IJARCCE

ISSN (Online) 2278-1021
ISSN (Print) 2319 5940

International Journal of Advanced Research in Computer and Communication Engineering
ISO 3297:2007 Certified
Vol. 5, Issue 7, July 2016

A review on the state of art of Internet of Things

T. Santhi Sri[1], J. Rajendra Prasad[2], Y. Vijayalakshmi[3]

Sr. Asst. Prof, Computer Applications, PVP Siddhartha Institute of Technology, Vijayawada, India[1]

Professor & Head, Information Technology, Siddhartha Institute of Technology, Vijayawada, India[2]

Assistant Professor, Computer Applications, PVP Siddhartha Institute of Technology, Vijayawada, India[3]

Abstract: The Internet of Things is fast growing technology with business opportunities and risks. It is confluence of wireless networks, internet and computing. IoT connects the physical objects like vehicles, buildings and other devices with embedded intelligent sensors and enables these objects to exchange and collect data. The domains where IoT is becoming popular are smart cities, e-health, smart grids, e-commerce, smart transportation, and e-commerce etc. The embedded and wearable computing will have greater impact in providing services in wide range of applications by 2020[1]. The architecture of IoT is incorporated with the latest technologies of communication protocols, intelligent sensor and RFID. The security and privacy issues of IoT are crucial as it connects large number devices. In this article we analyze a state of art review of IoT with regard to technologies, protocols, application issues.

Keywords: Internet of Things (IoT), IoT protocols, IoT, architecture, IoT applications

I. INTRODUCTION

Internet of Things (IoT) was proposed by Kevin Ashton, co-founder of AutoID. Internet of Things (IoT) is one of the major disruptive technological developments in recent years and can be considered as next era in the IT sector which would take the field of technology to new heights. IoT helps to communicate between people to people, people to physical objects and physical objects to other physical objects as shown in Fig. 1[4].

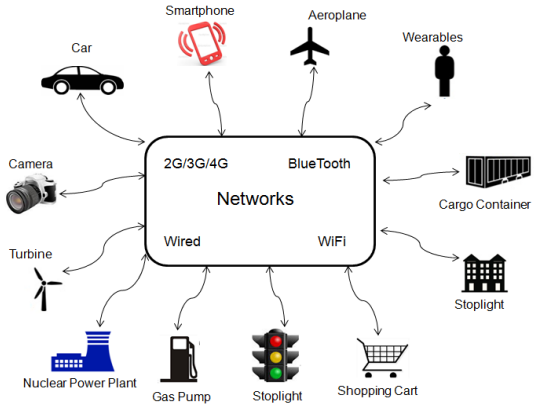

Fig. 1 IOT Scenario

II. ARCHITECTURE

In the perception of IoT, a large number of inexpensive, small devices surround us. Multiple connectivity options are required to connect them to internet. Connectivity also requires interoperability between different kinds of information. The architecture of IoT must be open, scalable, layered, to support heterogeneous future applications. IoT architecture consists of four layers viz. perception layer, network layer, middle ware layer and application layer Fig. 2[5].

Perception layer can be described as sensing layer. This layer resembles the physical layer of OST model. Acquiring Information from physical world is responsibility of perception layer. Sensing and recognition technologies can be used to acquire information.

Sensors are used to acquire information. Wireless sensor networks are deployed to collect, analyze, process required information. Sensors such as sound sensors, smoke sensors, vibration sensors etc., are available to collect information. Identification of physical world objects is done through recognition technology. RFID tags can be used to identify the objects. The other technologies used are bar codes and two dimensional codes.

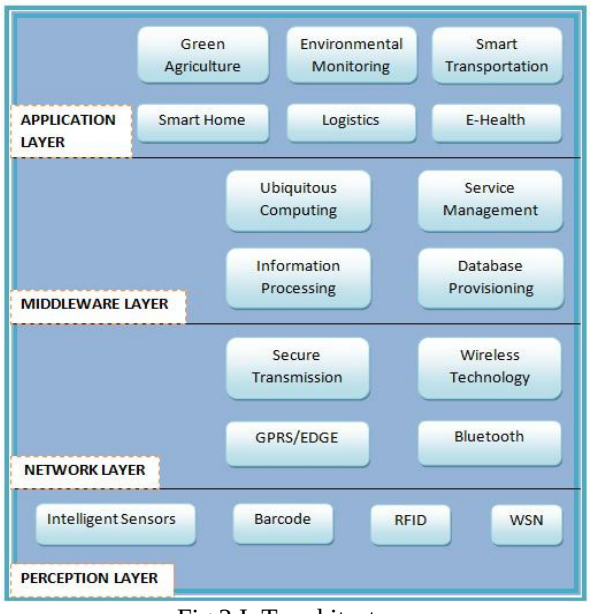

Fig.2 IoT architecture

IJARCCE

ISSN (Online) 2278-1021
ISSN (Print) 2319 5940

International Journal of Advanced Research in Computer and Communication Engineering
ISO 3297:2007 Certified
Vol. 5, Issue 7, July 2016

The information collected at perception layer is of the form: pH level, humidity, location, vibration etc. The sensed information is communicated through network to reach the information processing system. IoT technology mainly includes sensors and telecommunication networks. Sensor network acts as peripheral network which mainly uses short distance communication technologies. The technologies used in sensor networks are Zigbee, Bluetooth, RFID, Infrared light communication technology [6] etc. Telecommunication network acts as core host network which communicates between sensor and transmission network such as Wi-Fi, WiMAX technologies and with core telecommunication network such as 2G, 3G, 4G etc. An addressing schemes like IPV6 to uniquely identify network devices is crucial [8]. For transferring data across the network, secure data aggregation method is required [7]. Middleware layer abstracts between application and network layers. This layer provides services to customers along with storing lower layer information in database. As IoT generates huge volumes of data and concentrates providing information to user data storage and analytics, visualization techniques gained importance [9].The topmost layer which is application layer in the IoT architecture includes application management which is based on the information gained from middleware layer. The applications can be in various fields such as smart post, healthcare, media, smart car agriculture, smart home, logistics, smart business, mobile, utilities, smart transportation, environmental monitoring etc.

III. PROTOCOLS

Protocol is a set of rules and regulations used for communication in same or different networks. The protocols like HTTP and TCP/IP cannot be used for IoT due to the existence of smart devices and other constraints. For machine to machine communication, the protocols MQTT (Message Queue Telemetry Transport) and CoAP (Constraint Application Protocol) are used [10]. MQTT protocol includes the features of publish/subscribe message pattern, messaging transport .CoAP is a web transfer protocol for constrained nodes and constrained networks. Typical web architecture of IoT can be shown in Fig.3 [12].

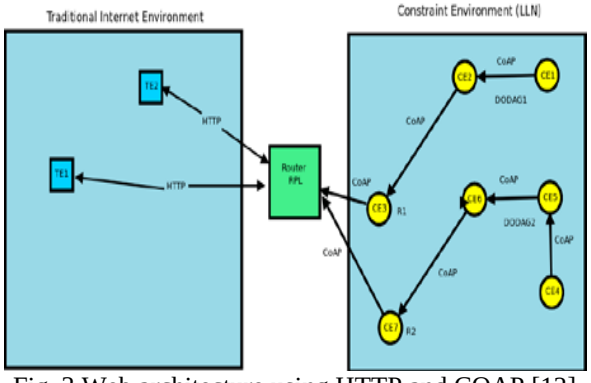

Fig. 3 Web architecture using HTTP and COAP [12]

For the web architecture mentioned above a protocol stack with existing protocols can be designed as shown in Fig.4 [12]. The protocol stack gives three categories. Category a) shows protocol stack for traditional environment (TE1, TE2). Category b) shows protocol stack for routing device. Category c) shows protocol stack for constrained environment (CE1 through CE2). As IoT consists of huge number of devices, the management of network becomes difficult.

To enable the proper network management the protocols like LNMP, SNMP protocols are used [11]. LNMP is LoW PAN network management 6LoWPAN networks, SNMP is Simple Network Management Protocol is a protocol used to control and manage IP network devices. SNMP can be used for various devices like routers, switches, workstations, servers, etc.

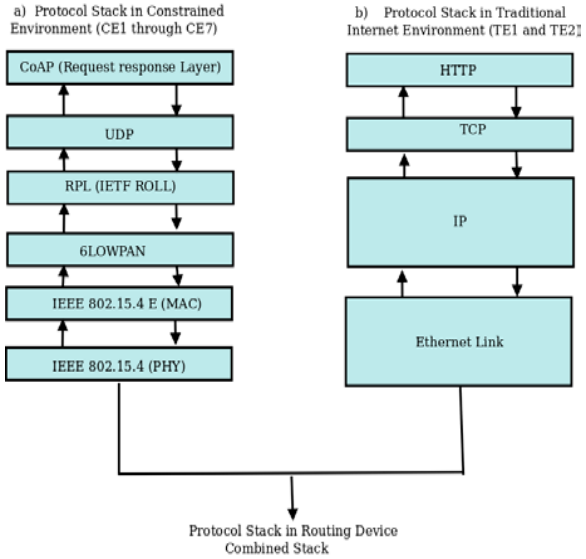

Fig.4 [12] protocol stack for web architecture in Fig.3

IV. DESIGN CHALLENGES

The development of IoT is the major revolution in IT sector. IoT will have greater impact on daily activities and life style. The design of IoT involves many issues from hardware components to software versions. Data storage, medium of deployment, interoperability, communication mechanisms, data fusion mechanisms, sensor energy, resource and service discovery, bootstrapping and setup security, authentication, access control and accounting, connectivity, mobility and scalability, etc. are some of the several design challenges that exists and need to be addressed. Some of these design challenges are discusses below. Data storage:

As IoT is being developed day by day large amounts of data is created. Space and power requirements are needed to handle data. While retrieving data from huge databases relevant data need to be extracted. Data organization, processing, retrieval will be a challenge in the process of proving it beneficial to business. Communication

DOI 10.17148/IJARCCE.2016.5738

IJARCCE

ISSN (Online) 2278-1021
ISSN (Print) 2319 5940

International Journal of Advanced Research in Computer and Communication Engineering
ISO 3297:2007 Certified
Vol. 5, Issue 7, July 2016

mechanisms: All the objects present in the IoT environment are called as 'things'. All these things need to be addressed uniquely. The standard protocol for this is Internet Protocol. The first version is IPV4 and in 2011 [13] the supply of IPV4 addresses was stopped by Internet Assigned Numbers Authority (lANA) as it was exhausted. The solution is deployment of IPV6. As IPV6 has the network auto-configuration capabilities and enhanced security features, the management of network will become less complex. SNMP protocol is adopted to work with IPV6 for network management. SNMP implementation for IPV6 is NET-SNMP [14]. Standardization and interoperability:

The IoT device manufacturers and vendors develop application based solutions resulting incompatible devices. The application areas like e-health, home, energy and industrial will have different architectures, mechanisms, sensors etc. if these vendors work according to standards, greater interoperability is possible. Standardization in terms of privacy, security, network architecture and IPV6 packet routing through heterogeneous networks [15] is required. These technical standards will be promoted with the creation of IoT-GSI Global Standards Initiative [16]. Sensor energy: For IoT, things will be the active participants in all aspects like business, information and other processes. To enable IoT for smart environments more focus is to be given on requirements of sensors. This can be implemented through large scale sensor networks. Giving continuous and reliable power to sensor nodes is major concern. To deploy IoT successfully [15] the power need to be supplied for prolonged period of time. Various technologies like solar cells, thermal generators, and rectification of radio signals need to be deployed to connect sensors located in remote and distant locations.
Identification and Naming:

IoT connects billions of things across the world, across the technologies, across various applications. Hence there is a need for unique identification and naming methods of these things and objects is needed. With the present technology of IoT the coordinator nodes allocate local addresses to peer devices. To provide common standard for this schemes like 6LoWPAN which enables each node to obtain unique IPV6 address need to be deployed. With the implementation of IPV6 the challenge of shortage of addresses can be solved [17].

V. SECURITY ISSUES

Security is the biggest issue of IoT industry. When data is transmitted through the internet, private networks, and VPNs security aspects are crucial. According to McKinsey, by 2020 ineffective cyber security cost will rise to $3 trillion [25]. When more number of devices are connected, security issues need to be addressed.

The data stored in IoT can be personal, home, industrial, enterprise, historical, healthcare, smart city, transportation, social, inventory and consumer. Due to the heterogeneity of IoT devices conventional security mechanisms does not directly suit IoT framework. The security constraints based on on hardware can be memory constraints, Computational and energy constraint, Tamper resistant packaging. Limitations of security based on software include, Embedded software constraint, Dynamic security patch. Based on network the security constrains are mobility, scalability, multiplicity of devices, multiplicity of communication medium, multli-protocol networking, and dynamic network topology [18].

The IoT security should be provided at physical objects level, while acquiring information and during information transmission and the requirements such as availability, confidentiality, integrity authentication and authorization, access control, exception handling, resiliency, self organization, anonymity, non-repudiation, freshness [17][18][19] need to be provided. Sensors are the important equipment in collecting information of IoT objects and sent for processing. They were generally deployed in the absence of monitoring system [24]. This sensed information can be attacked and programmed in such a way so that the information is sent to intruders. The possible threats to this sensed information can be eavesdropping, unauthorized access and denial of service attack.

Network in IoT also plays important role in transmission of information and quality of information. As large information is transmitted through network denial of service attacks exists in machine to machine communication. Sensed and transmitted data should be stored at back end for efficient analysis and management of data. This data needs to be provided with services like confidentiality, access control, integrity etc. Various security frameworks and protocols like IPSec [20], DTLS [21] [22], 6LoWPAN compression [23] have been proposed but they need to developed to suit IoT framework.

Objects in IoT should be protected from internal faults as well as external security breaches. Simply, embedded IoT devices must be provided with security. As and when a particular IoT device is successful it attracts more attackers. One framework of embedded IoT device is shown in product which is IoT enabled.Fig.5 [26].

VI. APPLICATIONS

The current hype is around IoT applications. Every other day a new company is announcing a new product. In near future the IoT filed will have enormous and rewarding growth in applications of domestic and commercial filed.

The applications of IoT are bases on various factors like bandwidth, coverage, utility level, scale of community, heterogeneity, real-time, non- real time requirements, domain, repetitive use and impact analysis.

IJARCCE

ISSN (Online) 2278-1021
ISSN (Print) 2319 5940

International Journal of Advanced Research in Computer and Communication Engineering
ISO 3297:2007 Certified
Vol. 5, Issue 7, July 2016

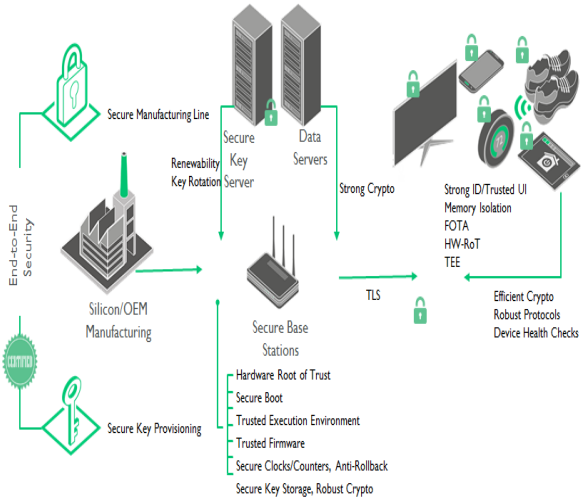

Fig. 5[26] security across the IoT devices

According to survey of IoT-I project [27], the loTs applications could be categorized into 14 domains which include Transportation, Smart home, Smart city, Lifestyle, Retail, Agriculture, Smart factory, Supply chain, Emergency, User Interaction, Healthcare, Culture and tourism, Environment and Energy. Other popular IoT applications include mobile, utilities, wearables, smart forming, connected car, smart postal, Smart Military, smart agriculture etc. Fig. 6[28] shows the top ten popular IoT applications right now. This study is according to a measurement by IoT ANALYTICS [28] based on Google, Twitter, LinkedIn. Out of ten IoT applications smart homes was given the highest ranking. The RFID, sensors and 6LowPan technologies can be used for sensing data and processing data in variety of applications. Singapore is one of the smart cities using IoT.

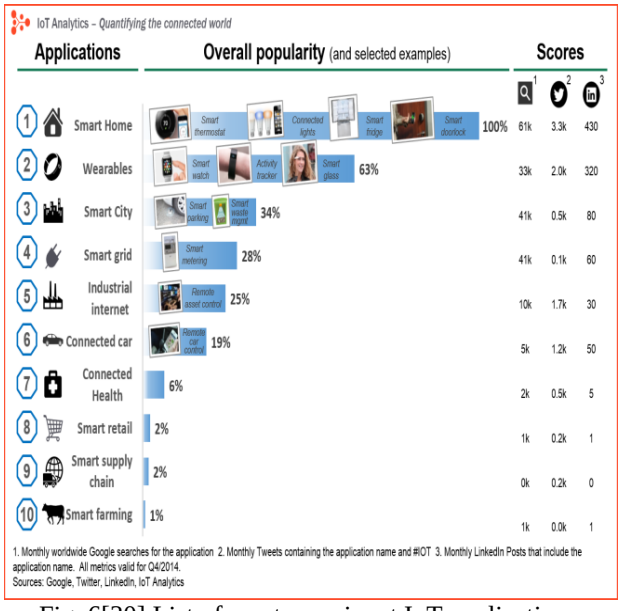

Fig. 6[30] List of most prominent IoT applications

Estimations show that by 2019 Singapore will become the smartest country in global.

VII. CONCLUSION

As a whole IoT changes the way we live. The deployment of IoT is under progress. As innovative and creative products will be designed and introduced every day, many challenges like Energy harvesting, power issues, wakeup delays, and identification of technology will come to the picture. These challenges have to be faced and solved carefully. In this paper we have analyzed the latest trends in IoT architecture, protocols for communication, design challenges, security issues, applications which have lot of scope to accommodate future development and with a view to give a clear view of IoT happenings.

REFERENCES

[1] Gartner Says a Thirty-Fold Increase in Internet-Connected Physical Devices by 2020 Will Significantly Alter How the Supply Chain Operates, http://www.gartner.com/newsroom/id/2688717.

[2] International Telecommunication Union, Internet Reports2005: The Internet of things. Geneva: ITU, 2005.

[3] Barnaghi, P., Wang, W., Henson, C., and Taylor, K., Semantics for the Internet of Things: Early Progress and Back to the Future, International Journal on Semantic Web and Information Systems, vol. 8, No. 1, 2012.

[4] Sachchidanand Singh, Nirmala Singh, Internet of Things(IoT): Security Challenges, Business Opportunities & Reference Architecture for E-commerce, IEEE International Conference on Green Computing and Internet of Things (ICGCIoT), 2015.

[5] Gurpreet Singh Matharu, Priyanka Upadhyay, Lalita Chaudhary, The Internet of Things: Challenges & Security Issues, IEEE International Conference on Emerging Trends(ICET), Islamabad, Pakisthan, 2014.

[6] Guinard D, Trifa V, Wilde E, Architecting a Mashable Open World Wide Web of Things (2010). USA: ETH, Department of Computer Science, 2009.

[7] Y. Sang, H. Shen, Y. Inoguchi, Y. Tan and N. Xiong, "Secure Data Aggregation in Wireless Sensor Networks: A Survey," 2006, pp. 315–320.

[8] M. Zorzi, A. Gluhak, S. Lange and A. Bassi, "From Today's Intranet of Things to a Future Internet of Things: A Wireless- and Mobility-Related View," IEEE Wireless Communications 17, 2010, pp. 43–51.

[9] J. Gubbi, R. Buyya, S. Marusic, and M. Palaniswami, "Internet of Things (IoT): A Vision, Architectural Elements, and Future Directions," Future Generation Computer Systems, vol. 29, no. 7, pp. 1645-1660, ISSN: 0167-739X, Elsevier Science, Amsterdam, the Netherlands, 2013.

[10] Surapon Kraijak, Panwit Tuwanut, A Survey on Internet of Things Architecture, Protocols, Possible Applications, Security, Privacy, Real-World Implementation and Future Trends, IEEE Proceedings of ICCT20 15.

[11] Hanane Lamaazi1, Nabil Benamar1, Antonio J. Jara2, Latif Ladid3 and Driss El Ouadghiri1, Challenges of the Internet of Things: IPv6 and Network Management, 2014 Eighth International Conference on Innovative Mobile and Internet Services in Ubiquitous Computing, DOI 10.1109/IMIS.2014.43.

[12] Suresh Kumar N., G. Santhosh Kumar, Internet of Things - A Communication Protocol Perspective, CSI Communications, February, 2016, Pg.No.11 to 13.

[13] Cisco, "How Can Service Providers Face IPv4?: A Review of Service Provider IPv4-IPv6 Coexistence Techniques," Cisco Internet Business Solutions Group (TBSG), Cisco Systems, Inc., San Jose, CA, USA, White Paper 2012. [Online]. http://www.cisco.comic/en/us/products/collateral/ios-nx-ossoftware/enterprise-ipv6-solution/whitepaper _c11-698132.pdf.

[14] ''La supervision des réseaux IPv6'' http://www.renater.fr/IMG/pdf/recommendations_supervision_IPv6.pdf.

ISSN (Online) 2278-1021
ISSN (Print) 2319 5940

International Journal of Advanced Research in Computer and Communication Engineering
ISO 3297:2007 Certified
Vol. 5, Issue 7, July 2016

[15] Dave Evans, "The Internet of Things: How the Next Evolution of the Internet Is Changing Everything," Cisco Internet Business Solutions Group (IBSG), Cisco Systems, Inc., San Jose, CA, USA, White Paper 2011. [Online]. http://www.cisco. com/web/about/ac79/docs/innovlIoT_IBSG_ 0411_ FINAL.pdf.
[16] "Internet of Things Global Standards Initiative" http://www.itu.int/en/ITU-T/gsi/iot/Pages/default.aspx.
[17] L. Li, "Study on Security Architecture in the Internet of Things," International Conference on Measurement, Information and Control (MIC), 2012, vol. 1, May 18-20, pp. 374-377.
[18] Md. Mahmud Hossain, Maziar Fotouhi, and Ragib Hasan, "Towards an Analysis of Security Issues, Challenges, and Open Problems in the Internet of Things", 2015 IEEE World Congress on Services, DOI 10.1109/SERVICES.2015.12.
[19] H. Suo, J. Wan, C. Zou, J. Liu., "Security in the Internet of Things: A Review", International Conference on Computer Science and Electronics Engineering (ICCSEE). 2012: 648-651.
[20] S. Raza, S. Duquennoy, T. Chung, T. Voigt, U. Roedig et al., "Securing communication in 6lowpan with compressed ipsec," in Distributed Computing in Sensor Systems and Workshops (DCOSS), 2011 International Conference on. IEEE, 2011, pp. 1–8.
[21] K. Hartke and O. Bergmann, "Datagram transport layer security in constrained environments", 2012.
[22] S. Raza, D. Trabalza, and T. Voigt, "6lowpan compressed dtls for coap," in Distributed Computing in Sensor Systems (DCOSS), 2012 IEEE 8th International Conference on. IEEE, 2012, pp. 287–289.
[23] S. Raza, D. Trabalza, and T. Voigt, "6lowpan compressed dtls for coap," in Distributed Computing in Sensor Systems (DCOSS), 2012 IEEE 8th International Conference on. IEEE, 2012, pp. 287–289.
[24] J. S. Kumar, D. R. Patel, "A Survey on Internet of Things: Security and Privacy Issues", International Journal of Computer Applications. 2014: 20-25.
[25] Mike Gault, CRUNCH NETWORK, "Rethinking security for the Internet of Things", Posted on May 6, 2016.
[26] Jenny Devoy, "securing embedded IoT word", https://iotsecurityfoundation.org/blog/, June 20th, 2016.
[27] O. Vermes an, P. Friess, A. Furness, "The Internet of Things 2012", By New Horizons, 2012. [Online], http://www.internet-of-things-research.eu/pdflIERC_Cluster_Book_2012_ EB.pdf.
[28] https://iot-analytics.com/10-internet-of-things-applications.

DOI 10.17148/IJARCCE.2016.5738