Proc. 1st International Conference on
Machine Learning and Data Engineering (iCMLDE2017)
20-22 Nov 2017, Sydney, Australia
ISBN: 978-0-6480147-3-7

A Survey on Cloud, Fog Computing and Internet of Things: An Architectural Viewpoint

Mohammad Sanaullah Chowdhury[1] and Ata Ullah[2]
[1]Department of Computer Science and Engineering, University of Chittagong, Chittagong, Bangladesh
[2]Dept. of Computer Science and Engineering, International Islamic University Chittagong, Bangladesh

Corresponding author's E-mail: sana1691@gmail.com

Abstract

It is the era of competitive technology, it is the era of cloud computing and smart world. The Internet of Things (IoT) provides the opportunity to connect billions of different types of every day's objects (things) with one another as well as with the Internet directly or through Local Area Network (LAN), paving a smooth and easy way to interact and share data and information. The primary concept of IoT is the pervasive presence of various types of wireless objects and embedded devices around us. However, the ultimate success of this IoT smart sensing environment depends heavily on a generally accepted, well-defined standard architecture that can provide a dynamic, scalable and secure framework for deployment of IoT. Full deployment of IoT and its applications in real life environment is not an easy task due to the limitations, challenges and security issues. IoT in collaboration with Fog computing and Cloud computing paradigm, revolutionizes the technology into a completely new dimension. In this paper, we discuss the employing and deploying of intelligent smart IoT devices in combination with Cloud and Fog computing paradigm. We also presented an improved and latency-minimized version of the Cloud and Fog centric IoT architecture. We then briefed on security and privacy issues along with challenges and future opportunities.

Keywords: Cloud Computing; Internet of Things; IoT; Fog Computing; Ambient Intelligence, Pervasive Computing.

1. INTRODUCTION

Nowadays, everything around us is going to be smart, can share data, information and services with one another. Of course this advancement facilitates improvement of public affairs. People can exchange information on the fly, can update themselves with the latest discount in shopping, instant traffic jam situation on the road, can access public health care info, can retrieve data and environment info from sensors, actuators and household appliances etc. All these are made possible due to the active participation of smart and intelligent devices comprising IoT. IoT is a dynamic network that connects smart physical objects (things) with high intelligence making use of the Internet. IoT devices doesn't necessarily need to be connected to the Internet, rather they can connect with each other through Bluetooth, ZigBee and NFC etc. You can control televisions, cameras, game consoles, cars, even washing machines from remote places. Your fridge can inform you about the kitchen-shopping list. The IoT goes far beyond that, with the help of sensor a farmer can know the conditions of the field by reading the data sent by the temperature and humidity sensor installed in the field [1].

Cloud computing, the next generational step in Information Technology [2], has emerged as the latest distributed computing model providing redundant, inexpensive and scalable resources on demand. As Cloud provides scalable storage and various computational resources IoT devices are able to implement a full scale ubiquitous computing environment [3]. On the other hand, Fog Computing is a

computing model similar to Cloud computing but at the edge of the networks and very close to the end users. It is specially created to focus on the IoT. As the IoT devices can transfer very huge amounts of data and computation offloading, and frequently need a very immediate response. Fog Computing paradigm is invented to work with IoT.
Rest of the paper is organized as follows. Section 2 reviews the background of IoT, Cloud and Fog computing systems. Section 3 explores the relevant architecture, while section 4 focuses on the security and privacy issues. Section 5 discussed the challenges and section 6 concludes the paper.

2. BACKGROUND

2.1. Internet of Things (IoT)

IoT is the concept of inter-connecting various devices and objects (things) together. The devices can be heterogeneous in nature and not necessarily needed to be connected to the Internet [4]. IoT devices are naturally connected via Wi-Fi, Bluetooth, ZigBee, Near Field Communications (NFC) and ZWave etc. The devices may be Smartphone, tablet, laptop, sensors, actuators etc. IoT devices can collect data and various sensitive information and share with other devices for further processes.

2.2. Cloud Computing

Cloud computing is a computing paradigm that provides scalable virtualized resources such as infrastructure, software, storage, database, servers and networks as per user's need via Internet technology. Based on the architecture and service providing system, there are 4 different types of service model, viz., 1) IaaS (Infrastructure as a Service), 2) PaaS (Platform as a Service) and 3) SaaS (Software as a Service). Cloud are becoming so popular and useful that private-public sectors are developing innovative technology to support industrialization, even in so many countries government facilities are moving towards the centralized cloud infrastructure.

2.3. Fog Computing

Fog computing is a paradigm similar to cloud computing typically located between the end users and traditional cloud data centers, but at the edge of the network [5] [6]. Fog computing also provides services such as data, computation, software and storage services on demand basis via Internet. Fog computing also enhanced Quality of Services (QoS) and location awareness for streaming and real-time applications. When IoT devices are connected to Fog server rather than Cloud data-centers, the latency and bandwidth can be reduced significantly as the Fog is situated at the vicinity [7] [8].

2.4. IoT with Cloud and Fog Computing

Due to the limitations of IoT devices, such as – battery life, computation, heat dissipation, limited storage – remote Cloud (Cloud computing) along with local Cloud (Fog computing) platforms are often employed to manage the data processing and storage needs. As the Cloud provides scalable storage and complicated computational resources big data processing, data analytics works, data mining and machine learning related resource-intensive processing can be performed seamlessly in Cloud-centric loT. There are so many examples of implemented and concept-level projects using the IoT and Cloud and/or Fog as main communication platform. Some name of the projects and applications are:
- **Vehicular Fog Computing Networks** to deliver flyer ads and discount offers of the stores to the mobile users through WiFi.
- **Wearable devices** such as fitness trackers, smart watches, augmented reality glasses etc.
- **Wireless Sensor and Actuator Networks** (WSAN),

- **Smart Homes and Smart Buildings** projects which focuses on the citizens' issues by collecting application specific data, e.g. public parking monitoring; microclimate monitoring; access and mobility (pedestrian, cyclists, cars and freight vehicles), and real-time public transport data etc.
- **Cloud based Smart city** also focuses on Health Care Services (hospitals and personal care); City Safety and Environmental situations (noise, air and water quality); Sustainability and Utilities (better energy usage); Transport (personal and logistics); Smart Farming and many more [3].

3. ARCHITECTURE

IoT experts proposed various types of architecture such as, four-layer based smart object oriented architecture, five-layer architecture, SOA based architecture as well as middle-ware based architecture [9]. The three-layer architecture is shown in fig. 1(a), and five-layer architecture is shown in fig. 1(b). As IoT devices can be heterogeneous and distributed in large geographical area but are connected to each other comprising LAN through short range and low power-consuming services like NFC, Bluetooth etc., the Internet connectivity is done by use of any other access point such as Roadside Unit (RSU). To better grasp the working process and architecture of this emerging IoT field, one should understand its primary building blocks. Six primary building blocks of IoT are (1) Identification, (2) Sensing, (3) Communication, (4) Computation or Processing, (5) Services, (6) Semantics or Knowledge Extraction. We presented them in fig. 2.

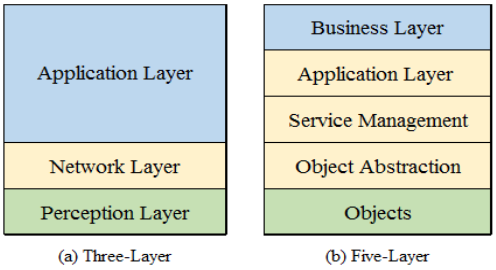

Figure 1. The architecture of IoT

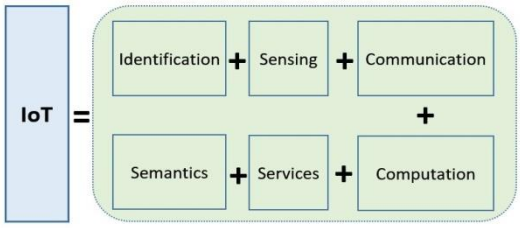

Figure 2. IoT elements

The end user device networks of IoT applications are dispersed in large-scale under geographically distributed network where devices are interconnected with Bluetooth, Zigbee, NFC, etc. Although these devices do not have direct Internet access, they keep generating application data and store it temporarily in local devices. Then they periodically send these data to the local cloud for further process. The existing architecture of IoT state that every things will send and receive data directly to and from Cloud data centers. But this is not possible for the local objects which has no Internet connectivity. As all IoT devices can communicate with each other via low-power-consuming technologies, placing a mobile device that can provide Internet facilities for communication with Cloud will help better for every type of IoT devices to function smoothly. [3] Introduced such a layer named as Mobile Access Points (MAP) for data collection and uploading process. MAP is a smart device with Internet access and travels among LANs of devices to collects all the application data generated by IoT devices and kept the data in a queue for uploading to the cloud.

As communication with the Cloud need stable Internet connection with higher bandwidth, moving IoT objects are often unable to achieve the expected result within due time. In some cases, such delay in communication process may be life threating (e.g. autonomous vehicles controlling system, vehicle-to-vehicle communication system or large-scale distributed rail network control system). That's why a closer to the end devices, low bandwidth consuming data processing system is needed. We deployed Fog platform for this purpose and proposed an enhanced architecture for low latency IoT environment with Fog computing. Fig. 3 depicted the roles of Fog computing and the cloud data-centers to deliver faster IoT services with low bandwidth. The proposed architecture is able to perform low latency computation and quickly store and retrieve data between end devices and Fog gateways. Fog gateways can play a vital role due to the following features [8]:
- Able to act as a mobile cloud as it is located at the edge of the networks and close to the IoT devices.
- Low setup price compared to the large cloud data-centers.

- Easily scalable and able to provide better performance for real-time interactive services.
- Fog servers can interoperate with all cloud providers with different deployment types.
- Smoothly perform data aggregation works and able to send partially processed result data to other Fog server or IoT objects instantly.

The deployment of Fog computing architecture between smart IoT devices and cloud platforms can increase the speed of computation services into manifold. Even big-data generated by billions of smart IoT devices can be transmitted and processed smoothly. We depicted the enhanced architecture in fig. 4, where all the end devices will comprise into various LAN according to their geographical locations. There will be a device such as Roadside Units (RSU) that will act as a Mobile Access Point (MAP). IoT devices will be able to connect and share the data with the MAP anytime via any low power wireless communication protocol such as Bluetooth, Zigbee etc. MAP will then perform offloading the data to the nearest Fog server for storage and computation.

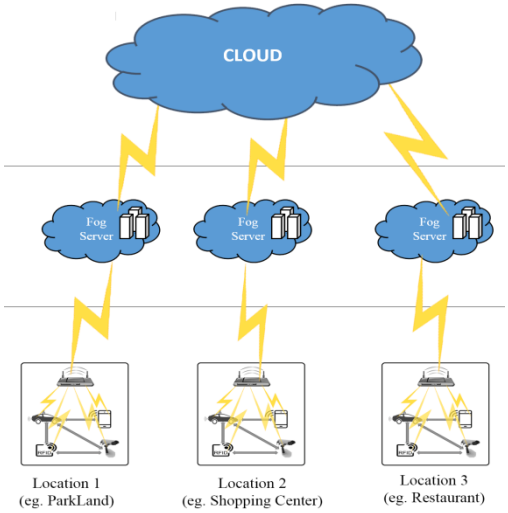

Figure 3. Roles of Fog Computing in IoT

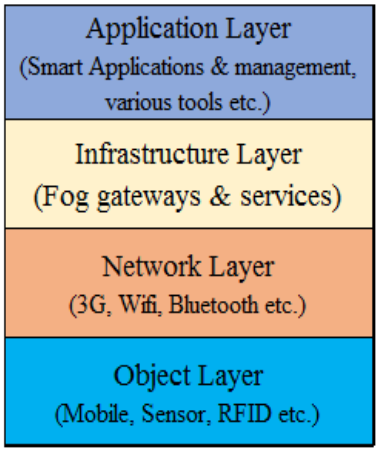

Figure 4. Four-Layer IoT architecture

4. SECURITY AND PRIVACY ISSUES

IoT is comprised of not only mobile devices and wearable objects, rather hundreds of thousands of sensors, integrated or embedded devices connected for a wide variety of tasks. The rapid growth of IoT faces different challenges and risk not only for the large companies and private sector, but also for the security and privacy of individual users of these devices. Visibility awareness and safety risk, public cloud vulnerability, security of confidential information, application security as well as authentication and authorization are most vulnerable fields targetable by the intruders. A recent study by HP [10] shows that 90% of devices collected at least one piece of personal information via the device, Cloud or its mobile application. 80% of devices raised privacy concerns while 70% of the devices does not encrypt the data, leading to increased problems of security. To make the IoT more secure, [11] recommended six actions for the companies, viz.,

i) Adopt a comprehensive framework, proactive, enterprise-wide strategy for securing the IoT.
ii) To run a full security audit to assess the complete IoT deployment (i.e. IoT devices, network infrastructure, mobile, web and cloud touch points etc.).
iii) Security procedures need to be instilled before deployment of the device.
iv) Mobilize the larger workforce (i.e. employees of product design, the supply chain, production and other traditional parts of the organization) around IoT security.
v) It need to ensure that customers, suppliers and others partners strictly adhere to standards of security.
vi) To change the role of IT as a skilled partner rather than service provider.

5. CHALLENGES

Efforts have been made by World Wide Web Consortium (W3C), Internet Engineering Task Force (IETF), EPCglobal, Institute of Electrical and Electronics Engineers (IEEE) and the European Telecommunications Standards Institute (ETSI) to create their individual protocol model for IoT, but unfortunately till now there is no common and generally accepted model protocol. Even though there are so many things to be considered as important for establishment process of IoT frameworks, making a standard IoT architecture and standardization of IoT protocol is very urgent. In this paper, we already explored and focused all the latest Cloud-oriented IoT innovative technologies, currently undergoing projects and concepts. Wide and fast spread of IoT applications in everywhere emerges several types of challenges both in technical and social arena. To adopt the future of IoT seamless and reliable, all these challenges needed to be overcome. The challenges currently facing by IoT are discussed below.

Availability: IoT functionalities must be available both in software and Hardware level. IoT applications must have the ability of providing services for everyone simultaneously at different places (i.e. everyone, everywhere and everything style).

Mobility: As IoT comprise with mobile devices, mobility challenge is highly concerned. For a moving object (thing), changing of fog gateway while processing services or transferring data might cause serious interruption or even loss of data.

The big data problem: Instant computation and real-time processing of the big data generated or collected by IoT devices is still a challenge.

Performance: Evaluation of heterogeneous IoT systems is still a very crucial thing as it depends not only on single system rather all the end devices, protocols and many other components and technologies.

Management: Managing billions of heterogeneous devices are an incredible task.

Reliability: For communication of IoT devices reliability is a very must important scheme without which processing of computation, transmission of data, and gathering of information may eventually lead to wrong direction forcing the ultimate result into unexpected or garbage.

Some more additional issues end users may face include but not limited to are: - privacy and trustworthiness issues, security problem, universal standard connectivity issue, lack of common architecture and lightweight protocol, power management etc.

6. CONCLUSION

The IoT is virtually making our environment ubiquitous systems integrating with Cloud and Fog computing paradigm. IoT have radically transformed many aspects of our daily lives. From a positive point of view, we have seen a wide range of applications and – from Nano-to-Mega devices, from shirt collar to bed, from home refrigerator to fire alarm – talking with every surrounding thing; making them smart and responsive. On the other hand, it imposes a great potential vulnerabilities and insecurities on privacy of individuals. Even though, several world class technology giants are working hard to make the IoT a well adopted secured form, it still need a lot of things to be done in order to fulfill the original vision of IoT. Lack of generally accepted model architecture is also hindering in progress of IoT's advancement. A common and standard model architecture, backward compatible system, and secure and reliable frameworks are needed to achieve the expected reality of IoT concept. In this paper, we have explored the existing architectures of IoT along with the IoT elements and building blocks generally deemed as well-adapted forms to suit IoT's requirements, and also provided an overview on proposed low latency architecture.

In future, we would like to implement a Fog computing oriented framework that will be able to interact with billions of smart devices from different manufacturers, of different throughput, having multiple communication protocols that can handle the various types of challenges.

7. REFERENCES

Tsai CW, Lai CF, Athanasios V. Vasilakos (2014). Future Internet of Things: open issues and challenges, Springer Science+Business Media New York.

Armbrust M, Fox A, Griffith R, Joseph AD, Katz R, Konwinski A, et al. (2010). A View of Cloud Computing, Communication of the ACM, vol. 53, pp. 50-58.

Yuan D, Jin J, Grundy J, Yang Y (2015). A Framework for Convergence of Cloud Services and Internet of Things, 19th International Conference on Computer Supported Cooperative Work in Design (CSCWD), pp. 349-354.

Carrillo E, Benitez V, Mendoza C, Pacheco J (2015). IoT framework for Smart Buildings with Cloud Computing, IEEE Smart Cities Conference (ISC2).

Al-Fuqaha A, Guizani M, Mohammadi M, Aledhari M, Ayyash M (2015). Internet of Things: A Survey on Enabling Technologies, Protocols and Applications, in IEEE Communications Surveys & Tutorials.

Stojmenovic I, Wen S (2014). The Fog Computing Paradigm: Scenarios and Security Issues, IEEE, Federated Conference on Computer Science and Information Systems, pp. 1–8.

Bonomi F, Milito R, Zhu J, Addepalli S (2012). Fog computing and its role in the internet of things, First Edition of the MCC Workshop on Mobile Cloud Computing, ser. MCC'12. ACM, pp. 13–16.

Yi S, Li C, Li Q (2015). A survey of Fog computing: Concepts, Applications and issues, ACM.

Babu SM, Lakshmi AJ, Rao BT (2015). A Study on Cloud based Internet of Things: CloudIoT. Global Conference on Communication Technologies (GCCT 2015), pp. 60-65.

Hewlett Packard Enterprise Security Research Report (2015). Accessed via http://www8.hp.com/h20195/V2/GetPDF.aspx/4AA5-4759ENW.pdf on 09-06-2016.

Securing Internet of Things: A report from The Economist Intelligence Unit & Hewlett Packard Enterprise (2016). Accessed via http://hpe-enterpriseforward.com/eiu-securing-iot/ on 08-07-2016.