IJCSE International Journal of Computer Sciences and Engineering Open Access
Survey Paper Vol.-7, Special Issue-16, May 2019 E-ISSN: 2347-2693

A Survey on Architecture, Elements, Protocols and Issues of Internet of Things

Meghana N M[1*], Surekha K B[2] Basavaraju TG[3]

[1,2]Dept. of Information Science & Engineering, Sapthagiri College of Engineering, Bengaluru, Karnataka, India
[3] Dept. of Computer Science & Engineering, SKSJTI, Bengaluru, Karnataka, India

Corresponding Author: nm.meghana5@gmail.com, Tel.: +91-7829372304

DOI: https://doi.org/10.26438/ijcse/v7si16.8892 | Available online at: www.ijcseonline.org

Abstract— In current era Internet of Things(IoT) is one of the trending technology. Automation system made up of IoT service reduces the human effort. This paper provides an overview of IoT three layer and five architecture, fundamental elements of IOT, protocols and about issues to be considered while developing IoT system.

Keywords— Identity-related service, Collaborative aware service, Ubiquition Service.

I. INTRODUCTION

In today's rapidly changing technological world numbers of devices which are connecting to internet are increasing with very high rate. These internet connected smart devices are creating the smart world Internet of Things plays a major role in creation of this smart world [1] .As this technique of IoT focuses mainly towards needs of user like smart home applications like automatic door open and close, room temperature monitoring and e-heath applications etc. In IoT system many smart machines should exchange the data to fulfill a common goal. As to support continuous communication between millions of IoT devices a layered architecture is considered.

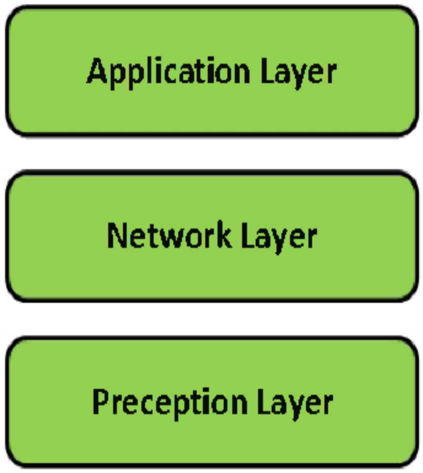

Figure 1: Three Layer architecture

As Figure 1 shows 3 layers are included in IoT architecture [2] . Those are

1. Perception Layer[Recognition layer]:It is the lowest layer of IoT architecture. Main responsibility of this layer is to the perceive the useful information from the devices or from the environment. Based on many sensing technologies like RFID, NFS, WSN this process of perception takes place [6]. And whatever data that is collected form things are converted in to digital signal format by this layer. And this layer also takes the responsibility of identifying other smart objects.

2.Network Layer: This Layer establishes connection between smart devices in the environment, network devices and between servers. And it transmit the information gathered by devices in perception layer to application layer by using technologies like LAN, Wired or Wireless network. Mainly it uses the mediums like FTTx, WiFi, blueetooth, ZigBee, IR Technology etc. To handle huge quantity of data concept of cloud computing is used to store and process the data efficiently.

3. Application Layer: This layer is the front end for entire architecture of IoT. This layer uses the data that is processed by network layer. Main responsibility is to provide services which are application specific to the user. It defines different applications where in which IoT can be used like smart health, Smart Home etc.

Though this three layer architecture provides main idea about IoT, This is not sufficient to understand finer aspects that have to be considered in IoT. So five layer architecture [3] have been introduced. Figure 2 shows five layer architecture of IoT.

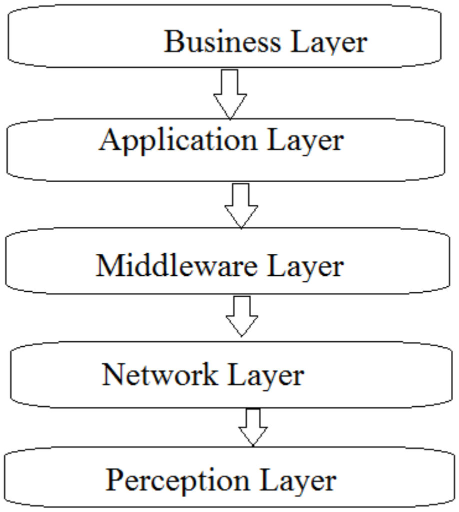

Figure 2: Five Layer architecture

Layers in this refined architecture are perception layer, transport layer, processing layer, application layer and business layer. Among these 5 layers, application and perception layer's roles are same as in three layer architecture. Remaining three layers are responsible for

1. Network Layer: It is mainly responsible for transferring the critical information which is gathered from sensor devices to central data processing unit[18]. It make use of technologies like 3G, Bluetooth, RFID, LAN, NFC to transfer data. In general responsibility of network layer is to transfer data from perception layer to processing layer.

2. Processing Layer[Middleware Layer]: It processes, analyzes and stores the large amount of data from the transport layer and it also responsible for service management. It provides many services to lower layers. And supports many technologies like database, bigdata and cloud computing. This layer retrieve ,process and compute the information and take decision based on computational outcomes.

3. Business Layer: This layer manages the entire IoT system. All IoT systems like applications, business model, user's privacy model, profit model is managed by this business layer. It analyze the data which is received from lower layer and creates graphs, flow chart, business models. By seeing this functional managers can take accurate decision about business strategies.

Section I contain Introduction about two types of IoT architecture, Section II contain fundamentals of IoT, Section III contain Different protocols that are used in IoT, Section V contain challenges of IoT, Section V conclude the survey work.

II. FUNDAMENTALS OF IOT

For proper functioning of IoT system six main elements [4] have to be considered. Those are

1. Identification: If we consider the Internet then one of the main thing we need to consider is how to identify each object in internet. These objects may be physical things like gateways, devices and may also be virtual things like application software and multimedia contents. As like domain names are assigned in internet, in IoT also things are assigned with IoT ID's. Many identification methods for IoT are available like EPC(Electronic Product Code) and UCode(Ubiquitous Code) IPV6 addressing scheme is included in IoT to uniquely identify things in internet.

2. Sensing: Sensing means collecting the data from all the devices in the network. Gathered data is send to database or to cloud where these data's are analyzed based on requirement. Sensors in IoT can be actuators, shrewd sensors or can be wearable detecting gadgets.

3. Communication: Communication technique in IoT connects together different heterogeneous devices to achieve particular smart services. Some of the communication technologies used in IoT are RFID, NFC(Near Field Communication) and UWB(Ultra Wide Bandwidth). WiFi can be used to establish data exchange with 100m range. To establish high speed data transfer LTE(Long Term Evolution)can be used.

4. Computation: It is the unit of processing. To run IoT application different hardware platforms are developed like arduino, Friendly ARM, Resberry PI etc. Many software platforms are also available. Among these OS is the main thing need to be considered. Many RTOS are available to develop RTOS based IOT. If data is huge then concept of cloud computing and Bigdata are used for computation.

5.Services: Mainly four types of services are available

- Identity-related service: Here it brings the object to virtualization and these objects are uniquely identified.
- Information Aggregation Service: Gather raw information and process it.
- Collaborative aware service: Collect the processed data and provides the required reaction.
- Ubiquition Service: Allow all time support of collaborative aware service.

6. Semantics: In this phase by recognizing and analyzing data it smartly extract the knowledge from various devices to support required service. We can also call semantics as brain of IoT because demands are send towards right resources. Some of the semantics are RDF(Resource Description Framework), OWL(Web Ontology Language).

III. IOT PROTOCOL STACK

Because of the restricted environment of IoT like power constraints, less availability of memory, bandwidth constraints and high packet loss ratio it is not efficient to use traditional TCP/IP stack and existing web technologies for IoT communication . So to solve this problem many proprietary protocols has been developed. Below Figure 3 shows the IoT protocol stack [15] to establish wireless communication.

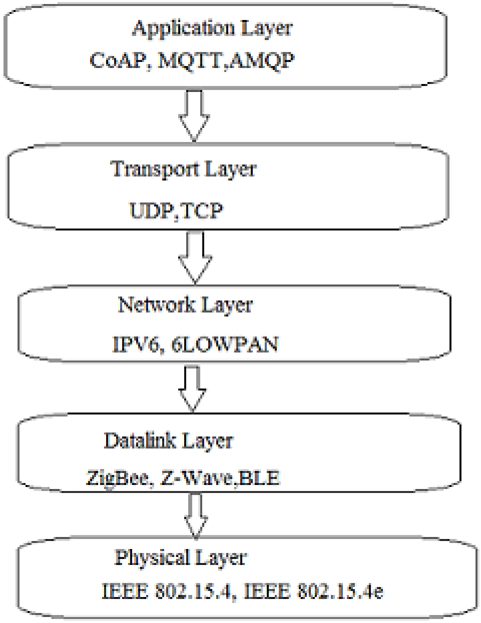

Figure 3: IoT Protocol Stack

A. Physical/ Link layer protocols

ZigBee: It is one of wireless communication technology mainly designed for short range and low data rate applications [16]. Mainly four layers in ZigBee protocol stack those are physical layer , MAC layer, Network layer and application layer .IEEE 802.15.4 standard defines physical and medium access control layer of ZigBee. Remaining two are defined as ZigBee specification. ZigBee network layer is mainly responsible for routing and addressing for mesh and tree topologies. Main application of ZigBee are ZigBee Home automation, ZigBee smart energy profile etc.

Z-Wave: It is a low energy radio wave enabled mesh network which provides the facility of reliable and low latency transmission of short message to one or more network nodes [17]. Z-wave operation is based on controller and slaves model, where controller send commands to the slaves and slaves execute the commands and replay the answer back to controller. Z-Wave is used in applications like smart hub, smart lighting, smart locks, smart sensors etc.

B. Network layer protocols

IPV6:As day by day the number of devices which are connecting to the internet are increasing IPV4 addressing methodology is not sufficient to address all the devices . IPV6 which provides 128 bit address have to be adopted in IoT. With this IPV6 without using any proxies or translation gateways any smart devices can be connected to the other network and IPV6 enable more distributed end to end connectivity for mobile end nodes and also for mobile routing nodes.

6LowPAN: It is one of the most commonly used network layer protocol which send the data as packets and uses IPV6 scheme addressing so it is called as IPV6 over Low Power Wireless Personal Area Network. Initially it is developed to work on top of IEEE 802.15.4 but now it has been adopted in many wireless technologies like Bluetooth, low power WiFi etc. 6LowPAN provides the mechanism of compression and encapsulation of data which is to be transferred through wireless network. Main goal of 6LowPAN is to provides wireless connectivity among devices with very low duty cycle and with less data rate . 6LowPAN is mainly used in applications like home automation ,smart grid and Industry monitoring etc.

C. Application Layer protocols

MQTT [Message Queue Telemetry Transport]: It is a messaging protocol works on top of TCP/IP protocol. This protocol is mainly works in areas where bandwidth and battery power constraints is their so this protocol is well suited for IoT. MQTT establishes lossless ordered bi-directional connections. It is based on publish –subscriber model that is message sent by one device (the publisher) is transmitted to many device (subscribers). The broker node acts as a central node for exchanging the message.

Three levels of QoS is supported by MQTT.

- Maximum once: Here best effort message takes place and once the message is received, the receiver will not send any acknowledgement.
- At least once: Here message transmission can be guaranteed but there is a chance of duplicate messages.
- Exactly once: Here without any duplicate occurrence of messages, message transmission can be guaranteed.

CoAP[Constrained Application Protocol]:This protocol is mainly designed to establish communication with the resource constrained devices and resource constrained network like low power network and lossy network etc. This CoAP allow communication between same constrained device and different constrained device and with general node in the network. CoAP can be easily converted to HTTP to provide easy integration with web to meet certain requirements like low overhead communication, multicast service etc. CoAP uses the request and response message types to communicate with devices. By default CoAP uses the UDP protocol and optionally supports DTLS to allow high communication security.

AMQP[Advanced Message Queuing Protocol]:This is the recently proposed protocol to support transmission of huge quantity of data without affecting the overall performance of entire system. AMQP middleware supports transmission of different messages without any restriction on programming language and platform used. It supports 3 ways of message transmission those are publish and subscribe, Store and forward and point to point.

IV. CHALLENGES IN IOT

Implementing the concept of IoT is not easy because of certain challenge [10] that has to be considered. To efficiently implement any of IoT services following challenges have to be addressed.

1. Availability: In some real world application availability plays a major role. Availability in IoT means everyone at different places are able get services from IoT application simultaneously. By providing redundancy for critical services and devices [11] high availability can be achieved in IoT. In certain applications like healthcare IoT application and military applications service must be available all the time. And some tools [11][12] can be used to achieve high availability.

2. Reliability: IoT systems must work properly based on the requirement, reliability means increasing the success rate of IoT. Reliability can be implemented in software and hardware in all IoT layers .In IoT reliability must be in terms of less delay in transmission, minimize packet loss. It is required to design self aware IoT system to quickly adopt changes in the environment to maintain the required reliability.

3. Mobility: In IoT most of the service requirement is expected by mobile users. Establishing continuous connection with devices that are moving is the major challenges. Service interruption may occur when these devices move from one network gateway to another network gateway. So IoT system required an efficient approach for managing the mobility. One of the mobility management method is introduced in [13] by the mechanism of distributed lifecycle management. Managing the mobility plays a very important in case of IoV(Internet of Vehicle) area.

4. Performance: Since IoT system performance depends on many components and performance of technology that is used measuring the IoT service performance is the big challenge. Many factors can be considered while measuring the performance of IoT these factors are communication speed, processing speed, cost, device from factors etc. Better approach to measures the performance of IoT services is required to properly measure the performance.

5. Management: In IoT system million of devices are connected to each other for proper functioning of the entire system each of devices must be managed properly [9]. In case of IoT based on application requirement different management techniques have to be used. Management scheme also includes managing the connectivity speed and guarantee the service delivery. So it necessitates the development of new efficient light weight protocol for management.

6. Scalability: IoT system must support extensible operation and service that is if any new device are added or if existing devices are detached from network in any situation IoT system must work properly [4]. IoT Daemon include 3 layers introduces automation and no configuration required in each object. It guarantees the interoperability and scalability in IoT environment.

7. Limited Energy resource: IoT devices have to perform multiple task like sensing the data and transferring the data all these operations consume adequate amount of energy [7]. Main power consumption in IoT is because of collisions during channel access and radio transmission. So proper methodology or protocol have to be designed to increase the life span of battery used in IoT devices.

8. Interoperability: Science in IoT huge number of heterogeneous things has to communicate with each other but each of these devices not sharing the common working platform establishing the communication among the device is a major challenge. Interoperability [8] issue must be considered in both IoT device manufacture and application developers to support service for all end users irrespective of hardware platform that they are using. IoT programmer develops an IoT application that allows adding new functionalities without harming existing operational functionalities. The main challenge to establish the Interoperability is same standard must have to be implemented in different devices.

9. Security and Privacy: Security and Privacy issues[14] is one of the great challenge in IoT. In IoT since availability of resources is limited, heterogeneous technologies and lack of specific IoT standards made it more vulnerable to the cyber threats. In each layer of IoT architecture different attacks are possible they are, Security attacks possible in perception layer are

- Physical attack: Attack focus on hardware components like node tampering, malicious code injection.
- Impersonation: Authentication by fake identity.

Security attack possible in network layer is

- Routing attack: Right routing path may modified by malicious nodes in network.
- DoS attack: Attackers making the network resources unavailable for actual operation
- Data Transit attacks: Causing integrity and confidentiality attack while transmitting the data.

Main security attacks involved in Application layer are

- Data leakage: Stealing the data.
- Malicious Code Injection: By knowing the vulnerabilities of application attacker upload the malicious code to software applications.

V. CONCLUSION

With the quick development of the IoT industry, significance of understanding the factors to be consider while developing the IoT service is very important. Because of this, understanding the basic IoT architecture model and functionalities to be considered while developing IoT system is very much necessitated. This paper provide the brief description about architecture of IoT, elements of IoT, protocols and about issues to be considered in IoT system development.

REFERENCE

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

[2] Pallavi Sethi and Smruti R. Sarangi *"Internet of Things: Architectures, Protocols, and Applications"*. Hindawi Journal of Electrical and Computer Engineering Volume 2017, Article ID 932403

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

[4] Muhammad Burhan , Rana Asif Rehman , Bilal Khan and Byung-Seo Kim *"IoT Elements,Layered Architectures and security issues: A comprehensive survey"* Sensors 2018,18, 2796; doi:10.3390/s18092796

[5] Chayan Sarkar, Akshay Uttama Nambi S. N, R. Venkatesha Prasad, Abdur Rahim, Ricardo Neisse *"DIAT: A Scalable Distributed Architecture for IoT".* Ieee Internet Of Things Journal, Vol. 2, No. 3, June 2015

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

[7] Farzad Samie , Vasileios Tsoutsouras , Lars Bauer , Sotirios Xydis , Dimitrios Soudris , J¨org Henkel *"Computation Offloading and Resource Allocation for Low-power IoT Edge Devices"* 978-1-5090-4130-5/16/$31.00 c_2016 IEEE

[8] Venkateswara Raju Konduru , Manjula R. Bharamagoudra *"Challenges and Solutions of Interoperability on IoT How far have we come in resolving the IoT interoperability issues" 2017 International Conference On Smart Technology for Smart Nation*

[9] Koustav Routh, Tannistha Pal*" A survey on technological, business and societal aspects of Internet of Things by Q3, 2017",* 978-1-5090-6785-5/18/$31.00 © 2018 by IEEE

[10] Er. Pooja Yadav, Er. Ankur Mittal, Dr. Hemant Yadav *"IoT: Challenges and Issues in Indian Perspective*" 978-1-5090-6785-5/18/$31.00 © 2018 by IEEE.

[11] D. Macedo, L. A. Guedes, and I. Silva, *"A dependability evaluation for Internet of Things incorporating redundancy aspects,"* in *Proc. IEEE 11th ICNSC*, 2014, pp. 417–422.

[12] I. Silva, R. Leandro, D. Macedo, and L. A. Guedes, *"A dependability evaluation tool for the Internet of Things," Comput. Electr. Eng.*, vol. 39, no. 7, pp. 2005–2018, Oct. 2013.

[13] T. Elsaleh, A. Gluhak, and K. Moessner*, "Service continuity for subscribers of the mobile real world Internet,"* in *Proc. IEEE ICC Workshops*, 2011, pp. 1–5.

[14] Mirza Abdur Razzaq, Muhammad Ali Qureshi, Sajid Habib Gill, Saleem Ullah *"Security Issues in the Internet of Things (IoT): A Comprehensive Study",(*IJACSA) International Journal of Advanced Computer Science and Applications, Vol. 8, No. 6, 2017.

[15] Cheena Sharma, Dr. Naveen Kumar Gondhi *"Communication Protocol Stack for Constrained IoT Systems"* 978-1-5090-6785-5/18/$31.00 © 2018 by IEEE.

[16] Luca Mainetti, Luigi Patrono, Antonio Vilei *"Evolution of Wireless Sensor Networks towards the IoT:A Survey".*

[17] Shadi Al-Sarawi, Mohammed Anbar , Kamal Alieyan , Mahmood Alzubaidi *"Internet of Things (IoT) Communication Protocols : Review"* 2017 8th International Conference on Information Technology (ICIT)

[18] Surapon Kraijak1 , Panwit Tuwanut *"A Survey On Iot Architectures, Protocols, Applications, Security, Privacy, Real-World Implementation And Future Trends"*

Authors Profile

Mrs. Meghana N M pursued Bachelor of Engineering and Master of Technology from Visveswarya Technological University, Belagavi.karnataka, India in the year 2016. She is currently working as Assistant Professor in Department of Information Science And Engineering at Sapthagiri College of engineering Bengaluru,Karnataka,India. Area of interests are Internet of Things, Wireless Networks.

Surekha K.B. is currently working as Associate Professor and Head of ISE at Acharya Institute of Technology,Bangalore. She holds bachelor degree from Kuempu Uniersity,Masters from VTU,Belgaum. She holds a PhD from JNTU,Hyderabad.Her research area are Wireless Sensor Network, IoT and cognitive IoT

T. G. Basavaraju is currently working as professor and head of CSE Department at Government SKSJ Technological Institute, Bangalore. He is a board of studies member in computer science and engineering stream, VTU, belgaum from the year 2013 to 2017. Basavaraju holds a Ph.D. (Engg.) from Jadavpur University, Kolkata in the area of mobile adhoc networks. He obtained his ME in CSE from UVCE, Bangalore University, Bangalore and secured first rank. He has more than 19 years of experience in teaching and industry. He has authored and co-authored five text books in the area of computer networking. One of his co-authored text book on "mobile wireless ad hoc networks: principles, protocols and applications" was published from auerbach publishers (Taylor and Francis group), USA. He has to his credit more than 55 research publications in international journals and conferences