National Conference on Recent Advances in Computer Science and IT (NCRACIT)
International Journal of Scientific Research in Computer Science, Engineering and Information Technology
© 2018 IJSRCSEIT | Volume 4 | Issue 1 | ISSN: 2456-3307

Fog Approach in Internet of Things: A Review

Rukhsana Thaker[1], Yusera Farooq Khan[2], Shafqat Mughal[3]

[13]Computer Science And Engineering, Computer Science And Engineering, SoET, BGSB University, Rajouri, J&K,India
[2]Electrical & Renewable Energy Engineering, SoET, BGSB University, Rajouri, J&K,India
[1]rukhsana@bgsbu.ac.in, [2]yusrakhan.205@gmail.com, [3]snmughal@bgsbu.ac.in

ABSTRACT

Internet of Things (IoT) connects billions of physical objects to collect and exchange data for various applications. IoT has many unsupported features such as geographic features, location, latency etc that are critical for various IoT application. To support these features fog computing is added to IoT. This review paper discusses the difference between cloud and fog and why fog is used over cloud for IoT. This paper discusses the architecture and features of fog computing for IoT applications. Security and privacy issues of fog related to various applications are also discussed.

Keywords: Fog computing, Internet of Things IoT, Cloud computing, security and Privacy

I. INTRODUCTION

The Internet of Things (IoT) is the network of physical devices, vehicles, home appliances and other items embedded with electronics, software, sensors, a ctuators, and connectivity which enable these objects to connect and exchange data. Each thing is uniquely identifiable through its embedded computing system but is able to inter-operate within the existing Internet infrastructure. The figure of online capable devices increased 31% from 2016 to 8.4 billion in 2017.Experts estimate that the IoT will consist of about 30 billion objects by 2020. It is also estimated that the global market value of IoT will reach $7.1 trillion by 2020. The IoT allows objects to be sensed or controlled remotely across existing network infrastructure, creating opportunities for more direct integration of the physical world into computer-based systems, and resulting in improved efficiency, accuracy and economic benefit in addition to reduced human intervention. When IoT is augmented with sensors and actuators, the technology becomes an instance of the more general class of cyber-physical systems, which also encompasses technologies such as smart grids, virtual power plants, smart homes, intelligent transportation and smart cities [10]. "Things", in the IoT sense, can refer to a wide variety of devices such as heart monitoring implants, biochip transponders on farm animals, cameras streaming live feeds of wild animals in coastal waters, automobiles with built-in sensors, DNA analysis devices for environmental/food/pathogen monitoring, or field operation devices that assist fire fighters in search and rescue operations. Legal scholars suggest regarding "things" as an "inextricable mixture of hardware, software, data and service"[9]. These devices collect useful data with the help of various existing technologies and then autonomously flow the data between other devices.

II. IOT REQUIRES NEW ARCHITECTURE

The emerging IoT introduces many new challenges that cannot be adequately addressed by today's cloud and host computing models alone [1].Some challenges are discussed below.

a) Low latency: Many IoT application requires latency between sensor and control node below milliseconds. Some IoT like vehicle-to-vehicle communication, vehicle to roadside application, real time application even requires latency time below 10^{th} of milliseconds and that is not possible in cloud computing.

b) Network bandwidth: Bandwidth is a big issue in IoT. More data required more bandwidth. The vast and rapidly growing number of connected things is creating data at an exponential rate. Sending all the data to the cloud will require prohibitively high network bandwidth. It is often unnecessary or sometimes prohibited due to regulations and data privacy concerns. ABI Research estimates that 90% of the data generated by the endpoints will be stored and processed locally rather than in the cloud.

c) Resource dependent devices: IoT devices have many limited resources. For example, sensors, relay, data collector, actuator, controllers, cameras etc. these resources need to communicate to each other's frequently. In addition to these resources IoT device need additional data for processing. Connecting all these devices directly to the cloud is impractical and unrealistic and cost prohibitive as well, because such interactions often require resource-intensive processing and complex protocols.

d) Intermittent connectivity: Cloud services will have difficulty providing uninterrupted services to devices and systems that have intermittent network connectivity to the cloud. As another example, when a car traverses an area where it loses Internet connectivity, many services and applications for the devices and people in the car must continue to be available. When a car breaks down in such an area and needs to have one of its electronic control unit (ECU) replaced before it can run again, the new ECU should be authenticated to prevent any unauthorized and potentially malware-infected ECUs from being installed on the vehicle. However, cloud-based authentication services will not be available in this scenario.

e) Cyber-Physical Systems: As more cyber-physical systems are connected to the IoT, the pendulum between the brick versus the click is starting to swing back toward the brick again, where interactions, and often times close integrations, between cyber systems and physical systems are becoming increasingly important and bring new business priorities and operational requirements. Examples of cyber-physical systems include industrial control systems, smart cities, and connected cars and trains. In such systems, uninterrupted and safe operations are often the top priority.

f) Security: Summary of potential security issues found in Fog applications. The development of security measures in Fog systems is rapidly progressing, and some of the current publications do not contain sufficient detail to provide a thorough evaluation. This results in some of the knowledge gaps being speculative and futuristic and based on the latest research activity. It is important to note that due to continuous increase in attack vectors, it is not an exhaustive list and some security issues may have been missed. With the advancement in Fog infrastructure development, new security issues will need to be identified and acknowledged.

III. EMERGING ERA OF FOG COMPUTING

In this section, we review the evolution from cloud to fog computing, present the architecture and features of fog computing and introduce the fog-assisted IoT applications.

A. From Cloud To Fog

IoT enables connected devices to collect data and communicate with each other. Physical objects with small size, widely distributed, with limited storage and processing capacity, such that IoT lacks various important features, including scalability, flexibility, reliability, interoperability and efficiency, generally characterize the IoT devices. Cloud computing has offered a practical solution to address these issues for IoT applications [4].

Cloud-based IoT architecture can be divided into two layers, the top layer and the bottom layer. The top layer is the data storage and control layer, in which the cloud offers an effective approach to manage and composite IoT services and implement IoT applications by exploiting the devices and data collected from these devices. Specifically, the cloud not only provides centralized storage, processing and access for large scale data, but also offers various applications and services through the virtualization technique to users. It bridges the gap between objects and applications and hides all the complexity and functionalities in implementation[2].

The bottom layer has billions of IoT devices connected with each other and the cloud. The pervasive presence of IoT devices around human enables to measure, infer, understand and reconstruct the environment. These devices may not only include complex devices, e.g., mobile phones, smart glasses, cameras and vehicles, but also comprise daily objects, e.g., appliances, furniture, food, clothing and work of arts. The two layers are connected through communication medium and equipment, such as gateways, routers and bridges, and exchange data via standard communication protocols. Despite the benefits of the integration of cloud computing and IoT are attractive, cloud computing is not a panacea that can address all the problems in IoT. This centralization of resources implies a large separation between IoT devices and the cloud, which results in the increase of the average network latency and jitter. Due to this physical distance, the cloud cannot directly access local contextual information, e.g., local network condition, users' mobility pattern and precise location information. Further, the IoT devices and end users are unable to access delay-sensitive applications because of communication delay, e.g., smart traffic lights and augmented reality. Therefore, there should be a novel technology to expand the IoT to support delay-sensitive, location-aware and mobility-supported applications. The concept of fog computing was introduced by Cisco in 2012, which is defined as "an extension of the cloud computing paradigm that provides computation, storage, and networking services between end devices and traditional cloud servers". Fog computing is not a replacement of the cloud for remote data storage and processing but complement it. Fog nodes facilitate the creation of a hierarchical infrastructure, along with the cloud, in which transit data storage and local data analysis are performed at fog nodes, and permanent storage and global analysis are executed at the cloud. The fog nodes are deployed heterogeneously at the edge of network proximate to the devices. Fog and cloud complement each other to form a service continuum between the cloud and the endpoints by providing mutually beneficial and interdependent services to make computing, storage, control, and communication possible anywhere along the continuum.

1) Fog Enables a Service Continuum*:* Fog fills the gap between the cloud and the things to enable a service continuum. For example, to the wearable devices, a mobile phone may become the fog to provide local control and analytics applications to the wearable devices. When the user is inside her vehicle, the vehicle can become the fog for her mobile phone to allow many smart phone functions, such as display, user interface, audio,

phone book, to be moved to the vehicle. Roadside traffic control equipment can in turn serve as the fog for the vehicle to provide traffic information to the vehicle.

2) Fog and Cloud Are Interdependent: For example, cloud services may be used to manage the fog. Fog can act as the proxy of the cloud to deliver cloud services to endpoints, and act as the proxy of the endpoints to interact with the cloud. Furthermore, fog can be the beachheads for collecting and aggregating data for the cloud.

3) Fog and Cloud Are Mutually Beneficial: Some functions are naturally more advantageous to be carried out in the fog while others in the cloud. Determining which functions should be carried out in the fog and how the fog should interact with the cloud will be key aspects of fog research and development. Traditionally, services and applications are provided with large, centralized, expensive, and hard-to-innovate "boxes" such as the service gateways and packet data network gateways in the LTE core, large servers in a data center, and the core gateways and routers in a wide-area-network backbone. The traditional view is that the edge uses the core networks and data centers. The fog view is that the edge is part of the core network and a data center. Table I outlines the main characteristics of fog and how it complements cloud.

B. Fog Architecture

Fog architecture consist of three layers. One is device layer one is fog layer and the third layer is cloud layer as show in fig 1. To achieve the communication between these layer various communication devices has been used such as ethernet, Bluetooth, ZigBee,LTEetc. Device layer consist of two types of IoT devices, mobile IoT devices and fixed IoT devices. Mobile IoT devices are carried by owner such as tracker, camera etc. Fixed IoT devices are fixed at a position such as RFID, sensors etc. These IOT devices have limited, computing, storage and bandwidth. Their responsibility is to collect data and send it to the upper layer i.e. fog layer. The fog layer consists of network equipment, such as routers, bridges, gateways, switches and base stations, augmented with computational capability, and local servers (e.g., industrial controllers, embedded servers, mobile phones and video surveillance cameras). These devices, called fog nodes in fog computing, can be deployed anywhere with network connections: in a smart phone, on a factory floor, on a roadside unit, in a vehicle or on top of a power pole [3]. The fog nodes are hierarchically distributed between the IoT devices and the

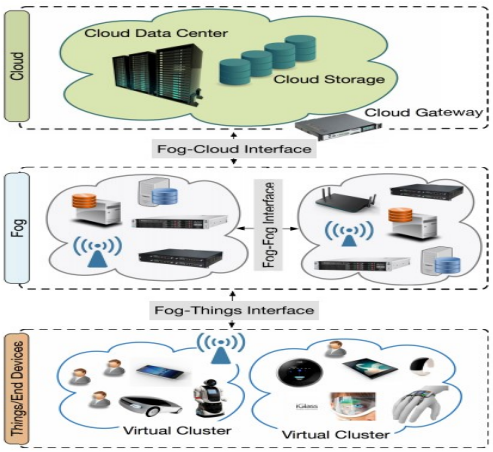

Figure 1. Three-layer architecture of fog

cloud servers in the Cloud-Fog-Device framework or above the IoT devices in Fog-Device framework. This layer tends to extend the cloud computing to the network edge. It has certain computing and storage prowess and autonomy to reduce the processing load on resource-constrained IoT devices. Apart from conventional communications (e.g., package forwarding and routing), some real-time and latency-sensitive applications can be relegated from cloud servers to fog nodes. Since the applications are located in the fog nodes only one/two-hopaway from devices, they possess regional knowledge about the devices and their owners (i.e., users), e.g., local network condition, users' mobility pattern and precise location information. In Fog-Device framework, the fog nodes cooperatively offer various services without the involvement of cloud servers, e.g., decentralized vehicular navigation, indoor floor

plan reconstruction, smart traffic lights and local content distribution. In Cloud-Fog-Device framework, the fog nodes provide transient storage and real-time analysis on the data collected by IoT devices and periodically send data summaries to the cloud through the forwarding of other fog nodes located at higher levels in the network hierarchy. The cloud layer in Cloud-Fog-Device framework is a consolidated computing and storage platform that provides various IoT applications from a global perspective. The cloud has significant storage space and computing resources and is accessible for users at anytime and from anywhere, as long as their devices are connected to the Internet. It utilizes virtualization technology to achieve the isolation of distinct users' data and IoT applications, such that these applications can independently and concurrently provide different services to distinct users. The cloud receives data summaries from various fog nodes and performs global analysis on the data submitted by fog nodes and the data from other sources to improve business insight in IoT applications, such as smart power distribution, health status monitoring and network resource optimization. In addition, the cloud also sends policies to the fog layer to improve the quality of latency-sensitive services offered by fog nodes.

C. Characteristics of Fog Computing

Fog computing is a distributed framework that offers IoT applications at the edge of the network by leveraging edge resources. The major feature of fog computing [6] is to tackle the IoT data locally by utilizing the fog nodes placed near users to bring about the convenience of data storage, computation, transmission, control and management. [7]Compared with cloud computing, fog computing has five distinguished features as follows:

- Location Awareness: The location of fog nodes can be traced actively or passively to support devices with rich services at the network edge. Fog computing dedicates on local IoT applications accessible for the devices at certain areas via specific fog nodes. Therefore, it is aware of the devices' regions based on the locations of fog nodes.

- Geographic Distribution: The fog nodes are deployed at certain positions, such as along highways and roadways, on cellular base stations, on a museum floor and at a point of interest.. Characteristics of Fog Computing. IoT devices, even when these devices pass between two fog nodes.

- Low Latency: Thanks to the computing and storage resources, fog nodes can provide computation services and make decisions based on local data without the cloud. Since the fog nodes are proximate to the IoT devices, the latency of the response is much lower than that made by the cloud.

- Large-Scale IoT Applications Support: Fog computing is introduced to support large-scale IoT applications, which bring heavy management overhead to the centralized cloud. In large-scale IoT applications, such as environment monitoring, power grid management, water treatment management and climate change monitoring, fog computing has its prowess and autonomy to manage billions of IoT devices.

Decentralization: Fog computing is a decentralized architecture that there is no centralized server to manage resources and services.

Table 1. Summary Of Fog Computing, Cloud Computing, And IoT Features.

Features	Fog computing	Cloud computing	Internet of things
Target user	Mobile user	General internet user	Stationary and mobile devices
Number of Server node	Large	Few	Large
Architecture	Distributed	centralised	Dense and distributed
Service type	Localized information service limited to specific deployment location	Global information collected world wise	Information specific to the end device
Working environment	Outdoor (e.g. Street, fields, tracks) or indoor (e.g. home , mall , restaurant)	Indoor with massive space and ventilation	Outdoor and indoor
Location awareness	Yes	No	Yes
Real time interactions	supported	supported	Supported
mobility	supported	Limited support	Supported
Big data and duration of storage	Short duration as it transmits big data	Months and years as it manages big data	Transient as it the source of big data
Major service provider	Cisco I Ox	IBM, Microsoft, Amazon	Atmel , Bosch, ARM

The fog nodes self-organize to cooperatively provide real-time services and IoT applications to users. In addition, fog computing has several general characteristics, including mobility support, predominance of wireless access, heterogeneity, online analytics and interplay with the cloud.

D. Interaction between Fog Computing, Cloud Computing and IoT

Fog computing brings cloud computing closer to Internet of Things (IoT) devices. The advent of IoT has resulted in an increasing number of cases that generate significant volume of data, compounding the challenges of dealing with big data from a number of geographically distributed data sources..

To harness the benefits of IoT and speed up awareness and response to events, we require a new set of infrastructures as current cloud models are not designed to handle the species of IoT. Specially, billions of previously unconnected devices are now generating over two Exabyte's of data every day and it has been estimated that by 2020, 50 billion ``things'' will be connected to the Internet. Therefore, fog computing has been identified as a viable solution. [8]A brief summary of IoT, cloud computing and fog computing is given in Table 1.

IV. HOW FOG HELP IN IOT

In particular, fog can provide effective ways to overcome many limitations of the existing computing architectures that rely only on computing in the cloud and on end-user devices[5]. Table II shows, as an example, how fog can help address the IoT challenges

Table II. Fog Assisted IoT Challenges

IoT Challenges	How fog can help
Latency constraints	Fog , performing data analytics , control with other time-sensitive task close to the end user, is the ideal and only opinion to meet the stringent timing requirements of many iot systems
Network bandwidth constraints	Fog enables the hierarchical data processing along the cloud –to-things continuum, allowing processing to be performed where It can be balanced between application requirements and available networking and computing resources. It also reduces the amount of data that needs to be sent to the cloud.
Resource constrained devices	Fog can carry out resource intensive tasks on behalf of resource constrained devices when such tasks cannot be moved to the cloud due to any reason, hence reducing the devices complexity, lifecycle cost and energy consumption.
Uninterrupted services with intermittent connectivity with cloud	A fog system can operate autonomously to ensure non-interrupted services even when it has intermittent connectivity with the cloud.
New IoT security challenges	A fog system can, example 1) act as the proxies for resource constrained devices to help manage and update security credentials and software's on these devices. 2) Provide a wide range of security functions, such as malware Scanning for resource constrained devices to compensate the limited security functionality on these devices. 3) Monitor the security status of nearby devices and 4) take the advantage of local information and context to detect the threats on timely basis.

V. FOG ASSISTED IOT APPLICATIONS

1. Video Streaming: Transmissions of video applications and services are more efficient in a fog computing implementation, due to the capability of fog computing to provide location awareness, low latency, mobility, and real-time analytics. Several smart devices support smart surveillance that can be used by law enforcement officers to display live video streams of events of interest.[11] For example, Hong et al. described a video surveillance application that requires a three-level hierarchy system to perform motion detection with smart camera, face recognition with fog computing instances, and identity aggregation with cloud computing instances.

2. Gaming: The advent of cloud computing has provided a platform for computer gaming without users (players) worrying about hardware requirements. Decoded by end devices such as smart phones or tablets. Wang and Dey described a cloud server based mobile gaming approach, cloud mobile gaming, where most of the workload for executing the game engine are placed on the cloud server. The mobile device only sends and receives user gaming commands to and from the servers.

3. Health Care :In order to facilitate easy access to healthcare service for the elderly, a body sensor network in fog computing was proposed in [49]. The fog computing gateway is used to enhance the system by offering different services such as ECG feature extraction, distributed database and graphical interface to ensure obtained health data are visualized and diagnosed in real time. Aazam and Huh proposed a Smartphone-based service, Emergency Help Alert Mobile Cloud (E-HAMC),which uses fog services for pre-processing and offloading purposes to provide an instant way of notifying relevant emergency department (e.g., ambulance) from the stored contact details. This service also sends the incident location to facilitate patient tracing [12].

4. Smart Grids: The current call for smart grids can be linked to the fact that the present-day energy demands have outpaced the rate at which energy is generated by conventional methods as well as the need to reduce gas emission to control or curtail climate change. Abdel Wahab *et al.* proposed a cloud-assisted remote sensing approach to measure and collect smart grid operational information to enable seamless integration and automation of smart grid components.

5. Smart Cities: A smart city is one key IoT application that ranges from smart traffic management to energy management of buildings, etc. Kitch in described smart city as a city that is

vastly controlled and made up of ubiquitous computing whose economy and governance are driven by innovation and creativity.

6. Smart vehicle: The advent of mobile cloud computing has necessitated the study of its agents such as vehicles, robots and humans that interact together to sense the environment, process the data and transmit the results. Lu *et al.* described connected vehicle that communicates with their internal and external environment such as Vehicle-to-Vehicle (V2V), Vehicle-to-Sensor on-board (V2S), Vehicle-to-Road infrastructure (V2R) and Vehicle-to-Internet (V2I). Vehicle cloud has been identified [57] as the leading application that facilitates safe driving, urban sensing, content distribution and intelligent transportation to render benefits such as sensing urban congestion and collaborative reconstruction of footage in a crime scene.

VI. SECURITY AND PRIVACY ISSUES IN FOG COMPUTING

A summary of security controls in respect to each application area is given in summary given below. It highlights the potential impact on Fog platforms with respect of CIA model. The development of security measures in Fog systems is rapidly progressing, and some of the current publications do not contain sufficient detail to provide a thorough evaluation. This results in some of the knowledge gaps being speculative and futuristic and based on the latest research activity. It is important to note that due to continuous increase in attack vectors, it is not an exhaustive list and some security issues may have been missed.[14] With the advancement in Fog infrastructure development, new security issues will need to be identified and acknowledged

1. Attack Category: Visualization Issues

Possible threats: Hyper vision attacks, VM attacks, weak or no logical segregation ,side channel attacks , privilege escalation service, abuse privilege escalation, attack insufficient resource policies.

Possible solutions: Multi-factor authentication , intrusion detection system, user data isolation, attribute/identity based encryption, role based access control , model user based permission, model Process isolation

Impact: As all services and VM's are executing in virtualized environment, its components will have adverse effects in all fog services, data and user's.

2. Attack Category: Web Security Issues

Possible threats: SQL injection, cross-site scripting, cross-site request, forgery, session/account hijacking, insecure direct object references, malicious redirections drive by attacks.

Possible solutions: Secure code find and patch, Vulnerabilities regular, Software updates periodic, Auditing firewall antivirus, Protection intrusion, Prevention system

Impact: Exposure of sensitive information, attacker become legitimate part of network and enable malicious applications to install

3. Attack Category: External /Internal Communication Issues

Possible threats: Man-in-the middle attack, inefficient rule, Poor access control, Insecure API's and services, Application vulnerabilities, Single point of failure.

Possible solutions: Encrypted communication, Mutual/multi factor, Authentication partial, compromised nodes, Encryption isolation, Number of connection transport layer security.

Impact: Attacker can acquire sensitive information by eavesdropping and get access to unauthorized fog resources

4. Attack Category: Data Security Related Issues

Possible threats: Data replication and sharing, Data altering and erasing attacks illegal data, Access Data owner ship issues low attack issues

Possible solutions: Policy enforcement security inside architecture Encryption secure key, Management obfuscation, Data masking.

Impact: High probability of illegal file and database access, whether attacker can compromise both user and fog systems data.

VII. CONCLUSION

Fog Computing is a new decentralized architecture that revolutionized the clod computing by extending storage, computing and network resources to the network edge for supporting IoT applications. In this manuscript we have mentioned how and why fog computing can be used in IoT applications. In this paper we have discussed architecture of fog computing, features of fog computing, comparison between fog and cloud. We have also discussed why we are using fog for IoT and how fog fulfils the conditions and criteria of IoT. Lastly, we have discussed the security and privacy issues in fog. There are so many security issues in fog, which can be taken as a problem statement for future work.

VIII. REFERENCES

[1] Mung Chiang, Fellow, IEEE, and Tao Zhang, Fellow, IEEE, "Fog and IoT: An Overview of Research Opportunities" IEEE INTERNET OF THINGS JOURNAL, VOL. 3, NO. 6, DECEMBER 2016

[2] Syed Noorulhassan Shirazi, Antonios Gouglidis, Arsham Farshad, and David Hutchison," The Extended Cloud: Review and Analysis of Mobile Edge Computing and Fog From a Security and Resilience Perspective", IEEE JOURNAL ON SELECTED AREAS IN COMMUNICATIONS, VOL. 35, NO. 11, NOVEMBER 2017

[3] Bonomi, R. Milito, P. Natarajan, and J. Zhu, "Fog computing: A platform for Internet of Things and analytics," in Big Data and Internetof Things: A Roadmap for Smart Environments. Cham, Switzerland :Springer, Mar. 2014, pp. 169–186.

[4] M. M. Islam, S. Morshed, P. Goswami, and B. Dhaka, "Cloud computing: A survey on its limitations and potential solutions," Int. J. Comput.Sci. Issues, vol. 10, no. 4, pp. 159–163, 2013.

[5] Jianbing Ni ,Student Member, IEEE, Kuan Zhang, Member, IEEE, Xiaodong Lin, Fellow, IEEE, and Xuemin (Sherman) Shen, Fellow, IEEE "Securing Fog Computing for Internet of Things Applications: Challenges and Solutions " IEEE COMMUNICATIONS SURVEYS & TUTORIALS, VOL. 20, NO. 1, FIRST QUARTER 2018.

[6] F. Bonomi, R. Milito, J. Zhu, and S. Addepalli, "Fog computing and its role in the Internet of Things," in Proc. 1st Ed. MCC Workshop Mobile Cloud Compute., 2012, pp. 13–16.

[7] M. Chiang and T. Zhang, "Fog and IoT: An overview of research opportunities," IEEE Internet Things J., vol. 3, no. 6, pp. 854–864, Dec. 2016

[8] S. Yi, Z. Hao, Z. Qin, and Q. Li, "Fog computing: Platform and applications," in Proc. 3rd IEEE Workshop Hot Topics Web Syst. Technol., Nov. 2015, pp. 73–78.

[9] A. Al-Fuqaha, M. Guizani, M. Mohammadi, M. Aledhari, and M. Ayyash, "Internet of Things: A survey on enabling technologies, protocols, and applications," IEEE Common. Surveys Tuts., vol. 17, no. 4, pp. 2347–2376, 4th Quart., 2015.

[10] J. Gubbia, R. Buyyab, S. Marusica, and M. Palaniswamia, "Internet of Things (IoT): A vision, architectural elements, and future directions," Future Gener. Comput. Syst., vol. 29, no. 7, pp. 1645–1660, 2013.

[11] D. Evans, "The Internet of Things: How the next evolution of the Internet is changing everything," Cisco, San Jose, CA, USA, White Paper, 2011.

[12] "Fog computing and the Internet of Things: Extend the cloud to where the things are," Cisco, San Jose, CA, USA, White Paper, 2015.

[13] Wikipedia. (2016). Fog Computing. [Online]. Available https://en.wikipedia.org/wiki/Fog-computing

[14] I. Stojmenovic and S. Wen, "The Fog computing paradigm: Scenarios and security issues," in Proc. Federated Conf. Comput. Sci. Inf. Syst.,Sep. 2014, pp. 1–8.