Exploring Architectures for Effective Processing of Internet of Things (IoT) Data

Nisha Saini[1*], Jitender Kumar[1]

[1]Department of Computer Science & Engineering, DCRUST, Murthal, 131039, Sonipat, Haryana, India

Corresponding author- 21001901005nisha@dcrustm.org

Abstract

Internet of things (IoT) has become a revolutionary paradigm in the academia as well as in industries. This concept is usually used to describe the network of physical objects i.e. "things". These things are embedded with different types of sensors and software for connecting and exchanging the data with the other devices and systems over the internet. However, in the absence of standard architectures, the research community has proposed different types of layered architectures for processing of IoT data. These architectures differ in the number of the layers, function assigned to each layer and the type of resources to be used for processing the IoT data. In this regard, this paper aims to review various layered architectures proposed by recent research and to highlight both their pros and cons. Moreover, it outlines the associated challenges that must be resolved for the IoT data processing architectures to succeed.

Keywords:

Internet of Things, IoT architectures, Layered Model, IoT challenges, Fog/Edge computing

1. Introduction

Significant progress has been made in the semiconductor domain, resulting in the proliferation for the use of low-cost sensor-based CPU systems. When modern communication technologies (e.g., Bluetooth LoRA, Zig-Bee, Wi-Fi, 3G, 4G, 5G, etc.) are added to these systems, they converge into an emergent kind of technical domain known as the Internet of Things (IoT) [1].The term "Internet of Things" was first introduced in 1999 by industry researcher Kevin Ashtonin the context of supply chain management [2]. Later, the IoT was formally documented by the International Telecommunication Union (ITU) in 2005. Different from the traditionally interconnected computer networks, IoTenvironment is slightly different because it involves smart IoT devices that support internet access and may communicate with other devices over the internet. Although the meaning of "Things" has evolved as technology has progressed, the primary goal of IoT is making a computer comprehend information without the assistance of a person. The proliferation of the IoT and the rapid development of related technologies resulted in a widespread connection of "things," such as sensors, actuators, and devices, resulting in the production of massive amounts of data that must be stored, processed, and retrieved [3]. So,IoT is an amalgamation a collection of technologies that function in tandem.Since no standard guidelines have laid for IoT architectures, therefore research community has proposed diverse layered architectures for processing the voluminous data of IoT devices. These architectures differ in the number of layers, role assigned to each layer and underlying platforms for processing the IoT data e.g. edge/fog computing or cloud computing. Under such circumstances, it is difficult for an individual to decide which architecture suits his/her needs. Moreover as usage of IoT devices is rapidly increasing in our day-to-day life, so the processing mechanism of each type of IoT devices should be uniform. Otherwise, it will be difficult for the individual users to get verse with the each technology [4]. Under such circumstances, this paper reviews the different layered architecture proposals of the contemporary research and highlights the pro and cons of each.

Rest of the paper is being organized as follows. Section 2 introduces the background of IoT environment building blocks. Section 3 presents taxonomy of layered architectures of IoT environment. In addition, it also presents the comparative summary of the different architectures. Section 4 discusses the open challenges in the IoT environment. Section 5 presents the concluding remarks of the work.

2. Background of IoT Environment Building Blocks

The standard IoT basically comprises for sub-entities namely: sensors and actuators, network infrastructure, cloud platforms and application domain as depicted in Fig. 1. The sensors and actuators are responsible for collecting and dissemination of the information from particular objects without the need of human intervention [5]. In particular, sensors collect physical information from the environment and convert them into electrical signals. Whereas, an actuator such as a temperature controller on an air conditioner works in reserve direction i.e.it is used to reflect a change in the environment andconverts the electrical signals into physical information (e.g. heat, sound etc.). The network infrastructure is responsible for all types' of communication in the IoT systems and backbone processing systems. It consists of gateways, routers and repeaters etc. All types of communication in IoT environment is wireless. Cloud platforms are used to store the voluminous data generated by the IoT devices [6].

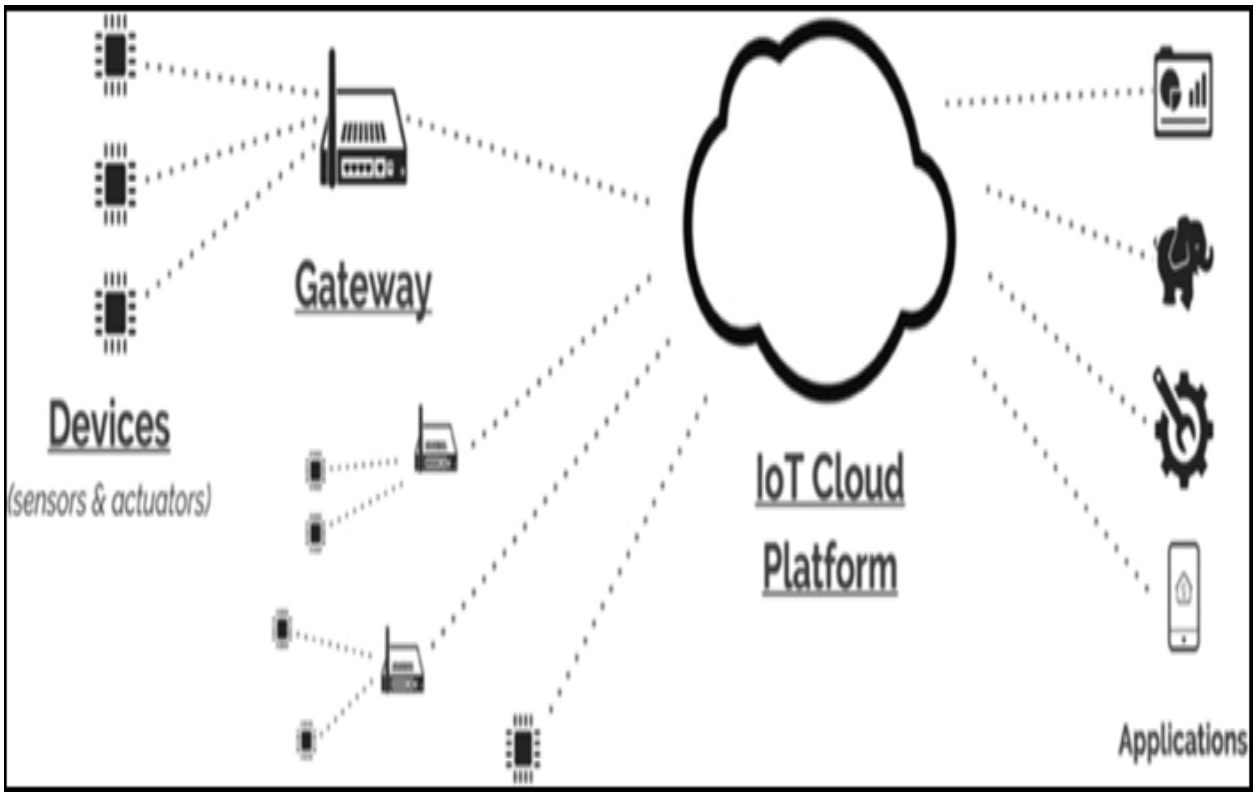

Figure 1: Building blocks of IoT systems

However, some pre-processing is generally applied in order to limit the relaying of raw data and save the precious battery resources of sensors. Finally, application

domain is generating meaningful results by processing the received data from the IoT devices [7].

3. Taxonomy oflayeredarchitectures ofIoT environment

The Internet of Things (IoT) was recognized as the third wave of web technology after the World Wide Web (WWW) and social networking web technology. In order to accomplish crucial IoT tasks, a number of research groups and experts are working for outlining the standard architectural guidelines for IoT environment[8].These proposals differ in the underlying concerns such as network security and privacy in the IoT, latency issues etc. As a result, we divide IoT architectures into five classes: class I with three layers, class II with four layers, class III with five layers, class IV with six layers, and class V with seven layers.The hierarchical organization of these architectures is shown in Fig. 2. This section reviews the contemporary architecture proposals on the basis of functions assigned to each layer and highlights the pros and cons of each.

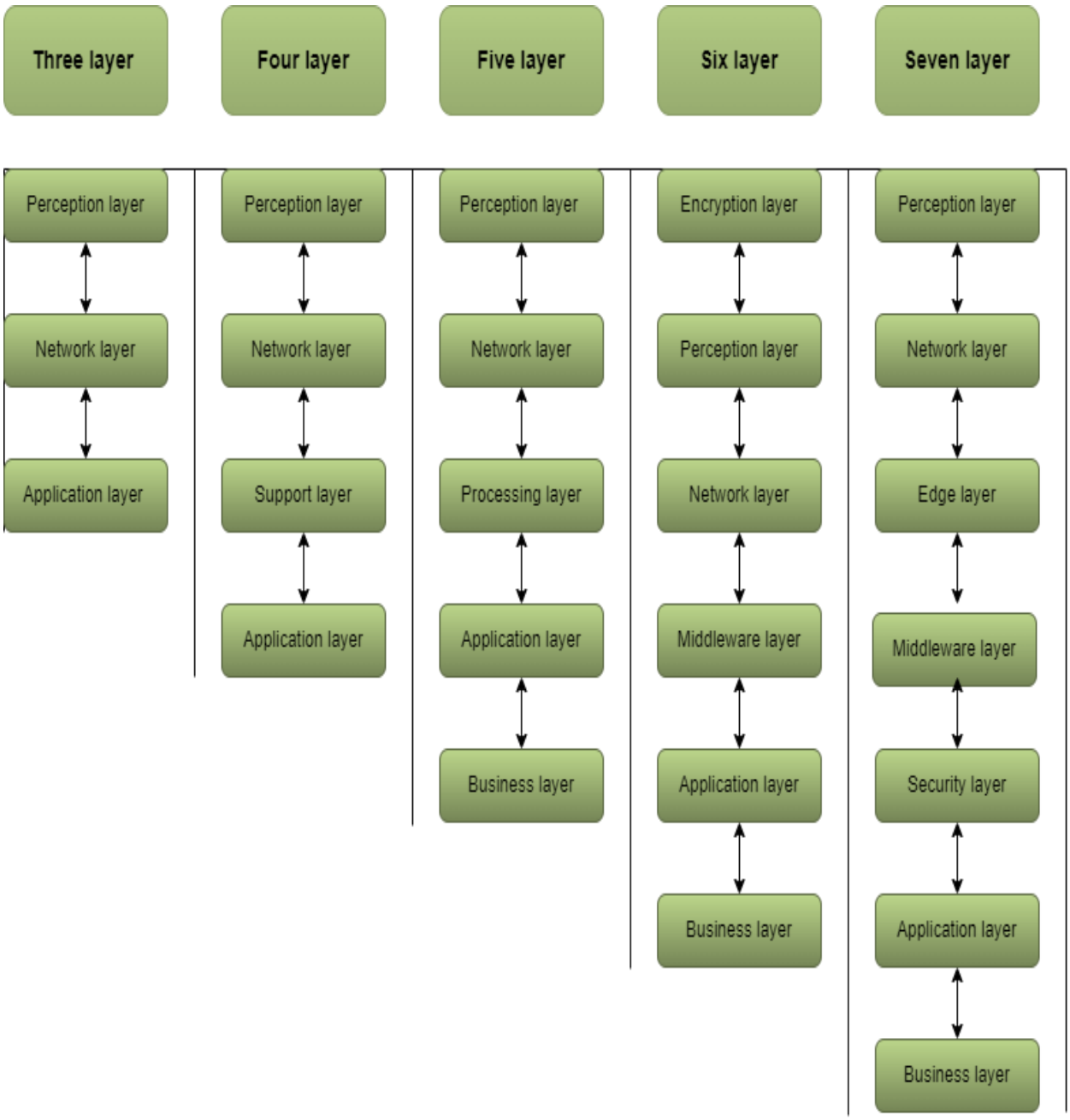

Figure 2: Layered architecture of IoT environment

3.1Three-layer architecture

Itis one of the elementaryarchitecture that adheres to the core principle of the IoT environment that chalks out only the fundamental blocks. In the early stages of IoT environment, a three-layered architecture was proposed [9]. In a three-layered architecture, the perception layer is the bottom layer. This layer is also more

profoundly referred as a Sensor layer or physical layer, because it comprises sensors for capturing environmental data [10]. Subsequently, the middle layeri.e. network layerdeals withrelaying and processing of the sensors data. Finally, followed by the middle layer is the application layerwhichreceives data from the network layer and transmits it to a particular service application of the IoT service users [11]. The proposed three levels explain the operation of IoT;however they cannot provide a reliable solution when addressing the more complex aspects of IoT.

3.2Four-layer architecture

The three-layer architecture fulfills only the elementary requirements for processing the IoT environment data i.e. it was only able to meet the limited requirements. So, a new architecture with four layers as shown in Fig. 2was later proposed by researchers. The support layer is a new layer that the researchers have added to the three-layer design already in place [12]. The four-layered architecture and suggested security measures to protect it against intrusions [13]. The remaining three layers function in the same way as the three layers design we've already described.

3.3Five-layer architecture

Interest of business industry led to the induction of the five layered architecture. For instance, prediction of future trends on the basis of current trends. These interests led to the introduction of modern trend prediction techniques like deep learning in getting more useful insights [14]. Consequently, five layer architecture contains additional layer i.e. business layer. The business layer controls and guides the complete operations of IoT environment, including the industrial interests and corresponding profit models. In addition, it handles the business data in an interactive way while preserving the privacy [15]. Moreover, this fivelayer architecture also advocates for processing of data at cloud surrogates in the processing layer.

3.4Six-layer architecture

The TCP/IP protocols used in the existing multilayer IoT designs can't support such a huge IoT network. Therefore, a new open architecture was sought that can support well established network protocols along-with the existing applications, and relay information byassuring security as well as quality of services [16].Without adequate security guarantees, the IoT environment could not have evolvedto the present scenario. IoT's main tasks therefore revolve around data protection and privacy. Therefore there is need for an additional layer i.e. Encryption layer. It assignsa distinct object ID to each type of communication that makes it simple to distinguish between them [17]. It is also known as coding layer. It supports several multilevel security protocols, based on a hierarchical network structure [18].

Table 1: Layer-wise features of seven-layered IoT environment architecture

Layers	Role and functional features
Perception Layer	One of this layer's features is its capacity to sense the environment in which smart items are present.
Network Layer	Its function is to make it possible for different devices to connect to the internet, transmit and process the data.
Edge Layer	The main functions of this layerare data filtering, aggregation, cleanup, packet content inspection, network and data level analytics.
Middleware Layer	It uses technologies like cloud computing, global computing, big data, and direct database access to process sensor data so that it can record all the information that is required. This layer is also known as the Processing layer.
Security Layer	Theprime objective of this layeris to maintain the security and integrity of IoT environment data.
Application Layer	Its primary function is to provide the user with the appropriate service in accordance with the type of application.
Business Layer	It controls the complete Internet of Things (IoT) system, including the industrial interests and corresponding profit models.In addition, it also presents the information in a user-

friendly manner while maintaining privacy.

3.5 Seven-layer architecture

After deliberate consideration of surrounding environment of IoT devices and long-term wide area network latencies, the research community has proposed seven-layer architecture [19]. The functions of each layer are elaborated in Table 1. This new architecture advocates the use of proximate computing i.e. edge/fog clouds for real-time processing of sensors data [20]. The key premise of fog/edge computing is that these resources minimize long-term wide area network overheads. It is mainly used for filtering, aggregation and cleanup of data. In addition, these systems can survive during the failure of services from the remote clouds. Moreover, the security of the data is also enhanced due to storage in the proximity [21]. The comparative summary of different layered architectures is shown in Table 2.

Table 2:Comparison of different Layered IoT Architecture

Layer Model	Design Objectives	Proposed solution
3-Layer	Basic requirement of IoT devices	Conventional IoT architecture
4-Layer	Interface and services	Fulfills the present requirements of applications due to advancements in IoT
5-Layer	Security	To provide network security and privacy.
6-Layer	Authentication	To improve the security and authentication mechanism in IoT.
7-Layer	Real time access and reduce latency	To alleviate the latency problem and enhance the performance of IoT based systems.

4. Open challenges

Besides the pros and cons of different architectures, there are still challenges in IoT environment that need to addressed for the widespread adoption of IoT devices in

physical world. This section highlights the challenges associated with these architectures.

4.1 Vendor Lock-in: When a user commits to one vendor for the deployment of IoT infrastructure and some advance technology arrives, then the user has to rely on the mercy of the existing vendor to upgrade the services. So, rigorous efforts should be carried out to develop generalized IoT infrastructure so that users can switch between different vendors as per suitability.

4.2 Computation Platforms Heterogeneity: Some architectures advocate using edge/fog computing resources in collaboration with distant cloud resources. However, the underlying virtualization formats of different platforms can be different. Consequently, the integration of such platforms for processing the IoT data would be a subtle task. Moreover, the integration of edge/fog computing resourcesdoes still not exist.

4.3 Data Privacy at the Remote Surrogates: The data acquired by the sensors may contain some personal data of users e.g. health record of a patient. This data can also be misused by the IoT data processing platforms. The situation becomes more critical when data needs to be processed by the collaboration of edge/fog clouds and distant clouds which may practice different security policies.

4.4 State Synchronization from the IoT Devices: State synchronization at low intervals would generate bulk amount of datae.g. monitoring irrigation level at every seconds or at every minute. In contrast, state synchronization at large interval may overflow the water level in the fields. Under such circumstances, rigorous efforts need to be carried out for determining the optimal monitoring intervals.

5. Conclusion

The induction of IoT devices is gaining a vital role in the numerous domains of physical world. With the advancements in the data processing techniques like deep learning, these devices can be used for imparting more accurate and reliable

information. Since the standardization of IoT architecture is underway, therefore this paper has reviewed different layered architectures of IoT environments. In addition, it also highlighted the pros and cons of each. From the study, we found that there are several open challenges, particularly, vendor lock-in, computation platform heterogeneity, and data privacy at the remote surrogates; state synchronization frequencies are the most pertinent challenges that demand rigorous efforts for the widespread adoption of IoT devices.

References

[1] P. P. Ray, "A survey of IoT cloud platforms," Future Comput. Inform. J., vol. 1, no. 1, [pp. 35–46], Dec. 2016, doi: 10.1016/j.fcij.2017.02.001.

[2] K. Ashton, "That 'internet of things' thing," RFID J., vol. 22, no. 7, [pp. 97–114], 2009.

[3] R. Khan et al., "Future internet: the internet of things architecture, possible applications and key challenges," in 2012 10th international conference on fronlayers of information technology, 2012, [pp. 257–260].

[4] L. B. Bhajantri, "A comprehensive survey on resource management in internet of things," J. Telecommun. Inf. Technol., 2020.

[5] N. M. Kumar et al., "The Internet of Things: Insights into the building blocks, component interactions, and architecture layers," Procedia Comput. Sci., vol. 132,[pp. 109–117], 2018.

[6] A. Banafa, "IoT and blockchain convergence: benefits and challenges," IEEE Internet Things, vol. 9, 2017.

[7] H. Chen, et al., “A brief introduction to IoT gateway,” in IET international conference on communication technology and application (ICCTA 2011), 2011, [pp. 610–613].

[8] A. El-Moursy, et al., “Home Automation Using Augmented Reality (HAAR),” Wirel. Pers. Commun., vol. 124, [pp. 1–31], May 2022, doi: 10.1007/s11277-021-09419-7.

[9] C. Perera, et al., “Context Aware Computing for The Internet of Things: A Survey,” IEEE Commun. Surv. Tutor., vol. 16, no. 1, [pp. 414–454], 2014, doi: 10.1109/SURV.2013.042313.00197.

[10] S. Poorana Senthilkumar et al., “Study on IoT Architecture, Application Protocol and Energy needs,” Int J Sci Res Netw. Secur. Commun. Vol, vol. 8, no. 5, 2020.

[11] M. Burhan, et al., “IoT Elements, Layered Architectures and Security Issues: A Comprehensive Survey,” Sensors, vol. 18, no. 9, Art. no. 9, Sep. 2018, doi: 10.3390/s18092796.

[12] O. Said et al., “Towards internet of things: Survey and future vision,” Int. J. Comput. Netw., vol. 5, no. 1, [pp. 1–17], 2013.

[13] D. Darwish, “Improved layered architecture for Internet of Things,” Int J Comput Acad ResIJCAR, vol. 4, [pp. 214–223], 2015.

[14] F. Alshohoumi, et al., “Systematic review of existing IoT architectures security and privacy issues and concerns,” Int. J. Adv. Comput. Sci. Appl., vol. 10, no. 7, 2019.

[15] M. Wu, et al., “Research on the architecture of Internet of Things,” in 2010 3rd international conference on advanced computer theory and engineering (ICACTE), 2010, vol. 5, [pp. V5-484].

[16] H. Muccini et al., “Iot architectural styles,” in European Conference on Software Architecture, 2018, [pp. 68–85].

[17] A. Al-Fuqaha, et al., “Internet of things: A survey on enabling technologies, protocols, and applications,” IEEE Commun. Surv. Tutor., vol. 17, no. 4, [pp. 2347–2376], 2015.

[18] N. V. Titovskaia, et al., “Application of the IoT technology in agriculture,” IOP Conf. Ser. Earth Environ. Sci., vol. 548, no. 3, [p. 032021], Aug. 2020, doi: 10.1088/1755-1315/548/3/032021.

[19] J. Pan et al., “Future edge cloud and edge computing for internet of things applications,” IEEE Internet Things J., vol. 5, no. 1, [pp. 439–449], 2017.

[20] M. A. Pisching, et al., “An architecture based on RAMI 4.0 to discover equipment to process operations required by products,” Comput. Ind. Eng., vol. 125, [pp. 574–591], 2018.

[21] B. Mishra et al., “The Use of MQTT in M2M and IoT Systems: A Survey,” IEEE Access, vol. 8, [pp. 201071–201086], 2020, doi: 10.1109/ACCESS.2020.3035849.