Study on Internet-of-Things

Mahesh Joshi
Department of Computer Science and Engineering
VFSTR University Vadlamudi, Guntur, AP, India

N Gnaneswara Rao
Department of Computer Science and Engineering
VFSTR University Vadlamudi, Guntur, AP, India

Abstract- This paper is written for everyone who wants to know the details about Internet-of-Things in order to build Internet-of-Things based solutions. This paper covers from basics of Internet-of-Things to every aspect of this new revolutionary concept such as its key components, protocol stack for Internet-of-Things, communication technologies that are widely used in implementing Internet-of-Things, various issues like research opportunities and challenges for research in Internet-of-Things etc. We have touched all practical aspects of Internet-of-Things by giving an introduction to open source tools for IoT and IoT enabling technologies which can be further explored by the reader based on their application requirements and/or interest. We have tried to keep the contents of this paper up-to date by including some contents from web resources along with research papers.

Keywords – Internet-of-Things, Communication technologies, Protocols, Sensors, Actuators, Privacy and security issues, Tools for IoT, IoT enabling technologies.

I. INTRODUCTION

A. What is Internet-of-Things?

We have come across a great change in the world around us in last century. When computers came into reality we realized that we can let machines do some tasks that is repetitive. Later, people found that all these machines (i.e. computers) can communicate with each other to realize a bigger goal than their individual. Now with Internet-of-things we are making our universe so small that we feel not only connected to everything that we own all the time but also able to control them remotely. Some of these Things (or devices) are so smart that they even don't need human control.

Devices (or Things) in Internet-of-things is basically an embedded system with specific hardware components for dedicated purpose, which is uniquely identifiable over the global Internet (usually with the assignment of an IP address), and is capable of sensing it's environment, collect some kind of text or numeric raw data from the environment, send it to the cloud-based server for processing with wired or wireless communication technology and based on the information and knowledge received from server reply can respond or act on it's environment.

The term Internet-of-things was coined more than a decade ago and some of the industry and research communities have come up with a number of revolutionary products as a contribution to Internet-of-things.

Almost every device in Internet-of-Things environment follows a common pattern, where every device has to sense the environment and collect raw data in terms of numeric and number format which will be digitized using Analog-to-Digital converter. This digital data is transferred to either a cloud-based server and/or shared with the neighboring devices.

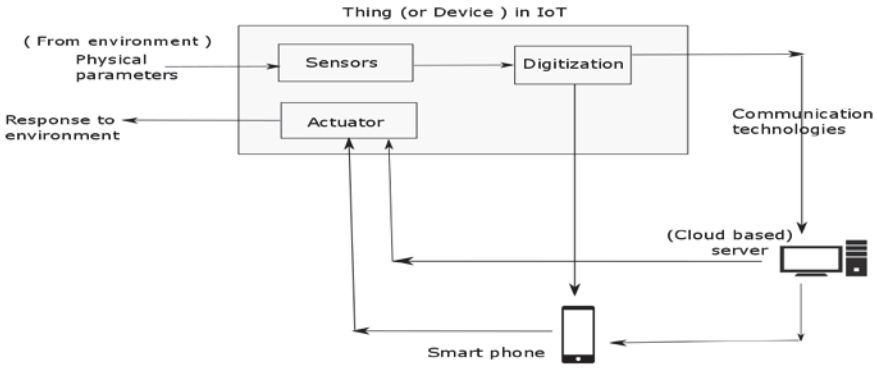

Fig. 1 Internet-of-Things at a glance

B. Elements of Internet-of-Things

A device in Internet-of-Things typical has I/O interfaces for sensors and actuators, audio/video interfaces, a processing unit, memory interfaces and several interfaces for connections to other devices (to gateway) and sometimes a GPU.

1) Sensors

Things (or devices) in Internet-of-Things have sensor which are capable of sensing their environment and collect data. Since the processing of this data will be done on cloud based server, typically the sensor collected data will not be stored on the device for long duration. This data will be transferred to the servers using wireless communication technologies. The sensors mainly used to sense temperature, humidity, fire/smoke, harmful gases, pressure, Volatile Organic Compounds (VOCs), dust, sound levels, light intensity, voltage, power, current, digital input/output, proximity(distance) etc.

2) Actuators

Actuators are the components which are responsible for acting on the environment. In some sense, we can say that actuators complete the loop of Internet-of-Things i.e. Collection of raw data (by sensors), transferring this data to either smart phone or cloud-based server (for processing, generating knowledge, and representing in required format) and responding to the environment (or taking some action) based on inputs from smart phone (i.e. user) or server. If a temperature sensor detects temperature at an office/room above a certain degrees, then the actuators may be informed to turn on AC or when the CO2 level in a room raises above a threshold level an exhaust will be turned on using actuator.

3) RFID

Radio frequency Identification (RFID) has evolved as a great contribution to applications based on Internet-of-Things. RFID is a kind of wireless communication and data collection technology which uses radio frequency to transfer data between RFID reader and an RFID tag attached to a movable (mobile) item with a purpose of identification, tracking or categorizing. The RFID tag represents a simple chip or label attached to provide object's identity. The RFID reader transmits a query signal to the tag and receives reflected signal from the tag, which in turn is passed to the database [1]. The range for identification of items by a RFID reader varies from few centimeters to several meters. RFID tags are cheap in cost and require little power. RFID technology has been successfully used in areas like inventory management, asset tracking, transportation industry, health care industry. RFID is the first technology used to realize the M2M concept (RFID tag and reader)[1].

4) Gateways

A gateway in Internet-of-Things is not just responsible for forwarding packets from local network to cloud-based server. It has to process the packets received from sensors before forwarding to data centers or cloud-based server. Such processing can be filtering of messages or avoiding forwarding redundant data to server. As an example, consider that a temperature sensor sends data packets to a local gateway. The gateway should be intelligent enough to decide that until there is variation in temperature value no packet should be forwarded to server for processing as it may create unnecessary traffic and also redundant processing on server. As it is easy to access a single gateway than a number of sensor nodes, a gateway should be the single point of monitoring the system.

5) Cloud based servers

The Internet-of-Things include cloud-based server as the core component. As the devices are typically small embedded systems which have limited processing capabilities and are power constrained, we can't perform the data processing, analysis, representation of data and generation of report on these devices. We collect the sensor data at local gateways and simply forward the packets to cloud-based server (or data centers) which have high storage capacities and are capable of processing stream data. These servers are available free of charge for almost all practical purposes. Some of these cloud platforms will be discussed in this paper.

II. COMMUNICATION TECHNOLOGY IN INTERNET-OF-THINGS

We have wired and wireless communication technologies available for connecting IoT devices to local gateway and local gateways to data centers or cloud based servers. Now a days ad hoc and wireless sensors networks are also widely used for IoT based applications. Some of the popular home automation technologies include X10, Z-Wave, Zigbee, INSTEON, EnOcean [4].

We are giving a short introduction about some of the short range communication technologies which are used between local gateways and sensors and wide range communication technologies which are mainly used for connecting to Internet i.e. sending gateway collected data to server for processing.

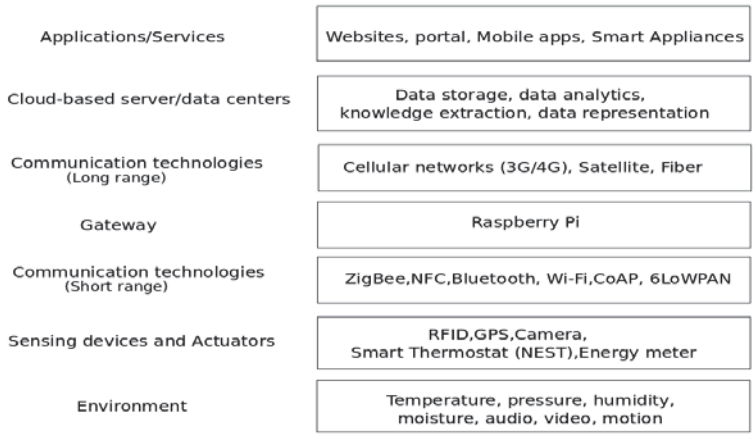

Fig. 2 Internet-of-Things Architecture

A. Local (Short range) Communication

1. Zigbee

Zigbee is one of the most widely utilized Wireless Sensor Network standards with low power, low data rate, low cost and short time delay characteristics, simple to develop and deploy and provides robust security and high data reliability [16]. Zigbee is the most widely used protocol for smart home applications.

2. Bluetooth LE

Bluetooth low energy (LE) (also called Bluetooth Smart or Version 4.0+ of the Bluetooth specification) is the power- and application-friendly version of Bluetooth that was built for the Internet of Things (IoT). The power-efficiency of Bluetooth with low energy functionality makes it perfect for devices that run for long periods on power sources such as coin cell batteries or energy-harvesting devices. The smart part is the native support for Bluetooth technology on every major operating system, for easy mobile application development and connectivity for cloud computing and the social economy [15].

3. Z-Wave

The Z-Wave protocol is an interoperable, wireless, RF-based communications technology designed specifically for control, monitoring and status reading applications in residential and light commercial environments. Mature, proven and broadly deployed (with over 50 million products sold worldwide), Z-Wave is by far the world market leader in wireless control, bringing affordable, reliable and easy-to-use 'smart' products to many millions of people in every aspect of daily life [14].

4. Wi-Fi

With industry momentum mounting around a low power Wi-Fi® solution, Wi-Fi Alliance® has introduced Wi-Fi HaLow™ as the designation for products incorporating IEEE 802.11ah technology. Wi-Fi HaLow operates in frequency bands below one gigahertz, offering longer range, lower power connectivity to Wi-Fi CERTIFIED™ products. Wi-Fi HaLow will enable a variety of new power-efficient use cases in the Smart Home, connected car, and digital healthcare, as well as industrial, retail, agriculture, and Smart City environments [13].

5. RFID

A radio-frequency identification system uses tags, or labels attached to the objects to be identified. Two-way radio transmitter-receivers called interrogators or readers send a signal to the tag and read its response. The readers generally transmit their observations to a computer system running RFID software or RFID middle ware. RFID technology works in the range between 10cm to 200m. RFID tags can be either passive, active or battery assisted passive. An active tag has an on-board battery and periodically transmits its ID signal. A battery assisted passive (BAP) has a small battery on board and is activated when in the presence of a RFID reader [5].

6. NFC

NFC is a set of short-range wireless technologies, typically requiring a distance of 10 cm or less. NFC always involves an initiator and a target; the initiator actively generates an RF field that can power a passive target. This enables NFC targets to take very simple form factors such as tags, stickers, key fobs, or cards that do not require batteries. NFC peer-to-peer communication is possible, provided both devices are powered [5].

7. UWB

Ultra-Wideband technology (UWB) uses an extremely wide band radio frequency spectrum to transmit data, which in turn helps to transmit more data in a given period of time. UWB technology has been implemented in a wide variety of applications in WPAN. UWB can currently transmit data at speed between 40 to 60 megabits per second and up to 1 gigabit per second.

8. IEEE 802.3 - Ethernet

IEEE 802.3 is a collection of wired Ethernet standards that provides data rates from 10 Mb/s to 40Gb/s and higher. The shared medium in these standards can be a coaxial cable, twisted-pair wire or an optical fiber. It's cheap and easy to install. This advantage makes it the most widely used data communications standards which find major use in LAN applications. With versions including 10Base-T, 100Base-T and now Gigabit Ethernet, it offers a wide variety of choices of speeds and capability.

9. 6LoWPAN

IPv6 over Low power Wireless Personal Area Network (6LoWPAN) is the first and most commonly used standard in this category. It efficiently encapsulates IPv6 long headers in IEEE802.15.4 small packets, which cannot exceed 128 bytes [10]. 6LoWPAN removes a lot of IPv6 overheads in such a way that a small IPv6 datagram can be sent over a single IEEE 802.15.4 hop in the best case. It can also compress IPv6 headers to two bytes [1].

10. LoRaWAN [17]

LoRaWAN is designed to provide Low Power Wide Area Network with features specifically needed to support low-cost, mobile, secure bi-directional communication for Internet of Things (IoT), machine-to-machine (M2M), and smart city, and industrial applications. It is optimized for low power consumption and to support large networks with millions and millions of devices. It has innovative features, support redundant operation; location, low-cost, low-power and can even run on energy harvesting technologies enabling the mobility and ease of use to Internet of Things.

11. VSCP [18]

VSCP stands for Very Simple Control Protocol. VSCP is a highly scalable, a very low footprint, a free and open solution for Device discovery and identification, Device configuration, Autonomous device functionality, secure update of device firmware, and a solution from sensor to UI.

B. Wide Area Communication

1. Cellular Network

Cellular mobile network include different generation of mobile communication standards such as 2G (i.e. second generation GSM and CDMA technologies), 3G (i.e. third generation UMTS and CDMA2000) and also 4G (i.e. fourth generation LTE and LTE-A). Devices in Internet-of-Things which are based on these standards can communicate over cellular network with a data rate ranging from 9.6Kb/s (for 2G) to up to 100Mb/s(for 4G) [11].

2. Sigfox

SigFox wireless systems send very small amounts of data (12 bytes) very slowly (300 baud) using standard radio transmission methods (phase-shift keying – DBPSK – going up and frequency-shift keying – GFSK – coming down)

[19]. Specifically, SigFox sets up antennas on towers (like a cell phone company), and receives data transmissions from devices like parking sensors or water meters [19].

3. Satellite

Satellite Communication has served mankind in many ways e.g. to predict weather, storm warning, provide wide range of communication services in the field of relaying television programs, digital data for a multitudes of business services and most recent in telephony and mobile communication. It may not surprise world community, if satellite communication links may be used for voice and fax transmission to Aircraft on International routes in near future. GPS Navigation, Global telephony, Multimedia video and internet connectivity, Earth Imaging through Remote sensing satellites for resource monitoring, Tele-medicine, Tele-education services etc. are other feathers in Satellite communication applications [20].

4. LTE and LTE-A

Long Term Evolution is the next-generation 4G technology for both Global System for Mobile communication (GSM) and Code Division Multiple Access (CDMA) cellular carriers. LTE works with download speeds of up to 173 Mb/sec [21].

LTE-A (i.e. Long Term Evolution - Advanced) encompasses a set of cellular communication protocols that fits well for Machine-Type Communications (MTC) and IoT infrastructures especially for smart cities where long term durability of infrastructure is expected [1].

5. Wi-Max

WiMAX (Worldwide Interoperability for Microwave Access) is a connection-oriented wide area network. It supports high bandwidth and hundreds of users per channel at speeds similar to currently seen for DSL, Cable or a T1 connection; Promises to provide a range of 30 miles as an alternative to wired broadband like cable and DSL. It could potentially provide broadband access to remote places. Use point-to-multipoint (P2MP) architecture. It is designed for delivering broadband seamless quality multimedia services to the end users [22].

III. PROTOCOL STACK FOR INTERNET-OF-THINGS

There are four different architecture (protocol stack) described in [1]. While trying to map the working model of Internet-of-Things in to a protocol stack, we come to a conclusion that the six layer model as shown in Fig. 3 fits most appropriately in Internet-of-Things.

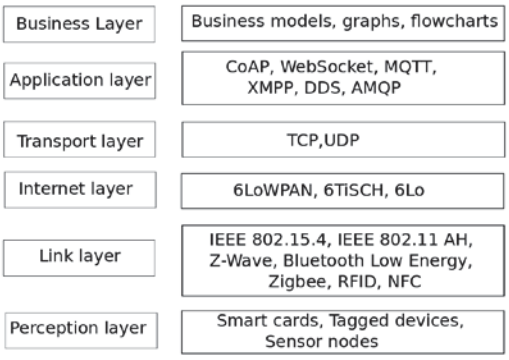

Fig. 3 Internet-of-Things Protocol Stack

The Perception layer represents the actual sensing devices of Internet-of-Things which collect data. Typically these devices sense location, temperature, weight, motion, vibration, acceleration, humidity, pressure etc. Also the items, devices like smart phone or vehicles which are tagged to be tracked or identified by NFC or RFID sensors fall under this layer. The sensors in this layer basically form the back bone for entire Internet-of-Things.

The link layer that lies just above perception layer is a collection of wired and/or wireless communication technologies that transfers the sensor collected data to gateways, data center or cloud based servers. Most of these technologies are specially designed for power constrained devices. IEEE 802.15.4 offers physical and media access control layers for low-cost, low-speed, low-power wireless personal area networks (WPANs) and is widely used in application like home networking, automotive networks, industrial networks, and remote metering [12].

At the Internet layer there are protocols such as 6LoWPAN, 6TiSCH and 6Lo, which are a light weight version of IPv6. IPv6 over Low power Wireless Personal Area Network (6LoWPAN) is the first and most commonly used

standard in this category. It efficiently encapsulates IPv6 long headers in IEEE802.15.4 small packets, which cannot exceed 128 bytes [10].

6TiSCH working group in IETF is developing standards to allow IPv6 to pass through Time-Slotted Channel Hopping (TSCH) mode of IEEE 802.15.4e data links. It defines a Channel Distribution usage matrix consisting of available frequencies in columns and time-slots available for network scheduling operations in rows [10].

IPv6 over Networks of Resource-constrained Nodes (6Lo) working group in IETF is developing a set of standards on transmission of IPv6 frames on various datelines. Although, 6LowPAN and 6TiSCH, which cover IEEE 802.15.4 and IEEE 802.15.4e, were developed by different working groups, it became clear that there are many more data links to be covered and so 6Lo working group was formed [10].

The transport layer in the protocol stack for Internet-of-Things has two main protocols namely TCP (Transmission Control Protocol) and UDP (User datagram Protocol). As the Internet-of-Things system finds no necessity in establishing connection with the other nodes and also the transfer of data requires to be faster, typical the connection-oriented protocol like TCP is not preferred. So, UDP is mostly the choice of application layer protocols i.e. most of the application layer protocols are implemented on top of UDP instead of TCP.

We have a number of choices for application layer protocol based on the system requirements. The reason for developing Internet-of-Things system can be messaging application, real time data collection and representation or a business analysis application. Some of the application layer protocols are CoAP, MQTT, WebSocket, XMPP, DDS, and AMQP.

CoAP (Constrained Application Protocol) defines a web transfer protocol. It is based on REpresentational State Transfer (REST) on top of HTTP functionalities. CoAP is bound to UDP by default which makes it more suitable for the IoT applications.

MQTT (Message Queue Telemetry Transport) is a messaging protocol, suitable for resource constrained devices that uses unreliable or low bandwidth links. As MQTT is able to provide routing for small, cheap, low power and low memory devices in vulnerable and low bandwidth networks, it is an ideal messaging protocol for the IoT and M2M communications. MQTT is applied in various applications including health care, monitoring, energy meter and Facebook notifications.

WebSocket protocol allows full-duplex communication over a single socket connection for sending messages between client (a browser, a mobile application or an IoT device) and server[11]. It is based on TCP and allows stream of messages to be sent back and forth between the client and server while keeping TCP connection open [11].

XMPP (Extensible Messaging and Presence Protocol) is an instant messaging standard used for multi-party chatting, voice and video calling and tele-presence [1]. XMPP allows users to communicate with each other by sending instant messages on the Internet no matter which operating system they are using. XMPP allows IM applications to achieve authentication, access control, privacy measurement, hop-by-hop and end-to-end encryption, and compatibility with other protocols [1].

DDS (Data Distribution Service) is a data-centric middleware standard for device-to-device or machine-to-machine communication. It uses a publish-subscribe protocol for real time M2M communication.

AMQP (Advanced Message Queuing Protocol) is a protocol mainly used for business messaging. It supports bot point-to-point and publish-subscribe protocol along with routing and queuing.

IV. SECURITY AND PRIVACY ISSUES

The application areas of Internet-of-Things are growing very rapidly due to interests from academicians and industry people around the world. But at the same time there are certain privacy and security concerns that must be handled very seriously. The privacy threats are categorized into seven categories in [24]. Identification, tracking and profiling are among the long known threats that will be greatly aggravated in the IoT. The remaining four threats of privacy include violating interactions and presentations, life cycle transitions, inventory attacks and information linkage. The threat that arises due to associating an identifier with an individual and his personal data is termed as identification threat. The use of GPS, cell phone tracking or internet traffic in order to determine and record an individual's location is referred as localization and tracking. The act of accessing information about individuals from various internet sources and use it for correlating with others profiles and data is the profiling threat. Privacy-violating interaction and presentation threat arises when an IoT application collects an individual's private information and transfers through a public medium (like Internet) and in turn discloses it to an unwanted audience. Privacy violations from life cycle transitions are mainly due to the collected and stored information. The act of collecting unauthorized information about the existence and characteristics of personal things has been termed as inventory attack. Linkage threat consists in linking different previously separated systems such that the combination of data sources reveals (truthful or erroneous) information that the subject did not disclose to the previously isolated sources and, most importantly, also did not want to reveal.

Some of the privacy and security are well discussed in [23] like attacks on secrecy and authentication, silent attacks on service integrity and attacks on availability of network. The attack on availability of network also called as denial of service (DoS) attacks can occur at all layers of IoT protocol stack. Jamming and node tampering are the attacks at physical layer. The DoS attacks taking place link layer are collision, unfairness and battery exhaustion. Spoofing, replaying and misdirection of traffic, hello flood attack, homing, selective forwarding, Sybil, wormhole, acknowledgment flooding are the examples of DoS attack in network layer. The DoS attack in transport layer includes flooding and de-synchronization.

V. OPEN SOURCE TOOLS FOR INTERNET-OF-THINGS

There are a number of cloud based web application which provide the resources, API and interfaces necessary to realize the IoT projects. At the initial phase in developing IoT solutions, it is always better to follow existing projects and extend them for solving new problems. The tools help the newbie to get the feel of IoT in reality. Some of them are listed below.

A. Thingspeak [25]

ThingSpeak Features include real-time data collection and storage, MATLAB analytics and visualizations, Alerts, Scheduling, Device communication, Open API, Geolocation data and Data collection server code available on GitHub. It works With Arduino, Particle Photon and Core, Raspberry Pi, Electric Imp, Mobile and web apps, Twitter, Twilio and MATLAB.

B. Sparkfun [7]

It is a free, robust service for use with all of your IoT projects. It allows creating a free data stream, exploring all of the public data streams on their server and configuring and deploying your own copy of the phant server.

C. DeviceHive [26]

DeviceHive is an open source IoT data platform with a wide range of device integration options. It works in public and private clouds like Microsoft Azure, Amazon Web Services, Apache Mesos, OpenStack or a private datacenter. It also provides big data solutions such as ElasticSearch, Apache Spark, Cassandra and Kafka for real-time and batch processing.

D. Sitewhere [6]

SiteWhere is an open source IoT platform. It provides a system that facilitates the ingestion, storage, processing, and integration of device data. SiteWhere provides the functionality like IoT server platform, device management and integration. The open source components used by SiteWhere include Apache Tomcat 7, Spring framework, Spring security, Hazelcast. Also MongoDB, Apache HBase, InfluxDB are the data storage technologies used at SiteWhere.

E. Kaaproject [8]

Kaa is a production-ready, multi-purpose middleware platform for building complete end-to-end IoT solutions, connected applications, and smart products. The Kaa platform provides an open, feature-rich toolkit for the IoT product development and thus dramatically reduces associated cost, risks, and time-to-market. For a quick start, Kaa offers a set of out-of-the-box enterprise-grade IoT features that can be easily plugged in and used to implement a large majority of the IoT use cases.

VI. INTERNET-OF-THINGS ENABLING TECHNOLOGIES

Internet-of-Things is basically a combination of various fields in electronics and computer science stream which includes wireless sensor networks, cloud computing, big data analytics and embedded system among others.

A. Wireless Sensor Networks

A typical wireless sensor network consists of a number of distributed sensor devices and routers for monitoring and sensing the environmental and physical conditions. WSN forms self-organizing networks and uses wireless communication protocols such as ZigBee. WSN are immensely used in weather monitoring systems, indoor air quality monitoring systems, surveillance systems, smart grids and structural health monitoring systems.

B. Cloud Computing

This technology has given a new dimension in solving IoT problems. Cloud computing basically provides solutions for delivering applications and services over Internet. It follows a very simple “pay as you use” model. The multi-tenant architecture of cloud computing allows multiple users to be served by the same physical infrastructure or

hardware. The services of cloud computing are available under different umbrella such as Infrastructure-as-a-Service (IaaS), Platform-as-a-Service (PaaS), Software-as-a-Service (SaaS).

C. Big Data Analytics

In the Internet-0of-Things enormous amount of data is generated which becomes difficult to store, manage, process and analyze using traditional relational; data processing tools. Big data analytics is the solution to such a huge data. With the big data analytics tools like Hadoop, Cloudera, MangoDB, Talend the data at cloud based server can be processed in real time to fetch knowledge, take decisions, data representation and many more.

D. Embedded Systems

An embedded system is a special purpose computer system having limited hardware and software (typically pre-installed) to perform a specific task. The major components on the embedded systems include a microprocessor or a micro-controller chip, RAM, ROM, cache, networking interfaces, input/output interfaces and storage. Embedded systems mainly run a dedicated RTOS (Real Time Operating System).

VII. RESEARCH DIRECTIONS, CHALLENGES AND OPPORTUNITIES IN INTERNET-OF -THINGS

When it comes to research in Internet-of-Things, there are enormous opportunities. If we closely look in to Internet-of-Things ecosystem, we see that from a top level of business analytics (layer that lies above application layer in Fig. 3) which include areas like big data analytics and cloud computing to the perception layer (bottom layer in Fig. 3) which can have wireless sensor network, RFID as its core components, we can explore any single area. There are issues like standardization of technologies in Internet-of-Things, standardization of LWC (Light-weight Cryptography) and many more which still have scope to carry the present work forward. Also, various security and privacy issues discussed earlier can be a great challenge to work up on.

Since we have a vast number of applications available with us in present time, Internet-of-Things can't be called as the technology of future. We need to identify some problems in the world surrounding us and at the same time apply the knowledge of Internet-of-Things to solve those problems. There are miles to travel with the evolving technology solutions, so the research has a great scope in Internet-of-Things.

VIII. CONCLUSION

In this paper we have tried to address all the issues related to Internet-of-Things. The paper will act as an introduction to new researchers who try to explore the field in order to build solutions for society. We have given theoretical and practical overview on this field in terms of explaining the working of an IOT application, the protocol stack used for implementing these solutions, various communication technologies required. The security and privacy issues in the IoT creates a bottleneck in applying IoT to fulfill its goal of connecting everything to everything but at the same time gives a new opportunity for researchers and industry people. We also gave a small introduction to open source tools for IoT development, IoT enabling technologies and research opportunities in IoT.

REFERENCES

[1] Ala Al-Fuqaha, Mohsen Guizani, Mehdi Mohammadi, Mohammed Aledhari and Moussa Ayyash, *Internet of Things : A Survey on Enabling Technologies, Protocols and Applications*, IEEE Communication Surveys and Tutorials, Vol-17, No. 4, Fourth Quarter 2015

[2] Vangelis Gazis et. al., *A Survey of Technologies for the Internet-of-Things*, 2015 International Wireless Communications and Mobile Computing Conference (IWCMC), page 1090-1095, 24-28 August 2015.

[3] Charith Perera, Chi Harold Liu and Srimal Jayawardena, *The Emerging Internet of Things marketplace From an Industrial Perspective: A Survey*, IEEE transactions on Emerging Topics in Computing 2015.

[4] Jaewoo Kim, Jaiyong Lee, Jaeho Kim, and Jaeseok Yun, *M2M Service Platforms: Survey, Issues, and Enabling Technologies*, IEEE Communications Surveys & Tutorials, Vol. 16, No. 1, First Quarter 2014

[5] http://postscapes.com/internet-of-things-technologies#communication

[6] http://www.sitewhere.org/

[7] https://data.sparkfun.com/

[8] http://www.kaaproject.org/

[9] http://postscapes.com/what-exactly-is-the-internet-of-things-infographic/

[10] http://www.cse.wustl.edu/~jain/cse570-15/ftp/iot_prot/

[11] Arshdeep Bahga, Vijay Madisetti, *Internet of Things A Hands on Approach*, University Press (India) Private Limited 2015.

[12] https://www.utwente.nl/ewi/dacs/colloquium/archive/2010/slides/2010-utwente-6lowpan-rpl-coap.pdf

[13] http://www.wi-fi.org/discover-wi-fi/wi-fi-halow

[14] http://z-wavealliance.org/about_z-wave_technology/

[15] https://www.bluetooth.com/what-is-bluetooth-technology/bluetooth-technology-basics/low-energy

[16] Muthu Ramya C, Shanmugaraj M, Prabhakaran R, *Study of ZigBee Technology*, 3rd International Conference on Electronics Computer Technology (ICECT), 8-10 April 2011, (Volume:6)

[17] https://www.lora-alliance.org/For-Developers/LoRaWANDevelopers

[18] http://www.vscp.org/
[19] http://www.link-labs.com/what-is-sigfox/
[20] Dipak Misra, Dinesh Kumar Misra, S. P.Tripathi, *Satellite Communication Advancement, Issues, Challenges and Applications*, International Journal of Advanced Research in Computer and Communication Engineering Vol. 2, Issue 4, April 2013
[21] Shihab Jimaa, Kok Keong Chai, Yue Chen, Yasir Alfadhl , *LTE-A an Overview and Future Research Areas*, Second International Workshop on the Performance Enhancements in MIMO-OFDM Systems, 10-12 Oct. 2011
[22] Mojtaba Seyedzadegan and Mohamed Othman, *IEEE 802.16: WiMAX Overview, WiMAX Architecture*, International Journal of Computer Theory and Engineering, Vol. 5, No. 5, October 2013
[23] http://arxiv.org/abs/1501.02211
[24] Jan Henrik Ziegeldorf, Oscar Garcia Morchon, and Klaus Wehrle, *Privacy in the Internet of Things: Threats and Challenges*, Special Issue Paper, Security and Communication Networks 2013
[25] https://thingspeak.com/
[26] http://devicehive.com/#