Survey on Internet of Things and Design for a Smart Parking Area

Sonali Sharma, Chhatarpal, Ramanand Harijan

Abstract*— *This paper introduces Internet of Things (IoTs), which offers capabilities to identify, share information and connect worldwide physical objects into a single system. In this research work, we will discuss how we can connect various objects in a better way and what are the basic requirements and functions to make them communicate and consequently make this world unified. This survey summarizes the easiest and most feasible way of connecting various objects of IoT and it also discuss about a prototype for smart parking area application of IoT. In this prototype we have used a microcontroller to handle all the devices. Security is also added to this model using scanners and finger print detectors.

Index Terms*—*Internet of Things (IoT), Parking, Security, Addressability

I. INTRODUCTION

Internet of Things is a new era technique, in which all things including every day and industrial objects are connected in such a way as to make the systems intelligent, programmable , self configuring and capable of interacting with humans. IoT will connect objects, people, anywhere and anytime. In IoT objects will communicate through various sensors, actuators, bluetooth connections, radio frequency identifications, etc. IoT is here because we want to make this world more technically advanced where objects can communicate to each other without any human interference. We are having various technical systems from super computers to desktop computers. But the problem is that every single system is human dependent for data. For example consider our desktop computer which is equipped with various applications and programs. But without human interference it cannot perform a single function. IoT will make objects smarter; the objects will be interconnected in such a way that if a trigger happens somewhere in the system then automatically information get distributed among other various interconnected systems. So IoT will enable objects to communicate. We can track objects by object's identity and can share information by broadcasting data to servers so that anyone can retrieve information (general information). To make our data secure the developers may have to add some security features in the system so that personal information will not become accessible to anyone and can only be retrieved when its urgent and that too after acquiring permissions from the administrator.

Manuscript Received on August 2014.

Sonali Sharma, Department of Computer Science Engineering, BMGI, Gurgaon, India.

Chhatarpal, Department of Computer Science Engineering, BMGI, Gurgaon, India.

Ramanand Harijan, Head of ECE & Department of EEE, BMGI, Gurgaon, India.

Figure 1 and 2 are describing the present scenario and future scenario of the technical world [1].

Figure 1.1 Present Scenario [1]

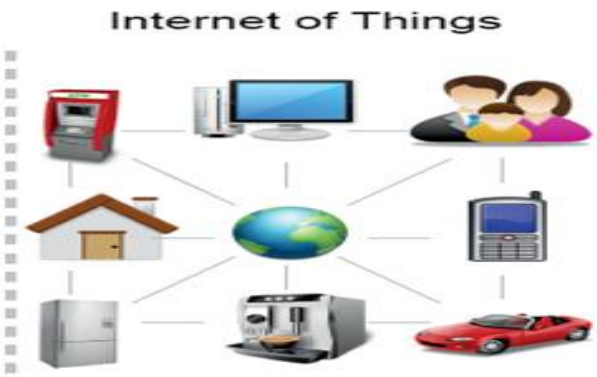

Figure 2 Future Scenario [1]

II. IMPORTANCE AND APPLICATIONS

A. Importance

In this technical world the next wave of technology will be outside the realm of the traditional desktops. In today's scenario most of the things that surrounds us are on the networks in one or another form.Therefore the various key factors for doing internet of things are as follows

i. The Internet of things is an adaptive and a self configuring system which makes it so important in present scenario. As it is adaptive in nature and we have to configure it just for once, after that it will itself respond correspondingly.

ii. The basic purpose of IoT is to make minimum number of human interferences, as humans are more prone to errors as compare to machines.

iii. Replacing humans with machines means increasing automation. No doubt it will reduce job opportunities for labour work but on the other hand it

Published By:
Blue Eyes Intelligence Engineering
& Sciences Publication Pvt. Ltd.

will also increase the job opportunities at technical end. So, the development and implementation of IoT is completely justified.

iv. By making parking area smart we can utilize the parking area more efficiently; car owners or drivers will have a hassle free and timely response from the system.

B. Applications

Rapid advancements in networking field together with extreme miniaturization of communication, electrical and computing devices enable emerging in exciting applications and services that connect the cybernetic and physical word. There are various applications under IoT that are partially implemented

i. Medical field.
ii. Smart homes.
iii. Transportation.
iv. Education.
v. Waste management.

III. BASIC TECHNOLOGIES RELATED TO IoT

A. Addressability for IOT

Addressing is important to provide object identification, so that we can easily track or identify object in this ambiguous world. Relating to this we are having four types of addressing schemes:

Figure 3 Types of Addressing

i. Logical Address (IP addressing): This address is globally unique and used to communicate world –wide.
Examples:
IPv4: 172.16.23.11(32 bits)
IPv6: 2021:0db5:55a3:0047:1004:7a2e:0370:7003(128 bits)

ii. Physical Address: This address is locally unique and used to communicate in a local area. This address is machine built in, written on the interface card of the machine. Also known as MAC (medium access control) address and Burned in address as it is written on read only memory. It helps in accessing the medium (transmission medium like Ethernet cables etc.) during transmissions.
Examples:
Mostly in 48-bit and 64-bit format.
01-14-23-01-23-45.
00-22-4D-47-FD-0E.

iii. Port Address: This type of address is application and process specific addresses. If we want to use a particular service then we have to specify its port address.
Example:
80 = http(hyper text transfer protocol)
443= https(hyper text transfer protocol secure)
20 & 21 = ftp(file transfer protocol for data and control respectively)
23= telnet (terminal network)
25= smtp(simple mail transfer protocol)

iv. Specific Address: This type of address is related to any specific individual or institute or company that uses it for the purpose of communication in the network.
Example**:**
sonalisharma@gmail.com
bmctm@gmail.com
analyst.relation@tcs.com etc.

Usage of Addresses

If we want to connect the objects then we have to convert networks of proprietary protocols to IP based networks. To make objects IP based network compatible we have to provide an identity to them so that they can communicate.
As by 2020 there will be nearly 20 billion devices on the IOT, to make them uniquely identifiable, only possible way is addressing. This urges towards the efficient use of available addresses. There is no lackness in addresses, as IPV6 has availability for billion of addresses. As per future needs we have to categorise there usage.

- The developer may use IP addresses for the objects which are meant to communicate world-wide. For example in medical fields, the database need to be maintained for getting better services, experts opinion and any other information to be sought from past cases.
- On the other hand for a parking area we do not need to connect with worldwide systems. So here we can easily communicate through MAC addresses.

B. Technologies and Requirements of IoT

i. Technology:

In IOT we can make use of almost every technology like:

a. Intelligent System -To make object intelligent which makes them respond according to the conditions they surround. It comes under artificial intelligence. It can be provided with the programming languages like PROLOG, LISP etc.

b. Networking – To connect various things or objects effectively and efficiently world-wide.

c. Database Management – We need a good database manager so that all data can be managed in an effective manner.

d. Security – As all the objects has to communicate through network, so they require secure environment.

e. Embedded and Microcontroller Systems – It operates various signals and systems.

ii. Basic Requirements

a. Identity- If all objects in daily life are equipped with identifiers, they could be managed and inventoried by computers. To give a unique identity, it is required to add an identification number to every object during its manufacturing time like MAC addresses, bar codes, QR

Published By:
Blue Eyes Intelligence Engineering
& Sciences Publication Pvt. Ltd.

codes etc. If authentication is prime factor for an object like in medical appliances we can add digital water marker to them, as these will help out in source tracking, video authentication, broadcast monitoring, etc. Bar codes, QR(quick response) codes can also be used for identification. QR codes have fast readability and greater storage capacity compared to standard UPC barcodes.

b. Inter or Intra communication-

- Inter communication means when we have to communicate between a single system i.e a local communication, as a parking area technologies like RFID(radio frequency identification),NFC(near field communications)like android beams, Bluetooth, Wi-Fi, etc.
- Intra communication means communication among global networks, where we use internet services, IP addressing for various gateway devices like routers, gateways etc. to communicate. This type of communication is followed among various fields like medical fields, transportation field, among institutions etc.

c. Sensors, actuators, and RFID

These technologies [5,6,7] have been around us for a couple of decades. We can identify, track and conclude what an object is and where it has been used whether to monitor machinery, to exchange information, to manage inventory, or to track packages and live stocks. Sensors can be used or being used everywhere, including automobiles, cell phone, clothing, credit cards, exercise equipment, gaming consoles, on roads to control the traffic along highways, hospitals, smart homes, etc.

Survey regarding sensors: Today's mobile devices are outfitted with a host of sensors, including accelerometers, gyroscopes, and microphones, to say nothing of compasses, GPS capability, and cameras all sharing data wirelessly over the Internet. In 2012, about 3.7 million things were connected to the Internet via sensors, according to a report issued by Trillion Sensors Summit, held last October at Stanford University and attended by representatives of more than 100 organizations from 14 countries. The goal of the meeting was to think on sensor-based applications to enter the market in the coming decade. The result was a startling prediction: The number of connected machines and devices will grow to 1 trillion by 2022. The IoT is expected to affect how businesses operate, including unlocking new revenue from existing products and inspiring new processes. An *Economist* survey of more than 770 businesses around the world found that 75 percent of them are already exploring the IoT and 95 percent expect to be using IoT applications by 2016. The magazine published its findings in June as part of its *Internet of Things business index* report. But as smart as the sensors already are, the success of the IoT depends on their becoming even smarter with, for example, their own IP addresses so they can be identified together with their location, according to IEEE Senior Member Chonggang Wang, editor in chief of the new *IEEE Internet of Things Journal* and a senior staff engineer at InterDigital Communications, in King of Prussia, Pa. Wang's research interests include machine-to-machine communications and developing the architecture, protocols, applications, and other enabling technologies for the IoT. "Today's sensors generally have resource constraints, including limited computation and storage, short battery life, and the inability to communicate with each other," he says. He points to areas where IEEE can take the lead in making the IoT a reality, including standards, education, and promoting its benefits to business owners and the public.

IV. SECURITY CONCERNS IN IOT

We are dealing with an environment which is full of networks and signals, which makes security as prime concern. None of us like to expose our personal or confidential information to the public. We also don't want people to provide false information that changes the proper action of the system. Therefore, another IoT challenge is data security and privacy. We have to add security features at different levels like security at device, security in communication, security in storage, and security in processing.

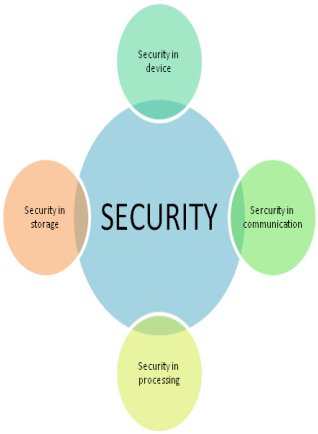

Figure 4 Types of Security

A. Security in Devices:

- Firewalls:
  A software firewall, hardware firewall or other network filtering (e.g. port or IP address filtering) technology must be used to protect the computer/device while on the network. Prefer hardware firewalls like SONIC, CYBERROAM, NETGENI etc. Because from some software firewalls, third party can make bypass proxies, and these are capable for windows firewall break down.
- Use up-to-date antivirus and antispyware software like NORTON, SYMANTEC, QUICK HEAL (Windows).
- Operating System: Keep your operating system up-to-date. As we know that Apple's product is more secure as compare to other brands because of their Macintosh operating system, which is very less prone to cyber attacks, threats etc. We know that Window's operating system is GUI based which makes it an easy victim to be attacked by hackers. So prefer LINUX, UNIX operating systems where security is the main concern.
- Backup:-Create a backup of the entire system periodically, and critical data files whenever they get updated. The ITS Home Directory Service provides adequate backup space for most people, but files consuming large amount of space—video or music—may require external disk drives to back them up adequately.
- Restrict Management Services:- SNMP, telnet and https (web) are protocols used to manage printers. Telnet is

Published By:
Blue Eyes Intelligence Engineering
& Sciences Publication Pvt. Ltd.

rarely used in older printers without web access. If https (web) access is available, telnet should be turned off. SNMP is used for large organizations managing hundreds to thousands of devices, including printers. SNMP should be turned off.

B. Security in Communication:

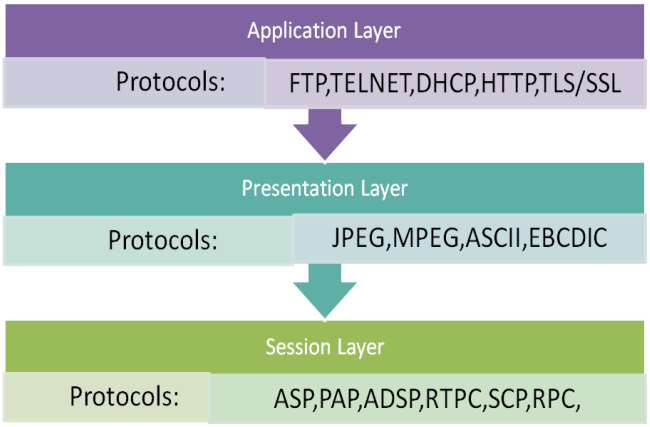

Figure 5 Upper Layers of OSI Model with Protocols

Session layer is responsible for the dialogue control so to perform a secure communication, we can use various secure protocols that will authenticate the communication. We can apply various encryption and decryption techniques to our data. For secure communication both parties should be secured with a secured password.

C. Security in Storage:

Generally to make our storage secure we use RAD0, RAD 1, RAD 2… RAD 5,as they have property of replicating the data. This is applicable only for the main hubs of information, not for every objects memory. We must secure our data in such a way that personal information data cannot be get easily accessed. In context to that do not retrieve personal information until it's very important.

D. Security in Processing:

As we know data get processed when it is under operational mode or in a network. For making our processing secure we have SSL/TLS protocols for application layer, which makes the processing of our data very secure. These all are some security features that we can apply to our systems. When it comes for the security of object in IOT we make sure that during the manufacturing time every object must have an identification no., by which it can get uniquely identified in the network and have some internal memory. So they will smoothly get operated on the network.

V. DESIGN FOR IMPLEMENTATION OF A SMART CAR PARKING

Internet Of things means to make objects communicate with minimum human interference and make this world smarter. Here we are implementing a smart parking area with security features in it. Already many systems [11-16] have been introduced keeping automatic parking in mind using microcontrollers, but they did not give any idea about effective storage. So here we are introducing how we can efficiently use available space for parking making it more automatic, using elevators and security features are also added using scanner and finger print machine.

A. Path to be followed During Arrival of a Car

- When car comes nearer to the parking area proximity sensor senses the presence of car and sends signal to the micro controller.
- In response micro controller checks the space availability by sending a signal to database management system.
- If it signals back as a high signal, it means there is a space availability for parking a car or if it sends a low signal then microcontroller display a" Sorry " message on LCD.
- On receiving a high signal micro controller activates the scanning device that will scan car's id(either engine number or number plate) and ask for finger print impression on biometric machine for security purpose.
- This information gets stored into database, during retrieval of car this information is used for counter checking.
- As scanner work gets completed it sends a low signal to microcontroller.
- Then microcontroller sends a signal to motor device for the opening of gate.

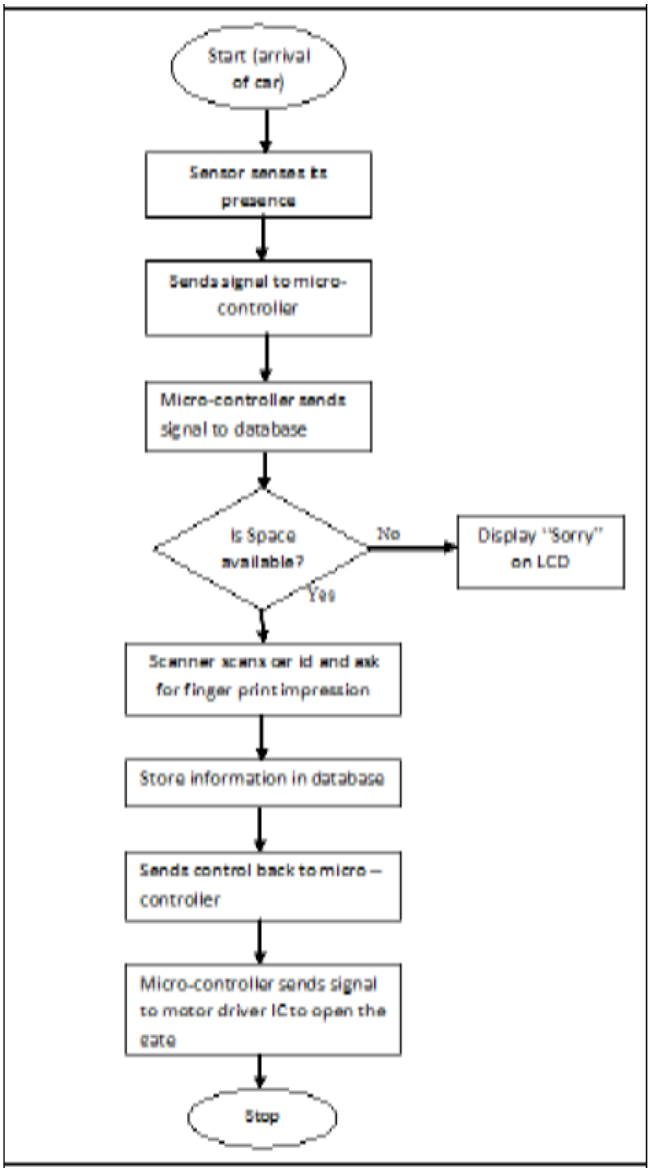

Figure 6 Flow Chart for Entry Gate

Published By:
Blue Eyes Intelligence Engineering
& Sciences Publication Pvt. Ltd.

Storage and Retrieval Process

When the car enters into the parking area, storage process starts, with the use of elevators car get parked without getting blocked from other cars. We can implement the storage and retrieval process using JAVA language. Using A*, D* Lite, Unblocking algorithms, it get implemented. As by applying the A* algorithm we can search for the used and unused spaces, using D* Lite we can plan for the path for retrieving the car and using unblocking algorithms we can store and retrieve cars without blocking the path of another car. We can also use the Manhattan Distance to decide the nearest path for the car from elevator. So by following all these algorithms storage and retrieval process gets completed. In this way we can efficiently utilize the parking space area.

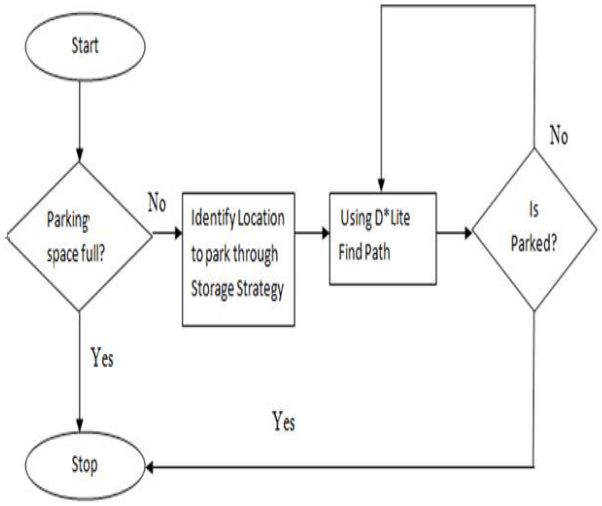

Figure 7 Car Storage Process

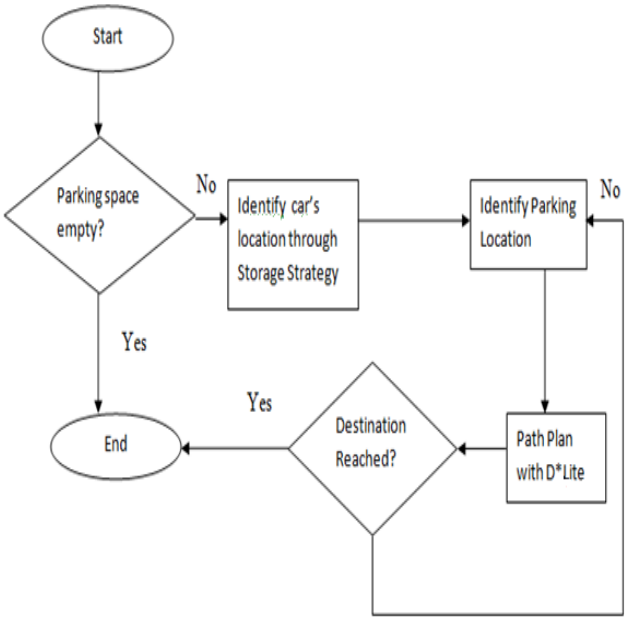

Figure 8 Car Retrieval Process

Path to be followed during exit process of a car

- When the car comes nearer to the exit gate, proximity sensor senses the presence of car and sends the signal to microcontroller.
- Micro-controller activates the scanning device and asks for the finger print impression. An owner can give finger print impression for at most 3 times. In 4rth time if he enters the wrong impression, the siren gets activated and security personnel's are alerted.
- If everything goes smoothly then database system sends signal to microcontroller.
- Micro-controller signals to motor driver for opening of the gate.

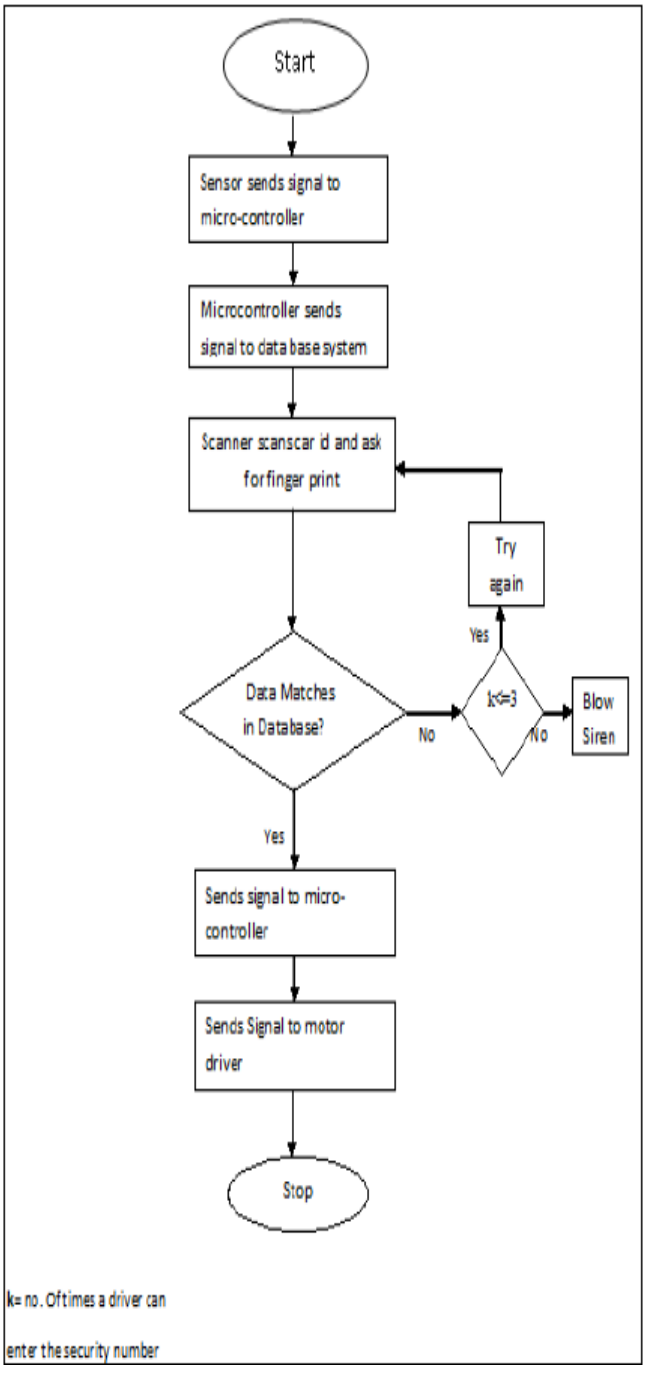

Figure 9 Exit Gate Flow Chart

To implement the entry and exit flow charts we are having various options which, we can implement by using Keil micro vision software which is a simulation tool for microcontrollers or we can implement it using the MAT lab. After implementing the entry and exit flow charts we have to create an interface between these three.

Published By:
Blue Eyes Intelligence Engineering
& Sciences Publication Pvt. Ltd.

VI. CONCLUSION

In this research paper we are bringing everyone's attention on the concept of new technology of IoT, as applications of old parking are not so updated towards automation and this technology of IoT opens the gate toward automation. So we have given an idea of automation towards the fully automatic parking world.

REFERENCES

[1] C. Perera, A. Zaslavsky, P. Christen, and D. Georgakopoulos, "Context Aware Computing for The Internet of Things: A Survey" IEEE Communications Surveys & Tutorials, 2013, pp. 1-41.

[2] M. Palattella, N. Accettura, X. Vilajosana, T. Watteyne, L. Grieco, G. Boggia, and M. Dohler, "Standardized protocol stack for the internet of (important) things," Proceedings of IEEE, 2012, pp. 1-18.

[3] O. Vermesan, P. Friess,and A. Furness, "The Internet of Things New Horizons" IERC - Internet of Things European Research Cluster, 3rd edition of the Cluster Book, ISBN hard cover: 978 - 0 - 9553707 - 9 – 3,2012.

[4] Bari, N. ; Mani, G. ; Berkovich, S., "Internet of Things as a Methodological Concept", IEEE, 2013, pp. 48 – 55.

[5] Yinghui Huang ; Guanyu Li, "Descriptive models for Internet of Things", IEEE International Conference on Intelligent Control and Information Processing (ICICIP), 2010, pp. 483 – 486.

[6] Coetzee, L. ; Eksteen, J., "The Internet of Things - promise for the future? An introduction", IEEE IST-Africa Conference Proceedings, 2011, pp. 1 – 9.

[7] Zhu Yu ; Wang Tie-Ning, "Research on the Visualization of Equipment Support Based on the Technology of Internet of Things", IEEE Second International Conference on Instrumentation, Measurement, Computer, Communication and Control IMCCC '12 Proceedings, 2012, pp. 1352 – 1357.

[8] Yinghui Huang ; Guanyu Li, "A Semantic Analysis for Internet of Things", IEEE International Conference on Intelligent Computation Technology and Automation (ICICTA), 2010, pp. 336 – 339.

[9] Lu Tan ; Comput.; Neng Wang, "Future internet: The Internet of Things", Advanced Computer Theory and Engineering (ICACTE), 2010 3rd International Conference on IEEE, 2010, pp. V5-376 - V5-380.

[10] Mingfang Du ; Jianjun Fang ; Haiqing Cao, "A new solution for city parking guiding based on Internet of Things and multi-level multi-agent", IEEE, 2011, pp. 4093 – 4096.

[11] Yanlin Yin ;Dalin Jiang, "Research and Application on Intelligent Parking Solution Based on Internet of Things", IEEE, 2013, pp. 101 – 105.

[12] Tsung-hua Hsu, Jing-Fu Liu, Pen-Ning Yu, Wang-Shuan Lee and Jia-Sing Hsu, "Development of an automatic parking system for vehicle", IEEE, 2008, pp. 1-6.

[13] Daobin Wang ; Huawei Liang ; Tao Mei ; Hui Zhu, "Research on self-parking path planning algorithms", IEEE, 2011, pp. 258 – 262.

[14] Oentaryo, R.J. ,Pasquier, M., "Self-trained automated parking system", IEEE, 2004, vol. 2; pp. 1005 – 1010.

[15] M. Nizam Kamarudin, "Development of an automatic parallel parking system for nonholonomic mobile robot", IEEE International Conference on, Electrical, Control and Computer Engineering (INECCE) 2011, pp. 45-49.

[16] Tang, V.W.S. ,Yuan Zheng ; Jiannong Cao, "An Intelligent Car Park Management System based on Wireless Sensor Networks", IEEE 1st International Symposium on Pervasive Computing and Applications, 2006, pp. 65 – 70.

Ms. Sonali Sharma, received the B.Tech degree in Computer Science Engineering from Maharishi Dyanand University Rohtak and Pursuing M.Tech under the Department of Computer Science Engineering from B.M. Group of Institutions, Farrukhnagar, Gurgaon. Her research interests are in Networking and Graphics.

Mr. Chhatarpal, received the M.Tech degree in Computer Science Engineering from Kurukshetra University, Kurukshetra. He has 9 years of Teaching Experience. He is currently working as HOD, Department of Computer Science Engineering at B.M. Group of Institutions, Gurgaon. His research interests are Networking and Operating System.

Mr. Ramanand Harijan, received the B.Tech degree in ECE, and M.Tech degree in VLSI Design from CDAC Mohali. He is currently working as HOD, Department of ECE & EEE at B.M. Group of Institutions, Gurgaon. His research interests are Low Power Circuits, Analog Design, and Digital Design and CMOS RF Circuits.

Published By:
Blue Eyes Intelligence Engineering
& Sciences Publication Pvt. Ltd.