International Journal of Smart Home
Vol. 10, No. 2, (2016), pp. 187-196
http://dx.doi.org/10.14257/ijsh.2016.10.2.18

From Cloud to Fog and IoT-Based Real-Time U-Healthcare Monitoring for Smart Homes and Hospitals

Chandra Sukanya Nandyala[1] and Haeng-Kon Kim[1*]

[1]*School of Information Technology, Catholic University of Daegu, Korea*
[1]*sukanya.chandu@gmail.com,*[1*]*hangkon@cu.ac.kr*

Abstract

Healthcare in the past, decision making was merely based on doctor's personal experience, domain knowledge, patient's physical signs and symptoms and diagnostic laboratory reports. In contrast, devices or things and technologies came into existence playing significant role and helps doctors or physicians to add wisdom to their decision in healthcare monitoring. Cloud paradigm stands as the backbone for on-demand network use of a shared pool of configurable computing resources (e.g., networks, servers, storage, applications, and services) in U-healthcare monitoring system architectures but attached limitations which are solved by Fog(significant extension of cloud). This paper proposed architecture for IoT based u-healthcare monitoring with the motivation and advantages of Cloud to Fog(C2F) computing which interacts more by serving closer to the edge (end points) at smart Homes and Hospitals.

Keywords*: Internet of Things (IoT), U-Healthcare Monitoring, Fog Computing, Cloud Computing, Smart Homes, Smart Hospitals*

1. Introduction

In today's world, the way to store and retrieve or access personal as well as other information has captured a massive revolution. Carrying the personal/official data on a physical device has become outdated with the rapid growth of network and users can connect virtually to data from anywhere and anyplace. That how cloud computing has emerged and widespread to meet the demand of latency, reliability, security and efficiency.

From the past few years, Cloud computing has served abundant opportunities for business by providing users a wide length of computing services. It also overcomes platform dependency problems with no software installation on user side which makes enterprise applications mobile and collaborative. The pay only for service used model becomes an economical substitute for managing and be responsible for data centers to web applications and batch processing users [3]. With the less maintenance and cost based on service usage, cloud computing's layered architecture allows the client to purchase services at different levels such as IaaS, PaaS and SaaS, depending upon their customer requirements. It permits location independence facility as users can access these services anywhere with an internet connection and a web browser. But the problem is too much data is going to strike in coming years.

Increase in the huge number of devices getting connected to the network is mainly by two sources: Devices and sensors or actuators. In IoT, devices assemble and communicate information directly with each other via internet and the cloud manages to collect record and analyze data blocks. But the 'things or devices' which are producing massive amount of data is blowing out day-to-day that needs to be treated, managed, analyzed and stocked at cloud. For example, Boeing 787 creates half a terabyte of data/flight says Virgin

* Corresponding Author

ISSN: 1975-4094 IJSH

Atlantic [4]. According to statistics: Back in 2008, there are already more objects connected to the Internet than people. This year, 4.9 billion connected things. The number will reach or exceed 50 billion by 2020[1]. The outbreak in the number of devices/person is interpreted by the generation of mobile devices like mobile phones and tablets. From [10], 30.7 % of IoT devices found in Healthcare and 69.7% of IoT devices found elsewhere (Business, Manufacturing, Retail, Security and Transportation) and this shows the constantly growing of loads of data.

From [8], IoT devices generate data constantly, and often analysis must be very rapid. Handling the volume, variety, and velocity of IoT data requires a new computing model. The main requirements are to:

- **Minimize Latency:** Analyzing data close to the device that collected the data can make the difference between averting disaster and a cascading system failure.
- **Conserve Network Bandwidth:** Offshore oilrigs generate 500 GB of data weekly. It is not practical to transport vast amounts of data from thousands or hundreds of thousands of edge devices to the cloud. Nor is it necessary, because many critical analyses do not require cloud-scale processing and storage.
- **Address Security Concerns:** IoT data needs to be protected both in transit and at rest. This requires monitoring and automated response across the entire attack continuum: before, during, and after.
- **Operate Reliably:** IoT data is increasingly used for decisions affecting citizen safety and critical infrastructure. The integrity and availability of the infrastructure and data cannot be in question.
- **Move Data to the best Place for Processing:** Which place is best depends partly on how quickly a decision is needed. Extremely time-sensitive decisions should be made closer to the things producing and acting on the data. In contrast, big data analytics on historical data needs the computing and storage resources of the cloud.

Traditional cloud computing architectures do not meet all of these requirements. The prevailing approach—moving all data from the network edge to the data center for processing—adds latency. Traffic from thousands of devices soon outstrips bandwidth capacity. In addition, cloud servers communicate only with IP, not the countless other protocols used by IoT devices. The ideal place to analyze most IoT data is near the devices that produce and act on that data. We call it Fog computing.

This “fog computing” concept has been launch as a bridge linking IoT devices and far off data centers. IoT devices are producing large amount of data that is necessary to be processed. With this model, by treating and outlining the data to reduce quantity, improve value and purpose by processing some of by computation resources at the edge.

To certain extent the concept of fog computing is similar to cloud computing, both are created with virtual systems and contributes lot of the similar structures and features which supports the flexibility and scalability of on demand supplies of computation, storage and networking resources. Still with respect to demand emerging trend in networking, the two technologies have a wide barrier. Cloud computing frees the enterprises and their end users from the specification of many details, such as storage resources, computation limitation and network communication cost. However, this bliss becomes a problem for latency-sensitive, real-time applications, which require nodes in the vicinity to meet their delay requirements [2].

What about the security of these oceans of data, which is the main concern for any business because they do not only cause problem to their reputation and also constrained by the law to keep it safe. By registering to cloud, it provides the liberty of accessing data from service providers in any part of world. But this comfort comes with the peril of security and privacy. This triggers the idea of cutoff focusing on cloud and embarks figuring out how to store and operate the cascade of data that is being generated

by IoT these days. The advancement, CISCO recently delivered the vision of fog computing to enable applications on billions of connected devices, already connected in the Internet of Things, to run directly at the network edge [5].Fog computing, also known as fogging, is a distributed computing base in which application and its services are handled either at the network edge or in a remote data center. Fog is about interacting with the physical world. The Edge or Fog paradigm solves the problems by the simple idea of locating small servers called edge servers in the vicinity of the users and devices [2].The proposed architecture in this paper used Fog computing, the appropriate platform for a number of critical Internet of Things (IoT) services and applications in U-healthcare monitoring.

2. Motivation and Related Work

The emerging technologies: Cloud and Fog computing are in support to the IoT. Cloud computing [CC] enables researchers and businesses to use and maintain many resources remotely, reliably and at a low cost. The IoT employs a large number of embedded devices, like sensors and actuators that generate big data which in turn requires complex computations to extract knowledge. Therefore, the storage and computing resources of the cloud present the best choice for the IoT to store and process big data. Employing CC for the IoT is not an easy task due to the following challenges [12]:

- **Synchronization:** Synchronization between different cloud vendors presents a challenge to provide real-time services since services are built on top of various cloud platforms.
- **Standardization:** Standardizing CC also presents a significant challenge for IoT cloud-based services due having to interoperate with the various vendors.
- **Balancing:** Making a balance between general cloud service environments and IoT requirements presents another challenge due to the differences in infrastructure.
- **Reliability:** Security of IoT cloud-based services presents another challenge due to the differences in the security mechanisms between the IoT devices and the cloud platforms.
- **Management:** Managing CC and IoT systems is also a challenging factor due to the fact that both have different resources and components.
- **Enhancement:** Validating IoT cloud-based services is necessary to ensure providing good services that meet the customers' expectations.

The applications of Fog are as multiple as the IoT itself. Monitoring or analyzing data in real-time from network-connected things and initiating an action are something similar they have. Fog Computing is a highly virtualized platform that provides networking services between end devices and traditional Cloud Computing Data Centers, but not exclusively located at the edge of network.

Fog Computing can act as a bridge between smart devices and large-scale cloud computing and storage services. Through fog computing, it is possible to extend cloud computing services to the edge devices of the network. Because of their proximity to the end-users compared to the cloud data-centers, fog computing has the potential to offer services that deliver better delay performance. It should be emphasized here that, typically there is a significant difference in scale between the fog and the cloud such that the cloud has massive computational, storage and communications capabilities compared to the fog.

Figure 1 presents the idealized information and computing architecture supporting the future IoT applications and illustrates the role of Fog Computing. It defined key characteristics and vision of Fog Computing. The outlined features are mobility, heterogeneity, low latency, location awareness, large geographical distribution, multiple numbers of nodes, strong existence of streaming and real time applications. This paper

argued that the above aspects make the Fog the relevant platform for critical IoT services and applications namely Connected Vehicle, Smart Grid, Smart Cities, and general WSAN's. It envision the Fog to be a unifying platform, rich enough to deliver this new set of emerging services and enable the development of new applications [2].

Fog computing can serve as an optimal choice for the IoT designers for the following features [12]:

- **Location:** Fog resources are positioned between smart objects and the cloud data-centers; thus, providing better delay performance.
- **Distribution:** Since fog computing is based on "micro" centers with limited storage, processing and communication capabilities compared to the cloud, it is possible to deploy many such "micro" centers closer to the end-users as their cost is typically a small fraction compared to cloud data-centers.
- **Scalability:** Fog allows IoT systems to be more scalable such that as the number of end-users increase, the number of deployed "micro" fog centers can increase to cope with the increasing load. Such an increase cannot be achieved by the cloud because the deployment of new data-centers is cost prohibitive.
- **Density of devices:** Fog helps to provide resilient and replicated services.
- **Mobility support:** Fog resources act as a "mobile" cloud as it is located close to the end-users.
- **Real-time:** Fog has the potential to provide better performance for real-time interactive services.
- **Standardization:** Fog resources can interoperate with various cloud provides.
- **On the fly analysis:** Fog resources can perform data aggregation to send partially processed data as opposed to raw data to the cloud data-centers for further processing.

Therefore, fog computing has the potential to increase the overall performance of IoT applications as it tries to perform part of high level services which are offered by cloud inside the local resources.

In [7], it explains how Fog computing accompanies and extends Cloud Computing and they scrutinize key characteristics of Fog paradigm and examine some rich use cases like wind farm and smart traffic light system that motivated the need for Fog, emphasizing Fog's relevance to several verticals within IoT and Big Data space. Also present a high-level architecture description of Fog's software by underlining the different technology components required to reach the fog vision.

Actually what happens in Fog and Cloud Computing, below points helps in understanding [13]:

Fog Nodes:

1. Receive feeds from IoT devices using any protocol, in real time.
2. Run IoT-enabled applications for real-time control and analytics, with millisecond response time.
3. Provide transient storage often.
4. Send periodic data summaries to the cloud.

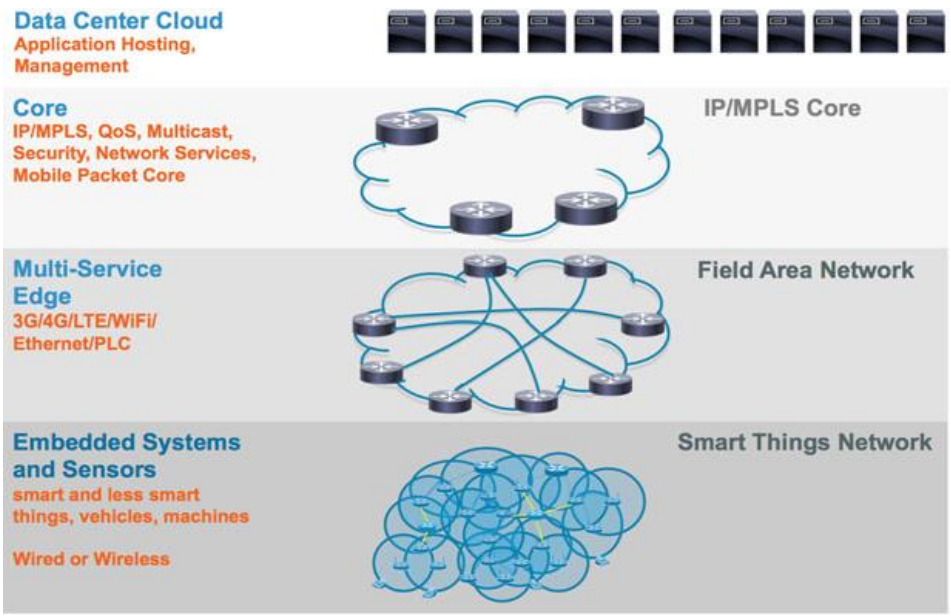

Figure 1. Cisco Fog and IoT Distributed Architecture [7]

Cloud Platform:

1. Receives and aggregates data summaries from many fog nodes.
2. Performs analysis on the IoT data and data from other sources to gain business insight.
3. Can send new application rules to the fog nodes based on these insights.

Data Interplay between Fog and Cloud

Fog collectors at the edge ingest the data generated by grid sensors and devices. Some of this data relates to protection and control loops that require real-time processing (from milliseconds to sub seconds). This first tier of the Fog, designed for machine-to-machine (M2M) interaction, collects, process the data, and issues control commands to the actuators. It also filters the data to be consumed locally, and sends the rest to the higher tiers. The second and third tiers deal with visualization and reporting (human-to-machine [HMI] interactions) as well as systems and processes (M2M). The time scales of these interactions, all part of the Fog, range from seconds to minutes (real-time analytics), and even days (transactional analytics). As a result of this the Fog must support several types of storage, from ephemeral at the lowest tier to semi-permanent at the highest tier.

We also note that the higher the tier, the wider the geographical coverage, and the longer the time scale. The ultimate, global coverage is provided by the Cloud, which is used as repository for data that that has a permanence of months and years, and which is the bases for business intelligence analytics. This is the typical HMI environment of reports and dashboards the display key performance indicators [2]. Below Table 1 concludes the differences between Cloud and Fog Computing [11]:

Table 1. Comparison of Cloud and Fog Computing

Main Features	Cloud Computing	Fog Computing
Server nodes location	Within the internet	At the local network edge
Density of nodes(If IoT devices are in millions)	Few(Hundreds)	Plenty(Thousands)
Distance between devices and server	Multiple steps	Single step
Latency	High	Low
Distribution	Centralized	Distributed
Scalability	Less(Big cloud centers - Cost prohibited)	More (Micro fog centers – Easy to deploy)
Mobility support	Limited	Supported
Real-time interactions	Supported	Supported
On the fly analysis	Data aggregation at cloud	Data aggregation partially and remaining to cloud
Security	Less secure	More secure
Attack on moving data	High probability	Very low probability

3. Proposed Cloud to Fog (C2F) Computing Model:

U-Healthcare monitoring finds a way in the Fog. The Architecture of a Fog and IoT-based real-time u-healthcare monitoring which can be used in smart hospitals or home is shown in Figure 2. There are 4 tiers in which this architecture gives reason of moving from cloud to fog and how it benefits the healthcare monitoring ubiquitously.

3.1. Tier 1: Smart Devices or Things Network

In this proposed C2F U-healthcare monitoring system, tier 1 is called as Health Sensor tier. This is designed for machine-to-machine (M2M) interaction, collects, process the data, and issues control commands to the actuators. It also filters the data to be consumed locally, and sends the rest to the higher tiers. It consists of "Things" (T in IoT) which means sensors and devices. Here the patient related health information is captured by networked sensors, either body worn or embedded in our daily living activities with which the patient is equipped for personal monitoring of multiple parameters. The captured data can be also augmented with situation information like time, temperature, date. Context-knowledge helps in identifying uncommon patterns and makes more accurate regarding the situation [6]. Remaining sensors and actuators like medical equipment also connected with the network to transfer data to medical staff like CAT scan *etc*.

It is essential to analyze and act on the data in less than a second which makes monitoring real-time and helps the patient/adult at hospital room/home and family members takes quick decisions at emergency times. This analysis of data from either body worn or embedded devices close to where they collected minimizes latency.

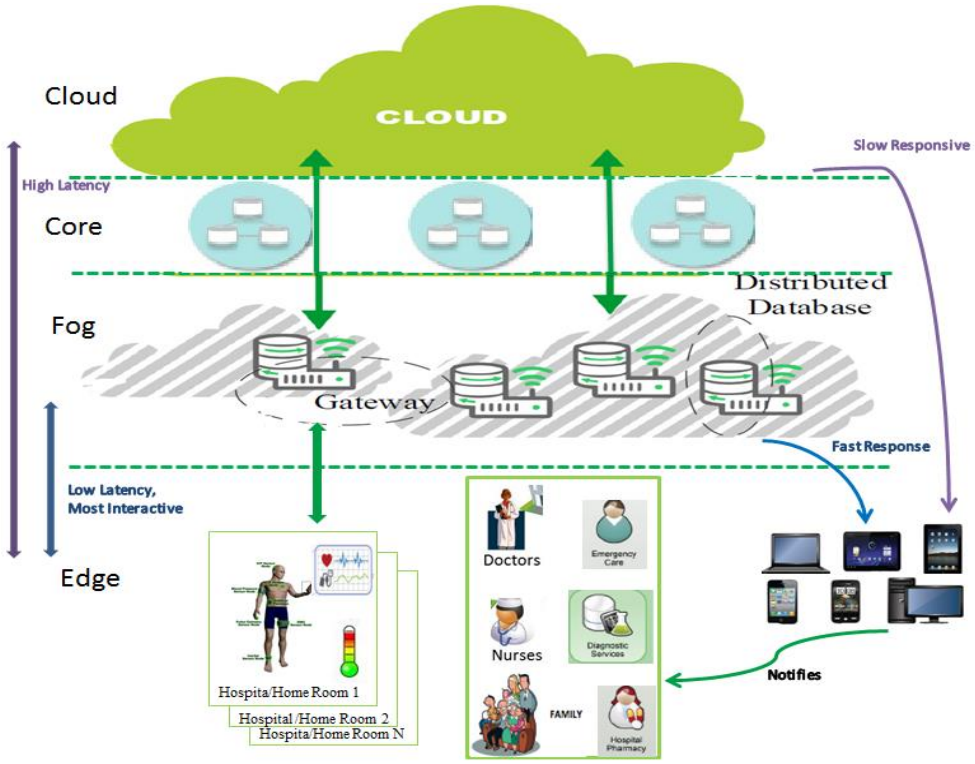

Figure 2. C2F Computing and IoT Based Architecture for Real-time U-Healthcare Monitoring

3.2. Tier 2: Fog

Fog (Edge) tier also called as multi-service edge. While Fog nodes provide localization, therefore enabling low latency and context awareness, the Cloud provides global centralization. Many applications require both Fog localization and Cloud globalization, particularly for analytics and Big Data. Let's take a scenario where health sensors, health actuators and health controllers are all exists within the fog. Health sensors collect data and forward that information to the controllers. The controller can forward any information gathered from the sensors to other devices in the Fog. The health controller is able to process this data locally, analyze and determine optimal health patterns to take action on it. Using this information the controller will send signals to actuators in the system to transmit data or notifies to medical staff and family members via mobile devices.

At this layer, cycle works like sensing, control and correlation. The variety and their potentially enormous numbers of endpoint devices spotlight the significance of the fog layer in the IoT architecture. This multi-service edge even supports both wired and wireless connectivity. In [14], even within two categories, this layer must support many different protocols, such as Zigbee, IEEE 802.11, 3G and 4G to accommodate a variety of endpoints. In some cases, the protocols used by endpoint devices may not even have any inherent security capabilities at all. It is imperative for security services to protect these inherently insecure endpoints. Additionally, this layer must be modular to scale to meet growth requirements. The components and services offered within one module should be similar so that additional modules can be added in a short span of time.

3.2.1. Why U-healthcare Considering C2F Computing in Monitoring

Fog overcomes some problems facing by cloud which makes itself a better paradigm. C2F computing benefits healthcare monitoring in following ways:

1. It is necessary to analyze and act on the data in milliseconds(less than a second).
2. Data collection is at the utmost edge: Homes, Hospitals and other examples like roads, railways, vehicles, ships, grids *etc*.
3. Thousands or millions or billions or trillions (in future) of things (either planted or wearable body sensors) across the world in our daily living activities are/will generating huge data.

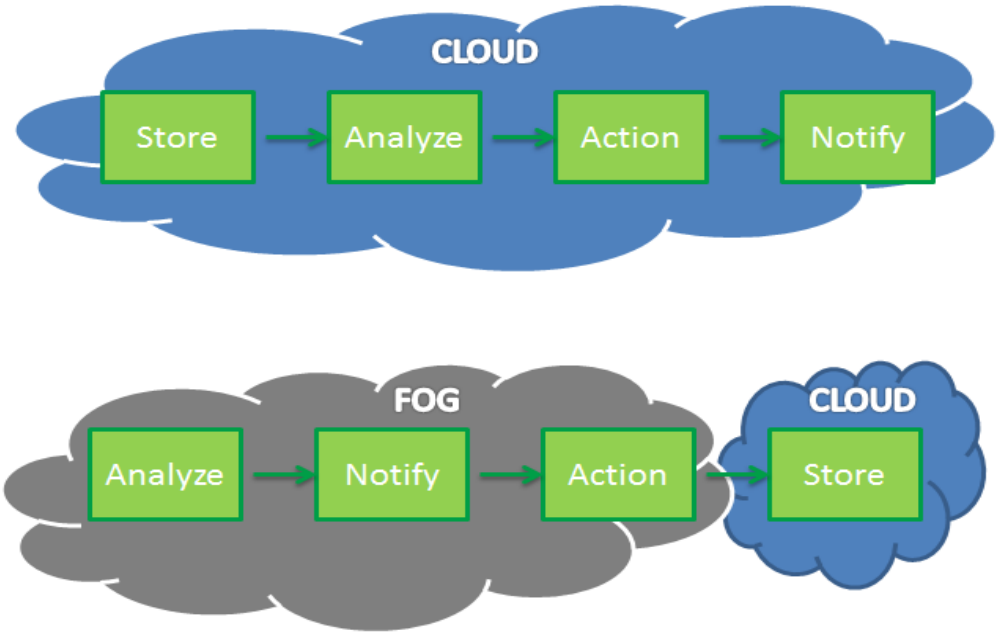

Figure 3. C2F Computing Model Move with Edge Intelligence

3.2.2. Essential Features between Cloud and Fog Computing

Data is an interesting thing, very difficult and very expensive to deliver. Analytics are changing [9]; a) Massive data that cannot move fast enough to analytics in cloud. So, move analytics to the data and b) Real-time actions processing computation closer to the sources. In Figure 3, the process in the Cloud (past) follows as: 1.Captures the data 2.Store the data in cloud and performs analytics 3.Decision making for action 4.Notify. But with the Fog (future), the process follows as: 1. Analyze the data 2. Notify 3. Decision to act on it 4.At last, the remaining data pass to the cloud for storage. This flow of data shows that enhancement in high latency problem to low. And faster response as it aggregates data partially at fog nodes with local transient storage happens often and sends the remaining data to cloud for further analysis.

In fact, this says that an application to the data and not that data to applications. In terms of computation, it is changing from “Where” to “How” which means, where computation happens? – In cloud (which is located far from things). Now, how computation happens? – Distributed analytics processing and computational complexity to ETL (Extract, Transform and Load) and only essential data information to the core. Why Distributed analytics processing? With this fog achieved these challenges: Improved scalability and reliability, faster response, flexible processing and low transport cost.

3.3. Tier 3: Core

This core network tier architecture is similar to architecture deployed in traditional networks. This tier tasks are to provide paths to carry as well as transfer data and network information between numerous sub-networks. The traffic profile is the critical variation between IoT and traditional core network layers.

In [14], Cisco explains the various securities protection against threats at this tier. The traffic and data in IoT may be different for example, unique protocols and variable packet size. Security services at the core network ensure that the IoT/M2M system as a whole, and has been hardened to protect against threats such as Man-in-the-middle (MITM), Impersonation (spoofing), Confidentiality compromise, Replay attack.

3.4. Tier 4: Cloud

The data center or cloud network tier architecture is similar to architecture deployed in traditional networks. This tier tasks are to host applications and to manage the IoT architecture. This tier contains data centers for network management and applications. From [8], as per the naming, the cloud is located up in the sky, somewhere distant and remote, fog is close to the ground where process works. This shows the space in between the user and the server is carried over multiple hops in cloud and it takes single hop in fog.

We also note that the higher the tier, the wider the geographical coverage, and the longer the time scale because of two reasons: 1.Analytics algorithms become slimmer as it moves to edge. 2. Data volume from edge to core (Filtering must take place at each time). In this proposed U-healthcare monitoring, Cloud collaboration helps in long term storage essential data information passed from fog for historical analysis of intelligent data for early detection of chronic diseases or other problems and for further treatment.

4. Conclusions and Future Work:

It is quite apparent that C2F computing is delivering more effectively compared to cloud by meeting present requirements of emerging models that require quick processing with fewer delay. They both co-exist, serving two different sectors and complementing each other wherever required. This paper examined key features of Fog computing and how Fog adds and extends Cloud computing as well as proposed an C2F architecture for U-healthcare monitoring for smart home and hospitals with both emerging paradigms by highlighting the description of different tier necessary to achieve the C2F vision key characteristics in real-time U-healthcare monitoring.

The further research aims to extend with elaboration of framework for C2F U-healthcare monitoring system or other use cases of Internet of Things with enhanced support and other elements or technologies combinations.

Acknowledgment

This research was Supported by the MSIP (Ministry of Science, ICT and Future Planning), Korea, under the C-ITRC (Convergence Information Technology Research Center) support program (IITP-2015-H8601-15-1007) supervised by the IITP (Institute for Information & communication Technology Promotion).

This research was also supported by the International Research & Development Program of the National Research Foundation of Korea (NRF) funded by the Ministry of Science, ICT & Future Planning (Grant number: K 2013079410).

References

[1] E. Dave, "The internet of things how the next evolution of the internet is changing everything". Technical report, CISCO IBSG, **(2011)**.
[2] F. Bonomi, R. Milito, J. Zhu, and S. Addepalli, "Fog computing and its role in the internet of things," Proceedings of the First Edition of the MCC Workshop on Mobile Cloud Computing, ser. MCC'12. ACM **(2012)**, pp. 13–16.
[3] M. Armbrust, A. Fox, R. Griffith, A. D. Joseph, R. Katz, A. Konwinski, G. Lee, D. Patterson, A. Rabkin, I. Stoica, and M. Zaharia, "A view of cloud computing," Commun. ACM, vol. 53, no. 4, **(2010)**, pp. 50–58.
[4] http://www.computerworlduk.com/news/data/boeing-787s-create-half-terabyte-of-data-per-flight-says-virgin-atlantic-3433595/.
[5] F. Bonomi, "Connected vehicles, the internet of things, and fog computing", Proceeding of the Eighth ACM International Workshop on Vehicular Inter-Networking (VANET), Las Vegas, USA **(2011)**.
[6] A.M. Rahmani , N.K. Thanigaivelan , T.N. Gia , G.Jose , N. Behailu, L. Pasi, and T. Hannu , "Smart e-Health Gateway: Bringing Intelligence to Internet-of-Things Based Ubiquitous Healthcare Systems", Proceedings of the 12th Annual IEEE Consumer Communications and Networking Conference (CCNC), **(2015)**.
[7] F. Bonomi, R. Milito, P. Natarajan, and J. Zhu. "Fog Computing: A Platform for Internet of Things and Analytics". Big Data and Internet of Things: A Roadmap for Smart Environments, Springer International Publishing, Studies in Computational Intelligence, Vol. 546, **(2014)**, pp.169–186.
[8] http://rankwatch.com/blog/evolution-of-cloud-to-fog-computing/.
[9] http://www.slideshare.net/MichaelEnescu/michael-enescu-cloud-io-t-at-ieee/8.
[10] http://www.slideshare.net/stockerpartnership/the-many-faces-of-internet-of-things-iot-in-healthcare/11
[11] L.M. Vaquero and L. Rodero-Merino, "Finding your way in the fog: Towards a comprehensive definition of fog computing." ACM SIGCOMM Computer Communication, Review 44 no.5 **(2014)**, pp. 27-32.
[12] A. Al-Fuqaha, M. Guizani, M. Mohammadi, M. Aledhari, M. Ayyash." Internet of things: A survey on enabling technologies, protocols, and applications". Communications Surveys & Tutorials, IEEE 17, no.4, **(2015**), pp: 2347-2376.
[13] Cisco, "Fog Computing and the Internet of Things: Extend the Cloud to Where the Things Are", White Paper, **(2015)**.
[14] http://www.cisco.com/web/about/security/intelligence/iot_framework.html.

Authors

Nandyala Chandra Sukanya, she received her Bachelor degree from National Institute of Technology, Warangal, India in 2012. She also worked as a software developer in AtoS India pvt Ltd. from 2012 to 2015. She is currently pursuing her M.S. degree with the Department of IT Engineering at Catholic University Of Daegu, Korea. Her research interests include IoT, Component Based Development, Design and Architecture of ubiquitous systems.

