GIAP Journals

International Journal of Students' Research In Technology & Management
Vol 4 (2) March-June 2016, pg 30-34
eISSN 2321-2543, doi: 10.18510/ijsrtm.2016.422

Internet of Things: The next evolutionary step- A Review

Parnika Tandon
B. Tech. (Computer Science), Kalinga Institute of Industrial Technology, KIIT University, Bhubaneswar-751024, India.
parnikatandon@gmail.com

Abstract: **Now-a-days the world is witnessing the start of a new era of Internet of Things (IoT) also known as Internet of Objects. In this era, computing will be outside the realm of the traditional desktop and many of the objects surrounding us will be on the network in one form or another. Generally speaking IoT refers to the networked interconnection of everyday objects, which are often equipped with ubiquitous intelligence i.e. we can say that IoT stands for virtually interconnected objects that are identifiable and equipped with sensing, computing, and communication capabilities. IoT promises a great future for the internet where the type of communication is machine-to-machine (M2M). This review presents a vision for worldwide implementation of IoT while also discussing the key enabling technologies and application domains that are likely to drive IoT research in the near future.**

Keywords: IoT, M2M, RFID, communication,

INTRODUCTION

The concept of Internet of Things (IoT) can be traced back to the vision, which is reality now, given by Kevin Ashton in 1999 [1] and it is initially linked to the new idea of using Radio-Frequency IDentification (RFID) in supply chain. The basic concept of IoT centres around the idea to allow autonomous exchange of information between identifiable real world devices around us, aided by technologies like RFID and Wireless Sensor Networks (WSNs) [2], sensed by the sensor devices and further processed for decision making, on the basis of which an automated action is performed [3]. Through IoT we shall be able to incorporate transparently and seamlessly a large number of heterogeneous end systems, while providing open access to selected subsets of data for the development of a plethora of digital services. IoT envisions a near future, in which the objects of everyday life will be equipped with microcontrollers, transceivers for digital communication, and suitable protocol stacks that will make them able to communicate with one another and with the users, by becoming an integral part of the Internet [4]. It will create more opportunities for direct integration of the physical world into computer based systems, and resulting in improved efficiency, accuracy and economic benefit. The IoT concept, hence, aims at making the Internet even more immersive and pervasive. Through the use of Internet of Things (IoT) we will be able to make real-world objects such as sensors, actuators, wearable devices, smartphones, and appliances available over the Internet to provide data or to be controlled remotely. Mobile access to the Internet, coupled with the rapid growth of the smartphone market, has begun to create consumer demand for the Internet of Things. Thus, Internet will evolve from a network of personal computers and servers toward a huge network interconnecting billions of smart communicating objects. The gadgets would disappear and weave themselves into the fabric of our everyday life to support us in carrying out daily life activities, tasks and rituals in an easy and natural way. This will be done by using information and intelligence, hidden in the network connecting the gadgets. Billions of devices connected to the Internet will be integrated into complex systems and use sensors and actuators to observe and interact with their physical environment, and hence allowing interaction among autonomous systems. Radio Frequency IDentification (RFID) and sensor network technologies will rise to meet this new challenge, in which information and communication systems are invisibly embedded in the environment around us.

In the IoT environment, the seamless interactions among different types of devices, such as monitoring cameras, home appliances, vehicles, medical sensors, etc., have led to the emergence of many applications such as smart city, home automation, smart grid, smart logistics, smart health care, smart agriculture, traffic management, etc. A common factor in all such applications is the inherent smartness. Being part of a "smart" application, various devices within an application domain can automatically collect data, share information among themselves, and initiate and execute services with minimal human intervention. Thus, we can say that IoT is an enabling technology for cyber-physical systems or systems of systems.

Now-a-days PC era is leaving way to smart phones and other handheld devices which make our environment more interactive as well as informative. Attempts to monitor and control devices by combining computers with internet have been around for decades. Advances in wireless technology allowed "machine–to–machine" (M2M) equipment monitoring and operation by the 1990s although many of these were based on closed purpose–built networks [5]. These unusual beginnings led research into smart object networking which laid the foundation of today's IoT [6]. At present, the broad range of potential applications are considering the potential for incorporating IoT technology into their products, services, and operations. These include wearable and ingestible devices attached with the human body (or present inside) to monitor and maintain human health and wellness, disease management, increased fitness, higher productivity; home controllers and security systems in buildings where people live; self-checkout, in-store offers, inventory optimization in stores, banks, restaurants, arenas etc.; energy management and security in office buildings; operating efficiencies, optimizing equipment use and inventory in the factories and hospitals; condition-based maintenance, usage-based design, pre-sales analytics in vehicles including cars, trucks, ships, aircraft, and trains; adaptive traffic control,

International Journal of Students' Research In Technology & Management
Vol 4 (2) March-June 2016, pg 30-34
eISSN 2321-2543, doi: 10.18510/ijsrtm.2016.422

smart meters, environmental monitoring, resource management public spaces and infrastructure in urban settings; and outside uses like railroad tracks, flight navigation; real-time routing, connected navigation, shipment tracking etc.

The European Commission has predicted that by 2020 there will be 50–100 billion devices connected to the Internet [7] and the presently existing architecture of Internet cannot handle such a big network as IoT. Thus, a new open architecture is needed that should be able to support the existing network applications using open protocols [8] and which may assure the protection of data and privacy of users [9]. Multilayered security architectures comprising of three [10], four [11], five [12], and six [13] key level architectures have been described. Foundation of IoT has been described as the coding layer in which each object is assigned a unique ID which makes it easy to discern the objects [13]. Secondly the Perception Layer consisting of data sensors in different forms like RFID tags, IR sensors or other sensor networks [14] senses the temperature, humidity, speed and location etc of the objects and after converting it into the digital signals passes the information to the third Network Layer which transmits the digital signals to the processing systems in the fourth Middleware Layer through the transmission mediums like WiFi, Bluetooth,WiMaX, Zigbee, GSM, 3G etc with protocols like IPv4, IPv6, MQTT, DDS etc [15]. In the fourth layer information is processed with the technologies like Cloud computing, Ubiquitous computing and a fully automated action is taken based on the processed results of the information. Fifth layer, the Application layer is very helpful in the large scale development of IoT network [12] as it realizes the applications of IoT for all kinds of industry, based on the processed data. Finally the sixth layer known as the Business Layer, responsible for all the research related to IoT, manages the applications and services of IoT and it generates different business models for effective business strategies. In the present review introduction and vision of IoT is followed by various technologies that IoT is composed of. This is followed by the applications, the security threats and concluding remarks.

IOT EQUIPMENTS

Ubicomp is a concept in software engineering and computer science where computing is made to appear anytime and everywhere. In contrast to desktop computing, ubiquitous computing can occur using any device, in any location, and in any format. The development of a seamless ubicomp requires a combination of new and effective technologies so that the objects can be identified and can communicate with each other. The three components of IoT, which enable seamless ubicomp are (i) hardware made up of sensors, actuators and embedded communication hardware, (ii) middleware consisting of on demand storage and computing tools for data analytics and (iii) novel, easy to understand visualization and interpretation tools which can be widely accessed on different platforms and which can be designed for different applications. Technologies which make up these components are discussed below.

RADIO FREQUENCY IDENTIFICATION (RFID)

RFID is the main technology which makes any object uniquely identifiable. Microchips for wireless data communication help in the automatic identification of anything with which they are attached by acting as an electronic barcode [16, 17]. Its miniature size and low cost makes it integrable into any object [10]. It is both active and passive transceiver microchip which is similar to an adhesive sticker depending on the type of application [4]. In the passive RFID tags no battery is used and the reader's interrogation signals are used as the power source to communicate the ID to the RFID reader thus, they get activated only when they are triggered. The active tags are costly and are always active due to the power supplied by the attached battery and continuously emit the data signals. In the RFID system RFID tags are associated with readers. Identification, location or any other specifics about the object are given out in the form of signals which are emitted when RFID tags are triggered [18]. The emitted data signals using radio frequencies are transmitted to the readers and then to processors to analyze the data. Depending on the application, RFID frequencies ranging from 125 KHz band to 5.8 GHz band can be used. They affect operating distance, speed and the minimum size of objects which can be tagged. RFID is more effective than the Bar Code. Being a radio technology RFID does not require the physical presence of the reader while Bar Code being an optical technology, cannot work unless its reader is placed in front of it. Further, an RFID can work as an actuator to trigger different events and it can be modified as per need, the ability which Bar codes don't have.

WIRELESS SENSOR NETWORKS (WSN)

The combination of low power integrated circuits and wireless communications has improved the viability of utilizing a sensor network consisting of a large number of intelligent sensors, which enable the collection, processing, analysis and dissemination of valuable information, gathered in a variety of environments [19]. Several nodes are 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. Each sensor is a transceiver and has an antenna, a micro-controller and an interfacing circuit for the sensors which act as a communication, actuation and sensing unit respectively along with a source of power which could be battery or any energy harvesting technology [20]. Memory Unit can also be added as a part of the sensing node. Wireless Sensors Network technology and RFID technology have their own advantages but RFID sensor networks have a low range and their communication is asymmetric while WSNs have a comparatively longer range and their communication is Peer-to-Peer.

CLOUD COMPUTING

For analyzing millions of devices cloud appears to be the only technology which can analyze and store all the data effectively in which number of servers are converged on one cloud platform to allow sharing of resources between each other. These resources can be accessed at any time and any place with increased processing power and help in analyzing the useful information obtained from the sensors while providing good storage capacity [21]. Cloud computing, on which

IoT depends, interfaced with smart objects can be of enormous benefits to IoT. However, developing IoT applications using low-level Cloud programming models and interfaces such as Thread and MapReduce models is complex. To overcome this, we need an IoT application specific framework for rapid creation of applications and their deployment on Cloud infrastructures. This is achieved by mapping the proposed framework to Cloud APIs offered by platforms such as Aneka. Aneka is a .NET-based application development Platform-as-a-Service (PaaS), which can utilize storage and compute resources of both public and private clouds [22]. It offers a runtime environment and a set of APIs that enable developers to build customized applications by using multiple programming models such as Task Programming, Thread Programming and MapReduce Programming. Aneka provides a number of services that allow users to control, auto-scale, reserve, monitor and bill users for the resources used by their applications.

NETWORKING TECHNOLOGIES

For the success of IoT we need a fast and an effective network also to connect a large number of potential devices. For wide-range transmission network we commonly use 3G, 4G etc. and similarly for a short-range communication network we use technologies like Bluetooth, WiFi etc. Stepping into the modern ubiquitous computing will also need a super-fast, super-efficient fifth generation wireless system which should offer a lot more bandwidth. Apart from it realization of smaller and improved version of the things that are interconnected can only be possible by incorporating the nano devices obtained from nanotechnology resulting in the Internet of Nano-Things [23]. Nano technologies combined with Micro-Electro-Mechanical Systems (MEMS) Technologies will be a cost-effective solution for improvising the communication system of IoT.

Fig. 1. Internet of Things schematic diagramme showing th end users and application areas based on data.

APPLICATIONS

IoT finds applications in nearly every field because of its ability to network embedded devices with limited CPU, memory and power resources. IoT can be regarded as an extension of existing interaction between people and applications through a new dimension of "Things" for communication and integration. "Things" in the IoT sense, refer not only to devices like desktops, laptops, smart-phones, tablets, security systems, thermostats and vending machines, but also to a wide variety of devices such as operation devices that assist fire fighters in search and rescue operations, heart monitoring implants, automobiles with built-in sensors, biochip transponders on farm animals, DNA analysis devices for environmental/food/pathogen monitoring, electric clams in coastal waters etc. Based on the application domain, IoT products can be classified broadly into six different categories: smart wearable, smart home, smart city, smart hospitals, smart environment, and smart enterprise.

Smart Wearable

Health- and fitness-oriented wearable devices that offer biometric measurements such as heart rate, perspiration levels, oxygen levels in the bloodstream etc. are already available in the market and are revolutionizing the general health of citizens like never before. These wearables can communicate any results outside of a programmed range to the patient and to her physician including information like oxygen saturation, heart rate and more.

SMART HOME

Smart homes will implement technologies for home automation and security systems. Not only will the automation save energy by placing sensors around the house and controlling lighting by detecting movements around the place, but people will also be able to control these systems while in their offices or on the move. 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. Smart refrigerators will be able to detect what food item is missing and notify the users accordingly or straightaway order items online, while also monitoring the health and eating habits of the family; visitor identification for unlocking doors in the absence of owners will be another feature.

SMART CITY

According to Navigant Research [24], the global smart city technology market is expected to be worth approximately $27.5 billion annually by 2023, compared to $12.1 billion in 2016. The quality of life of residents of IoT-powered smart cities will be bettered in various ways, like through the delivery of connected health/care services to citizens anywhere, anytime , and sustainable and eco-friendly environments. IoT will revolutionize in connected cities by reducing city energy costs for streetlights by detecting movement, handling parking through connected parking spots with the help of real time parking finders. Availability of parking spaces throughout the city will be accessible by everyone. 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

International Journal of Students' Research In Technology & Management
Vol 4 (2) March-June 2016, pg 30-34
eISSN 2321-2543, doi: 10.18510/ijsrtm.2016.422

be weather adaptive to save energy. It will also help in efficient waste management through connected garbage bins (which communicate the type of waste in them and, hence proper disposal) and benefitting the retail industry through the use of smart shopping carts and monitoring the shopping habits of residents.

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 [45]. There are many medical emergencies such as cardiac arrest which require immediate treatment. Ambulances take some time to reach patient, and these prove fatal to patients. Drone Ambulances are already in the market which can fly to the scene with the emergency kit. With proper monitoring, doctors will be able to track the patients and can send in the drone to provide quick medical care until the ambulance arrives.

SMART ENVIRONMENT

A city-wide network of sensors provides real-time valuable information on the flow of citizens, traffic and weather conditions, and also monitoring air quality, noise and other forms of environmental pollution, so that appropriate actions can be taken to minimize pollution in these cities. This better equips local and regional authorities to streamline city operations including better environmental management, reducing carbon footprint by efficient management of traffic, and improving economic, social and environmental sustainability. For example, garbage bins are fitted with sensors that monitor trash levels and these are wirelessly connected to a central monitoring office. It has been proposed to equip future versions of these sensors with technology that can detect the presence of hazardous materials that might be dumped in the bin. All this data reaches the city council's team, enabling them to plan the optimal routes for garbage collection as well as updating garbage truck drivers in real time regarding which routes to take, hence optimizing productivity and reducing waste management service costs.

SMART ENTERPRISE

Real-time optimization of manufacturing production and supply chain networks, rapid manufacturing of new products and dynamic response to product demands, all through the use of networking machinery , sensors and control systems together will immensely profit businesses. By unifying information from diverse sources and applications, businesses will be better equipped to accelerate product development and deployment cycles in an effiecient manner. Smart connected workplaces will have data concerning the shopping habits of citizens in each area , hence increasing the profitability of businesses. All these new connected devices will produce a ton of data that can be disseminated and quantified for more reliable outcomes.

SECURITY AND PRIVACY CHALLENGES

As the boundary between virtual and physical world is eliminated, security threats also become rampant. To a potential attacker, a device presents an interesting target for several reasons. First, many of the devices will have an inherent value by the simple nature of their function. A connected security camera, for example, could provide valuable information about the security posture of a given location when compromised. Hidden security risks, namely, eavesdropping on the wireless communication channel, unauthorized access to devices, tampering with devices, and privacy risks are posed as challenges to be overcome to make IoT safer. Apart from this, there are concerns about device bootstrapping, key management, authorization, privacy, and message fragmentation issues in the IoT as well. The first step towards an interoperable IoT would be standardizing the communication security. The network has to be transformed to IPv6 enabled network to address the huge number of smart objects. Although IPv6 brings significant assurance of a higher level of security and confidentiality of the transmitted data, it also comes with the possibility of new attacks. IoT will generate a huge amount of personal data of the users and this will pose serious threat to the privacy of users, especially in the situations where people do not want to disclose their detailed personal information. A secure communication channel is needed along with object authentication to track interacting objects. If the objects in IoT are sensed through RFID or sensors achieving the integration of human society and the information system, the security issue of RFID becomes more and more important. It is possible that the RFID tag may leak sensitive information of the owner to the unauthorized reader; attackers might clone the tags if they are able to collect the EPC (Electronic Product Code) . Once the RFID readers are controlled by an attacker, they can emit the specific electromagnetic wave to destroy the data in the RFID tag. In RFID system wireless communication is adopted between the RFID readers and RFID tags. Due to the openness of the wireless signals, it is very easy for an attacker to search, intercept, monitor, and jam wireless communication signals. So encryption and authentication are needed to protect the wireless transmission between the RFID readers and RFID tags. In conclusion the traceability and identification of the tags can lead to personal privacy leak.

CONCLUSION

Several technologies such as information technology, cognitive sciences, communication technology, and low-power electronics are included in the IoT in which the sensing and actuation functions seamlessly blend into the background and new capabilities are made possible through access of rich new information sources. The development of IoT will depend on technological advances in silicon scaling and energy-efficient devices, in getting the information from heterogeneous sources, in reducing costs, and in improving efficiencies. A number of potential challenges may stand in the way of this vision – particularly in the areas of security; privacy; interoperability and standards; legal, regulatory, and rights issues; and the inclusion of emerging economies. The Internet of Things involves a complex and evolving set of technological, social, and policy considerations across a diverse set of stakeholders and there is a need to address its challenges and maximize its benefits while reducing its risks. Large-scale service deployment needs

to be framed within a set of standards. IoT have become an inevitable trend of development in the information industry, which is bound to bring new changes to our lives.

REFERENCES

1. K. Ashton, " That 'Internet of Things' thing", RFID Journal (2009).
2. G. Shen; B. Liu, "The visions, technologies, applications and security issues of Internet of Things," E-Business and E -Government (ICEE) (2011), 1-4.
3. R. Khan; S. U. Khan; R. Zaheer; S. Khan, "Future Internet: The Internet of Things Architecture, Possible Applications and Key Challenges," in Proceedings of Frontiers of Information Technology (FIT), (2012), 257-260.
4. L. Atzori; A. Iera; G. Morabito, "The internet of things: A survey," Computer Networks, 54 (2010), 2787–2805.
5. P. Chantal. "Know the Difference Between IoT and M2M." Automation World, July 15, 2014. http://www.automationworld.com/cloud-computing/know-difference-between-iot-and-m2m.
6. RFC 7452, "Architectural Considerations in Smart Object Networking" (March 2015), https://tools.ietf.org/html/rfc7452.
7. Gartner, Inc. It can be accessed at: http://www.gartner.com/newsroom/id/2905717.
8. J. An; X-Lin Gui; X. He, "Study on the Architecture and Key Technologies for Internet of Things," Advances in Biomedical Engineering, Vol.11, IERI (2012) 329-335.
9. "The Internet of Things," ITU Report, Nov 2005.
10. W. Chen, "An IBE Based Security Scheme of Internet of Things," Cloud Computing and Intelligent Systems (CCIS), (2012) 1046, 1049 .
11. H. Suo; J. Wan; C. Zou; J. Liu, "Security in the Internet of Things: A Review," Computer Science and Electronics Engineering (ICCSEE) (2012) 648-651.
12. M. Wu; Ting-L. Lu; Fei-Y. Ling; L. Sun; Hui-Y. Du, "Research on the architecture of Internet of things," Advanced Computer Theory and Engineering (ICACTE) (2010) 484-487.
13. X. Cheng; M. Zhang; F. Sun, "Architecture of internet of things and its key technology integration based-on RFID," Fifth International Symposium on Computational Intelligence and Design (2012) 294-297.
14. D. Bandyopadhyay; J. Sen, "Internet of Things: Applications and Challenges in Technology and Standardization" Wireless Personal Communications (2011) 58, 49-69.
15. Y. Zhang, "Technology Framework of the Internet of Things and Its Application," Electrical and Control Engineering (ICECE) (2011) 4109-4112.
16. E. Welbourne; L. Battle; G. Cole; K. Gould; K. Rector; S. Raymer, Building the Internet of Things using RFID The RFID ecosystem experience, IEEE Internet Computing (2009) 13, 48–55.
17. A. Juels, RFID security and privacy: a research survey, IEEE Journal on Selected Areas in Communications (2006) 24, 381–394.
18. H. Zhang; L. Zhu, "Internet of Things: Key technology, architecture and challenging problems", Computer Science and Automation Engineering (CSAE) (2011) 4, 507-512.
19. I. F. Akyildiz; W. Su; Y. Sankarasubramaniam; E. Cayirci, Wireless sensor networks: a survey, Computer Networks (2002) 38, 393–422.
20. K. Sohraby; D. Minoli; T. Znati, "Wireless sensor networks: technology, protocols, and applications", John Wiley and Sons (2007) ISBN 978-0-471-74300-2, pp. 15-18.
21. X. Xiaohui, "Study on Security Problems and Key Technologies of The Internet of Things," Computational and Information Sciences (ICCIS) 2013, 407-410.
22. Y. Wei; K. Sukumar; C. Vecchiola; D. Karunamoorthy; R. Buyya, Aneka cloud application platform and its integration with windows Azure, in: R. Ranjan; J. Chen; B. Benatallah; L. Wang (Eds.), Cloud Computing: Methodology, Systems, and Applications, first ed., CRC Press, Boca Raton, 2011, p. 30.
23. I. Akyildiz; J. Jornet, "The Internet of Nanothings," IEEE Wireless Communications, (2010) 17, 58-63.
24. Available at www.navigantresearch.com/research/navigant-research-leaderboard-report-smart-city-suppliers.