ISSN: 0971-1260
Vol-22-Issue-3-July-2019

Iot Architecture, Challenges and Future Directions – A Mirror Review

Umer Iqbal Wani[1], Mir Mohammad Yousuf[2], Mamoon Rashid[3]

[1, 2, 3]Assistant Professor, School of Computer Science &Engineering, Lovely Professional University, Jalandhar,India

Email for Correspondence: umerwani20@gmail.com

Abstract

IOT is anamalgam of different technologies like, smart sensors, RFID, Internet Protocols and communication technologies.IoT enables a network of wide variety of physical devices to exchange data. The number of IoT devices rouse to 31% totalling 8.4 billion in 2017 and by 2020 the number is estimated to reach 30 billion. Currently IoT is enabled by an improvement in Internet,machine-to-machine and mobile technologies. In the future, IOT is expected to support intelligent decision making by allowing a wide variety of physical objects to share data in an efficient and secure way. The paper starts with a general overview of IOT,after that IOT enabled technologies, protocols and applications is discussed.An elaborative summary of the most recent and upto-date protocols is discussed and issues to understand the protocol suite to deliver desired functionalities is also provided. Key IoT challenges and relevant research areas is also discussed.

Keywords: IoT Architecture, challenges, protocols, future.

INTRODUCTION TO IOT

With the emerging technology of IOT, physical devicesget added in abundance to the internet at a faster pace, e.g., HVAC (Ventilation, Heating, Air conditioning) systems that form main components of smart homes[1]. IoT based physical-objects share information and also coordinate decisions. IoT enabled objects are considered to be smart devices because of ubiquitous and pervasive nature of IoT enabled technology[2].

At the heart of IOT, many physical objects get connected to the internet .IoT isthe interconnection between physical world objects with the information generated in the virtual world. IOT enables physical objects identify and sense each other, to have network and computing capabilities that allows information sharing and different objective accomplishments.Finally, IOT allows physical objects to get connected anytime, anywhere, with anything and anyone using a number of paths/ networks and services[3].

In future, IoT will add to the wellness of life and will lead to a boost in world’s economy, IoT will impact a number of home and business applications. With the idea of smart homes, people will be getting inside the home without opening the garages, coffee will be prepared

ISSN: 0971-1260
Vol-22-Issue-3-July-2019

automatically, home appliances can be controlled remotely etc[4]. For achieving this, market demands need to be kept in check by emerging technologies and innovations and by the growth of service applications. In addition to this, devices should be modified catering to customer requirements (anywhere and anytime). New protocols have to be designed for compatibility of heterogeneous groups. Moreover, architecture needs to be standardized forIOT to enablecompetitive environment for manufacturing of quality -products.A revised internet architecture is also required, to keep ahead with the IoTchallenges[5].In 2010, it was seen that the number of interconnected physical objects was more than the human population, this means use of a vast addressing-space (e.g., IPv6) catering customers. Because of inherent heterogeneous behaviourof the collection of objects and the property of monitoring and controlling physical devices, security and privacy become other important requirements for the IoT[6]. For delivering high quality service at an efficient cost,monitoring as well as management of the IoT should be taken into consideration.

IOT ARCHITECTURE

A number of different architectures are proposed in a number of literatures, a 5 – layer model is the most discussedone[7][9]. A brief discussion of its 5 layers is provided in Figure 1.

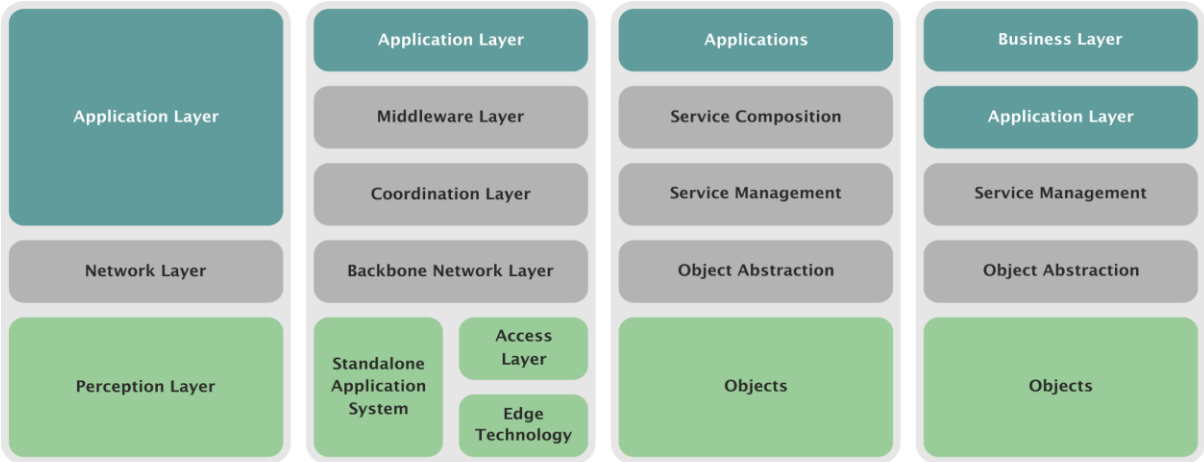

Figure 1. Five Layer IoT Architecture

(a) Objects layer(Perception layer or Recognition layer)

The layer comprises of devices that collect and process information. All the data collection occurs here[8]. Data from a number of devices(heterogeneous) is collected at this layer. Various sensing technologies used are: RFID, WSN, GPS,NFC etc. Perception layer transfersvarious data types collected from a number of devices into digital information[9]. Actuators and sensors are used for performing different

ISSN: 0971-1260
Vol-22-Issue-3-July-2019

functions such as location-querying, vibration,weight motion, temperature, humidity, acceleration, etc.

(b)Object Abstraction Layer

For processing purposes, data has to be transferred to the upper layers from the Objects layer. Object Abstraction Layer sendsdata via protected channels. The technologies used are RFID, GSM,3G, UMTS,Wi-Fi, ZigBee, etc. Data management processes and cloud computing processes are also handled here.

(c) Service Management Layer

The service-management layerfacilitates information processing, and decision-making[10].This layer is used byapplication programmers to deal with different objects of heterogeneous nature without taking into consideration a particular hardware platform.

(d) Application Layer

The application layer assures pre-request based high-quality facilitiesfor the customers,example - the application layer provides temperature as well as air-humidity data to the customersinterested[11].This layer ensuresbetter quality functions meeting customers' needs[12].

(e)Business Layer

The Business layer provides a model of the business and data that is received from the application layer. This layer deals with the entire IoT system activities, services. It also supports decision-based Big-Data analysis[13]. Apart from this, management related activities is achieved at this layer.

2.1.3:Characteristics of IOT

Following are the characteristics of IoT:

a. Interconnectivity: Interconnectivity in IoT means bringing together of various objects to share data. Connectivity of objects leads to creation of data in IoT, which forms the basis for analysis purposes[14]. Connectivity between objects is achieved by internet mostly, creating a common communication infrastructure for all the objects connected together. Interconnectivity in IoT enables devices across various platforms to share data using a common communication channel[15]. Devices in IoT can be connected using a number of different topologies such as P2P,Star, Mesh and Hybrid. The common types of protocols used are WiFi, Thread, ZigBee, Bluetooth, RFID and NFC.

ISSN: 0971-1260
Vol-22-Issue-3-July-2019

b. Heterogeneity: Devices used in IoT are heterogeneous. Different devices with different hardware platforms and different networks are used. Devices with different processing powers and storage capabilities, as well as completely different architecture can be part of IoT[16]. Heterogeneity is one of the essential features of IoT , which lead to its widespread use across different platforms and domains. Heterogeneity in IoT makes possible for a number of devices, based on different technologies, to interact with each other, without any compatibility issues among the devices.
c. Dynamic changes: Devices in IoT keep changing on their states, e.g., on and off state. Moreover devices in IoT keep changing their location as well as speed(An IoT enabled vehicle).The total number of devices in an IoT environment keeps on changing also,depending upon the need devices get added up and sometimes devices are also removed[17]. The use of a particular resource in a number of devices also changes dynamically, a device might be using a particular resource(say storage) more at one point of time and at some other point of time ,the same device can be using its other resource(say processor) more than other resources.
d. Enormous scale: An enormous number of devices are getting added to IoT at a larger scale ,day by day. Devices from different architectures and platforms add to the enormous structure of IoT[18]. The enormity of IoT can be conceptualized by a report in Gartner(2015) which states that 5.5 million devices will get added every day and 6.6. billion connected things will be in use worldwide by 2026 - 30 percent increase from 2015.The report also predicts that the number of connected devices will be 20.8 billion in 2020.The enormous scale feature of IoT makes data management in IoT very critical. With such an enormous data, the interpretation of data for application purposes is a big challenge. To differentiate between useful and vague data, in such a huge database, utmost care and use of sound methodologies have to be implemented[19].
e. Security: With a large number of things added to IoT, the vulnerabilities of data breach and various security issues are bound to arise. An attack in a single IoT device means breaching the security of a big network[20]. IoT devices are usually resource constrained and don't possess the compute power necessary to implement strong security features. As a result many IoT devices don't afford advanced security features. For instance, sensors for temperature detection can't handle advanced encryption and or other security features. Currently IoT security doesn't have any

ISSN: 0971-1260
Vol-22-Issue-3-July-2019

industry accepted standard[21]. There is no single agreed-upon framework in IoT, organizations usually have their own specific standards.

IOT common Standards

A number of IoT standards have been proposed to simplify and facilitate programming IoT applications and sevices.IOT protocols broadly have four categories: application protocols, service discovery protocols, infrastructure protocols and other influential protocols.

A. Application Protocols:

a. Constrained-Application-Protocol (CoAP): CoAPis meant for IOT based applications.CoAP specifies a protocol for web transfer using Representational-State-Transfer(REST) on the top of HTTP, used in mobile and social network applications.REST is used by clients plus servers to highlight and make use of web-services, e.g., SOAP in a better way using Uniform Resource Identifiers(URIs) and various HTTP methods(get, post, put) etc. For message exchanges, there is no need of XML[22].

b. Message Queue Telemetry Transport (MQTT):MQTT provides a connection between devices (embedded) and networks using applications plus middleware.Connections work on routing based mechanism enablingMQTT to be an appropriate protocol for IOT, M2M. MQTT works with TCP protocol and is suitable for devices with low resource availability, unreliable or low bandwidth links[23]. MQTT includes three components - a subscriber, a publisher,and a broker. For specific topics, device will register as a subscriber, a broker will inform the registered subscriber once the publisher publishes some topics of interest. The publisher generates interesting data, the broker acts as an informer to the subscriber.

c. Extensible Messaging and Presence Protocol (XMPP): XMPP is IETF (instantaneous messaging) based standard for multi-user chatting applications, voice applications and video calling. Users can send instant messages on the internet using XMPP. With XMPP, IM applications achieveaccess control,authentication, and compatibility with other protocols.

d. Advanced Message Queuing Protocol (AMQP): AMQP focuses on message oriented environments and is open standard protocol used in application layer. It provides efficient Communication through primitive message deliver guarantee[24]. For exchanging messages,AMQP uses TCP(Transport Control Protocol)

e. Data Distribution Service (DDS): Introduced on behalf of Object Management Group, DDS is meant for real-time M2M communications. DDS makes use of broker-less

ISSN: 0971-1260
Vol-22-Issue-3-July-2019

architecture and multicasting. Because of broker-less publish subscribe architecture, its real time constraints are highly applicable. From a developers perspective, DDS addresses a number of communication issues like, urgency, security, durability, reliability etc.

B. Service Discovery Protocols:

For scalability purposes, IoT needs a management for resource mechanism which can register and discover resources, services in a better way. The protocols that are used include multicast DNS (mDNS) and DNS Service Discovery (DNS-SD).

a. Multicast DNS (mDNS):mDNS acts as a base service, in the form of Name Resolution, for fewIoT applications e.g.,chatting[25]. In mDNS, DNS namespace use islocal without extra expenses or configuration, adding to its flexibility. Some of the advantages which makes mDNS appropriate choice for the internet based embedded devices are:

   To manage devices, no need of manual reconfiguration .

   For its smooth functioning, mDNS doesn't need infrastructure.

   If a failure of infrastructure occurs, mDNS still works.

b. DNS Service Discovery (DNS-SD):DNS-based service discovery (DNS-SD) involves matching of desired service based functionalities by clients through mDNS. Using this protocol, standard DNS messages are employed so that clients can discover desired services of a specific network.

C. Infrastructure Protocols:

a. Routing Protocol for Low Power and Lossy Networks (RPL): A routing-protocol which is link-independent andbased on IPV6 for minimal resource nodes, standardized by IETF (ROLL) working group. RPL was created to support least routing requirements, building a powerful topology over lossy links.
b. IEEE 802.15.4: This protocol is utilized by IOT because of low power consumption, low data rate, low cost , and high message throughput[26]. The protocol specifies a sub-layer for MAC and a physical layer for low rate wireless private area networks(LR-WPAN).The protocol works with a number of nodes(about 65k), and assures interoperability between a number of nodes. The services provided are secure and encrypted.

ISSN: 0971-1260
Vol-22-Issue-3-July-2019

c. EPCglobal: Used to identify items, in the form of unique identification number on an RFID tag.The EPCglobal architecture is based on RFID technology.Because of its scalability,openness, reliability and interoperability, this architecture is considered as one of the promising technique in future forIOT.
d. Z-Wave: This protocol is primarily used for home based automation and works on low RF signals. The Z-wave alliance has mandated for all Z-wave based devices to be interoperable. It is a low power based protocol and is based on interoperability.

QOS CRITERIA, IoT CHALLENGES AND FUTURE DIRECTIONS

Key challenges in IoT include:

A. Availability: To provide anytime and anywhere services for customers, the availability in IOT must be realized in the hardware as well as software level[24]. Software availability means IoT applications guarantee services all the time (for everyone and everywhere). Hardware availability ensures that devices are able to work independently on different technological platforms.
B. Reliability: Reliability plays an important role for increasing the progress rate of IOTdelivery services.It showscriticality and has more requirements when it comes to responding emergencies[27]. For IoT system to be called as efficient, the communication ought to be reliable.
C. Performance: The IoT performance is dependent on the components' performance and the performance of the underlying technology[28]. Metrics to access performance of IoT include: communication speed, processing speed,device form factor, and cost.
D. Management: Management in IoT includes managing Fault, managing Configuration, Accounting management, Performance management, and management of Security(FCAPS)[29]. Thus a need for new light- management protocols.
E. Scalability: Scalability in IoT refers to adding more resources without any affects on the QoS[30]. With the presence of diverse hardware platforms and communication protocols, scalability remains an issue in IoT.
F. Interoperability:IoT consists of a number of connected things from different platforms. Interoperability has to be taken into consideration from an application developers perspective and IoT device manufacturers too, so that services are delivered without any hindrance from the hardware platform they are based upon.

ISSN: 0971-1260
Vol-22-Issue-3-July-2019

G. Security and Privacy: IoT security lacks common standard and architecture, thus poses a significant challenge.Also because of heterogeneity, IoT poses a great security threat. A number of security issues arise e.g., keydistribution amongst devices.

REFERENCES:

[1] D. Evans, "The Internet of things: How the next evolution of the Internetis changing everything,"CISCO, San Jose,CA, USA,White Paper, 2011.

[2] L. Atzori, A. Iera, and G. Morabito, "The Internet of Things: A survey,"*Comput. Netw.*, vol. 54, no. 15, pp. 2787–2805, Oct. 2010.

[3] R. Khan, S. U. Khan, R. Zaheer, and S. Khan, "Future Internet: The Internetof Things architecture, possible applications and key challenges,"in *Proc. 10th Int. Conf. FIT*, 2012, pp. 257–260.

[4] J. Gubbi, R. Buyya, S.Marusic, and M. Palaniswami, "Internet of Things(IoT): A vision, architectural elements, and future directions," *FutureGener. Comput. Syst.*, vol. 29, no. 7, pp. 1645–1660, Sep. 2013.

[5] P. Lopez, D. Fernandez, A. J. Jara, and A. F. Skarmeta, "Survey ofInternet of Things technologies for clinical environments," in *Proc. 27thInt. Conf. WAINA*, 2013, pp. 1349–1354.

[6] D. Yang, F. Liu, and Y. Liang, "A survey of the Internet of Things," in*Proc. 1st ICEBI*, 2010, pp. 358–366.

[7] A. Gluhak*et al.*, "A survey on facilities for experimental Internet ofThings research," *IEEE Commun. Mag.*, vol. 49, no. 11, pp. 58–67,Nov. 2011.

[8] Z. Sheng *et al.*, "A survey on the IETF protocol suite for the Internetof Things: Standards, challenges, and opportunities," *IEEE WirelessCommun.*, vol. 20, no. 6, pp. 91–98, Dec. 2013.

[9] J. Gantz and D. Reinsel, "The digital universe in 2020: Big data, biggerdigital shadows, and biggest growth in the far east," *IDC iView: IDCAnal. Future,* vol. 2007, pp. 1–16, Dec. 2012.

[10] S. Taylor, "The next generation of the Internet revolutionizing the waywe work, live, play, and learn," CISCO, San Francisco, CA, USA,CISCO Point of View, 2013.

[11] J. Manyika*et al., Disruptive Technologies: Advances thatWill TransformLife, Business, and the Global Economy*. San Francisco, CA, USA:McKinsey Global Instit., 2013.

[12] M. Z. Shafiq, L. Ji, A. X. Liu, J. Pang, and J. Wang, "A first look at cellularmachine-to-machine traffic: Large scale measurement and characterization,"in *Proc. ACM SIGMETRICS Perform. Eval. Rev.,* 2012, pp. 65–76.

[13] D. Floyer, "Defining and sizing the industrial Internet," Wikibon,Marlborough, MA, USA, 2013.

[14] "Commercial building automation systems," Navigant Consulting Res.,Boulder, CO, USA, 2013.

ISSN: 0971-1260
Vol-22-Issue-3-July-2019
[15] S. Krco, B. Pokric, and F. Carrez, "Designing IoT architecture(s):A European perspective," in *Proc. IEEE WF-IoT*, 2014, pp. 79–84.

[16] EU FP7 Internet of Things Architecture Project, Sep. 18, 2014. [Online].Available: http://www.iot-a.eu/public

[17] Z. Yang *et al.*, "Study and application on the architecture and keytechnologies for IOT," in *Proc. ICMT*, 2011, pp. 747–751.

[18] M. Wu, T. J. Lu, F. Y. Ling, J. Sun, and H. Y. Du, "Research onthe architecture of Internet of Things," in *Proc. 3rd ICACTE*, 2010,pp. V5-484–V5-487.

[19] L. Tan and N. Wang, "Future Internet: The Internet of Things," in *Proc.3rd ICACTE*, 2010, pp. V5-376–V5-380.

[20] M. A. Chaqfeh and N. Mohamed, "Challenges in middleware solutionsfor the Internet of Things," in *Proc. Int. Conf. CTS*, 2012, pp. 21–26.

[21] N. Koshizuka and K. Sakamura, "Ubiquitous ID: Standards for Ubiquitouscomputing and the Internet of Things," *IEEE Pervasive Comput.*,vol. 9, no. 4, pp. 98–101, Oct.–Dec. 2010.

[22] N. Kushalnagar, G. Montenegro, and C. Schumacher, "IPv6 over Low-Power Wireless Personal Area Networks (6LoWPANs): Overview,assumptions, problem statement, and goals," Internet Eng. Task Force (IETF), Fremont, CA, USA, RFC4919, vol. 10, Aug. 2007.

[23] G. Montenegro, N. Kushalnagar, J. Hui, and D. Culler, "Transmissionof IPv6 packets over IEEE 802.15. 4 networks," Internet Eng. TaskForce (IETF), Fremont, CA, USA, Internet Proposed Std. RFC 4944, 2007.

[24] K. Pilkington, "Revolve teams up with Home Depot to keep your houseconnected," Centre National d'Etudes des Telecommunications (CNET),San Francisco, CA, USA, CNET—News, 2014. [Online]. Available:http://Ces.Cnet.Com/8301-35306_1-57616921/Revolv-Teams-Upwith-Home-Depot-to-Keep-Your-House-Connected/

[25] "SmartThings | Home automation, home security, and peace of mind,"SmartThings, Palo Alto, CA, USA, Sep. 2014. [Online]. Available:http://www.smartthings.com

[26] U. Rushden, *Belkin Brings Your Home to Your Fingertips With WeMoHome Automation System*. Los Angeles, CA, USA: Press RoomBelkin, 2012.

[27] R. Want, "An introduction to RFID technology," *IEEE PervasiveComput.*, vol. 5, no. 1, pp. 25–33, Jan.–Mar. 2006.

[28] R.Want, "Near field communication," *IEEE Pervasive Comput.*, vol. 10,no. 3, pp. 4–7, Jul./Sep. 2011.

[29] R. S. Kshetrimayum, "An introduction to UWB communicationsystems," *IEEE Potentials*, vol. 28, no. 2, pp. 9–13, Mar./Apr. 2009.

[30] "Lakhwani, Kamlesh, et al. "Development of IoT for Smart Agriculture a Review." *Emerging Trends in Expert Applications and Security*. Springer, Singapore, 2019. 425-432. "