Fog-Based IoT Sensor Integration Framework

Elena Vasquez, Kristof Janssen
University of Amsterdam, The Netherlands

Abstract—*The Internet of Things (IoT) interconnects various identifiable devices within Internet for sensing and monitoring processes. In particular, Wireless Sensor Network (WSN) is formed by connecting identifiable devices like smart sensor, embedded CPU (Central Processing Unit), low power radios, to the internet through gateway that interfaces WSN to the internet. To handle the large amount of data generated by devices in IOT environment, cloud infrastructure provides Sensing as a Service(SeaaS) which can make sensor data available in cloud infrastructure for sensing and observing the environment conditions. Today's cloud models are not designed for the volume, variety, and velocity of data that the IoT generates. Handling the volume, variety, and velocity of IoT data requires a new computing model. In this paper, we surveyed some typical applications of Sensor Network using Cloud computing as backbone spotlighting on fog computing to overcome some of the management issues of cloud computing and to handle time-sensitive data. Since Cloud computing provides plenty of application, platforms and infrastructure over the Internet, it may combined with Sensor network and fog computing in the application areas such as environmental monitoring, weather forecasting, transportation business, healthcare, military application etc which requires to handle within a second.*

Keywords—*WSN,cloud computing, fog computing, CSaaS, Internet of Things*

1. INTRODUCTION

As numerous devices and sensors get connected to the internet, IoT is becoming a key topic of interest. Many organization predicts that billions of devices will be connected to the internet by 2020.These devices and sensors will generate approximately 403 zetta bytes of data per year by 2018. In this fast-paced environment, the management of these devices, the networks, and the generated data is vital. As the management and provisioning of such sensor devices and data opens door to new business opportunities and possess new challenges, industry and academics must manage these interconnected devices. Due to the huge investment and high maintenance cost of sensor network restricts the user to build their own IOT systems.

Today, the boundaries between the physical world and the digital world continue to blur due to advances in the areas of ubiquitous computing and wireless sensor networks. The communication among sensor nodes using Internet is often a challenging issue. Hence, it makes a lot of sense to integrate sensor networks with Internet .At the same time the data of sensor network should be available at any time, at any place. It is possibly a difficult issue to assign address to the sensor nodes of large numbers; so sensor node may not establish connection with internet exclusively and it also not efficient in providing computation and storage properties [1].

Cloud computing can be the better solution to get rid of that problem. Since cloud computing provides a huge computing power and storage, we can integrate it with sensor network to resolve the problem of limited computation power and limited storage capacity. Sensor database system is integrated with cloud to provide database for cloud sensor network. To eliminate the computation constraint of WSN, cloud computing can be integrated. The deployment of WSN is provider specific i.e. providers define their own standard. Cloud is also integrated with WSN to provide a common data sharing and computation support platform.

Today's cloud models are not designed for the volume, variety, and velocity of data that the IoT generates. The prevailing approach—moving all data from the network edge to the data center for processing—adds latency. Traffic from thousands of devices also enhances the bandwidth capacity. Handling the volume, variety, and velocity of IoT data requires a new computing model, called Fog Computing.

Fog computing can be incorporate on the sensor-cloud infrastructure to reduce the above mentioned demerits of using cloud computation. The fog extends the cloud to be closer to the things that produce and act on IoT data, analyzing IoT data close to where it is collected minimizes latency. It offloads gigabytes of network traffic from the core network, hence reduces bandwidth capacity and it keeps sensitive data inside the network. This paper is organized as follows: Section 1 introduces to the evolution of various efficient computing paradigm in IoT. Section 2 depicts the overview of cloud computing and fog computing. Section 3 illustrates the issues of sensor-cloud and exaggerates the management issues of sensor-cloud. Section 4 illustrates the various applications that require cloud-sensor integration with fog computing for its efficient usage.

2. OVERVIEW OF COMPUTING

Numerous devices around us generate an enormous amount of data. The deployment of these devices in a communicating-actuating network creates IoT, in which sensors and actuators blend extremely with the environment around us, and the information is shared across platforms in order to develop a common operating picture[2]. IoT has been defined as object sensing, object identification, and communication of object specific information. The information is the sensed data related to temperature, orientation, motion, vibration, acceleration, humidity, chemical changes in the air, and so forth, depending on the type of sensors. A multitude of these sensors connected wirelessly form a sensor network. These sensor networks can be leveraged for a variety of applications. Some of these applications, mentioned in [3], are natural-disaster prediction, industrial applications, water-scarcity monitoring, smarthomes design, medical applications, agricultural applications, intelligent transport system design, smart-cities design, smart metering and monitoring, and smart security [4,5,6,7].

2.1 Sensor Network: Overview

A wireless sensor network (WSN) consists of spatially distributed autonomous sensors to cooperatively monitor environmental or physical conditions, such as sound, vibration, temperature, pressure, pollutants or motion. The development of WSN was motivated by military applications such as battlefield surveillance. They are now used in many civilian application areas and industrial application areas including industrial process control and monitoring, environment and habitat monitoring machine health monitoring , home automation, healthcare applications & traffic control. Each node in a WSN is typically equipped with a radio transceiver or a small microcontroller or other wireless communications device, and an energy source, usually a battery. Size and cost constraints on sensor nodes result in corresponding rules on resources such as memory, energy, speed and bandwidth [8]. The development of WSN requires technologies from three different research areas: sensing, computing (including hardware, software, and algorithms), and communication. Thus, combined and separate improvement in each of these areas has driven research in WSN.

The features of Wireless sensor networks are as follows:

1) Communication paradigm: Compared to traditional communication networks, individual node Identifiers (IDs) are not important. Instead, WSNs are data-centric meaning that the communication should be targeted to nodes in a given location or with defined data content.

2) Application specific: WSN is deployed to perform a particular task.

3) Dynamic nature: In typical WSNs, node platforms are error-prone due to harsh operating conditions. Communication links between nodes are not stable due to node errors, unreliable and simple modulations, mobility of nodes, and environmental interferences.

4) Scale and density: Compared to other wireless networks, the number of nodes comprising WSNs may be enormous. Further, the density of nodes can be more.

5) Resource constraints: A typical WSN node is small in physical size and battery powered. This implies that communication, computation, and memory resources in nodes are minimum.

6) Deployment: In large-scale WSNs, the deployment of nodes is arbitrary and their maintenance and replacement is unrealistic. Still, the requirements and applications of the deployed WSN may alter, which accuse that runtime reconfiguration and reprogramming are needed.

7) Lifetime: The nodes are battery powered or the energy is scavenged from the environment and their maintenance is very difficult. Thus, energy saving and load balancing must be taken into account in the implementation and design of WSN platforms, applications, and protocols.

8) Scalability: The number of nodes in WSN is typically very high. Thus, the WSN protocols must deal with very high densities and numbers of nodes.

9) Real-time: WSNs are closely related to the real world. Therefore, strict timing constraints for processing, sensing, and communication are present in WSNs.

10) Security: The need for security in WSNs is obvious, especially in security, health care, and military applications. Most of the applications relay data that contain private or confidential information.

2.2 .Cloud-Computing: Overview

Cloud computing has evolved as the future generation computing paradigm [9]. The NIST (National Institute of Standards and Technology, US) defines the concept of cloud computing as follows:

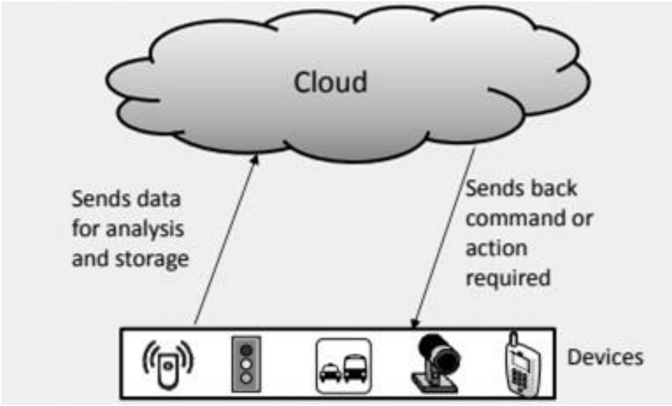

Figure 1. Present day cloud model

Cloud computing is a model for enabling convenient, on demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage applications and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction [10].

Cloud computing allows the systems and users to use Platform as a Service (PaaS) (e.g. Operating Systems (OSs)), Infrastructure as a Service (IaaS) (e.g. storages and servers) and Software as a Service (SAAS) (e.g. application level programs) and so forth at a very low cost which are being provided by several cloud providers (e.g., Amazon, Google and Microsoft) on the basis of pay per use services [11]. As Cloud provides a huge computing power and storage, we can integrate it with sensor network to resolve the problem of limited computation power and limited storage capacity as shown Figure 1.

The features of cloud-computing are as follows:

1) On-demand self-service: A consumer can unilaterally provision computing capabilities, such as server time and network storage, as needed automatically without requiring human interaction with each service provider.

2) Broad network access: Capabilities are available over the network and accessed through standard mechanisms that promote use by heterogeneous thin or thick client platforms (e.g., mobile phones, tablets, laptops and workstations).

3) Resource pooling [12]: The provider's computing resources are pooled to serve multiple consumers using a multi-tenant model, with different physical and virtual resources dynamically assigned and reassigned according to consumer demand. There is a sense of location independence in that the customer generally has no control or knowledge over the exact location of the provided resources but may be able to specify location at a higher level of abstraction (e.g., country, state or datacenter). Examples of resources include storage, processing, memory and network bandwidth.

4) Rapid elasticity: Capabilities can be elastically provisioned and released, in some cases automatically, to scale rapidly outward and inward commensurate with demand. To the consumer,

the capabilities available for provisioning often appear to be unlimited and can be appropriated in any quantity at any time.

5) Measured service: Cloud systems automatically control and optimize resource use by leveraging a metering capability at some level of abstraction appropriate to the type of service (e.g., storage, processing, bandwidth and active user accounts). Resource usage can be monitored, controlled and reported, providing transparency for the provider and consumer.

2.3 Fog-Computing: Overview

Fog computing[13] or fog networking, also known as fogging[14][15], is an architecture that uses one or more collaborative end-user clients or near-user edge devices to carry out a substantial amount of storage (rather than stored primarily in cloud data centers), communication (rather than routed over the internet backbone), control, configuration, measurement and management (rather than controlled primarily by network gateways such as those in the LTE core network). 40% of the whole world's data will come from sensors alone by 2020. 90% of the world's data were generated only during the period of last two years.2.5 quintillion bytes of data is generated per day. Total expenditure on IoT devices will be $1.7 Trillion by 2020. The total number of connected vehicles worldwide will be 250 million by 2020. There will be more than 30 billion IoT devices. The amount of data generated by IoT devices is simply huge.

Fog Computing is not any alternative or substitute for cloud-computing but it is used to enhance the efficiency of sensor –cloud infrastructure as shown in the Figure.2 and its architectural representation is shown in Figure 3.

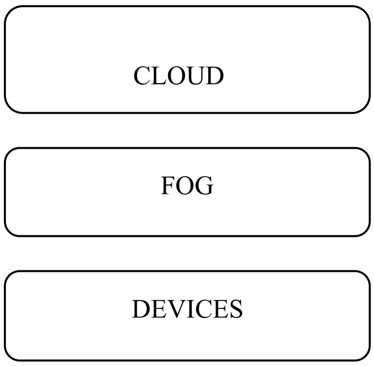

Figure 2. Fog Computing in Cloud

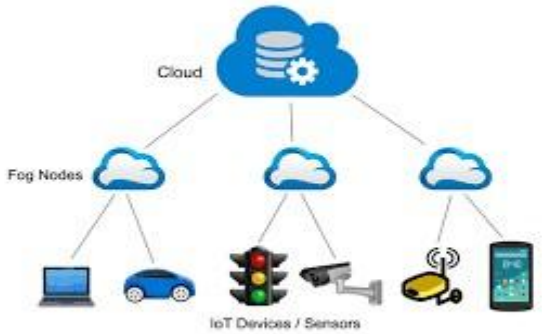

Figure 3. Architecture of Fog-Computing

Hierarchy of various types of sensors, fog computing, and cloud computing are represented in above Figure. It shows that the various IOT devices and sensors in lower layer, then fog computing nodes such as smart devices, hubs, routers, and gateways in middle layer and cloud servers are in higher layer.

Why Fog Computing?

The ability of the current cloud model is insufficient to handle the requirements of IoT. Issues are in terms of Volume, Latency, and Bandwidth. Cloud Sends data for analysis and storage, Sends back Command or action required.

Data Volume: By 2020, about 50 billion devices will be online. Presently billions of devices produce Exabyte of data every day. Device density is still increasing every day. Current cloud model is unable to process this amount of data.

Private firms, Factories, airplane companies' produces colossus amount of data every day.

Current cloud model cannot process these many data within a short period of time. As a result, Data need to be filtered; this can be done using neural networks for storage [16].

Latency: Latency is defined as a time taken by a data packet for a round trip. It is an important aspect for handling a time sensitive data. If edge devices send time sensitive data to cloud for analysis and wait for the cloud to give a proper action, then it can lead to many unwanted results. While handling time sensitive data, a millisecond can make huge differences by sending time-sensitive data to cloud for analysis. Consider the case of patient monitoring where the time sensitive data has to be analyzed within a second or millisecond. But in case of traditional cloud model, Latency will be increased. And it is given by,

$$\text{Latency} = T_{\text{from device to cloud}} + T_{\text{data analysis}} + T_{\text{from cloud to device}} \quad (1)$$

Where T = Time. Therefore, when the action reaches the device, accident may have already occurred.

Bandwidth: Bandwidth is defined as a bit_rate of data during transmission. If all the data generated by IoT devices are sent to cloud for storage and analysis, then, the traffic generated by these devices will be simply gigantic. Since billions of devices consuming bandwidth, it consumes almost all the bandwidths. Handling this kind of traffic will be simply a very hard task. If all the devices become online even IPv6 will not be able to provide facility to all the devices. Data may be confidential which the firms do not want to share online.

Fog-computing provides the following features:

Reduce latency of data: Appropriate actions at the right time prevent major accidents, machine failure etc. A minute delay while taking a decision makes a huge difference. Latency can be reduced by analyzing the data close to the data source.
Data security: IoT data must be secured and protected from the intruders. Data are required to be monitored 24x7. An appropriate action should be taken before the attack causes major harm to the network.
Data reliability: The data generated from IoT devices are used to solve real time problem. Integrity and availability of the data must be guaranteed. Unavailability and tampering of data can be hazardous.
Processing of data at respective suitable place: Data can be divided into three types based on sensitivity: Time sensitive data, less time sensitive data, data which are not time sensitive. Extremely time sensitive data should be analyzed very near to the data source. Data which are not time sensitive will be analyzed in the cloud.

Monitor data across large geographical area: The location of connected IoT devices can be spread across a large geographical region. Examples: monitoring the railway track of a country or a state. The devices are exposed to the harsh environments condition.

Table 1. Comparison of Fog and Cloud nodes

Features	For node closest to devices (fog nodes)	For aggregate nodes	Cloud
Analysis duration	Fraction of second	Seconds to minutes	Hours to weeks
IoT data storage duration	Transient	Hours to days	Months to years
Geographical coverage	Very local	Wider	Global

3. ISSUES ON SENSOR-CLOUD ENVIRONMENT

As we know that the sensor cloud is not only the mere integration of sensors and cloudcomputing or not only dumping the sensor data into cloud, but it is more than that the concept of virtualization of sensor node, Pay_per_use, one sensor node/network appears as many, an intermediate between sensor nodes and end_users. However sensor-cloud provides both the merits of wireless sensor network and cloud computing as well, but as we all know that every day must have its night, sensor-cloud also involves many issues that need to be inferred. Here in this paper we are going to discuss some of the management issues of sensor cloud.

- Optimal Composition of virtual sensor nodes[17]
- Data Caching [18]
- Optimal Pricing [19]

A) Optimal Composition of Virtual Sensor:

Optimal composition of virtual sensor (VS) is very essential because the Sense-Cloud is Resource_constrained with sensor nodes. Due to the dynamic change in sensor conditions, the composition of virtual sensors is non_traditional.

(i) Efficient virtualization of the physical sensor nodes:

Since sensor-cloud involves the virtualization of sensor. It needs to be virtualized properly. The Figure 4 represents the homogeneous sensor node within the same geographic region. Simply, the formation of virtual sensors must be incurred properly.

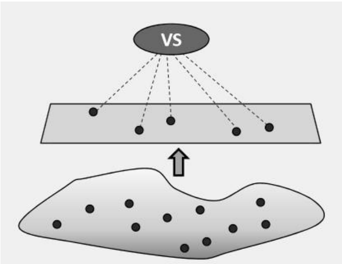

Figure 4.Formation of Virtual Sensors

(ii) An optimal composition of VSs:

Traditional sensor network involves virtualization of same sensor, software system. But in case of sensor-cloud, the nodes involved may be heterogeneous so grouping of the virtualized sensor needs special considerations.

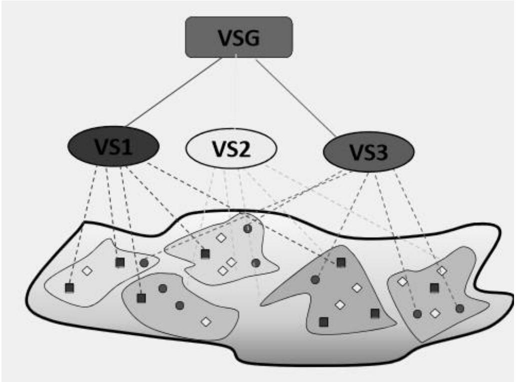

Figure.5.formation of virtual sensor group

The Figure 5 infers us the heterogeneous physical sensor nodes across different geographical locations. Simply, the formation of virtual sensor groups (VSG) must be incurred promptly.

(B) Dynamic and Adaptive Data Caching Mechanism

Dynamic and adaptive data caching mechanism can be processed by introducing internal and external caching mechanisms. This strategy ensures efficiency in resource utilization and flexible with the varied rate of change of the physical environment. It is carried out in order to reduce the energy consumption which is caused as end-users request for the sensed information through a Web_interface, Allocation of physical sensor nodes and virtualization cycle continues whenever it needs. Therefore, Physical sensor nodes continuously sense and transmit data to sensor_cloud which correspondingly leads to more energy consumption. Practically, in some cases, the change in environmental condition is significantly slow. Due to the slow change in environment, the sensed data of physical sensors unaltered. In such a situation, unnecessary sensing causes energy consumption.

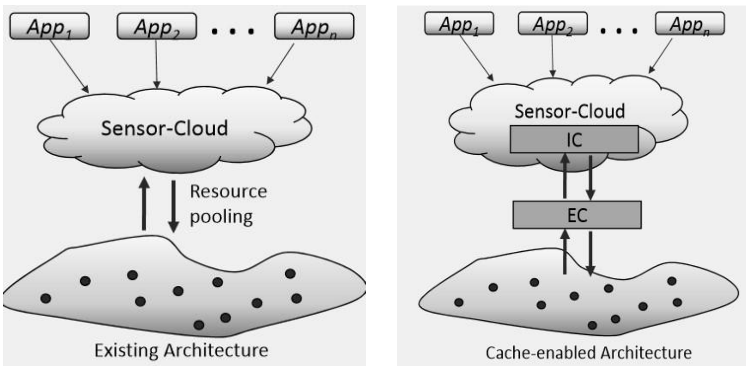

Figure 6.comparison of sensor-cloud architecture with cache-enabled architecture.

i) External and Internal Caching Mechanism:

Internal Cache(IC) handles requests from end_user takes decision whether the data should be provided directly to the end user or is it required to re_cache the data from external cache. External Cache (EC) is used to re-cache the data after certain interval of time. Initially, few data are used to be transmitted to IC in order to process the time-sensitive data. The Figure 6 compares the cache-enabled architecture with existing traditional architecture.

(C) Dynamic Optimal Pricing for Sensor-Cloud Infrastructure:

As cloud computing provides various homogeneity of service (e.g. for IaaS, SaaS), there is no scheme for sensing as a service (SeaaS).The proposed pricing scheme comprises of two components: pricing attributed to hardware (pH), pricing attributed to infrastructure (pI).

i) Pricing attributed to hardware (pH): It deals with the usage of physical sensor nodes.

ii) Pricing attribute to infrastructure (pI): It deals with the price associated with the infrastructure of the virtual sensor nodes or sense-cloud.

The goal of the proposed scheme is to maximize the profit of sensor-cloud service provider, maximizing the profit of sensor owner and end-user's satisfaction.

4. APPLICATIONS

A) **Ubiquitous Healthcare Monitoring**: Sensor-Clouds can be used for health monitoring by using a number of easily available and most often wearable sensors like accelerometer sensors, proximity, ambient light and temperature sensors and so forth to collect patient's health-related data for tracking sleep activity pattern, blood sugar, body temperature, and other respiratory conditions.

B) **Military Use:** Sensor networks are used in the military for Monitoring friendly forces, ammunition and equipment, Battlefield surveillance, inspection of opposing forces, Targeting, Battle damage evaluation and Nuclear, biological and chemical attack detection scouting etc .The data collected from these applications are of greatest importance and needs top level security which may not be provided using normal internet connectivity for security reason[20].

C) **Agriculture and irrigation Control System:** Sensor-Cloud can be used in the field of agriculture to monitor the crop fields in order to conservation it. For this a field server is developed that comprises of a temperature sensor, camera sensors, air sensor, soil moisture, CO2 concentration sensor, and temperature sensors etc. These sensors continuously upload the field data via Wi-Fi access point to the field owner to track the health of their crops. These sensors are used to match the needs of growers, farmers, and agricultural organizations. This reliable and robust irrigation control system enables monitoring and control over an unlimited number of field valves. This can also be used for harvesting [21].

D) **Earth Observation:** A sensor grid is developed for data gathering from several GPS stations, as well as to process, analyze, manage, and visualize the GPS data. This GPS data would then be uploaded onto the cloud for efficient monitoring, early warning, and decisionmaking capability for critical situations like the volcanic eruptions, earthquakes, tsunamis, cyclones, and so forth to the users all around the world.

E) **Wildlife Monitoring:** Sensor-Cloud can also be used for tracking the wildlife sanctuaries, forests, and so forth to regularly monitor the endangered species in real time.

F) **Weather Forecasting:** Weather forecasting is the application to predict the state of the atmosphere for a future time and a given location. Weather monitoring and forecasting system typically includes- Data collection, Data assimilation, Numerical weather prediction and Forecast presentation. The data collected from these sensors is huge in size and difficult to maintain using the traditional database approaches, and assimilation is done. The complied equations manage how the state of atmosphere changes [22].

5. CONCLUSION

Earlier, most WSN systems which were included to several calculating/monitoring schemes were closed in nature, minimum interoperability, and application specific and non extensible. However, integrating the existing sensors with cloud will enable an open, scalable, extensible, interoperable, and easy to use, re-constructible network of sensors for numerous applications. In this paper, we surveyed the use and advantages of Sensor- Cloud architecture in the context of several applications by harnessing fog computing on it. The Cloud Sensor architecture enables the sensor data to be stored categorized, and processed in such a way that it becomes timely efficient, commercial, and easily reachable.

REFERENCES

[1] J. Gubbi, R. Buyya, S. Marusic, and M. Palaniswami, “Internet of Things (IoT): a vision, architectural elements, and future directions,”Future Generation Computer Systems, vol.29, no.7, pp.1645–1660, 2013.

[2] R.Khan, S.U.Khan, R.Zaheer, and S.Khan, “Future internet: the internet of things architecture, possible applications and key challenges,” in Proceedings of the 10th IEEE International Conference on Frontiers of Information Technology (FIT’12), Islamabad, Pakistan,), pp.257-260,December 2012.

[3] X. Sheng, J. Tang, X. Xiao, and G. Xue, “Sensing as a service: challenges, solutions and future directions, ”IEEE Sensors Journal,vol.13,no.10, pp. 3733–3741,2013.

[4] M. A. E. Al-Fagih, F. M. Al-Turjman, W. M. Alsalih, and H. S. Hassanein, “Priced public sensing framework for heterogeneous IoT architectures, ”IEEE Transactions on Emerging Topics in Computing,vol.1,no.1,pp.133–147,2013.

[5] D.B.Hoang and L.Chen, “Mobile Cloud for Assistive Health-care(MoCAsH),” in Proceedings of the IEEE Asia-Pacific Services Computing Conference (APSCC ’10), Hangzhou, China, pp. 325–332, December 2010.

[6] B. B. P. Rao, P. Saluia, N. Sharma, A. Mittal, and S. V. Sharma, “Cloud computing for

Internet of Things & sensing based applications, ”in Proceedings of the 6th International Conference on Sensing Technology (ICST ’12), Kolkata, India, pp. 374–380, December 2012.
[8] J. Cheng, R.K. Balan, M. Satyanarayanan, “Exploiting rich mobile environments,Technical Report”, 2005.

[9] Alamri, A., Ansari, W, S., Hassan, M, M., Hossain, M, S., Alelaiwi, A., and Hossain, M, A., “A Survey on Sensor-Cloud: Architecture, Applications and Approaches”, International Journal of Distributed Sensor Networks, Vol.2013, pp.9-26, 2013.

[10] Dash, S, K., Sahoo, J, P., Mohapatra, S., and Pati, S, P., “Sensor-cloud: assimilation of wireless sensor network and the cloud”, Advances in Computer Science and Information Technology. Networks and Communications- Second International Conference, CCSIT 2012, Bangalore, India, Vol. 84, pp. 455-464, January 2-4, 2012.

[11] Dinh, H, T., Lee, C., Niyato, D., and Wang, P., “A Survey of Mobile Cloud Computing: Architecture, Applications, and Approaches”, Wireless Communications and Mobile Computing-Wiley Online Library, Vol: 13, Issue: 18, pp: 1587-1611, 2011.

[12] Gomathi, B.,Karthikeyan, K. and Saravana Balaji, B., “Epsilon-fuzzy dominance sortbased composite discrete artificial bee colony optimisation for multi-objective cloud task scheduling problem”, Int. J. Business Intelligence and Data Mining, Vol. 13, Nos. 1/2/3, pp.247–266,2018.

[13] Bar-Magen Numhauser, Jonathan, “Fog Computing introduction to a New Cloud Evolution”, Escrituras silenciadas: paisaje como historiografía. Spain: University of Alcala. pp. 111–126. *ISBN 978-84-15595-84-7,2012.*

07.

[14] LP Dinesh, S. Shakena Grace, Akshaya Krishnan, V. M. Manikandan, R. Chinraj, and M. R. Sumalatha. "Data filtering in wireless sensor networks using neural networks for storage in cloud. " In Recent Trends In Information Technology (ICRTIT), 2012 International Conference on, pp. 202-205.IEEE, 2012.

[15] S. Chatterjee and S. Misra, “Dynamic Optimal Composition of a Virtual Sensor for Effi cient Virtualization Within Sensor_cloud”, IEEE ICC 2015.

[16] S. Chatterjee, S. Misra, “Dynamic and Adaptive Data Caching Mechanism for Virtualiz ation within Sensor_Cloud”, IEEE ANTS 2014.

[17] S. Chatterjee, R. Ladia, and S. Misra, “Dynamic Optimal Pricing for Heterogeneous Ser vice_Oriented Architecture of Sensor_Cloud Infrastructure”, IEEE TSC 2017.

[18] Chee-Yee Chong; Kumar, S.P., "Sensor networks: Evolution, opportunities, and challenges, "Proc IEEE, August 2003.