A Review on Cloud and Fog Computing Integration for IoT: Platforms Perspective

Asrar A. Baktyan1,* and Ammar T. Zahary 1

1Information Technology Department, FCIT, Sana’a University, Sana’a, Yemen; asrar@yemenmobile.com.ye, aalzahary@gmail.com

Abstract

The fourth industrial revolution can connect ecosystems of more than 20 billion devices with an unpredictable gross of the local consumption. Connected devices will produce approximately 44 ZB of raw data by 2020, which provides interesting challenges relatively to privacy, connectivity, and scalability. The Internet of Things (IoT) is earning growing attention that provides the interconnection between the physical and the digital world. Consequently, the physical world needs to be measured and converted into expressible statistics. Cloud for IoT introduces precious application and unique services in several domains. However, fog computing helps in efficient utilization and better performance in case of bandwidth utilization, and low power consumption. This review focuses on the IoT platforms used for fog and cloud computing to serve IoT end-to-end services. In addition, the application of the cloud of thing and fog roles to improve the challenges of the cloud of things are also provided.

Keywords: Cloud computing, CoT, Fog computing, IoT Platform, IoT Paradigm, Software Defined Networks

Received on 27 October 2018, accepted on 17 December 2018, published on 20 December 2018

Copyright © 2018 Asrar A. Baktyan and Ammar T. Zahary, licensed to EAI. This is an open access article distributed under the terms of the Creative Commons Attribution licence (http://creativecommons.org/licenses/by/3.0/), which permits unlimited use, distribution and reproduction in any medium so long as the original work is properly cited.

doi: 10.4108/eai.20-12-2018.156084

1. Introduction

The huge variety of IoT devices that are connected to the Internet is resulting in the rise of the worldwide use of IoT communication paradigms. IoT permits both public and private organizations to combine always-connected, smart objects to enhanced everyday human lives in many aspects [1]. Furthermore, smart industries and smart supply chains are the examples of the IoT to discourse efficiency in several business domains. Industrial production is varying from the employment of robots to the self-learning ubiquitous adoption of advanced smart sensors and objects. The businesses shall improve pursuit and control of supply chains, with more computational power and more reliable secure connections.

The integration of IoT and cloud computing is producing the new tiers of competence in providing services. The evolving business views coming from IoT are pushing the private, public, and hybrid Cloud Service Providers (CSPs) to associate their networks with IoT devices (including sensors and actuators) that are connected to the Internet to introduce the Sensor and Actuator as a Service (SAaaS). The IoT-cloud combination demands a wide range of “big data” technologies and services to control both semi-structured and unstructured data [2].

Millions of sensors and devices are endlessly creating data and exchanging control messages via compound networks to offer machine-to-machine communications and monitoring the smart networks. To help in mitigating the growth in resource congestion, edge computing has been presented to localize the computing near the terminal devices. In contrary to the centralized cloud computing, edge computing shifts the data computation and storage to the network “edge”. However, Variety of computation

*Corresponding author. asrar@yemenmobile.com.ye
nodes distributed across the network can reduce the load of
the computational strain away from the centralized data
centre, and can obviously decrease the delay in the
messages’ transfer. Furthermore, the benefit of the
distributed construction is stabilizing the traffic load in the
IoT network. Moreover, by tacking computation and
communication load from nodes with restricted battery
supply to nodes with strong power resources, the network
can expand the lifetime of the terminal devices [3].

The IoT competence is unrestricted and its usage can
transform the entire models of the whole technology. It
relays on attaching network interface into objects, enabling
communications between them with slightest inputs from
human beings to produce services for customers. However,
each device will have its own identifier, like an Internet
Protocol address (IP address) that can join and
communicate with other devices through the IoT network
and Internet. While the users could get data only from the
service provider of the network before IoT, the users
nowadays can directly access the sensors and give
instructions to the actuators. As a result, data from IoT
applications will be utilized to harvest a novel service to
manufactures, academia, and even individual use. All the
objects, animals, and people are put in the network with
unique identifiers and are capable to transmit data without
requiring human-to-human or human-to-computer
interaction. Yet, there are some restrictions in the recent
study to build a full IoT network. First, the applications and
services for IoT are basically established by various
vendors without any standard technology. Second, there is
no existing standard network protocol for all IoT
applications. Recently, there have existed many different
network protocols like Wi-Fi, Bluetooth, ZigBee, Z-wave,
and Long-Term Evolution (LTE)[4]. However, there is no
protocol for the current devices that could communicate
with all existing network protocols at the same time. To
overcome this issue, the gateway which is called fog
computing providing homogeneous networks is vital to
creating a whole IoT network. Additionally, the growing
number of IoT devices and the need for Big Data
processing will extend the number of packets sent to a
network, where this issue can be a serious problem to the
network infrastructure [5].

This study provides the cloud and fog computing
integration for IoT devices focusing on the most popular
platform used to support fog and end to end services. In
addition, this overview produces the roles of fog plays in

IoT application and solves many challenges in Cloud of
Things (CoT). The remainder of this review is structured
as follows Section 2, explains the structure of CoT, the
integration of fog and cloud computing, and IoT
paradigms. Then Section 3, introduces the fog computing
heterogeneity of resources, and the fog and cloud
platforms. Section 4, gives the application categories of
the CoT. Section 5 provides the challenges of CoT and
whose fog helps to overcome those challenges. The
conclusion in section 6 Summarizes the study.

2. IoT Architecture

There are three major layers for IoT architecture as shown
in figure 1. The service layer is on the surface that
communicates with the users directly; for example,
autonomous driving, healthcare, intelligent
communication, industrial automation, governmental
sectors, smart industries, smart homes, smart cities,
and personal smart devices. These services are connected with
a platform layer. The platform layer is below the service
layer and provides the IoT applications and services.
Examples of the platforms are the device platform, data
analysis platform, service development platform, and
service platform. The device platform provides the
environment for executing the services and development
for users [6] [7]. On the other hand, data analysis platform
works as context awareness prediction, collaborates
through things and connects the service layer and other
layers with the translation of natural language to machine
language. Analytics support reducing the tension on the
network layer, reducing power desires for sensors by less
frequent communication backend and let faster replies to
data received by the sensors. Moreover, the service
development platform cares about development toolkits
produced to users in order to easily develop IoT services.
Finally, the service platform provides the generation and
implementation of a wide range of applications [4].

The use of centralized cloud computing increases the
concerns about bandwidth limitation and delay. Though, a
new platform called Fog/edge Computing has been
presented to serve the IoT applications that cannot be
performed in the cloud due to the demand of the gateway
pre-processing and analysing [8].
The device layer is utilized, and it monitors the different open infrastructure at the edge. It sends the separated data that demands services used up locally by the fog layer. In the fog layer, the device layer spreads the filtered raw data to the fog layer, where the high-performance distributed SDN controller is located. Every fog node covers a small area and provides data analysis and service delivery in a timely manner. The fog layer communicates with the cloud layer to inform it with the result of the processed data, and sometimes informs the device layer about the output reports. The fog layer introduces localization services, whereas the cloud layer provides central monitoring and controlling. Fog layer provides a wide range of events detection, behavioural analysis, and semi-permanent pattern recognition by introducing distributed computing and storage. Cloud layer proposes a distributed cloud based on the block chain technique that has secure, low-cost, and on-demand access to the foremost competitive computing infrastructures. Clients can use all the computing resources like servers, data storage, and applications that they need. For the fog layer, the use of a block chain-based, distributed computing is to secure SDN controller network architecture in the fog node. All the SDN controllers are communicated in a distributed pattern using the block-chain technique [9]. Every SDN controller is approved by an analysis function of the stream rule and a packet migration function to secure the network from overload attacks. At the edge of the network, the multi-interfaced Base Stations (BSs) are used with SDN switch to support the wireless communication technologies implemented in IoT devices. The fog nodes have SDN controllers which work as the programming interfaces to produce a wide range of network services. A fog node can access the distributed cloud to the Internet to run the application service and computing capability. Fog nodes transfer the computing load to the cloud when they run out of resources to handle the increased latency communications [6] [10].

2.1. Fog and Cloud Integration for Internet of things

The rapid movement toward web3, which is pervasive computing web, has already made the connected devices reach 9 billion and are going to reach 24 billion by 2020. Since the number of connected devices is quickly increasing, there will be a lot of data as well. Storing that data locally and temporarily will be difficult [11]. There is a need for rental storage space. Context will be modelled to rage device knowledge along to deduce new information. So, the data is utilized and processed to form information and knowledge then wisdom to the users. While IoT devices are low in cost and light in weight, they cannot manage to process the huge data. In CoT, heterogeneous networks will provide various types of data and services with the help of fog computing. The network must have the flexibility to support all types of data according to its requirements and QoS [12].
Mobility-awareness service is a service in 5G enabled Fog computing, and it forwards a large amount of data from one fog node to another in real-time, overcoming communication overhead. However, due to decentralized orchestration and heterogeneity of fog nodes support, management of 5G network resources are not as simple as other computing paradigms. Nonetheless, fog infrastructures can be owned by different providers that can significantly resist developing a generalized policy for IoT networks. Besides arranged network slicing for forwarding latency-sensitive IoT, data can also contribute additional complications in 5G networks with enabled Fog computing [13]. To bring the IoT software mass to a suitable concept, there is a need to construct a software-defined machine (SDM) by joining different IoT elements. In this framework, the SDM acts as a small cloud infrastructure in which the deployment of different IoT components accomplishes a configuration and management at runtime. IoT services are decided by the IoT Service Provider who uses SDM Profile (and its APIs). The IoT Service Provider concerns are about the APIs and other service limitations. The IoT Infrastructure Provider and the IoT Service Provider give a consideration about the SDM APIs utilization and they monitor SDM APIs to maintain security, service contracting, and outlining [14].

As Figure 3 shows, the Software Defined Machine (SDM) for IoT has three layers. The lowest layer of the SDM is flexible and has a lot of configurations to preserve the cloud network, permitting IoT services to transfer data through communication devices that provide software-defined networking (SDN) for various workloads. The operating systems are in the intermediate layer with virtualization capabilities. The cloud network hardware serves as a software-defined router, which is programmable to control the communication protocol and interfaces. The data approved by the SDM can go to another SDM or cloud server. Storage drivers and cloud server allow the data to be kept in an SDM locally or to go directly to the cloud central storage. The imperative aspect in SDM structure is how to store the data into the SDM storage using software-defined APIs, and whether to store the data locally or transmit it to another SDM or cloud servers [15].
Figure 3 Software-defined machine (SDM) for the Internet of Things (IoT) part, which includes infrastructures and IoT elements deployed next to the “things”

Table I Sample of requirements for establishing an Internet of Things (IoT) fog and cloud network [15] [16] [17] [18].

<table>
<thead>
<tr>
<th>Type</th>
<th>IOT</th>
<th>Cloud</th>
<th>Fog</th>
</tr>
</thead>
<tbody>
<tr>
<td>Infrastructure machines</td>
<td>industrial and popular gateways (like Intel IoT Gateway) and operating system containers (like Dockers).</td>
<td>Virtual machines and operating system containers.</td>
<td>Virtual machines and operating system containers with limited resources.</td>
</tr>
<tr>
<td>Connectivity protocols</td>
<td>(MQTT), (CoAP), HTTP, (CAN) bus.</td>
<td>MQTT, (AMQP), HTTP, and so on.</td>
<td>MQTT, CoAP, XMPP, AMQP, DDS.</td>
</tr>
<tr>
<td>Platform software services</td>
<td>Lightweight data services (like NiagaraAX/Obix), lightweight compound event processing (CEP) and data synthesis, topology description and distribution service (like TOSCA), and lightweight application containers (like OSGi and Sedona).</td>
<td>Load balancers (like HAProxy), message-oriented middleware MOM (like ActiveMQ and Kafka), NoSQL, stream/batch processing (like Hadoop and Spark), factor repositories/markets, and distribution services (like TOSCA, HEAT, and Chef).</td>
<td>FogHorn, fogflow, OpenVolcano</td>
</tr>
<tr>
<td>Working environment</td>
<td>everywhere</td>
<td>Carefully selected Warehouse building with air conditioning systems.</td>
<td>Outdoor shelters (e.g., Streets, gardens, parks) or indoor (e.g., Restaurants, shopping mall).</td>
</tr>
<tr>
<td>Security</td>
<td>Hard to define</td>
<td>Defined</td>
<td>Hard to define</td>
</tr>
<tr>
<td>Attack on data</td>
<td>High possibility</td>
<td>Less probability</td>
<td>High probability</td>
</tr>
<tr>
<td>Security and Privacy</td>
<td>encryption chips and communication technology security</td>
<td>Authentication, authorization, firewall, and antivirus.</td>
<td>Cryptographic suites and security in communication protocols.</td>
</tr>
</tbody>
</table>
### 2.2. Cloud IoT paradigms

The approval of the CoT paradigm permits new scenarios for IoT services and applications based on the integration of cloud and the things, as shown in Table 2 [19] [20] [21] [22] [23] [24] [25] [26] [27]:

<table>
<thead>
<tr>
<th>IOT paradigms</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>SaaS (Sensing and Actuation as a Service)</td>
<td>enabling programmed control logical implementation in the cloud.</td>
</tr>
<tr>
<td>SEaaS (Sensor Event as a Service)</td>
<td>enabling pervasive management of remote sensors.</td>
</tr>
<tr>
<td>SenaaS (Sensor as a Service)</td>
<td>providing pervasive control of remote sensors.</td>
</tr>
<tr>
<td>DBaaS (Database as a Service)</td>
<td>providing pervasive database management.</td>
</tr>
<tr>
<td>Daas (Data as a Service)</td>
<td>providing pervasive access to all database types.</td>
</tr>
<tr>
<td>EaaS (Ethernet as a Service)</td>
<td>providing pervasive layer-two connectivity to remote devices.</td>
</tr>
<tr>
<td>Cloud-Based Analytics as a Service (CLAaaS)</td>
<td>Providing data storage and analytics in the form of the cloud as services.</td>
</tr>
<tr>
<td>IPMaaS (Identity and Policy Management as a Service)</td>
<td>providing pervasive access to policy and authentication management services.</td>
</tr>
<tr>
<td>VSaaS (Video Surveillance as a Service)</td>
<td>Providing pervasive access to documented video and application.</td>
</tr>
<tr>
<td>BIaaS/BIaS (Business Integration as a Service)</td>
<td>enabling connections between various clouds services and joins a variety of other services and business activities to achieve the efficient processes.</td>
</tr>
</tbody>
</table>
| SecuaaS/SaaS (Security as a Service)   | -providing the cloud-based solution for data, host and application safety.  
                                         -validating the security over a geographically spread scalable, multi-cloud and cloud federation infrastructure. |
| ObaaS (Object as a Service)           | Building the service on each item as required and subsequently participate it into the whole configuration. |

<p>| | |</p>
<table>
<thead>
<tr>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>MobiaaS (Mobility as a Service)</td>
<td>providing the required connectivity service stability to the consumers. It also brings a continuous handoff for communication flows such as speech as the subscribers using a host of the devices to communicate.</td>
</tr>
<tr>
<td>FRRaaS (Forensics as a Service)</td>
<td>providing a comprehensive cloud-powered forensics resolution to progress a repeatable system.</td>
</tr>
<tr>
<td>FaaS (Failure as a Service)</td>
<td>Executing the routine large-scale failure workouts in real time distributions. FaaS is accomplished to introduce the large-scale failures online. However, it may support mitigation, respond, or recovery from failures at the individual or organizational level.</td>
</tr>
<tr>
<td>CaaS (Context as a Service)</td>
<td>providing a customized data provision method in which the Fog and Edge Computing (SEC) nodes can collect and process the data to generate expressive information for the clients.</td>
</tr>
<tr>
<td>UCaaS (Unified Communications as a Service)</td>
<td>Providing communications such as voice over IP (VoIP or Internet telephony), instant messaging (IM), and video conference applications by using either fixed or mobile devices.</td>
</tr>
<tr>
<td>DRaaS (Disaster Recovery as a Service)</td>
<td>Providing the replication and hosting of physical or virtual servers by a third party to produce failover in the event of a man-made or natural catastrophe.</td>
</tr>
<tr>
<td>BaaS (Backend as a Service)</td>
<td>Providing connection features such as user management and notifications to backend cloud.</td>
</tr>
<tr>
<td>DaaS (desktop as a service)</td>
<td>Providing Virtual Desktop Integration (VDI) system that enterprise’s users can log into.</td>
</tr>
<tr>
<td>Faas (Framework as a Service)</td>
<td>Providing hybrid of Software as a service and platform as a service which is customized to fit business demands.</td>
</tr>
<tr>
<td>ITaaS (Information Technology as a Service)</td>
<td>Providing the delivery of all technologies needed to creating, storing, exchanging and using enterprise data with high-level support and regular upgrade.</td>
</tr>
<tr>
<td>TaaS (Transportation as a service)</td>
<td>Providing alternative option to car ownerships toward mobility solution that people can consume it as a service.</td>
</tr>
</tbody>
</table>
2.3. Fog Heterogeneous Physical Resources

ints, and even terminal devices like vehicles, sensors, and cell phones etc. The various hardware structures have distinctive levels of RAM, and secondary storage to provide new services. The platforms use various kinds of OSes and software applications consequential in a wide range of hardware and software abilities. The Fog network infrastructure is heterogeneous in nature, varying from high-speed links joining enterprise, data centres, and the core network to the various wireless access technologies (ex: 3G/4G, LTE, Wi-Fi etc.) end up to the terminal devices [28]. Communication between the tiers is done in four different ways. (a) smart device to smart device, (b) smart device to Fog node, (c) fog node to Fog node, and (d) fog node to cloud data centre.

The data transfer between the smart devices and electric vehicles is done in the first-tier communication. But if any two smart devices that are not in the same fog area need to be interconnected, the connection can be done in a higher level i.e. the fog tier. The fog tier fundamentally communicates with different smart terminals and collects the data from the users. As a result of fog tier defining the private and public data, the data storage and bandwidth are reduced. Usually, the private data is gathered and kept as encrypted data and the public data as a non-encrypted data. The intermediate level cannot translate the encrypted data since there is privacy between the cloud server and the subscriber. Fog computing does not need third parties to interfere while communicating with different kinds of IoT devices and also with metrics of processing tasks, for instance, fog computing introduces a good resource of multi-latency compared to cloud computing [29]. The need for geographical distribution and low-latency computational resources led to the technological progress of fog computing. Fog promotes the development of more dedicated nodes that propose low computational resources. These gateway nodes are known as mist nodes which are introduced as lightweight fog nodes. These mist nodes produce the mist computing layer that are placed even closer to the devices than the more powerful fog nodes that work with the smart end-devices they serve [30].

3. IoT platform

In the least complex terms, an IoT platform is an integrated service that offers you the components you need to bring physical items on the web. It needs to be suitable for supporting millions of simultaneous device connections and effectively allows you to arrange your devices for machine-to-machine communication [31].

The three-level architecture comprises the edge tiers, platform tiers, and enterprise tiers that are joined by access and service networks. The system designs apply a combination of wireless and/or wired technologies like RFID, Bluetooth, Cellular, ZigBee, Z-Wave, and Ethernet. As shown in Figure 4, the data is passed through the access network to the platform tier, which confirms the processing of the data forwarding it to the enterprise tier. In addition, the processing and control commands from the enterprise tier go back down to the edge tier (again, over the access network).

The platform tier allows the service network to connect with the enterprise tier, which provides end user interfaces, control commands and domain applications [32].
3.1 IoT platform Types

There are four different types of IoT platforms: End-to-End, connectivity, cloud, and data:

- **End-to-end IoT Platforms**

  Essentially, end-to-end IoT platform gives the hardware, software, connectivity, security, and device management tools to work with a great number of simultaneous device connections. Additionally, it gives all the managed integrations you need like OTA firmware updates, device management, cloud connection, cellular modem, etc., to connect and monitor a wide range of devices online [31]. The high-scalable and high-reliable software platform support IoT architecture with connectivity, security and device management functionalities utilized to work in energy constrained environments. In addition, the Open-Standards are provided interoperability embedded in the firmware for connectivity with third-party applications and device management.

  Examples: Particle [33].

- **Connectivity Management Platforms (M2M platforms)**

  These kinds of platforms offer low power and low-cost connectivity management solutions either by Wi-Fi or cellular technologies. This can vary from hardware connectivity, cellular networks, to the data routing features of the same set of sensor data.

  Examples: Mulesoft, Hologram, Sigfox

- **IoT Cloud Platforms**

  Cloud platforms reduce the complexity of building the network stack and offer the essential services (plus other services) to monitor and track a huge range of concurrency device connections. The cloud platform is willing to use a comprehensive web portal for scalable data storage and management for cloud applications.

  Examples: Google Cloud IoT, Salesforce Cloud IoT

- **Data Platform**

  Every type of IoT platform deals with data in different ways. But these IoT data platforms combine many of the tools you need to route device data and control data analytics [31]. The wide range of IT infrastructure collect, secure and analyze the data received from all the connected IoT Service Platforms [33].

  Examples: Clearblade, Azure, ThingSpeak

3.2 IoT Platform Verticals

Categorizing IoT platforms under a single category is probably representing it too simple. All these platforms offer more solutions and the solution should be more than
a single category. So, you need to test what they are offering, and whom they are offering it to.

- **Hobbyists**
  - Prototyping Solutions
  - Development Kits
  - DIY solutions

- **Consumer Electronics**
  - Utilities (Smart Bike Locks & Trackers, Smart Bluetooth Tracker)
  - Home automation (Smart Lock, Smart Home App)
  - Wearables
  - Anything with Alexa-involved

- **Industrial IoT (IIoT) Solutions**
  - Smart factory warehousing applications
  - Predictive and remote maintenance.
  - Industrial security systems
  - Asset tracking and smart logistics
  - Energy optimization
  - Transportation monitoring
  - Connected logistics

- **Industry-Driven**
  - Agricultural Oil and Gas
  - Healthcare Services
  - Transportation
  - Smart Cities
  - Energy Consumption monitoring

### 3.3 Fog and Cloud IoT Platform

The gap between the device sensors and data networks is stuffed by IoT Platform. The platform connects the data network to the device and introduces insights using backend applications to create a sense of knowledge generated by many sensors.

Recently, there has been a variety of IoT platforms that give options to deploy IoT applications on the market. Whereas there are many corporations work on IoT platform development, providers like Amazon and Microsoft are way ahead of others within the competition [35].

Choosing an IoT platform can be a challenging task in terms of sufficient knowledge about a selected vendor. However, two key paradigms are important for the IoT, open-source and commercial platforms that are clearly differentiated on many concept lines. Comparing IoT platforms through these lines can help you build a frame of reference for selecting a proper platform for your company’s needs [36]. According to [35] the top 20 IoT platforms in 2018 used for the application and the popular fog platform are mentioned in the table below:

<table>
<thead>
<tr>
<th>Platform</th>
<th>Industry</th>
<th>Protocols Data collection</th>
<th>Main Features</th>
</tr>
</thead>
</table>
| FogHorn        | industry IoT middleware platform relay | OPC/UA, MODBUS, MQTT      | - FogHorn’s software platform produces the power of machine learning and advanced analytics to the edge network.  
- providing a new kind of applications for improved monitoring, diagnostics, quality performance optimization, operational intelligence, and predictive maintenance use cases. |
| FogFlow        | NEC Laboratories Europe | NGSI                      | - It enables on-demand context information processing.  
- FogFlow extends the capabilities of FIWARE context data management to bring AI-based information processing close to the IoT terminals.  
- FogFlow is mobility support. |
| macchina.io Edge Device SDK and Remote Manager | licensed under Apache 2.0 (Open Source) | MQTT, COAP                | - macchina.io works with a web-enabled, modular and extensible C++ and JavaScript runtime environment.  
- Runs on Embedded Linux devices with only 32 MB of RAM or more. |
| FIWARE         | European Union and the European Commission | CoAP, JSON, HTTP/MQTT, OPC-UA | - It produces an improved OpenStack-based cloud, whose capabilities and Catalogue are hosted.  
- The FIWARE Catalogue has Generic Enablers (GEs), providing a wide range of devices.  
- FIWARE only separates between Devices and NGSI gateway Devices. |
| OpenMTC        | Open Source          | HTTP, CoAP, MQTT, Weeve’s TEE-MQTT | - It interconnects various sensors and actuators from different vertical domains.  
- It allows you to develop new or test existing IoT/M2M applications, create your own IoT/M2M infrastructure, or extend an existing one. |
| SiteWhere      | CPAL 1.0 (Open Source) | MQTT, JSON, AMQP, XMPP, Stomp, JMS, and WebSockets | - Speed time to market for your IoT application.  
- Control framework and APIs for custom development.  
- Focus on giving a solution to business problems, not reinventing the wheel. |
<table>
<thead>
<tr>
<th>Platform</th>
<th>Organization</th>
<th>Communication Protocols</th>
<th>Features</th>
</tr>
</thead>
<tbody>
<tr>
<td>Webinos</td>
<td>European Union FP7 project (Open Source)</td>
<td>HTTPS and JSON-RPC</td>
<td>- Enables web applications and services to be used consistently and securely over a wide spectrum of spread and connected devices, including smart Devices, PC, TV, and in-car units. - Helps a &quot;single service for every device&quot; vision, webinos will change the present baseline from installed applications to services running steadily.</td>
</tr>
<tr>
<td>IBM Watson IoT Platform</td>
<td>IBM</td>
<td>MQTT, HTTP</td>
<td>- Device Management. - Secure Communications. - Real-Time Data Exchange. - Data Storage. - Recently added data sensor and weather data service.</td>
</tr>
<tr>
<td>Microsoft Azure IoT Hub</td>
<td>Microsoft</td>
<td>HTTP, AMQP, MQTT</td>
<td>- Device observation. - A rules engine. - Identity registry. - Data monitoring.</td>
</tr>
<tr>
<td>SmartThings</td>
<td>Samsung</td>
<td>CoAP</td>
<td>- The core functionality of the platform is produced by the Subscription Processing and the Application Management System, including the SmartApp Management &amp; Implementation mechanisms.</td>
</tr>
<tr>
<td>Kaa</td>
<td>Apache 2.0 license (Open Source)</td>
<td>MQTT and CoAP</td>
<td>- Horizontally scalable can handle millions of devices. - Raw, unstructured data can also be converted into well-structured time series, convenient for analytics, pattern analysis, visualization, charting, etc.</td>
</tr>
<tr>
<td>ThingWorx</td>
<td>PTC</td>
<td>MQTT, REST, ODBC, SNMP</td>
<td>- ThingWorx is the best-in-class Industrial Innovation platform for developing industrial IoT applications and augmented reality (AR) experiences. - Eliminate complication from IoT application development. - Distribute platform through developers. - Integrated machine learning for multifaceted big data analytics. - Prevalent cloud, embedded or based on IoT solutions.</td>
</tr>
<tr>
<td>Cisco IoT Cloud Connect</td>
<td>Cisco</td>
<td>MQTT, CoAP, XMPP and RESTful HTTP</td>
<td>- Voice and data connectivity. - SIM lifecycle management. - IP session control. - Customizable billing and reporting.</td>
</tr>
<tr>
<td>Universal of Things</td>
<td>Hewlett Packard Enterprise</td>
<td>MQTT, LTN Gateway, CoAP, SMTP</td>
<td>- Secure Monetization: HPE has been in control of the data monetization of many organizations. - Data Analytics: controls and analyses data so that business can develop. - Application Designer and Marketplace: Built-in application to let you create the new IoT services fast. - Platform Architecture: Single Point, Single vendor to control M2M devices.</td>
</tr>
<tr>
<td>Salesforce IoT Cloud</td>
<td>Thunder (open Source)</td>
<td>REST HTTP</td>
<td>- Creating sales orders and capturing potential opportunities. - Services: Request and order repairs automatically. - Marketing: Notifies customers through texts directly on their devices. - Apps: Automatic inspections of inventory.</td>
</tr>
<tr>
<td>Datav</td>
<td>BSquare</td>
<td>HTTP</td>
<td>- Predictive Failure: Increases uptime. - Adaptive Diagnostics: Repairs the failure and avoid any extra costs. - Manages the device. - Enhances efficiency. - Enhances the asset condition. - Keeps track.</td>
</tr>
<tr>
<td>Mindsphere</td>
<td>Siemens</td>
<td>HTTPS or MQTT</td>
<td>- Mind Apps: let you control engine data to follow up new opportunities. - Open cloud Platform: as data Analytics and visions. - Cybersecurity: Follows Manufacturing Standards.</td>
</tr>
</tbody>
</table>
A Review on Cloud and Fog Computing Integration for IoT: Platforms Perspective

4. Fog CoT Applications

Different kinds of data (e.g., sound, light, heat, electricity, mechanics, chemistry, biology, and location) can be acquired in real time by RFID technique, global position system (GPS), sensors, infrared sensors, laser scanners, gas sensors, and other devices. IoT has been involved in various application domains; for example, the applications of smart homes or smart buildings, smart cities, smart business, smart inventory, health-care, environmental monitoring, social security, surveillance. It is essential to provide the production and supply chain with the help of intelligent manufacturing [45].

Fog computing, on the other hand, introduces the same services as the cloud (compute, storage and networking) and has the same mechanisms (virtualization, multi-tenancy, etc.). These common attributes of the cloud and the fog make it possible for the developers to build applications that operate the interact between the fog and the cloud.

Fog computing is complementary to cloud computing and can provide applications that are not suitable for centralized cloud computing:

- Applications having strict latency requirements, such as mobile gaming, video conferencing, etc. Operating these applications on the fog can improve user experience compared to the unreliable QoS produced by the cloud.
- Geo-distributed applications where the distributed data collection points spread over a huge area, for example, pipeline monitoring, or monitoring the environment by the sensors.
- Fast mobile applications connecting smart mobile users (connected vehicles, connected rail).
- Large distributed control systems utilizing a huge number of sensors and actuators to enhance user experience. For example, applications in the transportation, energy, manufacturing, business, and agriculture domains that can operate the interact between the fog and the cloud.
instance, smart grid connected to the rail, and smart traffic light systems [46] [47].

![Figure 5 Applications of IoT supporting by fog](image)

Table 4. IoT vertical markets and fog use cases [3] [19] [20] [21] [45] [48] [49] [50] [51] [52] :
Low Latency (a), Reduced Network Bandwidth (B), Enhanced Security and Privacy (C), Geographic Locality of Control (D), Data Rich Mobility (E), Reliability and Robustness (F), Supporting Advanced Analytics and Automation (G), Hierarchical Organization (H), Energy Efficiency (I), Environmental Constraints (J), Programmability at Multiple Levels (K), Multi-Tenancy (L), Virtualization, Orchestration, and Management (M), Scalability (N), Agility (O), Modularity (P), Openness (Q)

<table>
<thead>
<tr>
<th>IoT Type</th>
<th>Example fog-enabled application</th>
<th>Limitation</th>
<th>Fog overcomes the limitation</th>
<th>Imperatives</th>
</tr>
</thead>
</table>
| Transportation| Smart roads, autonomous vehicles, PCT/rail, parking, UAV ground support, maritime, ports, logistics. | To work with serious and dynamic tasks during real-time vehicle tracking. Since vehicles and smart devices enter or leave from vehicular network very often, access control turns out to be an important issue in context-aware services to guard the privacy of UE. | -Smart urban surveillance based on fog computing.  
- Enables multi-target tracking using a single tracking algorithm.  
-Attribute-based access control scheme is introduced. | A, B, C, D, E, F, G, H, I, J, K, L, M, N, O, P, Q |
| Utilities     | Smart grid, smart meters, water distribution, sewer monitoring, energy management, renewables, Photovoltaic Installations. | Multiple location-aware and low latency applications, where most of the smart logic analysis is executed on smart objects itself.  
-Interoperability and interactivity between heterogeneous terminals in energy management platform. | Stack4Things middleware is provided to implement SaaS (Sensing and Actuation as a Service) and Energy management as a service.  
-Fog computing platform offers the flexibility, interoperability, connectivity, data privacy, and real-time | A, B, C, D, F, G, H, J, L, N, O, P |
5. Challenges and Trends of the CoT with Fog

The cloud with the IoT integration has a lot of benefits. Specifically, it manages IoT resources and gives more low-cost configurations and well-organized IoT services. Also, CoT makes the flow of the IoT processing quick and easy.

The CoT paradigm with fog is not simple; it also handles the new challenges to the IoT environment that cannot be overcome by the centralized cloud architecture, like latency constraint, capacity constraint, resource-constrained devices, network connectivity, and security constraint [53]. Furthermore, the centralized cloud concept is not appropriate for IoT applications whose procedures are time-sensitive. There are many scenarios when a fraction of milliseconds can make significant difference such as telemedicine and patient care. In addition, in the scenario of vehicle-to-vehicle communications, preventing collisions or accidents cannot accept the latency produced.
by the centralized cloud. However, an improved cloud computing paradigm that enhances the capacity and latency constraints is needed to manage these challenges. Cisco in 2012 introduced fog computing to overcome most of these challenges. The service provider produces fog nodes across its geographic area which works as a service point to many tenants for many vertical markets [17]. Fog computing is a paradigm with fewer capabilities compared to the cloud in a distributed manner between various end devices and cloud computing. It introduces an efficient solution for IoT applications that need latency-sensitive. Fog computing is considered to be the basic block of cloud computing [54].

The contribution of fog computing in CoT can be summarized as follows in table 5 [1][3][17][55][56][57][58]:

<table>
<thead>
<tr>
<th>Cloud Challenge</th>
<th>IoT Constraint</th>
<th>How the Fog Can Overcome the Challenge</th>
</tr>
</thead>
<tbody>
<tr>
<td>Latency constraints</td>
<td>The fog performs all computation operations needed such as handling and analysing data and other time-sensitive operations near to the edge, which is the suitable solution to meet the aim of low latency of many IoT applications.</td>
<td></td>
</tr>
<tr>
<td>Network bandwidth constraints</td>
<td>Fog computing is classified data processing toward the CoT devices. The fog permits data processing to be done relying on application needs, available networking, and computing resources. Hence, fog cuts the total of data demanded to be sent to the cloud, which saves network bandwidth.</td>
<td></td>
</tr>
<tr>
<td>Resource-constrained devices</td>
<td>Fog computing is preferred with devices that demand a lot of resources. In such devices, the procedures cannot be uploaded to the cloud. Hence, this results in dropping devices’ complexity, lifecycle costs, and power consumption.</td>
<td></td>
</tr>
<tr>
<td>Uninterrupted services</td>
<td>Fog computing can work alone with IoT devices even though the connection with the cloud has been disconnected.</td>
<td></td>
</tr>
<tr>
<td>IoT security and privacy challenges</td>
<td>Fog computing acts as the proxy for IoT devices to update the software of these devices and security credentials. The fog also uses to monitor the security status of devices under controlled area.</td>
<td></td>
</tr>
<tr>
<td>Mobility</td>
<td>Fog provides an important aspect to the applications which is the connection to mobile devices and though produces mobility parameters like locator ID and separation protocol (LISP) which needs a distributed directory system.</td>
<td></td>
</tr>
<tr>
<td>Heterogeneity constraint</td>
<td>Fog nodes are designed by diverse constructors’ providers and come in various patterns and demand to be deployed depending on their relevant platforms. So, the fog nodes have the capability to work on different platforms.</td>
<td></td>
</tr>
<tr>
<td>Interoperability constraint</td>
<td>Fog nodes can interoperate with different vertical market domains and across various service providers.</td>
<td></td>
</tr>
<tr>
<td>Real-time interactions</td>
<td>Fog computing applications produce real-time interworking among fog nodes in addition to the processing done in the cloud.</td>
<td></td>
</tr>
<tr>
<td>Distributed Data Analysis</td>
<td>Fog nodes perform monitoring and analysis of IoT devices’ data in a distributed way, so detection and transition of incorrect data can be avoided in a timely manner.</td>
<td></td>
</tr>
<tr>
<td>Local Autonomous Operations</td>
<td>Fog nodes provide autonomous operations and self-decision to reduce the amount of data that needs to be sent to the central cloud, as a result of decreasing the latency in the communication and enhancing the response time in case of network failures.</td>
<td></td>
</tr>
<tr>
<td>Federation</td>
<td>The federation of many domains as a part of the fog system suitable conformation mechanisms for the applications’ components, such a conformation should be performed in a well-defined order with respect to the business functionality of the application.</td>
<td></td>
</tr>
<tr>
<td>Power Management constraint</td>
<td>The IoT devices are battery-powered, so low-power system consumption is a major requirement. Many mechanisms can be approved to reduce the power consumption while modelling the IoT devices that use a wireless network.</td>
<td></td>
</tr>
</tbody>
</table>

There are a lot of challenges for existing CoT with fog structure that need to improve [59][60]:
- Standardization (lack of it).
- Heterogeneity network, load or route management, and balancing traffic load.
- Context awareness of IoT sensors and IoT data node identity.
• Data analytics (a lot of IoT platforms support real-time but interactive data is also important).
• Benchmark platform (to measure and analyze the system performance and fault recovery).
• Other issues (the concern about stored personal data, energy management data and security issues).

6. Conclusion

With the increase in the number of devices that are communicated to the Internet through the cloud, there is a strong demand for a computing paradigm like a fog computing to perform the computations and storage at the edge of the network near the terminal devices. This review introduced the concept of fog computing, which acts as an enabler for delay-sensitive data services, giving a better solution for the users in several circumstances. By implementing the edge devices paradigm like the fog computing nodes, IoT will be able to satisfy the corporations’ needs with reliability. This overview also introduced IoT diagrams, fog and cloud platforms, and IoT applications. Finally, several roles and challenges of fog computing in CoT systems are summarized. As consequences of the Characteristics that need to be improved in existing COT with fog, there are still a lot of trends need more researches and work to improve the QoS and produce effective analytics to the fog and CoT integration to serve all IoT application domains efficiently.

References


