An Overview of Internet of Things (IoT): From Literature Survey to Application Implementation Perspective

Rajinder Tiwari

Asst. Professor, Department of Electrical & Electronics Engg, Amity University, Lucknow, Uttar Pradesh, India

---***---

Abstract - *The government has adopted in the field of "Internet of Things" as national strategic project, announcing that it is a master plan to achieve a leading country of a hyper-connected digital revolution. The government has a promotional strategy of reinforcing the competitiveness in software (SW) sensor and its application based component and devices. IoT basically refers to the internet environment where people and machines all are connected to the guided and unguided network so as to mutually collect, create, utilize, and share information and services that includes sensors i.e. input information, devices for acquisition, clyde sharing of data i.e. utilization for application software. This domain has been highly exploited in the present scenario due to the effect of increasing export businesses and jobs opportunities. It has a tendency to grow in the future as IoT is extended from social infrastructure (transportation, utilities, automation, etc.) and safety management to the consumer sector centered on the life services. The future scope of IoT, which will transform any real world object into intelligent virtual object. The IoT aims to unify everything in this world under a common infrastructure; giving us not only controls of the things around us, but also keeping us informed of that the state of the things. In this discussion, the authors have presented a study that addresses IoT concepts through systematic review of corporate white papers, scholarly research papers, professional discussions with experts and online databases. Moreover this research article focuses on definitions, geneses, basic requirements, characteristics and aliases of Internet of Things. Many technical communities are vigorously pursuing research that contribute to the Internet of Things (IoT) domain. In today's world , as sensing, communication, actuation, and control become ever more sophisticated and ubiquitous, there is significant overlap in these communities, sometimes from slightly different perspectives. Internet which is a revolutionary invention and is always transforming into some new kind of software and hardware making it unavoidable for anybody. The form of communication which we see now is either human-device or human-human, but Internet of Things (IoT) promises a great future for internet where a type of communication is device-device (D2D) or machine-machine (M2M). The authors have also aims to provide the comprehensive overview of IoT reviews and scenario it's enabling technologies and a sensor network. The IoT is an innovative idea which will transform any real world object into intelligent virtual objects in the future. It enables user to identify everything in this world uniquely, take control over identified the things (e. g. Door Locks, Microwave, Lights, TV, Coffee Maker etc.) and keep informed about state of the things. This term IoT describes several technologies and research disciplines which tells that the internet reachable to every real world physical objects.*

***Key Words*:** IoT, IPv6, EPC, Bluetooth, ZigBee, Sensors, Actuators, Mobile Computing, Wireless Sensor Networks, Operating System for IoT, Applications of IoT.

1. INTRODUCTION

Smart devices. Smartphones. Smart cars. Smart homes. Smart cities. A smart world. These notions have been espoused for many years. Achieving these goals has been investigated, to date, by many diverse and often disjoint research communities. Five such prominent research communities are: Internet of Things (IoT), Mobile Computing (MC), Pervasive Computing (PC), Wireless Sensor Networks (WSN), and most recently, Cyber Physical Systems (CPS). However, as technology and solutions progress in each of these fields there is an increasing overlap and merger of principles and research questions. Narrow definitions of each of these fields are no longer appropriate. Further, research in IoT, PC, MC, WSN and CPS often relies on underlying technologies such as real-time computing, machine learning, security, privacy, signal processing, big data, and others. Consequently, the *smart vision of the world* involves much of computer science, computer engineering, and electrical engineering. Greater interactions among these communities will speed.

The Internet of Things represents a vision in which the Internet extends into the real world embracing everyday objects. Physical items are no longer disconnected from the virtual world, but can be controlled remotely and can act as physical access points to Internet services. An Internet of Things makes computing truly ubiquitous – a concept initially put forward by Mark Weiser in the early 1990s. This development is opening up huge opportunities for both the economy and individuals. However, it also involves risks and undoubtedly represents an immense technical and social challenge. The Internet of Things vision is grounded in the belief that the steady advances in microelectronics, communications and information technology we have witnessed in recent years will continue into the foreseeable future. In fact – due to their diminishing size, constantly falling price and declining energy consumption – processors, communications modules and other electronic components are being increasingly integrated into everyday objects today [1-2].

"Smart" objects play a key role in the Internet of Things vision, since embedded communication and information technology would have the potential to revolutionize the utility of these objects. Using sensors, they are able to perceive their context, and via built-in networking capabilities they would be able to communicate with each other, access Internet services and interact with people. "Digitally upgrading" conventional object in this way enhances their physical function by adding the capabilities of digital objects, thus generating substantial added value. Forerunners of this development are already apparent today – more and more devices such as sewing machines, exercise bikes, electric toothbrushes, washing machines, electricity meters and photocopiers are being computerized" and equipped with network interfaces.

In other application domains, Internet connectivity of everyday objects can be used to remotely determine their state so that information systems can collect up-to-date information on physical objects and processes. This enables many aspects of the real world to be "observed" at a previously unattained level of detail and at negligible cost. This would not only allow for a better understanding of the underlying processes, but also for more efficient control and management. The ability to react to events in the physical world in an automatic, rapid and informed manner not only opens up new opportunities for dealing with complex or critical situations, but also enables a wide variety of business processes to be optimized. The real-time interpretation of data from the physical world will most likely lead to the introduction of various novel business services and may deliver substantial economic and social benefits [3-4].

2. VISION OF IoT

Many people, including myself, hold the view that cities and the world itself will be overlaid with sensing and actuation, many embedded in "things" creating what is referred to as a *smart world*. But it is important to note that one key issue is the degree of the density of sensing and actuation coverage. I believe that there will be a transition point when the degree of coverage triples or quadruples from what we have today. At that time there will be a *qualitative* change. For example, today many buildings already have sensors for attempting to save energy; home automation is occurring; cars, taxis, and traffic lights have devices to try and improve safety and transportation; people have smartphones with sensors for running many useful apps; industrial plants are connecting to the Internet; and healthcare services are relying on increased home sensing to support remote medicine and wellness. However, all of these are just the tip of the iceberg. They are all still at early stages of development. The steady increasing density of sensing and the sophistication of the associated processing will make for a significant qualitative change in how we work and live. We will truly have systems-of-systems that synergistically interact to form totally new and unpredictable services.

In 2005, ITU reported about a ubiquitous networking era in which all the networks are interconnected and everything from tires to attires will be a part of this huge network. Imagine yourself doing an internet search for your watch you lost somewhere in your house. So this is the main vision of IoT, an environment where things are able to talk and their data can be processed to perform desired tasks through machine learning. A practical implementation of IoT is demonstrated by a soon-to-be released Twine, a compact and low-power hardware working together with real-time web software to make this vision a reality [10]. However different people and organizations have their own different visions for the IoT [5-6].

An article published in Network World revealed IoT strategies of top IT vendors, they carried out some interviews from the key IT vendors. As of HP's vision, they see a world where people are always connected to their content. Cisco believes in the industrial automation and convergence of operational technology. Intel is focused on empowering billions of existing devices with intelligence. Microsoft does not consider IoT as any futuristic technology; they believe that it already exists in today's powerful devices and that the devices just need to be connected for a large amount of information which could be helpful. While, IBM has a vision of a Smarter Planet by remotely controlling the devices via secured servers. Despite of having different visions, they all agree about a network of interconnected devices therefore more developments within the coming decades are expected to be seen including that of a new converged information society [7].

3. ARCHITECTURE & BASICS OF IoT

More than 25 Billion things are expected to be connected by 2020 which is a huge number so the existing architecture of Internet with TCP/IP protocols, adopted in 1980, cannot handle a network as big as IoT which caused a need for a new open architecture that could address various security and Quality of Service (QoS) issues as well as it could support the existing network applications using open protocols. Without a proper privacy assurance, IoT is not likely to be adopted by many. Therefore protection of data and privacy of users are key challenges for IoT. For further development of IoT, a number of multi-layered security architectures are proposed i.e. a three key level architecture of IoT while described a four key level architecture. proposed a five layered architecture using the best features of the architectures of Internet and Telecommunication management networks based on TCP/IP and TMN models respectively. Similarly a six-layered architecture was also proposed based on the network hierarchical structure. So generally it's divided into six layers as shown in the Fig. 1 [8-10]. The six layers of IoT are described below:

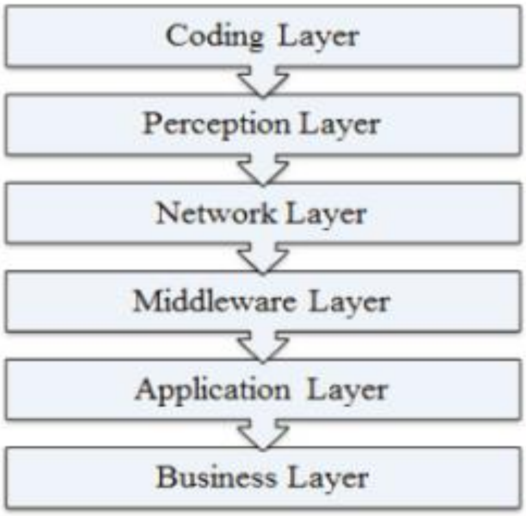

Fig -1: Six-Layered Architecture of IoT [11]

3.1 Coding Layer

Coding layer is the foundation of IoT which provides identification to the objects of interest. In this layer, each object is assigned a unique ID which makes it easy to discern the objects.

3.2 Perception Layer

This is the device layer of IoT which gives a physical meaning to each object. It consists of data sensors in different forms like RFID tags, IR sensors or other sensor networks which could sense the temperature, humidity, speed and location etc. of the objects. This layer gathers the useful information of the objects from the sensor devices linked with them and converts the information into digital signals which is then passed onto the Network Layer for further action.

3.3 Network Layer

The purpose of this layer is receive the useful information in the form of digital signals from the Perception Layer and transmit it to the processing systems in the Middleware Layer through the transmission mediums like WiFi, Bluetooth, WiMaX, Zigbee, GSM, 3G etc with protocols like IPv4, IPv6, MQTT, DDS etc.

3.4 Middleware Layer

This layer processes the information received from the sensor devices [2]. It includes the technologies like Cloud computing, Ubiquitous computing which ensures a direct access to the database to store all the necessary information in it. Using some Intelligent Processing Equipment, the information is processed and a fully automated action is taken based on the processed results of the information.

3.5 Application Layer

This layer realizes the applications of IoT for all kinds of industry, based on the processed data. Because applications promote the development of IoT so this layer is very helpful in the large scale development of IoT network. The IoT related applications could be smart homes, smart transportation, smart planet etc.

3.6 Business Layer

This layer manages the applications and services of IoT and is responsible for all the research related to IoT. It generates different business models for effective business strategies [12-18]

From a technical point of view, the Internet of Things is not the result of a single novel technology; instead, several complementary technical developments provide capabilities that taken together help to bridge the gap between the virtual and physical world. These capabilities include:

- *Communication and cooperation:* Objects have the ability to network with Internet resources or even with each other, to make use of data and services and update their state. Wireless technologies such as GSM and UMTS, Wi-Fi, Bluetooth, ZigBee and various other wireless networking standards currently under development, particularly those relating to Wireless Personal Area Networks (WPANs), are of primary relevance here.
- *Addressability:* Within an Internet of Things, objects can be located and addressed via discovery, look-up or name services, and hence remotely interrogated or configured.
- *Identification:* Objects are uniquely identifiable. RFID, NFC (Near Field Communication) and optically readable bar codes are examples of technologies with which even passive objects which do not have built-in energy resources can be identified (with the aid of a "mediator" such as an RFID reader or mobile phone). Identification enables objects to be linked to information associated with the particular object and that can be retrieved from a server, provided the mediator is connected to the network
- *Sensing:* Objects collect information about their surroundings with sensors, record it, forward it or react directly to it.
- *Actuation:* Objects contain actuators to manipulate their environment (for example by converting electrical signals into mechanical movement). Such actuators can be used to remotely control real-world processes via the Internet.

- *Embedded information processing:* Smart objects feature a processor or microcontroller, plus storage capacity. These resources can be used, for example, to process and interpret sensor information, or to give products a "memory" of how they have been used.
- *Localization:* Smart things are aware of their physical location, or can be located. GPS or the mobile phone network are suitable technologies to achieve this, as well as ultrasound time measurements, UWB (Ultra-Wide Band), radio beacons (e.g. neighboring WLAN base stations or RFID readers with known coordinates) and optical technologies.
- *User interfaces:* Smart objects can communicate with people in an appropriate manner (either directly or indirectly, for example via a smartphone). Innovative interaction paradigms are relevant here, such as tangible user interfaces, flexible polymer-based displays and voice, image or gesture recognition methods [19-26].

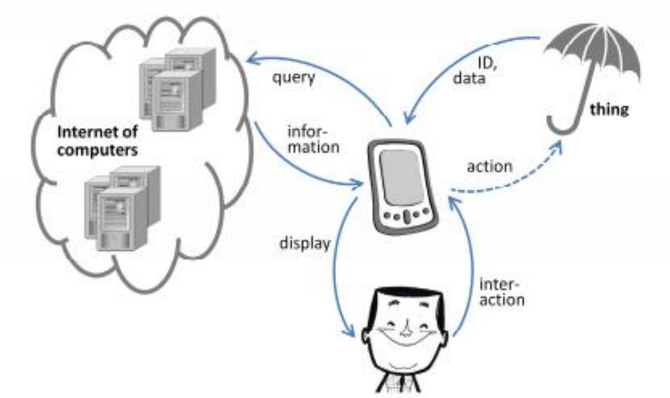

Fig -2: The smartphone as a mediator between people, things and the Internet [27].

Most specific applications only need a subset of these capabilities, particularly since implementing all of them is often expensive and requires significant technical effort. Logistics applications, for example, are currently concentrating on the approximate localization (i.e. the position of the last read point) and relatively low-cost identification of objects using RFID or bar codes. Sensor data (e.g. to monitor cool chains) or embedded processors are limited to those logistics applications where such information is essential such as the temperature-controlled transport of vaccines.

Forerunners of communicating everyday objects are already apparent, particularly in connection with RFID – for example the short-range communication of key cards with the doors of hotel rooms, or ski passes that talk to lift turnstiles. More futuristic scenarios include a smart playing card table, where the course of play is monitored using RFID-equipped playing cards. However, all of these applications still involve dedicated systems in a local deployment; we are not talking about an "Internet" in the sense of an open, scalable and standardized system [28].

4. TECHNOLOGIES

The development of a ubiquitous computing system where digital objects can be uniquely identified and can be able to think and interact with other objects to collect data on the basis of which automated actions are taken, requires the need for a combination of new and effective technologies which is only possible through an integration of different technologies which can make the objects to be identified and communicate with each other. In this section we discuss the relevant technologies that can help in the large-scale development of IoT [29].

4.1 Radio Frequency IDentification (RFID)

RFID is the key technology for making the objects uniquely identifiable. Its reduced size and cost makes it integrable into any object. It is a transceiver microchip similar to an adhesive sticker which could be both active and passive, depending on the type of application. Active tags have a battery attached to them due to which they are always active and therefore continuously emit the data signals while Passive tags just get activated when they are triggered. Active tags are more costly than the Passive tags however they have a wide range of useful applications. RFID system is composed of readers and associated RFID tags which emit the identification, location or any other specifics about the object, on getting triggered by the generation of any appropriate signal. The emitted object related data signals are transmitted to the Readers using radio frequencies which are then passed onto the processors to analyze the data [30].

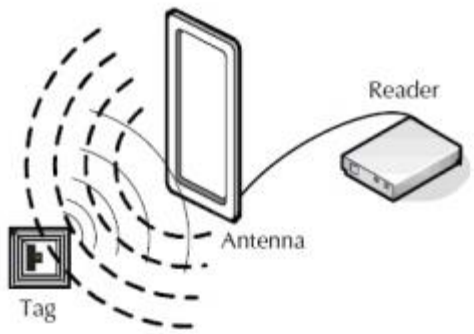

Fig -3: RFID Scenario [31]

Depending on the type of application, RFID frequencies are divided into four different frequencies ranges, which are given below:

- Low frequency (135 KHz or less)
- High Frequency (13.56MHz)

- Ultra-High Frequency (862MHz 928MHz)
- Microwave Frequency (2.4G , 5.80)

Bar Code is also an identification technology which has almost the same function as an RFID but RFID is more effective than a Bar Code due to a number of its benefits. RFID being a radio technology doesn't require the reader to be physically in its vision while Bar Code is an optical technology which cannot work unless its reader is placed in front of it. Moreover, an RFID can work as an actuator to trigger different events and it has even modification abilities which Bar codes clearly don't have [32-33].

4.2 Wireless Sensor Network (WSN)

WSN is a bi-directional wirelessly connected network of sensors in a multi-hop fashion, built from several nodes scattered in a sensor field each connected to one or several sensors which can collect the object specific data such as temperature, humidity, speed etc and then pass on to the processing equipment. The sensing nodes communicate in multi-hop Each sensor is a transceiver having an antenna, a micro-controller and an interfacing circuit for the sensors as a communication, actuation and sensing unit respectively along with a source of power which could be both battery or any energy harvesting technology. However, has proposed an additional unit for saving the data, named as Memory Unit which could also be a part of the sensing node. A typical sensing node is shown in the figure below [34-36]:

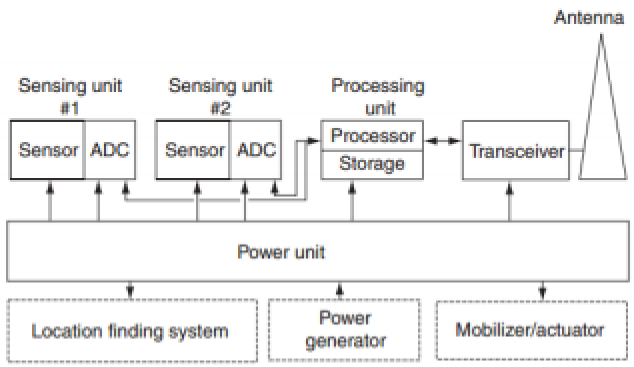

Fig -4: A typical sensing node [37]

4.3 Cloud Computing

With millions of devices expected to come by 2020, the cloud seems to be the only technology that can analyze and store all the data effectively. It is an intelligent computing technology in which number of servers is converged on one cloud platform to allow sharing of resources between each other which can be accessed at any time and any place. Cloud computing is the most important part of IoT, which not only converges the servers but also processes on an increased processing power and analyzes the useful information obtained from the sensors and even provide good storage capacity. But this is just a beginning of unleashing the true potential of this technology. Cloud computing interfaced with smart objects using potentially millions of sensors can be of enormous benefits and can help IoT for a very large scale development so researches are being carried out since IoT will be totally dependent on the Cloud Computing [38].

Fig -5: A typical Cloud Computing Scenario [39]

4.4 Networking Technologies

These technologies have an important role in the success of IoT since they are responsible for the connection between the objects, so we need a fast and an effective network to handle a large number of potential devices. For wide-range transmission network we commonly use 3G, 4G etc. but As we know, mobile traffic is so much predictable since it only has to perform the usual tasks like making a call, sending a text message etc. so as we step into this modern era of ubiquitous computing, it will not be predictable anymore which calls for a need of a super-fast, super-efficient fifth generation wireless system which could offer a lot more bandwidth. Similarly for a short-range communication network we use technologies like Bluetooth, WiFi etc [40].

4.5 Nano Technologies

This technology realizes smaller and improved version of the things that are interconnected. It can decrease the consumption of a system by enabling the development of devices in nano meters scale which can be used as a sensor and an actuator just like a normal device. Such a nano device is made from nano components and the resulting network defines a new networking paradigm which is Internet of Nano-Things [41].

4.6 Micro-Electro-Mechanical Systems (MEMS) Technologies

MEMS are a combination of electric and mechanical components working together to provide several applications including sensing and actuating which are already being commercially used in many field in the form of transducers and accelerometers etc. MEMS combined with Nano technologies are a cost-effective solution for improvising the communication system of IoT and other advantages like size reduction of sensors and actuators, integrated ubiquitous computing devices and higher range of frequencies etc [42].

4.7 Optical Technologies

Rapid developments in the field of Optical technologies in the form of technologies like Li-Fi and Cisco's BiDi optical technology could be a major breakthrough in the development of IoT. Li-Fi, an epoch-making Visible Light Communication (VLC) technology, will provide a great connectivity on a higher bandwidth for the objects interconnected on the concept of IoT. Similarly Bi-Directional (BiDi) technology gives a 40G ethernet for a big data from multifarious devices of IoT [43].

5. APPLICATIONS

Most of the daily life applications that we normally see are already smart but they are unable to communicate with each other and enabling them to communicate with each other and share useful information with each other will create a wide range of innovative applications. These emerging applications with some autonomous capabilities would certainly improve the quality of our lives. A few of such applications are already in the market, let's take the example of the Google Car which is an initiative to provide a self-driving car experience with real-time traffic, road conditions, weather and other information exchanges, all due to the concept of IoT. There are a number of possible future applications that can be of great advantage. In this section, we present few of these applications [44-48].

5.0.1 Smart Traffic System.
Traffic is an important part of a society therefore all the related problems must be properly addressed. There is a need for a system that can improve the traffic situation based on the traffic information obtained from objects using IoT technologies. For such an intelligent traffic monitoring system, realization of a proper system for automatic identification of vehicles and other traffic factors is very important for which we need IoT technologies instead of using common image processing methods. The intelligent traffic monitoring system will provide a good transportation experience by easing the congestion. It will provide features like theft-detection, reporting of traffic accidents, less environmental pollution. The roads of this smart city will give diversions with climatic changes or unexpected traffic jams due to which driving and walking routes will be optimized. The traffic lighting system will be weather adaptive to save energy. Availability of parking spaces throughout the city will be accessible by everyone.

5.0.2 Smart Environment.
Prediction of natural disasters
such as flood, fire, earthquakes etc will be possible due to innovative technologies of IoT. There will be a proper monitoring of air pollution in the environment.

5.0.3 Smart Home.
IoT will also provide DIY solutions for Home Automation with which we will be able to remotely control our appliances as per our needs. Proper monitoring of utility meters, energy and water supply will help saving resources and detecting unexpected overloading, water leaks etc. There will be proper encroachment detection system which will prevent burglaries. Gardening sensors will be able to measure the light, humidity, temperature, moisture and other gardening vitals, as well as it will water the plants according to their needs.

5.0.4 Smart Hospitals.
Hospitals will be equipped with smart flexible wearable embedded with RFID tags which will be given to the patients on arrivals, through which not just doctors but nurses will also be able to monitor heart rate, blood pressure, temperature and other conditions of patients inside or outside the premises of hospital. There are many medical emergencies such as cardiac arrest but ambulances take some time to reach patient, Drone Ambulances are already in the market which can fly to the scene with the emergency kit so due to proper monitoring, doctors will be able to track the patients and can send in the drone to provide quick medical care until the ambulance arrive.

5.0.5 Smart Agriculture.
It will monitor Soil nutrition, Light, Humidity etc and improve the green housing experience by automatic adjustment of temperature to maximize the production. Accurate watering and fertilization will help improving the water quality and saving the fertilizers respectively.

5.0.6 Smart Retailing and Supply-chain Management.
IoT with RFID provides many advantages to retailers. With RFID equipped products, a retailer can easily track the stocks and detect shoplifting. It can keep a track of all the items in a store and to prevent them from going out-of-stock, it places an order automatically. Moreover the retailer can even generate the sales chart and graphs for effective strategies.

6. CONCLUSIONS

In summary, one vision of the future is that IoT becomes a utility with increased sophistication in sensing, actuation, communications, control, and in creating knowledge from vast amounts of data. This will result in qualitatively different lifestyles from today. What the lifestyles would be is anyone's guess. It would be fair to say that we cannot predict how lives will change. We did not predict the Internet, the Web, social networking, Facebook, Twitter, millions of apps for smartphones, etc., and these have all qualitatively changed societies' lifestyle. New research problems arise due to the large scale of devices, the connection of the physical and cyber worlds, the openness of the systems of systems, and continuing problems of privacy and security. It is hoped that there is more cooperation between the research communities in order to solve the myriad of problems sooner as well as to avoid re-inventing the wheel when a particular community solves a problem. With the incessant burgeoning of the emerging IoT technologies, the concept of Internet of Things will soon be inexorably developing on a very large scale. This emerging paradigm of networking will influence every part of our lives ranging from the automated houses to smart health and environment monitoring by embedding intelligence into the objects around us. In this paper we discussed the vision of IoT and presented a well-defined architecture for its deployment. Then we highlighted various enabling technologies and few of the related security threats. And finally we discussed a number of applications resulting from the IoT that are expected to facilitate us in our daily lives. Researches are already being carried out for its wide range adoption, however without addressing the challenges in its development and providing confidentiality of the privacy and security to the user, it's highly unlikely for it to be an omni-present technology. The deployment of IoT requires strenuous efforts to tackle and present solutions for its security and privacy threats.

ACKNOWLEDGEMENT

The authors are thankful to Hon'ble C–VI, Mr. Aseem Chauhan (Additional President, RBEF and Chancellor AUR, Jaipur), Hon'ble Pro VC Maj. General K. K. Ohri (AVSM, Retd.) Amity University, Lucknow, Wg. Cdr. (Retd.) Dr. Anil Kumar, (Director, ASET), Prof. S. T. H. Abidi (Professor Emeritus), Prof O. P. Singh (HOD, Electrical & Electronics Engg.), Parents, Family & Friends for their motivation, kind cooperation, and suggestions.

REFERENCES

[1]. T. Abdelzaher, S. Prabh, and R. Kiran, On Real-Time Capacity Limits of ad hoc Wireless Sensor Networks, RTSS, December 2004.

[2]. Y. Aguiar, M. Vieira, E. Galy, J. Mercantini, and C. Santoni, Refining a User Behavior Model based on the Observation of Emotional States. COGNITIVE , 2011.

[3]. V. Bradshaw. The Building Environment: Active and Passive Control Systems. John Wiley & Sons, Inc., River Street, NJ, USA, 2006.

[4]. B. Brumitt, B. Meyers, J. Krumm, A. Kern, and S. A. Shafer. Easyliving: Technologies for Intelligent Environments. HUC, 2000.

[5]. J. Deng, R. Han, and S. Mishra, Secure Code Distribution in Dynamically Programmable Wireless Sensor Networks, Proc. of ACM/IEEE IPSN, 2006. pp. 292-300.

[6]. R. Dickerson, E. Gorlin, and J. Stankovic, Empath: a Continuous Remote Emotional Health Monitoring System for Depressive Illness. Wireless Health , 2011.

[7]. C. Dixon, R. Mahajan, S. Agarwal, A. Brush, B. Lee, S. Saroiu, and P. Bahl, An Operating System for the Home, NSDI, 2012.

[8]. T. He, J. Stankovic, C. Lu and T. Abdelzaher, A Spatiotemporal Communication Protocol for Wireless Sensor Networks, IEEE Transactions on Parallel and Distributed Systems, Vol. 16, No. 10, Oct. 2005, pp. 995-1006.

[9]. M. Huang, J. Li, X. Song, and H. Guo, Modeling Impulsive Injections of Insulin: Towards Artificial Pancreas. SIAM Journal of Applied Mathematics 72, 5, 2012, pp. 1524–1548.

[10]. M. Kay, E. Choe, J. Shepherd, B. Greenstein, N. Watson, S. Consolvo, and J. Kientz, Lullaby: a Capture & Access System for Understanding the Sleep Environment. UbiComp, 2012.

[11]. A Liu, and D. Salvucci, Modeling and Prediction of Human Driver Behavior, Intl. Conference on HCI , 2001.

[12]. Lu, T. Sookoor, V. Srinivasan, G. Gao, B. Holben J. Stankovic, E. Field, and K. Whitehouse, The Smart Thermostat: Using Occupancy Sensors to Save Energy in Homes, ACM SenSys, 2010.

[13]. M. Maroti, B. Kusy, G. Simon, and A. Ledeczi, The Flooding Time Synchronization Protocol, ACM SenSys, November 2004.

[14]. S. Mohammed, P. Fraisse, D. Guiraud, P. Poignet, and H. Makssoud, Towards a Co-contraction Muscle Control strategy for Paraplegics. CDCECC, 2005.

[15]. S. Munir, J. Stankovic, C. Liang, and S. Lin, New Cyber Physical System Challenges for Human-in-the-Loop Control, 8th International Workshop on Feedback Computing, June 2013.

[16]. S. Ravi, A. Raghunathan, S. Chakradhar. Tamper Resistance Mechanisms for Secure, Embedded Systems, Proc. of 17th InternationalConference on VLSI Design, 2004. p. 605.

[17]. B. Rong Chen, G. Peterson, G. Mainland, and M. Welsh, LiveNet: Using Passive Monitoring to Reconstruct Sensor Network Dynamics, DCOSS 2008, June 2008.

[18]. S. Rost and H. Balakrishnan, Memento: A Health Monitoring System for Wireless Sensor Networks. SECON 2006, September 2006.

[19]. L. Ruiz, J. Nogueira, and A. Loureiro, MANNA: A Management Architecture for Wireless Sensor Networks. IEEE Communications Magazine,February 2003.

[20]. G. Schirner, D. Erdogmus, K. Chowdhury, and T. Padir, The Future of Human-in-the-Loop Cyber-Physical Systems. Computer 46, 1, 2013, pp. 36–45.

[21]. J. Stankovic, When Sensor and Actuator Networks Cover the World, invited Keynote Article, Special Issue on Ubiquitous Sensor Networks, ETRI Journal, Korea, Vol. 30. No. 5, October 2008, pp. 627-633.

[22]. J. Stankovic, I. Lee, A. Mok, R. Rajkumar, Opportunities and Obligations for Physical Computing Systems, IEEE Computer, Vol. 38, No. 11, Nov. 2005, pp. 23-31.

[23]. J. Stankovic, A Vision of a Smart City in the Future, Smart Cities, Vol. 1, Issue 10, Oct. 2013.

[24]. K. Tsui, D. Kim, A. Behal, D. Kontak, and H. Yanco, I Want That : Human-in-the-Loop Control of a Wheelchair-Mounted Robotic Arm. Journalof Applied Bionics and Biomechanics 8, 2011.

[25]. P. A. Vicaire, E. Hoque, Z. Xie, and J. A. Stankovic, Bundles: a Group Based Programming Abstraction for Cyber Physical Systems, ICCPS, 2010.

[26]. P. A. Vicaire, Z. Xie, E. Hoque, and J. A. Stankovic, Physicalnet: A Generic Framework for Managing and Programming across Pervasive Computing Networks, RTAS, 2010.

[27]. Wood, J. Stankovic, G. Virone, L. Selavo, T. He, Q. Cao, T. Doan, Y. Wu, L. FANG, and R. Stoleru, Context-Aware Wireless Sensor Networks for Assisted Living and Residential Monitoring. IEEE Network 22, 4, Jul./Aug. 2008, pp. 26–33.

[28]. Wood, L. Fang, J. Stankovic, and T. He, SIGF: A Family of Configurable, Secure Routing Protocols for Wireless Sensor Networks, ACM Security of Ad Hoc and Sensor Networks, Best Paper Award, October 31, 2006.

[29]. Y. Wu, J. Li, J. Stankovic, K. Whitehouse, S. Son and K. Kapitanova, Run Time Assurance of Application-Level Requirements in Wireless Sensor Networks, IPSN, April 2010.

[30]. W. Xu, W. Trappe, Y. Zhang, T. Wood, The Feasibility of Launching and Detecting Jamming Attacks in Wireless Networks, Proc. of MobiHoc, 2005. pp. 46-57.

[31]. Y. Yu, L. J. Rittle, V. Bhandari, and J. B. LeBrun, Supporting Concurrent Applications in Wireless Sensor Networks, ACM SenSys, 2006.

[32]. W. Zeiler, R. Houten, G. Boxem, D. Vissers, and R. Maaijen, Indoor Air Quality and Thermal Comfort Strategies: the Human-in-the-Loop Approach, ICEBO, 2011.

[33]. Fleisch, E., Mattern, F.: (eds.) Das Internet der Dinge. Springer (2005) Fleisch, E.: What is the Internet of Things? When Things Add Value. Auto-ID Labs White Paper WP-BIZAPP-053, Auto-ID Lab St. Gallen, Switzerland (2010)

[34]. Floerkemeier, C., Mattern, F.: Smart Playing Cards – Enhancing the Gaming Experience with RFID. In: Magerkurth, C., Chalmers, M., Björk, S., Schäfer, L. (eds.) Proc. 3rd Int. Workshop on Pervasive Gaming Applications – PerGames 2006, pp. 27–36 (2006)

[35]. Floerkemeier, C., Langheinrich, M., Fleisch, E., Mattern, F., Sarma, S.E.: (eds.) The Internet of Things. First International Conference, IOT 2008, LNCS 4952, Springer (2008)

[36]. Frank, C., Bolliger, P., Mattern, F., Kellerer, W.: The Sensor Internet at Work: Locating Everyday Items Using Mobile Phones. Pervasive and Mobile Computing 4(3):421–447 (2008)

[37]. Gershenfeld, N.: When Things Start to Think. Henry Holt and Company (1999) 12. Guinard, D., Trifa, V., Wilde, E.: Architecting a Mashable Open World Wide Web of Things. TR CS-663 ETH Zürich, www.vs.inf.ethz.ch/publ/papers/WoT.pdf (2010)

[38]. Hui, J., Culler, D.: IP is Dead, Long Live IP for Wireless Sensor Networks. Proc. 6th Int. Conf. on Embedded Networked Sensor Systems (SenSys), pp. 15–28 (2008)

[39]. Hui, J., Culler, D., Chakrabarti, S.: 6LoWPAN – Incorporating IEEE 802.15.4 into the IP architecture. Internet Protocol for Smart Objects Alliance, white paper # 3 (2009)

[40]. International Telecommunication Union: The Internet of Things. ITU (2005)

[41]. Kindberg, T., Barton, J., Morgan, J., Becker, G., Caswell, D., Debaty, P., Gopal, G., Frid, M., Krishnan, V., Morris, H., Schettino, J., Serra, B., Spasojevic, M.: People, Places, Things: Web Presence for the Real World. Mobile Networks and Applications 7(5):365–376 (2002)

[42]. Kollmann, K.: Das „Internet of Things" – Der kurze Weg zur kollektiven Zwangsentmündigung. Telepolis, www.heise.de/tp/r4/artikel/30/30805/1.html (2009)

[43]. Rafiullah Khan, Sarmad Ullah Khan, Rifaqat Zaheer and Shahid Khan, "Future Internet: The Internet of Things Architecture, Possible Applications and Key Challenges," in Proceedings of Frontiers of Information Technology (FIT), 2012, pp. 257-260

[44]. Guicheng Shen and Bingwu Liu, "The visions, technologies, applications and security issues of Internet of Things," in E -Business and E -Government (ICEE), 2011, pp. 1-4

[45]. Ling-yuan Zeng, "A Security Framework for Internet of Things Based on 4G Communication," in Computer Science
and Network Technology (ICCSNT), 2012, pp. 1715-171

[46]. Jason Pontin, "Bill Joy's Six Webs," MIT Technology Review,

[47]. Jian An, Xiao-Lin Gui, Xin He, "Study on the Architecture and Key Technologies for Internet of Things," in Advances in
Biomedical Engineering, Vol.11, IERI-2012, pp. 329-335

[48]. Lan Li, "Study of Security Architecture in the Internet of Things," in Measurement, Information and Control (MIC), 2012, Volume: 1, pp. 374-377

BIOGRAPHIES

RAJINDER TIWARI, currently pursuing PhD degree from Amity University, Lucknow. Presently, he is associated with Department of Electrical & Electronics Engineering, Amity University, Lucknow. Mr Tiwari has published ample research papers with high repute. His areas of interest are Analog CMOS Circuits (VLSI), Embedded System Design, He is the life member of several professional bodies i.e. MIETE, MIET (U.K.), MRSI, UACEEE.