IPASJ International Journal of Computer Science (IIJCS)
Web Site: http://www.ipasj.org/IIJCS/IIJCS.htm
A Publisher for Research Motivation ..... Email: editoriijcs@ipasj.org
Volume 2, Issue 8, August 2014 ISSN 2321-5992

Internet of Things:A vision, technical issues, applications and security

M.Newlin Rajkumar[1], C.Chatrapathi[2] and V.Venkatesakumar[3]

[1]Assistant Professor, Dept. of CSE, Anna University Regional Centre Coimbatore.

[2]PG Scholar, Dept. of CSE, Anna University Regional Centre Coimbatore.

[3]Assistant Professor, Dept. of CSE, Anna University Regional Centre Coimbatore.

ABSTRACT

Internet of Things (IoT) is a developing technology with lots of applications in society and the huge scope in the research field. Because of the impact IoT goes to make in our society and in our day to day activities; it is necessary for us to understand what is IoT; how it works; what challenges are in it; why it is needed and so on. This paper provides a detailed study on the Internet of Things and aims to answer all the above questions. Since Internet of Things had evolved from the collaboration of various existing technologies we provide a survey of various technologies and their contribution towards IoT. We also address various open issues in IoT which is helpful in understanding the challenges and research scope of this field. Various applications of IoT in different domains are deeply discussed in our paper. Finally, we conclude our work with presenting different security issues in IoT.

Keywords: Internet of Things (IoT), Survey, Issues, Security, Applications, Cloud Computing, RFID.

1. INTRODUCTION

Our computation world has gone past various technological waves, trends and eras. The next wave, trend or era will be around Internet of Things (IoT). This is because of the number of applications that IoT have on everyday life at home, office, transportation, medical and enterprise level. US national intelligence council predicts that "by 2025 internet nodes may reside in everyday things – food package, furniture, paper documents and more"[1]. In general; Internet of Things is the network of millions of things (things may physical or virtual varies from small pen in large car) that are uniquely identifiable and communicate with other things to exchange information to complete the job without the aid of human intervention. In general IoT has a large number of sensors that are invisibly embedded in our environment. These sensors collect and exchange the information with each other to create a virtual picture of the environment. This can be used to take appropriate decision based on the current situation. IoT causes the generation of large amounts of data that needed to be stored and processed in order to take appropriate decisions. In order to fulfil these requirements IoT uses cloud computing to provide necessary infrastructure needed for data storage and processing. It also provides analytic tools and support in decision making. With recent developments in devices with sensing and communicating capabilities; communication standards like ZigBee, WI-Fi and etc.; and ubiquitous computing Internet of Things are becoming more realistic and already many IoT based applications are developed. Already by 2011 number of connected devices exceeds the number of humans in the world. Presently there are 9 billion interconnected devices which expected to reach 24 billion devices by 2020. Even though there are several researches going on in the field of IoT; there are still lots of issues that are needed to be addressed. This paper provides an in depth review on the Internet of Things, including its related technologies, applications and open issues and also provide detailed analysis of security issues in the internet of things.

2. DEFINITIONS

Since Internet of Things is interdisciplinary in nature; IoT can be defined in several perspectives, including things oriented view, internet oriented view and semantic oriented view [3]. Some of the important definitions of IoT are discussed below. According to RFID group, IoT is "The worldwide network of interconnected objects uniquely addressable based on standard communication protocols". ITU defines IoT as "from anytime, anyplace connectivity for anyone, we will now have connectivity for anything [4]. According to cluster European research project IOT is "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 action and create services with or without direct human intervention"[5]. According to documents and communications of the European Commission definition of IoT involves "Things have identities and virtual personalities operating in a smart space using an intelligent interface to connect and communicate within social, environmental and user contexts"[6]. According to Gubbi, Buyya et al. [2], IoT in the context of cloud computing and wireless sensor networks 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 analysis and information representation with cloud computing as unifying framework".

3. ENABLING TECHNOLOGIES

As we discussed earlier IoT is interdisciplinary in nature. It is developed from the intelligent integration of several existing technologies. In this section several technologies its applications, how it integrates with other technologies and its contribution in realizing IoT are discussed briefly.

3.1 RFID TECHNOLOGY

RFID technology is used for monitoring an object. RFID system has an RFID reader and an RFID tag. RFID reader starts the communication with tag by sending query for identifying particular tag. The RFID tag is a small chip with antenna [7]. Each tag is associated with unique IDs. Chip can be attached to any object that needed to be tracked. There are two types of RFID tags are available. One is passive RFID tags which don't have battery for power supply. It takes power from the query signal for transmitting its ID to the reader. Another one is active RFID which contains a battery. It has the ability to start communication by transmitting its ID. Passive RFID is used in many applications including security, stock monitoring, transportation and etc., active RFID is mainly used for monitoring cargo. In the field of IoT RFID is used for identification of an object among a pool of millions of things. The main disadvantages of RFID is it can only used for monitoring objects, it can answer to incoming queries by replying its ID. It doesn't have the ability of sensing and monitoring. Hence it is combined with wireless sensor technology to provide a virtual picture of the environment in which it is embedded.

3.2 Wireless Sensor Networks

Wireless sensors are used for sensing and controlling environmental parameters. Each sensor node consists of sensor interface, small memory and processing units, analog to digital to analog converters and transceivers. These sensors have the ability to sense and process data and also communicate with other sensors in multi-hop fashion. The large number of such sensors combines to form a wireless sensor network (WSN). WSN has two nodes, namely source and sink. The source is sensor/actuator node that collects information about the environment and sends that information to sink. Sink collects information from various sources to get the big picture about the environment and take necessary action based on such information. Recent development in the integrated circuits operating at lower power and wireless communication standards results in devices with low cost, small size and increased processing and sensing power. This causes way for several new applications using wireless sensor networks, including disaster management, medical, agricultural, logistics and telematics application. Wireless sensor network is data centric and it works based on the data sensed by the sensor and won't consider much about the identity of sensor from which that data is coming. But for the IoT identity of each object is very important, hence wireless sensor network is combined with RFID technology to develop new network called RFID sensor network (RSN) [8]. This network has the ability to sense, process and transmit data. Also each node has a unique identity. This opens the door for several innovative applications in the field of IoT.

3.3 Ubiquitous Computing

The objective of the ubiquitous computing is to invisibly embed our technology in our environment and also in day to day life activities. Mark Weiser (fore father of ubiquitous computing) defines ubiquitous computing as "the physical world that is richly and invisibly interwoven with sensors, actuator, displays and computational elements, embedded seamlessly in the everyday objects of our lives, and connected through a continuous network"[9]. With the development in the micro-electro-mechanical system (MEMS) results in miniature devices with sensing, communication and processing power to help us to realize ubiquitous computing. The main goal of IoT is to make sense of information about the environment without intervention of human. Ubiquitous computing provides the way to achieve this goal.

3.4Cloud Computing

Cloud computing provides computing, on demand as a service to users in pay to use fashion. Cloud can provide infrastructure, software, and platforms as a service In IoT cloud is used to store and process huge volumes of data generated by sensors. Since sensors has constrained memory and processing power it can able to store and process only

local data. In order to get an overall picture about environment cloud provide infrastructures like datacenters to store data. It also allows IoT applications to monitor all the objects and run its software like mining and analysis tools. It supports artificial intelligence algorithm for decision making without human intervention.

3.5 Big Data

Big data is the term used to represent a large amount of data on which data related operations are unable to perform with the aid of normal data processing applications. In Big data provide some special techniques like Hadoop and Hiveql to manage these large volume data. Big data is very useful in many areas like social networks, research fields like meteorology and by governments and etc. In the IoT large amount of data are supported by cloud computing and on combining it with big data provide an excellent support to store and retrieve useful information from the large amount of sensor data.

4. APPLICATIONS

IoT has possible applications in almost every day to day activity and in a wide variety of domains. But only very few applications are currently coming into use. As we have seen already a number of connected devices already crossed the number of humans. Still, these devices lags in intelligence and in cross platform connectivity. By introducing proper intelligence and developing a common standard for these large heterogeneous devices; many new IoT applications can be developed. IoT has numerous application in a variety of domains. We here try to give some of the applications in the following domains.

4.1 Smart Environment

In smart home all the home appliances are equipped with intelligent sensor and the appliances can able to understand its environment and its user needs. They can also able to interact with each other. Some applications are automatic control of cooling/heating in air conditioner based on climate. Turn on and automatic turn off of lights based on available sunlight. Switch off the unnecessary gadgets in the rooms when no one is inside. These will not only increase comfort of the user, but also save power. In a smart office environment, employees are provided with smart ID cards which allow the management to automatically monitor in and out time of the employees. It also helps in access control inside the office premises. For example, we can signal an alarm when an unauthorized person entering into restricted area. Also company's assets can be attached with RFID tags; so that theft or missing of valuable assets can be avoided.
In smart industries by attaching tags with our products we can easily identify the status like in which plant the product is; what is its production status and so on. Also by attaching sensors with the machinery in industries we can monitor its vibrations and machine can be automatically shut down when some abnormalities are seen in vibration pattern.

4.2 Transportation

In transportation, vehicles are attached with intelligent sensors which allows a vehicle to communicate with another vehicle and share information. Using this several applications like accident avoidance system are evolved. A lot of research work is going on in developing an automatic vehicular system without driver. Government can also make use of these sensors embedded in vehicles for speed monitoring and enable it to fine penalties if vehicles are driven by high speed. Automatic traffic monitoring is another very important application of IoT in the transportation domain. It includes selecting an optimal path based on current road traffic. Also, it allows controlling traffic lights based on traffic flow and also giving priority to emergency vehicles like ambulance, police and rescue vehicles.

4.3 Medical Service

Patient monitoring is one of the important and existing applications of IoT. Sensors are attached to the patient's body for monitoring essential parameters of the patient's like heart beat, blood pressure, breathings and so on [10]. When some abnormalities are found in the readings, then it automatically alerts the doctor and also emergency medical service. IoT is very useful in remote patient monitoring and monitoring aged people who are alone at home. A lot of such applications are already available today. Evan some smart phones are having the ability to monitor certain human parameters. IoT also include patient identification which is very helpful in monitoring drug dosage and dosage interval. It avoids patient mismatch during treatments or in medical supply. Also, we can authenticate doctors, nurses and maintenance workers.

4.4 Personal

In these domain sensors attached with user and allow him to interact with others and things. One example for applications in this domain is an automatic status update on social networking sites. With the help of RFID tags embedded in user it automatically updates location status and status like watching movies or in coffee shop based on current location. With RFID tags attached to keys and other easily forgettable things we can easily find those objects.

This application also extends to theft detection schemes. When an object like a laptop or some things moved from the home region without authentication an automatic alarm message can be sent to owner's phone.

4.5 Disaster Management

One of the very interesting and useful applications of IoT is disaster management. During the time of disaster like flood, cyclone, volcanic eruption, tsunami and earthquake, it is very important to alert the peoples in nearby areas and evacuate people in danger region as soon as possible. With the help of wireless sensor network disaster can be sensed at the origin and alert is sent to the surrounding region automatically and provide them some extra time to protect their lives [11]. If the peoples are embedded with RFID tags disaster recovery works can be easily carried out [12]. With the help of tags people's position can be identified and it can be very useful to rescue them soon. For example, during earthquake time it is very useful to identify location of people who are trapped inside demolished buildings so that they are rescued on time.

5. OPEN ISSUE

As we seen in section 3 IoT is evolved from the integration of several existing technologies. This integration and nature of IoT bring several new challenges in realizing IoT in practical. Currently only a very few issues are addressed so far. Most of the other issues are still in research stage only. In this section we present some of the major issues in IoT. We also present current and possible future development in this issue in table 1.

5.1 Standardization

An important issue in IoT is the development of open and standard architecture for IoT. Developing such standard architecture is made very challenging because of the diversity of devices involved in IoT. In IoT things may vary from small RFID tags to well sophisticated smart phones. IoT also has distributed resource availability. Developing a standard architecture with considering above issue is a major challenge. IoT also needed to form peer to peer connection autonomously. Architecture must able to adapt these requirements. For this, architecture must decentralized and distributed with search, discovery and peer network ability. Since large amounts of data are generated by IoT it is necessary that intelligence should be extended to end of the network so that end devices can perform decision making, and other filtering techniques to reduce the amount of data being transmitted in IoT system Seamless connectivity requirement and large number of devices involved in the IoT creates new challenges for connectivity. Different kind of communications like things to things communication, communication with the data centre, and communication with sensor/ actuators are supported by IoT. Hence standard communication protocol that supports these types of communication has to be developed.

5.2 Addressing

IoT is the network of billions of things. Unlike wsn in which nodes won't contain specific IDs; all the nodes in IoT must contain a unique identifier. It creates new challenges on addressing schemes. Ipv4 is only 32 bit addressing scheme and it has the problem of address exhaustion. Hence obvious choice for addressing IoT is ipv6 as it is 128 bit dressing scheme. But again, using ipv6 addressing for RFID tags creates new challenges. According to the EPCglobal standard rigid can support only 64-96 bit IDs. Lot of schemes are proposed to tackle this problem; like using the first 64 bits of address to mention RFID tag identifier, and the next 64 bits to address gateway between RFID and internet [13]. But all the schemes have certain disadvantages when it comes into practical use. If we consider mobility of node, then addressing createss to lot of scalability and adaptability issues.

5.3 Power Storage and Ussage

Almost all the devices in IoT are wireless. In that some of the devices like passive RFIDs don't need battery; but most of the devices had to depend on battery for its power. It creates new challenge in creating small devices with long lifetime. If we use a battery with high capacity, then the size of the device will be large. If we design small device then battery life will be short and we need to charge or replace the battery. Energy harvesting is one of the solution for this issue. This allows the sensor to produce energy from its environment. But this technology is still in very early stage and a lot of research has to be done on MEMS and energy harvesting. Some of the potential sources for energy harvesting are photovoltaic, temperature gradients, vibrations and pressure variations in the environment. Energy consumed by the devices for sensing and processing can be reduced by developing a framework that makes use of spatial and temporal detail of sensing data.

5.4 Data Processing

As we know IoT generate very large amounts of data. Since most of the IoT application is real time it is necessary that sensed data has to be processed immediately. Hence advanced data mining algorithms have to be developed. The goal

of IoT is to give intelligence to things. So advance learning methods and artificial intelligence algorithms have to be developed to handle automatic decision making.

5.5 Search and Discovery

As we know IoT is made up of millions of things. IoT contain distributed resource source and sinks. In many cases application needs to find the particular node based on its type (sensor/actuator), available content, location, and type of service provided. Even though all the nodes in IoT have a unique identifier these requirements create challenge in identifying a particular group of nodes from the whole sensor pool. Efficient search and discovery technology are very important to map real world object or environment in virtual space.

6. SECURITY CHALLENGES

Security is one of the major issues in IoT that is why we present security as a separate section rather than in section 5. Even though IoT makes people's life more sophisticated and having wide range of application; people won't adopt IoT unless they have confidence that IoT is secure. As we know main contributors for IoT like wireless sensor networks, cloud computing and RFID technology itself has many security issues that yet to be addressed. By combining these technologies and due to IoT characteristics several IoT security challenges are raised. In this section we see major security issues in IoT.

6.1 Authentication

Authentication is the process of checking the originality of the user or entity participating in the communication. Authentication is one of the major issues in IoT. Most of the devices participating in IoT are constrained in terms of resources and lack of an authentication infrastructure (like third party authenticator) and server it becomes very difficult to carry out authentication mechanisms in IoT. Ensuring authentication in an RFID tag is critical issue since passive RFID tags lags in processing and it simply reply to the incoming query signal without performing any authentication. It creates a serious threat for authentication also RFID tags are very constrained in memory and processing; it is unable to exchange many messages. Hence, implementing authentication mechanisms in RFID is very challenging. IoT system is seriously suffered by man in middle attack. Several approaches are proposed for providing authentication for IoT but all approaches are having some severe disadvantage and failed to provide complete authentication. Still lot of research is going on in addressing the authentication issue.

6.2 Data Integrity

Data integrity deals with the validity of the data. It enforces that data stored in the sensor or being transmitted are unable to modify without identifying by system or owner. In most of the case sensors in the IoT are left alone in an environment without any monitoring. Hence attacker can easily destroy or alter the data in sensor. In order to protect from these kind of attacks now sensor memories are protected. Another issue is protecting data during transmission. Keyed hash-message authentication (HMAC) scheme is used to protect transmitted data [14]. In IoT it is difficult to implement cryptographic schemes because of the constrained resource availability in sensors. Only small length keys can be used because of reduced memory. Complex cryptographic algorithms can't be executed by the sensor. This also leaves data integrity of IoT in danger since small key is easily breakable by attackers. Thus, some novel method having ability to balance this tradeoff between resource and security has to be developed.

IPASJ International Journal of Computer Science (IIJCS)
Web Site: http://www.ipasj.org/IIJCS/IIJCS.htm
A Publisher for Research Motivation ..... Email: editoriijcs@ipasj.org
Volume 2, Issue 8, August 2014 ISSN 2321-5992

Table 1. Future Development in IoT [18]

Domain	Before 2010	2010-2015	2015-2020	Beyond 2020
IoT Architecture Technology	x IoT architecture specifications x Context-sensitive middleware x Intelligent reasoning platforms	x IoT architecture developments x IoT architecture in the FI x Network of networks architectures x F-O-T platform interoperability	x Adaptive, context based architectures x Self-* properties	x Cognitive architectures x Experiential architectures
Data Processing Technology	xSerial data processing x Parallel data processing x Quality of services	x Energy, frequency spectrum aware data processing, x Data processing context adaptable	x Context aware data proc- essing and data responses	x Cognitive processing and optimization
Search and Discovery Technologies	x Sensor network ontologies x Domain specific name services	x Distributed registry, search and discovery mechanism x Semantic discovery of sensors and sensor data	x Automatic route tagging and identification management centres	x Cognitive search engines x Autonomous search engines
Power and Energy Storage Technologies	x Thin batteries x Flat batteries x Power optimized systems (energy optimization) x Energy harvesting (electrostatic) x Short and medium range wire- less power	x advanced Energy harvesting (photovoltaic) x Printed batteries x Long range wireless power	x Energy harvesting (bio- logical, chemical, induction) x Power generation in harsh environments x Energy recycling x Wireless power	x Biodegradable batteries x Nano-power processing unit
Security and Privacy Technologies	x Security mechanisms and proto- cols defined x Security mechanisms and proto- cols for RFID and WSN devices	x User centric context-aware privacy and privacy policies x Privacy aware data processing x virtualization and anonymisation	x Security and privacy pro- file selection based on security and privacy needs x Privacy needs automatic evaluation x Context centric security	x Self adaptive security mechanisms and protocols

6.3 Privacy

This is one of the serious issues in IoT and acts as a barrier between the people and IoT. If IoT wants to be established widely it requires to earn the trust of people. For this first of all people need to know what personal data about them are collected, by whom these data are collected, for what these data are collected and etc. people should capable of controlling personal data being collected. In case of sensor network it is difficult to control privacy. Since sensors are pervasive and ubiquitously embedded in the environment, peoples may unaware that they are under sensing or they are unable to control data being collected about them. For example, if one enters the place which is under video surveillance the he is unable to prevent us from being monitored and recorded. In case of RFID [15], the situation has gone even worse since the RFID reply to all the query signal without any verification, hence unauthorized persons can easily identify and locate any person or object with an RFID tag. It is easy to eavesdrops message to authenticate authorized user. The first issue is related to authentication. We can control eavesdropping by encrypting the message.

Even if we encrypt the message, unauthorized user may know the existence of RFID tag and able to track it. To avoid this message can be transmitted as pseudo noise [16]. One of the proposed solutions for privacy in IoT is introducing privacy broker [17]. This acts as a proxy between sensor and service. User can able to control proxy setting like which data can be collected, who can access it and so on. Privacy broker also provides information for service only when it is strictly needed.

6.4 Digital Forgetting

As the result of technological development, cost for storing data has reduced dramatically. It makes storing data simple and cheap. Once sensed data is stored into the system possibly it can exist infinitely in the system. It is possible to retrieve someone's personal data long time after it is actually sensed. It creates a serious threat for individual's personal data. Since data can be used either productively or destructively. It is necessary that some mechanisms had to be developed in order to delete this data periodically and ensure that data is stored in the system only as long as it is seriously needed.

7. CONCLUSION

IoT is the developing technology that is going to change the world and the way people lives today. Since IoT is going to occupy us in the near future, it is necessary for us to understand what is IoT. IoT emerges from the collaboration of many existing technology. Hence IoT is multi perspective and has several definitions in different perspective. This paper tries to give simple and clear vision about IoT. Here we also provide a detailed survey of several open issues and challenges in IoT. The security of IoT is also discussed very deeply to provide an overall picture of IoT.

REFERENCES

[1] National Intelligence Council, Disruptive Civil Technologies – Six Technologies with Potential Impacts on US Interests Out to 2025 – Conference Report CR 2008-07, April 2008, <http://www.dni.gov/nic/NIC_home.html>.

[2] J. Gubbi, R. Buyya et al. "Internet of Things: A vision, architectural element, and future directions". ELSEVIER, February 2013.

[3] L. Atzori, A. Iera, G. Morabito, The Internet of Things: a survey, Computer Networks 54 (2010) 2787–2805.

[4] ITU Internet Reports, The Internet of Things, November 2005.

[5] H. Sundmaeker, P. Guillemin, P. Friess, S. Woelfflé, Vision and challenges for realizing the Internet of Things, Cluster of European Research Projects on the Internet of Things—CERP IoT, 2010.

[6] INFSO D.4 Networked Enterprise & RFID INFSO G.2 Micro & Nano systems, in: Co-operation with the Working Group RFID of the ETP EPOSS, Internet of Things in 2020, Roadmap for the Future, Version 1.1, 27 May 2008.

[7] A. Jules, RFID security and privacy: a research survey, IEEE Journal on Selected Areas in Communications 24 (2) (2006) 381–394.

[8] M. Buettner, B. Greenstein, A. Sample, J.R. Smith, D. Wetherall, Revisiting smart dust with RFID sensor networks, in: Proceedings of ACM Hot Nets 2008, Calgary, Canada, October 2008.

[9] M. Weiser, R. Gold, The origins of ubiquitous computing research at PARC in the late 1980s, IBM Systems Journal (1999).

[10] D. Niyato, E. Hossain, S. Camorlinga, Remote patient monitoring service using heterogeneous wireless access networks: architecture and optimization, IEEE Journal on Selected Areas in Communications27 (4) (2009) 412–423.

[11] M. Castillo-Effen, D. Quintela, R. Jordan, W. Weshoff and W. Moreno, "Wireless sensor networks for flash-flood alerting", Proc. Of the 5th IEEE International Caracas Conference on Devices, Circuits and Systems, November, Dominican Republic, 2004.

[12] De-Li Yang Feng Liu Yi-Duo Liang, A Survey of the Internet of Things, The International Conference on E-Business Intelligence, 2010.

[13] S. -D. Lee, M. -K. Shin, H. -J. Kim, EPC vs. IPv6 mapping mechanism, in: Proceedings of Ninth International Conference on Advanced Communication Technology, Phoenix Park, South Korea, February 2007.

[14] H. Krawczyk, M. Bellare, R. Canetti, HMAC: Keyed-Hashing for Message Authentication, IETF RFC 2104, February 1997.

[15] T. Karygiannis, B. Eydt, G. Barber, L. Bunn and T. Phillips, Guidelines for Securing Radio Frequency Identification (RFID) Systems, NIST Special Publication 800-98, April 2007.

[16] O. Savry, F. Pebay-Peyroula, F. Dehmas, G. Robert, J. Reverdy, RFID noisy reader: how to prevent from eavesdropping on the communication? In: Proceedings of Workshop on Cryptographic Hardware and Embedded Systems 2007, Vienna, Austria, September 2007.

[17] G.V. Lioudakis, E.A. Koutsoloukas, N. Dellas, S. Kapellaki, G. N. Prezerakos, D.I. Kaklamani, I.S. Venieris, A proxy for privacy: the discreet box, in: EUROCON 2007, Warsaw, Poland, September 2007.

[18] Vision and Challenges for Realising the Internet of Things, published by CERP-IoT – Cluster of European Research Projects on the Internet of Things, March 2010.

AUTHOR

M. Newlin Rajkumar is presently working as Assistant Professor in The Department of Computer Science and Engineering, Anna University Regional Centre, Coimbatore. He received his Bachelor of Engineering Degree from Bharathiyar University, Master of Science (M.S by Research) from National Chiao Tuns University, Taiwan and Master of Business Administration (IBM) from Anna University, Coimbatore. Presently he is pursuing his Ph.D in Anna University Chennai. He has more than ten years of Teaching Experience. He has published several papers in reputed International Journals. He is a Professional Member of ACM, Member of IEEE India Council, Life Member of International Association of Computer Science and Information Technology, International Association of Engineers and in many International Associations. His research interest includes cloud Computing, Internet of Things, Big Data Analytics, Network Security, Security Protocols and Network Management.

C. Chatrapathi is pursing M.E Computer Science and Engineering (Specialization with Networks) in the Department of Computer Science and Engineering, Anna University Regional Centre, Coimbatore. He received his Bachelor of Engineering Degree from Anna University Chennai. His research interests are Cloud Computing, Internet of Things and VANET.

V. Venkatesakumar is presently working as Assistant Professor in The Department of Computer Science and Engineering, Anna University Regional Centre, Coimbatore. He received his Bachelor of Engineering Degree from Bharathiyar University, Master of Engineering Degree and Ph.D from Anna University Chennai. He has more than ten years of Teaching Experience. He has published many papers in reputed International Journals and has Chaired many Conferences. He is a Life Member of International Association of Computer Science and Information Technology, International Association of Engineers and in many International Associations. His research interest includes Cloud Computing, Internet of Things, Big Data Analytics, Operating System, Software Engineering and Web Technologies.