16

Internet of Things – Definition, Architecture, Applications, Requirements and Key Research Challenges

Dushyant Kumar Singh, Himani Jerath and P. Raja*

Lovely Professional University, Phagwara, Punjab, India

Abstract

Today internet is easily accessible to most of the population of the world. And with the increase in accessibility of the internet and advancement in the technology, a new form of technology has emerged i.e., Internet of Things (IoT). It is one of the trending and promising research topics with infinite research opportunities. IoT has been able to develop a new form of communication i.e., machine to machine communication apart from already existing communication, i.e., human to machine and human to human. IoT is penetrating deep in different application areas like consumer electronics, health care, industrial automation, smart homes, public administration, mobile health care, smart grids, intelligent energy management, traffic management and many others. But as with the other technologies, besides presenting numerous opportunities, IoT also comes with its own design challenges and security issues. This review chapter gives an overview of the various requirements for IoT system and architecture, highlights different research challenges in IoT and security issues connected with IoT.

Keywords: Internet of Things (IoT), IoT architecture, IoT design, IoT security

16.1 Introduction

IoT is a trending field these days and comes along with different standardization, design, architecture and security challenges. In the decade from 2010 to 2020 much research was conducted in the field of IoT but very few publications were found addressing and highlighting the challenges of IoT. Figure 16.1 below gives the publication data searched with keyboard "IoT" and "IoT Challenges".

The current chapter on IoT highlights the various definitions, proposed architecture, application, implementation requirement for IoT systems in section 16.2. Looking into the various heterogeneous application fields, it is always challenging to design a common solution for the IoT applications, which leads to various design challenges and security issues

**Corresponding author*: raja.21019@lpu.co.in

Suman Lata Tripathi, Dushyant Kumar Singh, Sanjeevikumar Padmanaban, and P. Raja (eds.) Design and Development of Efficient Energy Systems, (285–296) © 2021 Scrivener Publishing LLC

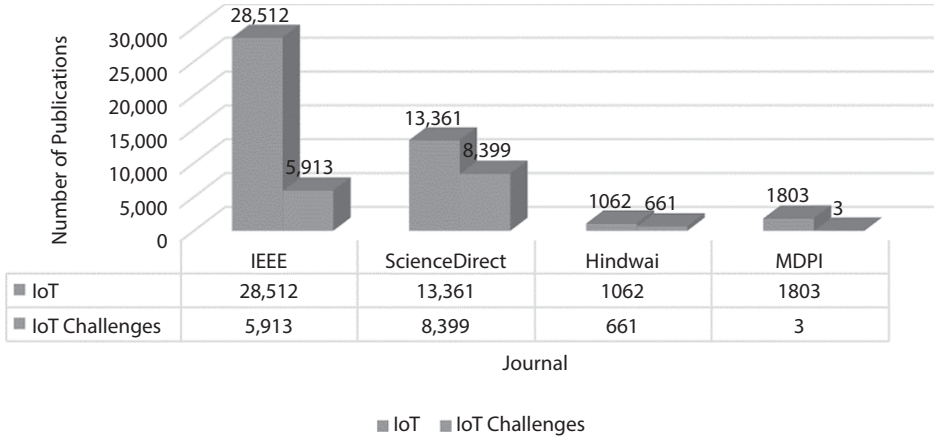

Figure 16.1 Publication data for IoT and its challenges.

associated with IoT which are presented in section 6 under Key Research Challenges in Internet of Things (IoT).

16.2 Defining the Term Internet of Things (IoT)

The main concept behind the IoT device is to exchange the valuable information between uniquely identifiable real-world devices equipped with leading technology like Wireless Sensor Network (WSN) and Radio-Frequency Identification (RFID) which is to be processed for decision making. With the IoT the communication process has been revolutionized. The generic form of communication is either human to human or human to machine but IoT has given rise to machine to machine (M2M) communication, giving a great future to internet [1].

IoT is an interconnected network of things that are used on a daily basis. It can also be treated as a self-configurable network. It allows day-to-day objects, embedded with electronic circuits, to be sensed and controlled remotely through a network. Connecting a number of objects to internet creates a dynamic global network with the ability of self-configuration [2].

In [3] and [4] IoT has been viewed in three paradigms – internet oriented (middleware), things oriented (sensors), and semantic oriented (knowledge). The IoT covers the various aspect of extending the internet into the physical world with the deployment of various distributed devices having embedded identification. IoT gives the concept of linking the digital entities with the physical on through suitable information and communication technology, thus giving a whole new area of applications.

In [3] various definitions of IoT have been given. As per one definition by RFID group,

"The worldwide network of interconnected objects uniquely addressable based on standard communication protocols."

European Research Cluster has defined IoT as follows:

> 'Things' are active participants in business, information and social processes where they are enabled to interact and communicate among themselves and with the environment

> by exchanging data and information sensed about the environment, while reacting autonomously to the real/physical world events and influencing it by running processes that trigger actions and create services with or without direct human intervention.

Yet another definition of IoT is given by Forrester Research:

> Uses information and communications technologies to make the critical infrastructure components and services of a city's administration, education, healthcare, public safety, real estate, transportation and utilities more aware, interactive and efficient.

The definition of IoT given by the authors in [3] is not restricted to any standard protocol and will allow long-lasting development and deployment of IoT applications with state-of-the-art protocols. The IoT definition according to authors in [3] is

> Interconnection of sensing and actuating devices providing the ability to share information across platforms through a unified framework, developing a common operating picture for enabling innovative applications. This is achieved by seamless ubiquitous sensing, data analytics and information representation with Cloud computing as the unifying framework.

16.3 IoT Architecture

The paper [1] has given the projected penetration of IoT by 2020 as given by the Cisco. The paper has discussed six-layer architecture of IoT, namely Coding layer, Perception layer, Network layer, Middleware layer, Application layer and Business layer as shown in Figure 16.2.

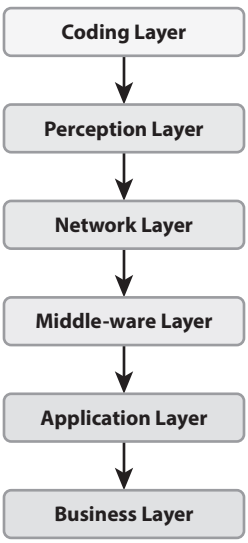

Figure 16.2 IoT Architecture [1].

The coding layer is responsible for assigning a unique ID to each device through which the device of interest is identified. The coding layer basically gives the address to each device on the IoT network. The second layer in the IoT architecture presented is the perception layer, which give the physical meaning to each and every object in the IoT network. It consists of sensors like temperature, humidity acceleration, etc. The function of the perception layer is to gather information about the object, like its temperature and humidity, and pass the gathered information to the network layer. Before passing the information to the network layer, the perception layer converts the information into digital signals. The network layer passes all the digital information received from the perception layer to the middleware layer of IoT architecture information using any of the transmission mediums like Wi-Fi, Bluetooth, Zigbee, etc. The middleware layer is basically the cloud which processes the information so received from the network layer. The application layer is helpful in developing the IoT on a large scale and includes applications like smart homes, industry, smart planet, smart transportation. The business layer of IoT architecture is responsible for managing the application, services and research related to the IoT [1].

After discussing the IoT architecture, paper [1] discussed the history of IoT. The first application of IoT was developed in 1982 as a modified coke machine, which was connected to internet for the purpose of reporting about drinks contained and their temperature. Thereafter, in 1991, a ubiquitous computing concept to IoT was given by Mark Weiser. In 1999, Bill Joy discussed Device to Device communication and Kevin Ashton coined the term Internet of Things in the same year.

IoT integrates the physical devices with cyber physical infrastructure by embedding the electronics into the everyday objects and making them "smart". In this context IoT may refer to i) a global network connecting the smart objects through extended internet technologies, ii) a set of technologies needed to support such vision, and iii) opening new opportunities in the market and business with the different applications and services exploiting such technologies. Three pillars of IoT, based on the ability of smart objects, are identification – a device should be identifiable; communication – a device should be able to communicate; and ability to interact – a device should be able to interact with other devices or with an end user or with other entities in a network. If IoT is viewed at the components level, IoT is based on the notion of "smart object" or "things" [4]. Smart object is defined in [4] is as follows:

- An object with physical embodiment and features such as shape, size, etc.
- An object having communication capabilities to get discovered, identified and be able to receive messages and respond to incoming messages.
- An object having a unique identifier for identification.
- An object with a minimum of one name and address. The name of the object is a human readable description of the object and address is the machine-readable string used to communicate or send messages to the device.
- An object with some computing capabilities. The processing capabilities can be as simple as just matching the incoming message string with the given footprint to the capability of the object of performing complex calculation like network discovery and management, image processing, etc.
- An object able to sense physical parameters like temperature, humidity, height above sea level, radiation level, etc. An object may also possess the facility to actuate or trigger actions depending on the sensed parameters.

16.4 Applications of Internet of Things (IoT)

In [4] the author has identified six major application areas where IoT can provide competitive solutions for current problems.

1. **Smart home** or smart building equipped with IoT technology helps in reducing the resource consumption and also helps to improve the satisfaction level of the people living in it. In a smart building application, sensors are required to sense the consumption of resources and other parameters to monitor the user's needs. This needs high standardization for the interoperability of various subsystems.
2. **Smart cities** are a cyber physical ecosystem deploying advanced communicating services to improve the quality of life of the citizens and optimize the usage of the city's physical resources. Smart parking system, automated parking advice system, monitoring of car traffic, flow of vehicles, detection of polluting level and accident scene analysis are some of the prominent applications where an important role is being played by the IoT.
3. In **Environmental monitoring,** IoT's real-time processing along with the capability to communicate with a large number of devices provides an excellent platform for monitoring of the environmental conditions that endanger human life. Due to its capability of sensing in a distributed and self-managing network, sensing the physical natural phenomena like temperature, wind, rain, etc., and effortlessly integrating such heterogenous data makes IoT suitable to be applied to environmental monitoring applications.
4. **Health care** is yet another application area where IoT can play a major role. Enhancing the monitoring of patient parameters like body temperature, blood pressure, breathing activities and wearables with sensors such as accelerometer and gyroscope monitoring patient activities are some of the areas where health care can benefit from IoT. By interconnecting such heterogenous sensors the comprehensive monitoring of a patient's condition is possible and may be helpful in addressing any deterioration in the condition of the patient.
5. **Smart business** is another application where RFID is already being used for inventory management. RFIDs are attached to the items for e-monitoring and RFID readers are placed throughout the monitoring facility. Real-time monitoring of product availability, stock maintenance and control over the production process, product quality, and detection of self-life deterioration of product are some of the tasks performed by an IoT system in Smart Business.
6. **Security and Surveillance** are considered to be an important application and challenge of IoT. Keeping a check on the behavioral monitoring through various sensors, personal identification using biometrics and early warning systems are a few aspects that are being provided as cheaper and less invasive solutions. On the basis of the data generated, the various IoT applications are given in Figure 16.3 [3].

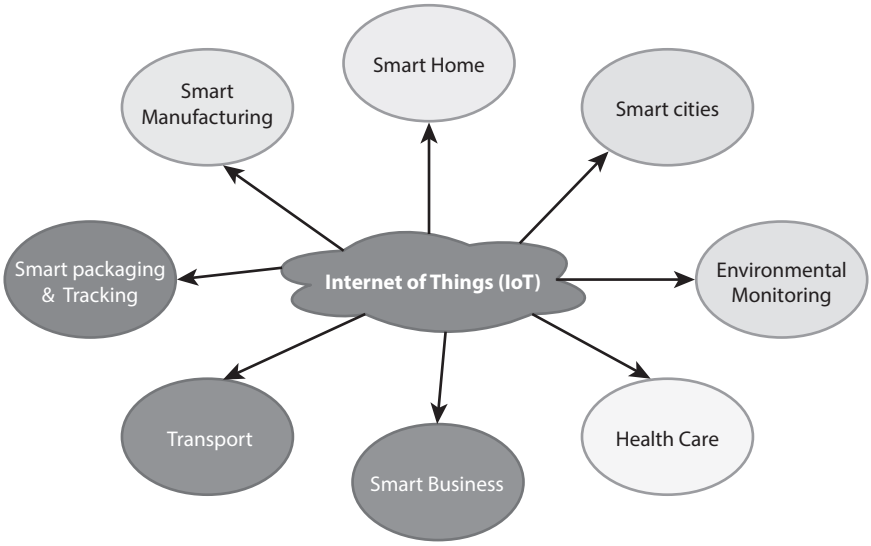

Figure 16.3 Application areas of Internet of Things (IoT) [3].

The components of IoT which make it ubicomp (ubiquitous computing) are: 1) Hardware consisting of sensors, communication technology, actuator and to be added on also consists of microcontroller or microprocessor-based processing boards, 2) Middleware comprises cloud service for storage and computing, and 3) Presentation, the easy to understand and visualize user interface accessible from any platform. The IoT elements identified in [3] which make up the above three components in IoT are Radio Frequency Identification (RFID), Wireless Sensor Networks (WSN) – WSN hardware, WSN communication stack, WSN middleware, secure data aggregation, Addressing schemes, Data storage and analytics and Visualization.

The IoT in the near future will make it possible for everyday objects to be equipped with microcontrollers; transceivers for communication and required protocol enabling them to communicate with each other and also with the users. This will make the internet more immersive and pervasive. The heterogeneous application fields of IoT, such as applications areas like consumer electronics, health care, industrial automation, smart homes, public administration, mobile health care, smart grids, and intelligent energy management, make it a daunting challenge to identify a solution capable of satisfying the requirements of all possible applications. This sometimes leads to propagation of different or sometimes incompatible solutions of practical implementation of IoT systems [5].

16.5 Requirement for Internet of Things (IoT) Implementation

The basic and key feature of IoT is embedding of computing and communication features into everyday objects. An IoT system should fulfill the following requirements:

1. **Scalability:** In 2013 there were about 9 billion interconnected devices and by 2020 this figure is expected to rise to 24 billion devices [3]. It is a perception

that every device has its own virtual representation and with that many devices are interconnected through IoT infrastructure; scalability is desired in IoT architecture for future new IoT applications [6].

2. **Interoperability:** IoT consists of the heterogeneous application areas, and IoT objects may communicate from various service networks. Therefore, in order to empower the IoT devices to communicate from various networks too, all types of IoT application, interoperability is desired [6].
3. **Identification:** In IoT each object needs to be identified specifically. The object may be identified as an individual or as a member of any class, like a pen is a member of a wide class of pens which is not specific and is taken in a generalized manner. This may be achieved by means of RFID tags or any suitable method, but identification of object is desired [2].
4. **Sensing/Actuation:** Sensing and actuation is desired to interface the IoT device with the real-time world around. A device can be interfaced with physical environment passively, performing sensing, or actively, performing action [2].
5. **Resource Control and Management:** The various devices participating in IoT application must be remotely operating as this will help in controlling the device remotely when operator is not present at site. This constraint of resource redundancy may affect the IoT application and it is necessary to balance the load for proper resource utilization [6].
6. **Energy Efficiency:** Lifetime is the most important aspect for smart objects; moreover, the energy consumption of networks is also increasing day by day with the increase in data rate and hence it is desirable for such devices to be more based on green technology; they should be energy efficient [6, 7].
7. **Quality of Service (QoS):** Quality of Service is also an important requirement of IoT architecture. QoS is nonfunctional facility factor which can be obtained by organizing the service provided and retrieval. For instance, Real Time Systems impose requirements of high precedence for a particular performance and it is desired that only compulsory information be retrieved in response to the addressed request [6].
8. **Security:** Security is the most important aspect for IoT objects, which may suffer physical damage and data loss as information is transferred and processed in a hostile environment [6, 7].

16.6 Key Research Challenges in Internet of Things (IoT)

The future of the IoT faces many challenges and needs deliberation by experts to address these challenges. Some of the key research challenges in IoT are listed below:

16.6.1 Computing, Communication and Identification

IoT is envisioned as the development of the technique to transform devices to smart devices and making them capable for communication, computing and identification. The process in which computation is distributed evenly in order to reduce communication overhead is

known as in-network processing or computing [4]. The existence of interconnected links between the objects in IoT needs research consideration with existing tools, methods [8]. There are many possible solutions proposed like RF front end activation pattern, i.e., sleep period, integrating energy harvesting from several sources for sensors like solar, piezocrystals and others [4]. IoT is a very heterogeneous network with a variety of devices from various application areas. This complicates the process of communication amounts the IoT nodes resulting in fraudulent, delayed communication [9, 10]. IoT also suffers from the challenge of identity management, which requires the unique identity for all the physical devices. The current technology deployed is short-range RF identifiers. As the IoT includes a very large number of nodes which are expected to increase in the future, further research is needed in the identification for IoT nodes to operate in a dynamic heterogeneous network [4, 8, 7]. The IPv4 protocol uses only a 4-byte address so new addressing policies are needed in which IPv6 may be a strong contender [8]. Consequently there is need of an IoT architecture that can support low-power, low-cost and yet fully functional networks and devices and is compatible with well-established communication technologies and standards, addressing the huge number of the devices connected to a system [4, 8].

16.6.2 Network Technology

The IoT consists of connecting the devices from various networks in which user happens to be human, machines. WSN is the dominant network technology in IoT [5, 8]. With the increasing number of connected devices in the system infrastructure, it is going to face many challenges like providing service to the different types of IoT-connected devices. Thus, there is a requirement of scaling up the IoT architecture in order to handle the large number of devices [15]. Interoperability of IoT devices amongst the various service providers is also important. The technical challenges in interoperability are standards, protocols, and semantics; the challenges are to ensure that every node in IoT architecture is trustworthy for processing and handling the data. The pragmatic challenges are to design a strategy for realization of ability in an IoT system to observe the intention of participating elements [15]. Protocol forms the backbone for a data tunnel between IoT node and the outer world. Many energy-efficient MAC protocols are proposed like TDMA (collision free), FDMA (collision free with additional circuitry), TCP/IP, Ipv4 and IPv6 for node addressing but none of them are suitable as more "things" available in IoT [5]. Research focus is needed on exploitation of networks for IoT, scalability of network infrastructure, interoperability of networks, identifying the new protocols to handle the network traffic with more devices added, adaptability to heterogeneous networks environment [5, 8, 15].

16.6.3 Greening of Internet of Things (IoT)

The network nodes in IoT need or are expected to be independent, battery operated, and life span is most important in smart objects participating in IoT application. Energy consumption increases with the computational capabilities and high rate transmission of data. In near future IoT will lead to significant increase in energy consumption, thus there will emerge the need and research for energy-efficient sensing and green energy to make the network devices more energy efficient [5, 13, 15].

16.6.4 Security

In IoT security of the embedded devices along with the data is the major issue and challenge. As for embedded system, security is not at all new but as more and more devices are connected, potential threats to security scales up [14]. In IoT, as all the devices are connected to each other, IoT architecture is complex because of the heterogeneity in IoT applications which provide attackers with a platform to invade the system [10, 15]. IoT architecture suffers from numerous device- or network-based security issues like object safety and security, data confidentiality, unauthorized access, network security and security due to diversity in the IoT applications [1, 5, 6, 8, 9, 11–13].

16.6.5 Diversity

IoT is a heterogeneous network and almost every application nowadays intends to use an IoT network. As a result, the market is being flooded with IoT devices with fewer safety checks, and it has been observed that more than 90% of the devices suffer from firmware security vulnerability. The challenge is that it is difficult to design a common security system for such diverse IoT devices [9].

16.6.6 Object Safety and Security

IoT objects may spread over a large geographical area in which they can be easily accessed by attackers. So they need to be protected against physical damage and logical attack by malicious entities [12, 13].

16.6.7 Data Confidentiality and Unauthorized Access

Data confidentiality and unauthorized access represent the fundamental security issues in IoT architecture. It includes defining the access control and object authentication process. Data confidentiality seems more relevant in the business context, as data confidentiality may be important to protect competitiveness and market values [1].

16.6.8 Architecture

Also, in IoT devices sensors provide the data for processing, and it is required to have proper encryption technique for data transmitted to maintain data integrity. The threat associated with this may be more logically represented in Figure 16.4 below [9].

Many access controls have been proposed to ensure authentication. Widely used is Role Based Access System (RBAS) [1]. The main advantage of RBAS is that the access rights can be changed based on the role assigned to the user. RFID is the main authorization technology and with more and more devices being integrated in the IoT, RFID lacks proper authentication mechanism [6, 13].

16.6.9 Network and Routing Information Security

In IoT data from a large number of sensors travels over the diverse network through wired or wireless links using various routing protocols like TCP/IP. The network should be able

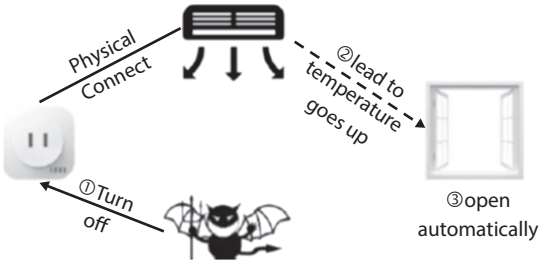

Figure 16.4 Block diagram showing an IoT system.

to handle the data and provide security against external interference or monitoring [6]. Routing information attacks mainly focus on routing protocols of IoT, which may lead to extended source path and end-to-end delay in transmission. This leads to requirement of secure network protocols to establish a secure link among IoT devices and provide quality services [13].

In the last few years IoT has emerged as a hot research and application area. The concept behind the (IoT is to embed the intelligence to the objects so that they can communicate autonomously and can exchange information. IoT transitions human-to-human communication to human-to-machine and machine-to-machine communication. This paper presents the major requirements for the implementation of an IoT system and finally addresses the various research and implementation challenges faced by IoT technology. Deployment of IoT solutions could be hard and will bring more serious security problems and other challenges. This creates a new era of research in which the focus of researchers will be to solve the issues presented by IoT. The major challenges being presented by IoT is scalability as more and more devices are being added at a very fast rate. The next most prominent research fields in IoT are communication range, data storage and power management. In addition to challenges presented, IoT will be significantly benefitting people, professionals and economies in the near future.

References

1. Farooq, M.U.; Waseem, M.; Mazhar, S.; Khairi, A.; and Kamal, T,; A Review on Internet of Things (IoT). International Journal of Computer Applications 2015, 113, 1:1-7.
2. Monika. and Sharma, R.; Research paper on Internet of things. International Journal in Multidisciplinary and Academic Research 2017, 6, 3:1-7.
3. Gubbi, J.; Buyya, R.; Marusic, S. and Palaniswami, M.; Internet of Things (IoT): A vision, architectural elements, and future directions. Future Generation Computer Systems 2013, 29: 1645-1660.
4. Miorandi, D.; Sicari, S.; Pellegrini, F.D. and Chlamtac, I.; Internet of things: vision, application and research challenges. Adhoc Networks 2012,10:1497-1516.
5. Zanella, A.; and Vangelista, L.; Internet of Things for Smart Cities. IEEE Internet of Things Journal 2014, 1:22-32.
6. Burhanuddin, M.A.; Mohammed, A.; Ismail, R. and Basiron, H; Internet of Things Architecture: Current Challenges and Future Direction of Research. International Journal of Applied Engineering Research 2017, 12,21:11055-11061.

7. Kahan, R.; Khan, S.U.; Zaheer, R. and Khan, S.; Future Internet: The Internet of Things Architecture, Possible Applications and Key Challenges. In: 10th International Conference on Frontiers of Information Technology, Islamabad: IEEE Xplore 2012, 257-260.
8. Ray, P.P.; A survey on Internet of Things architectures. Journal of King Saud University – Computer and Information Sciences 2018, 30:291-319.
9. Khalid, A.; Internet of Thing Architecture and Research Agenda. International Journal of Computer Science and Mobile Computing 2016, 5, 3:351-356.
10. Jindal, F.; Jamar, R. and Churi, P.; Future and Challenges of Internet of Things. International Journal of Computer Science & Information Technology 2018, 0, 2:13-25.
11. Lin, J.; Yu, W.; Zhang, N.; Yang, X.; Zhang, H. and Zaho, W.; A Survey on Internet of Things: Architecture, Enabling Technologies, Security and Privacy, and Applications. IEEE Internet of Things Journal 2017, 4, 5:1-17.
12. Zhou, W.; Zhang, Y.; and Liu, P.; The Effect of IoT New Features on Security and Privacy: New Threats, Existing Solutions, and Challenges Yet to Be Solved. IEEE Internet of Things Journal 2018, 6,2:1606-1616.
13. Suo, H.; Wan, J.; Zou, C. and Liu, J.; Security in the Internet of Things: A Review.In: International Conference on Computer Science and Electronics Engineering, Hangzhou: IEEE Xplore 2012, 3:648-651.
14. Babar, S.; Stango, A.; Prasad, N.; Sen, J. and Prasad, R.; Proposed Embedded Security Framework for Internet of Things (IoT). In: 2nd International Conference on Wireless Communication, Vehicular-Technology, Information Theory and Aerospace and Electronics System Technology (Wireless VITAE), Chennai: IEEE Xplore 2011.
15. Ukil, A.; Sen, J. and Koilakonda,S.; Embedded Security for Internet of Things. In: 2nd National Conference on Emerging Trends and Applications in Computer Science, Shillong: IEEE Xplore 2011.