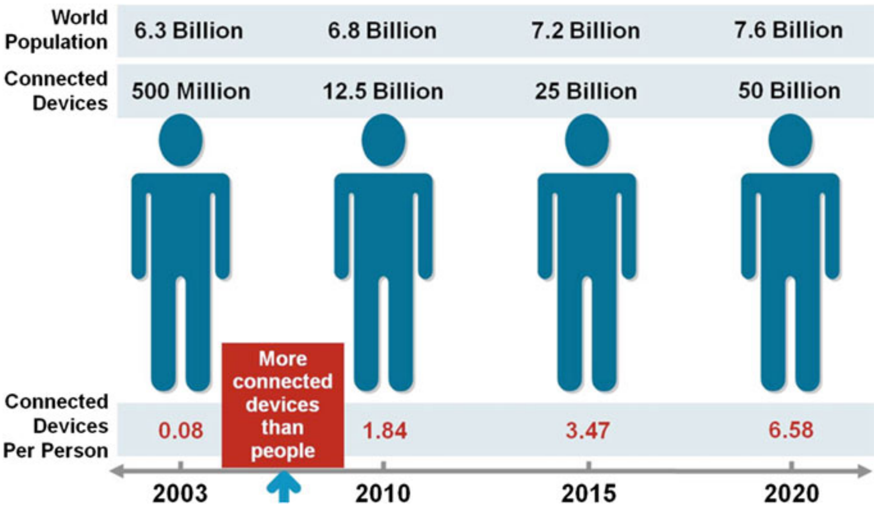

Fig. 3 The comparison of connected devices with human population [6]

A survey on IoT and future visions are reported in [8, 9]. CERP-IoT, cluster of European Research Project on the Internet of Things described the vision and challenges for realizing the Inter of Things [10]. In IEEE Xplore with the search words "Internet Of Things" gives 2071 articles, mostly published in different international conferences held in recent times (2010–2013).

A report titled "The Internet of Things Business Index: A quiet revolution gathers pace" [11], also found that 30 % of business leaders feel that the IoT will unlock new revenue opportunities, while 29 % believe it will inspire new working practices, and 23 % believe it will eventually change the model of how they operate [11]. The study found that European businesses are ahead of their global counterparts in the research and planning phases of implementing IoT [12]. Meanwhile, manufacturing is the leading sector when it comes to research and implementation of IoT technologies, driven in part by the need for real-time information to optimize productivity [12].

According to the report [11], the top five concerns that companies have around the IoT are: a lack of employee skills/knowledge; a lack of senior management knowledge and commitment; products or services that don't have an obvious IoT element to them; immaturity of industry standards around IoT; and high costs of required investment in IoT infrastructure [11]. The 779 respondents came from 71 countries across Europe (29 %), North America (29 %), Asia-Pacific (30 %) and rest of the world (12 %) [11]. However, a few steps need to be taken if the IoT revolution is to really take off [11]. The report suggests that data silos need to be removed and common standards need to be established in order to allow the IoT to scale to a size that will allow it to operate across all markets successfully [11].

In June 2013 The Economist Intelligence Unit conducted a global survey of 779 executives [13]. Some of the responses to the survey are highlighted in Fig. 4.

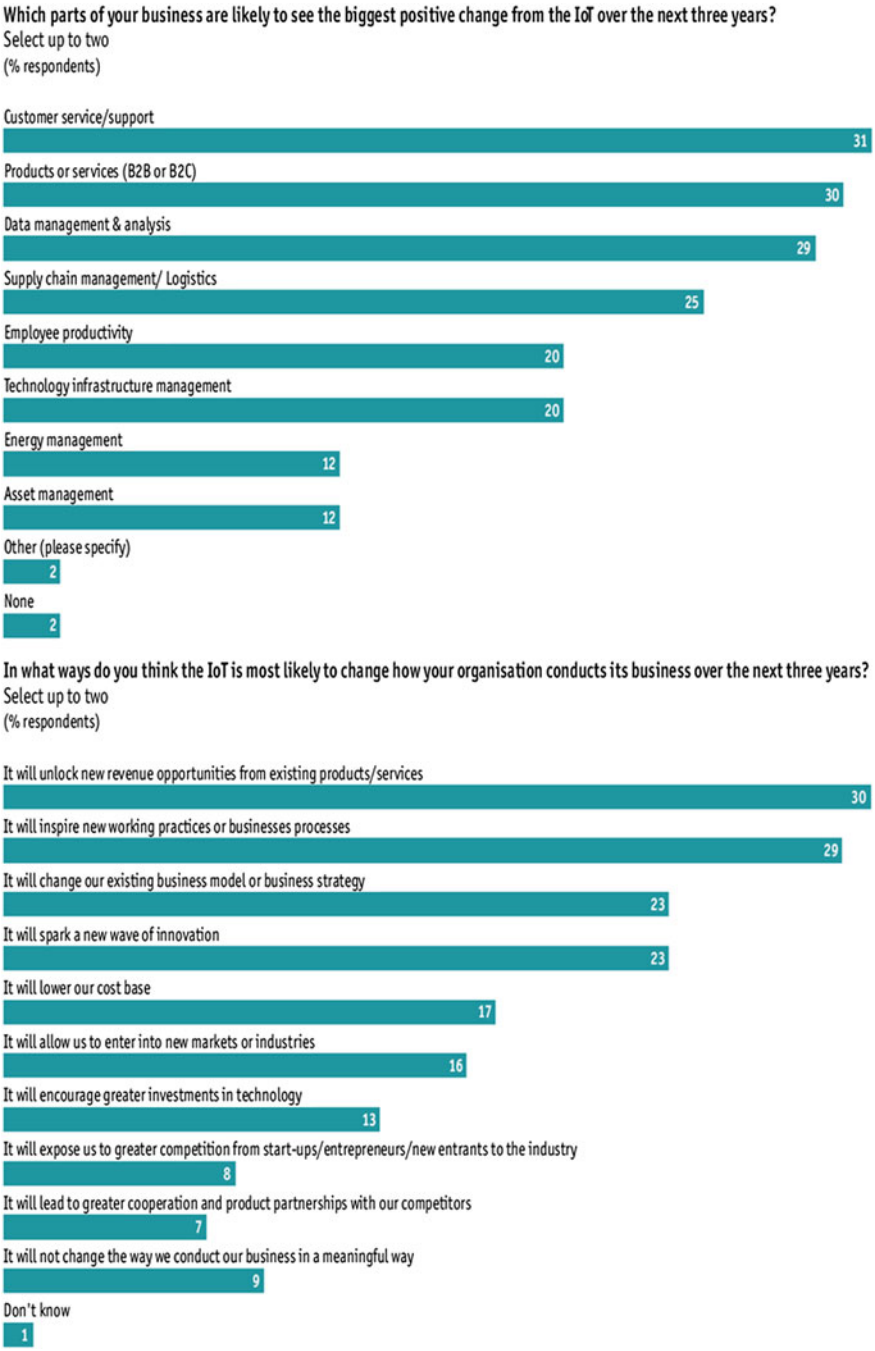

Fig. 4 Changes in the business perspective for the next 3 years [11]

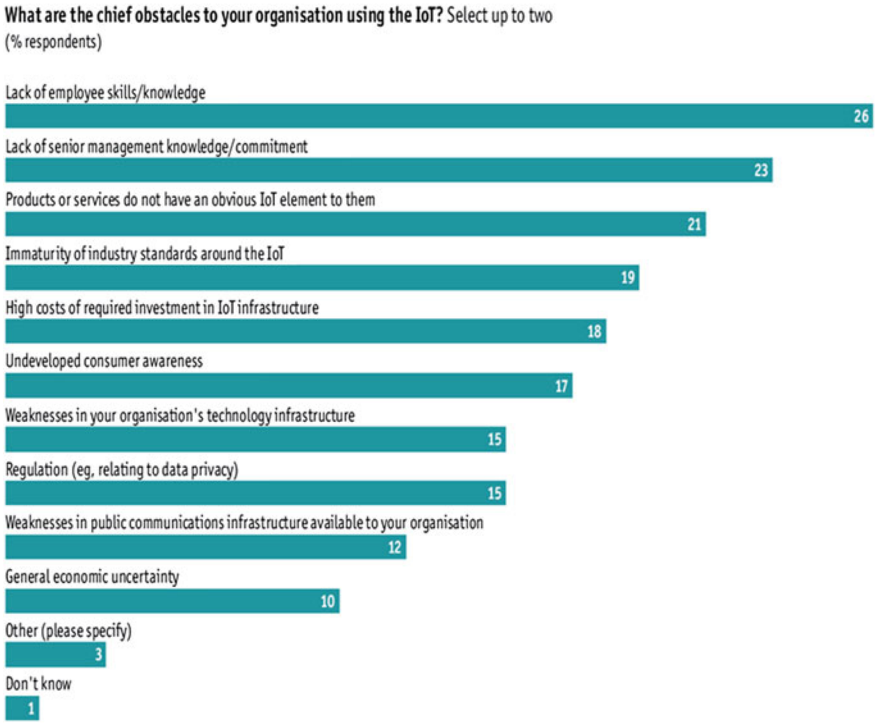

Fig. 5 Some of the main obstacles, businesses are facing in implementing IoT [11]

One of the biggest obstacles of using the IoT is the perception that products or services do not have any obvious IoT application (see Fig. 5) [11].

The full potential of the IoT will be unlocked when small networks of connected things, from cars to employee IDs, become one big network of connected things extending across industries and organizations [11]. Since many of the business models to emerge from the IoT will involve the sale of data, an important element of this will be the free flow of information across the network [11].

Another interesting fact is that the internet connectable consumer household devices will increase significantly in the next decade, with the computer network equipment that accounts for the majority of household devices, at about 75 % in 2010 and declining to 25 % by 2020 [10]. Figure 6 shows the share of Internet-Connectable consumer household devices by different types.

The IoT research needs including various technologies in terms of hardware and software are listed in the following Table 1.

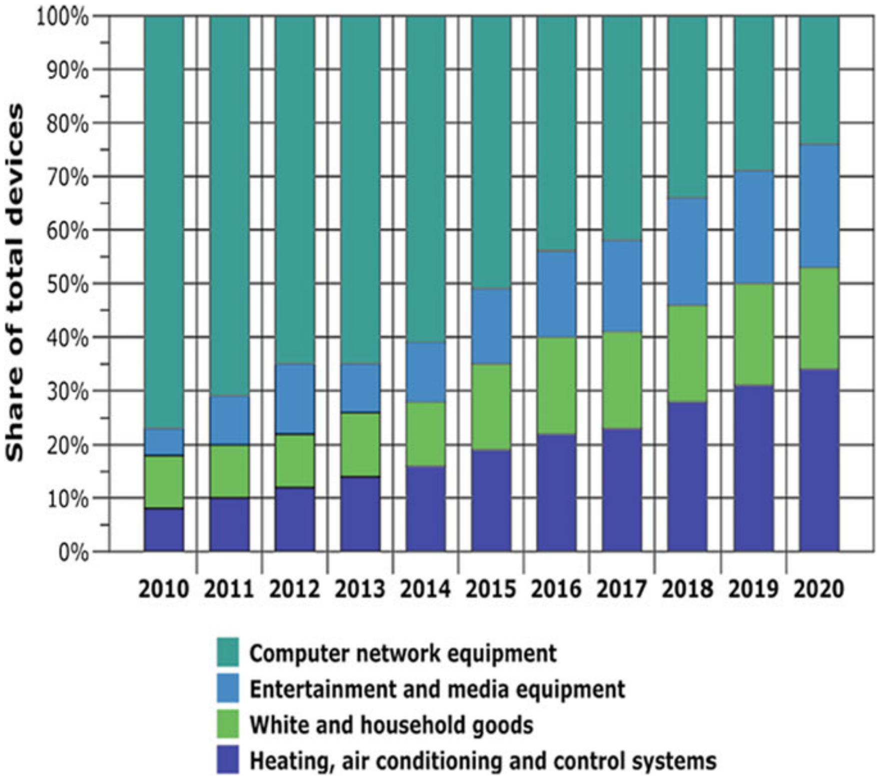

Fig. 6 Share of internet-connectable consumer household devices by type [10]

2 Challenges and Opportunities of IoT

Though development of many IoT based systems are reported there are many design challenges faced by the developers and engineers. Among many issues such as availability of internet, miniaturization, the IoT is entirely dependent on the development of Wireless Sensor Networks (WSN) and Radio Frequency Identification devices (RFID).

The wireless sensors are the extension of smart sensors with communication along with adaptation and learning capability. There are many wireless devices available around us with different functionality. The wireless devices offer many advantages in terms of cost, flexibility, power options, ease of installation and replacement. Figure 7 shows the normal situation in a house where there are so many chargers for different appliances and the wires get tangled with each other. It becomes very annoying to find the right devise at the right time so a labeling is required. The problem may be easily avoided if all the devices are made wireless eliminating the need of wired chargers. So the wireless devices may be designed with some form of

Table 1 Internet of Things scenario [14]

IoT-research needs	2011–2015	2015–2020	Beyond 2020
Identification technology	• Convergence of IP and IDs and addressing scheme • Unique ID • Multiple IDs for specific cases • Extend the ID concept (more than ID number) • Electromagnetic Identification (EMID)	Beyond EMID	Multi methods-one ID
IoT architecture	• Extranet (extranet of things) • Partner to partner applications, basic interoperability, billions-of-things	• Internet (Internet of Things) (global scale applications, global interoperability, many trillions of things)	
SOA software services for IoT	• Composed IoT services (IoT services composed of other services, single domain, single administrative entity)	• Process IoT services (IoT Services implementing whole processes, multi/cross domain, multi administrative • entities, totally heterogeneous service infrastructures)	
Internet of things architecture technology	• Adaptation of symmetric encryption and public key algorithms from active tags into passive tags • Universal authentication of objects • Graceful recovery of tags following power loss • More memory • Less energy consumption • 3-D real time location/position embedded systems • IoT governance scheme	• Code in tags to be executed in the tag or in trusted readers • Global applications • Adaptive coverage • Context awareness • Object intelligence • Context awareness	• Intelligent and collaborative functions

(continued)

Table 1 (continued)

IoT-research needs	2011–2015	2015–2020	Beyond 2020
Communication technology	• Long range (higher frequencies—tenth of GHz)	• On chip networks and multi standard RF architectures	• Self configuring, protocol seamless networks
Network technology	• Grid/Cloud network • Hybrid networks • Adhoc network formation • Self-organizing wireless mesh networks • Multi authentication • Sensor RFID-based systems • Networked RFID-based systems—interface with other networks—hybrid systems/networks	• Service based network • Integrated/Universal authentication • Brokering of data through market mechanisms	• Need based network internet of everything robust security based on combination of ID metrics autonomous systems for nonstop information technology service
Software and algorithms	• Self-management and control • Micro operating systems • Context aware business event generation • Interoperable ontologies of business events • Scalable autonomous software • Software for coordinated emergence • (Enhanced) Probabilistic and non-probabilistic track and trace algorithms, run directly by individual "things" • Software and data distribution systems	• Evolving software • Self-reusable software autonomous things: • Self configurable • Self-healing • Self-management • Platform for object intelligence	• Self-generating "molecular" software • Context aware software

(continued)

Table 1 (continued)

IoT-research needs	2011–2015	2015–2020	Beyond 2020
Hardware devices	• Paper thin electronic display with RFID • Ultra low power EPROM/FRAM	• Polymer based memory • Molecular sensors	• Biodegradable antennas • Autonomous “bee” type devices
Power and energy storage technologies	• Printed batteries • Photovoltaic cells • Super capacitors • Energy conversion devices • Grid power generation • Multiple power sources	• Paper based batteries • Wireless power everywhere, anytime. • Power generation for harsh environments	• Biodegradable batteries
Security and privacy technologies	• Adaptation of symmetric encryption and public key algorithms from active tags into passive tags • Low cost, secure and high performance identification/authentication devices	• Context based security activation algorithms • Service triggered security • Context-aware devices • Object intelligence	Cognitive security systems
Standardization	• Privacy and security cantered standards • Adoption of standards for “intelligent” IoT devices • Language for object interaction	• Dynamic standards • Adoption of standards for interacting devices	• Evolutionary standards • Adoption of standards for personalized devices

Fig. 7 A few practical wired devices at home

energy harvesting scheme and that need to be sustainable and cost-effective. This is a challenge for the designer but at the same time it provides an opportunity to design electronics which will not be power hungry.

The challenges of IoT can be summarized as:

- Availability of internet at everywhere and at no cost
- Security issues
- Low-cost smart sensing system development
- Energy
- Computational ability
- Scalability
- Fault Tolerance
- Power Consumption
- Acceptability among the society

The success of IoT is entirely dependent on the availability of internet at everywhere. It is seen from Fig. 2 that except North America, Europe and Oceania, over 50 % of population of the rest of the world still do not have access of internet. Figure 8 shows the availability of internet in the New Zealand in relation to an internet service provider.

There is a huge need of internet growth to make it available to everyone in the world. Moreover, the availability of internet to people does not mean that the internet is available to every remote corner of the world. In order to make it available to every parts of the world there is a need of huge investment of providing infrastructure and resources. The investment from private companies is not expected unless there is a clear indication of making profit so the government needs to come in picture. Under the current economic situation it will not be a quick decision for any government to go for it. But with time it is expected to happen.

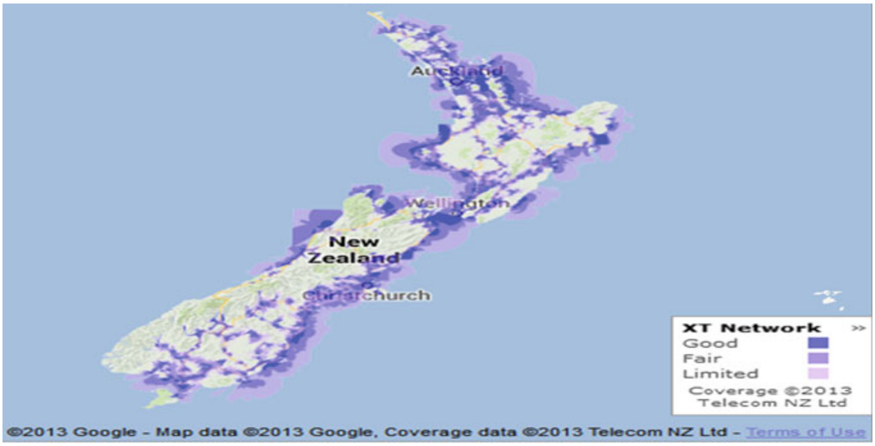

Fig. 8 Internet service availability in the New Zealand

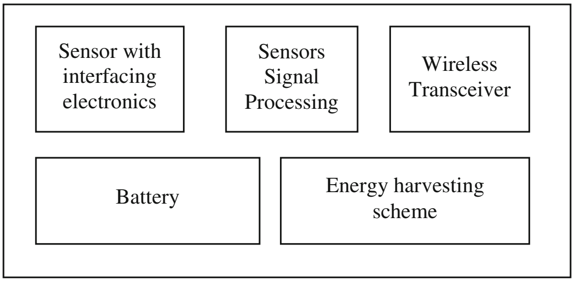

Fig. 9 The block diagram representation of wireless sensor node

A few countries such as Taiwan and China [15] are planning to have availability of internet at every parts of the country within a few years' time. It is expected that those action will inspire other countries to follow. Moreover, the internet needs to be available at free of cost and that may not be very easy to decide. It is not only the installation expenses, there is a running cost involved too. Along with the availability of internet there come the security issues. Under the current volatile situation where terrorism becomes a common word of people's life, accessibility of internet without any security may be a big ask. Then the design and development of internet without any security risk or threat may be huge challenge and that will gives an opportunity to the engineers. In relation to security to internet as well as in the wireless sensor network there may be malicious use. There can be use of sensor networks for illegal purposes, e.g. planting them in computers to extract private information. This is a challenge as this might happen at any time. So the challenge is to develop appropriate countermeasure.

The countermeasures could be to deploy sensor detectors to detect malicious sensor nets. It will not protect illegal sensor network deployment, but will make attacks expensive. So that's an opportunity for the developers of IoT. Since IoT will have trillions of sensor nodes around us and in the environment, the most important challenge is to develop and fabricate them very cheap [16]. A sensor node consists of a few blocks as is shown in Fig. 9. It is possible to develop the node cheap if all the five blocks can be fabricated from one fabrication process but it has got huge challenges. At the moment it is not possible to fabricate everything in one chip but it offers a huge opportunity to the designers to achieve it. It is expected to have a very tiny sensor node with all the functionality as shown in Fig. 9 to be available for use.

One of the important challenges is the power supply for sensor nodes. Usually batteries are used to supply the necessary energy required for sensor signal processing and communication.

The following parameters should be considered for the selection of batteries:

- Type of battery (Alkaline, Lithium-Ion, NiCad, NiMH, Lead-Acid)
- Life-time (Ahr requirement)
- Environmental impact
- Cost
- Size
- Memory effect
- Safety issue.

The Opportunity here lies on the development of environmentally friendly new types of rechargeable batteries. The rechargeable batteries will need to be charged from different renewable energy sources. Figure 10 shows the established renewable energy sources, wind and solar. The choice of wind energy may not be limited for sensor nodes due to its initial investment and availability of wind. So there is a need of Accelerating the Implementation of Environmentally Friendly Renewable Energy Systems.

There are some challenges and consequently opportunities on the development of renewable energy sources for powering sensor nodes:

Challenge—The world looks increasingly towards implementing renewable energy systems $\rightarrow$ but the large potential for renewable energy has not been realized due to many barriers.

Opportunity—An important task is to identify the means to remove the economic, regulatory, and institutional disadvantages that make renewable energy less competitive than other conventional sources.

Most of the energy is consumed for data communication and different protocols are reported to address the issues [17]. Though there can be different strategies but from the design consideration and users' perspective it may be useful to follow a standard. In recent times there is a growing interest to follow IEEE protocols especially zigbee and Wi-Fi for different wireless applications [18–23]. A few projects have been developed based on zigbee protocols [24–27].

Fig. 10 Established renewable energy source

Fig. 11 Dumped computers

3 E-Waste

It may be good to have the environment surrounded by millions of sensors but we need to realize that the life-span of electronic devices is not long enough. Replacement needs to be done at regular interval in order to make the complete system active all the time. But it becomes a practical problem and it is a nuisance to find the place to dump the old electronic devices. Figure 11 shows the old computer stacked at the corridor of a university in New Zealand. Usually the computers of the academic staff are replaced at every four years. In the particular case the computers were lying on the corridor for over 3 months.

The designer must be very aware of the situation as the problem is severe: As per the UN report [28], a few statistical figures in US alone are:

Between 1997 and 2007, over 500 million personal computers have become obsolete-almost two computers for each person.

15,000,000 PCs become obsolete every year.

7,000,000 computers will end up stockpiled for at least 3 years.

750,000 computers will end up in landfills this year alone.

It seems “Every day nearly 1,000 computers and 1,400 cell phone sets are being sold in India amounting to 7,000 tons per year of e-waste and that too in major cities only”. The report predicts that in South Africa and China, by 2020 e-waste from old computers will have jumped by 200–400 % from 2007 levels and by 500 % in India.

WSN contain hazardous and toxic materials that pose environmental risks if they are land filled or incinerated in future. Printed circuit boards contain primarily plastic and copper, and have small amounts of chromium, lead solder, nickel, and zinc.

In addition, WSN have batteries that often contain nickel, cadmium, and other heavy metals. Relays and switches, especially older ones, may contain mercury. Also, capacitors in some types that are now entering the waste stream may contain polychlorinated biphenyls (PCBs).

So guidelines to tackle the problems are [28]:

- Reuse is the environmentally preferable option for managing older electronic equipment. Extending the life of old products minimizes the pollution and resource consumption associated with making new products.
- Reuse also gives people who cannot afford new products access to electronic equipment at reduced or no cost.
- Electronic equipment which are too old and commercially and practically not viable for reuse or is broken beyond repair may be sent for disassembly i.e. salvaging parts, and selling reclaimed materials.
- Several electronic equipment, such as computers, monitors, printers, and scanners, contain materials suitable for reclamation and use in new products. These may include plastic, glass, steel, aluminum, copper, gold, silver, and other metals.

But re-use of old equipment will not solve the problem as it will just delay the process for a few years. This is a challenge for the engineering to come out with a solution how to deal with the e-waste situation.

We think here lays the opportunity for the engineers cum designers to design Biodegradable and Non-Hazardous sensor nodes. In future we need to explore materials which will not have any negative environmental impact and are suitable for fabricating sensor nodes.

More IoT-specific skills are needed for the next stage of development. A lack of IoT skills and knowledge among employees and management is viewed as the biggest obstacle to using the IoT more extensively [11]. To address these gaps, organisations are training staff and recruiting IoT talent, raising the potential for IoT talent wars. Others are hiring consultants and third-party experts, seeking to build knowledge and identify successful IoT business models. Moving executives and employees up the IoT learning curve should also help to ease the difficulty many firms experience in identifying IoT applications for existing products and services [11].

Big data, big privacy issues data, are thus a fundamental component of the IoT’s future [11]. Fitting sensors to a potentially infinite number of “things” will generate untold amounts of new information [11]. For now, however, most business leaders are confident that their organizations will be able to manage and analyze the data flowing from the predicted rapid expansion in IoT networks [11].

4 Conclusions

This chapter has briefly described different issues towards practical realization of Internet of Things. Though a lot of research going on towards technical implementation of IoT and will have positive impact on the society. At the same time many issues are arising which needs proper and appropriate attention to deal with them. The IoT should not be considered as a local development rather it is a global phenomenon and need to be treated with sincerity and priority.

References

1. http://www.internetworldstats.com/stats.htm. Accessed 10 Nov 2013
2. Kevin, A.: That 'Internet of Things' thing, in the real world things matter more than ideas. RFID J. (22 June 2009). Accessed 10 Nov 2013
3. http://en.wikipedia.org/wiki/Internet_of_Things. Accessed 10 Nov 2013
4. Analyst Geoff Johnson interviewed by Sue Bushell in Computerworld, on 24 July 2000 (M-commerce key to ubiquitous internet)
5. http://ec.europa.eu/information_society/policy/rfid/events/past/Info18022009/index_en.htm. Accessed 10 Nov 2013
6. Evans, D.: The Internet of Things: How the next evolution of the internet is changing everything, Cisco White paper. http://www.cisco.com/web/about/ac79/docs/innov/IoT_IBSG_0411FINAL.pdf (2011). Accessed 10 Nov 2013
7. Guest editorial on special issue on internet of things (IoT): architecture, protocols and services. IEEE Sens. J. **13**(10), 3505–3510 (2013)
8. Atzori, L., Antonio Iera, b., Giacomo Morabito, C.: The internet of things: a survey. Comput. Netw. (2010). doi:10.1016/j.comnet.2010.05.010
9. Gubbi, J., Buyya, R., Marusic, S., Palaniswami, M.: Internet of things (IoT): a vision, architectural elements, and future directions. Future Gener. Comput. Syst. **29**(7), 1645–1660 (2013)
10. Sundmaeker, H., Guillemin, P., Friess, P., Woelfflé, S. (eds.): Vision and Challenges for Realising the Internet of Things. http://www.theinternetofthings.eu/sites/default/files/Rob%20van%20Kranenburg/Clusterbook%202009_0.pdf. Accessed March 2010
11. http://www.arm.com/files/pdf/EIU_Internet_Business_Index_WEB.PDF. Accessed 10 Nov 2013
12. http://news.techworld.com/networking/3476043/arm-report-businesses-look-make-money-through-internet-of-things-revolution/. Accessed 10 Nov 2013
13. http://www.economistinsights.com/search/node/internet%20things%20business%20index. Accessed 10 Nov 2013
14. Vermesan, O., Harrison, M., Vogt, H., Kalaboukas, K., Tomasella, M., et al. (eds.): The Internet of Things—Strategic Research Roadmap. Cluster of European Research Projects on the Internet of Things (CERP-IoT) (2009)
15. http://en.wuxi.gov.cn/web111/Events/InternetofThings/AboutInternetofThings/index.shtml. Accessed 10 Nov 2013

16. Mukhopadhyay, S.C.: Intelligent Sensing, Instrumentation and Measurements, Smart Sensors, Measurement and Instrumentation, vol. 5. ISBN: 978-3-642-37026-7 (Print) 978-3-642-37027-4 (Online) (2013)
17. Villalba, L.J.G., Orozco, A.L.S., Cabrera, A.T., Abbas, C.J.B.: Routing protocols in wireless sensor networks. Sensors **9**(1), 8399–8421 (2009). doi:10.3390/s91108399, ISSN 1424-8220, www.mdpi.com/journal/sensors
18. ZigBee Alliance: Understanding ZigBee gateway, ZigBee Document 095465r13, Sept 2010
19. Howitt, I., Gutierrez, J.A.: IEEE 802.15.4 low rate -wireless personal area network coexistence issuues. In: Proceedings of the IEEE-Wireless Communications and Networking Conference (WCNC 2003), vol. 3, No. 20, pp. 1481–1486 (New Orleans, 2003)
20. Angrisani, L., Bertocco, M., Foortin, D., Sona, A.: Assessing coexistence problems of IEEE 802.11b and IEEE 802.15.4 wireless networks through cross-layer measuremennts. In: IEEE Instrumentation and Measurement Technology Conference Proceedings (IMTC 2007), 1–3 May 2007, pp. 1–6
21. Khaleel, H., Pastrone, C., Penn a, F., Spirito, M.A., Garello, R.: Impact of Wi-Fi traffic on the IEEE 802.15.4 channels occupation in indoor environments. In: International Conferrence on Electromagneticcs in Advanced Applications (ICEAA ’09), 14–18 Sept 2009, vol. 2, pp. 1042–1045
22. Khoshdelniat, R., Sinniah, G.R., Bakar, K.A, Shaharil, M.H.M, Suryady, Z., Sarwar, U.: Performance evaluation of IEEE802.15.4 6LoWPAN gateway. In: Proceedings of the 17th Asia-Pacific Conference on Communications (APCC), pp. 253–258 (2011)
23. Kushalnagar, N., Montenegro, G., Hui, J., Culler, D.: Transmission of IPv6 Packets over IEEE 802.15.4 Networks, RFC 4944 (2007)
24. Suryadevara, N.K., Mukhopadhyay, S.C., Wang, R., Rayudu, R.K.: Forecasting the behavior of an elderly using wireless sensors data in a smart home. Engineering Applications of Artificial Intelligence **26**(10), 2641–2652 (2013)
25. Kelly, S.D.T., Suryadevara, N.K., Mukhopadhyay, S.C.: Towards the implementation of IoT for environmental condition monitoring in homes. IEEE Sensors Journal **13**(10), 3846–3853 (2013)
26. Suryadevara, N.K., Mukhopadhyay, S.C.: Wireless sensor network based home monitoring system for wellness determination of elderly. IEEE Sensors Journal **12**(6), 1965–1972 (2012)
27. Suryadevara, N.K., Gaddam, A., Rayudu, R.K., Mukhopadhyay, S.C.: Wireless sensors network based safe home to care elderly people: behaviour detection. Sens. Actuators A: Phys. **186**, 277–283 (2012)
28. http://www.thegreenitreview.com/2010/02/un-reports-on-rocketing-e-waste-problem.html. Accessed 10 Nov 2013