# Fog computing: The cloud-IoT/IoE middleware paradigm

Mohammad Aazam and Eui-Nam Huh

©CAN STOCK PHOTO/EVERYTHINGPOSSIBLE. FOG—©CAN STOCK PHOTO/NIKKYTOK.

The Internet of Things (IoT) is a technological revolution that represents the future of connectivity and reachability. In the IoT, *things* refer to any object on the face of the Earth, whether it is a communicating device or a noncommunicating "dumb" object. From a smart device to a leaf of a tree or a beverage bottle, anything can be part of the Internet. The objects become communicating nodes over the Internet through data communication means, primarily through radio frequency identification (RFID) tags. The IoT includes smart objects as well. Smart objects are digital, physical entities, which perform some tasks for humans and/or the environment. This is why the IoT is not only a hardware and software paradigm but also includes interaction and social aspects.

The IoT works on the basis of machine-to-machine (M2M) communications but is not limited to it. M2M refers to communication between two machines, without human intervention. In the IoT, even unconnected entities can become part of it, with a data communicating device, like a bar code or an RFID tag, sensed through a device (it may even be a smartphone sensing it), which eventually is connected to the Internet. In the IoT, unintelligent objects (things) become the communicating nodes. When people become part of it and add more information, the IoT grows into the Internet of Everything (IoE). The IoE is a network of networks where trillions of connections create extraordinary opportunities. The IoE brings together people, data, processes, and things, making networked connections more relevant and valuable. In this way, information is turned into actions, creating new capabilities, richer experiences, and unparalleled economic opportunity for businesses, people, and countries. Today, people are connected to the Internet through gadgets, such as smartphones, personal computers, tablets, and social media. As the evolution continues in the IoE, this connectivity of people would happen in innumerous ways, particularly through various types of sensors. For example, different health-care-related sensors can provide important data on a person's vital signs. This data can be used to create further services. In other words, people themselves would become nodes on the Internet. Connected things would be able to send higher-level information back to people, machines, and other things, enabling more intelligent services, incorporating context awareness. This allows more control over the

Digital Object Identifier 10.1109/MPOT.2015.2456213
Date of publication: 6 May 2016

 

environment. Figure 1 shows the basic building blocks of the IoE.

IoT-based services are rapidly gaining importance. Since 2011, the number of connected devices has already exceeded the number of people on Earth. Connected devices have already reached 9 billion and are expected to grow more quickly and reach 24 billion by 2020. With increasing numbers of heterogeneous devices connected to the IoT and generating data, it is going to be a great challenge for a standalone IoT to perform power- and bandwidth-constrained tasks efficiently. In this regard, the IoT and cloud computing amalgamation has been envisioned. There comes a situation when the cloud is connected with the IoT that generates multimedia data. A visual sensor network or closed-circuit television connected to the cloud can be examples of such a scenario. Since multimedia content consumes more processing power, storage space, and scheduling resources, it will be very important to manage them effectively and perform efficient resource management in the cloud.

Other than that, mission-critical and latency-sensitive IoT services require a very quick response and processing. In this case, it is not feasible to communicate through the distant cloud, over the Internet. Fog computing plays a very vital role in this regard. Fog computing refers to bringing networking resources near the underlying networks. It is a network between the underlying network(s) and the cloud(s). Fog computing extends the traditional cloud computing paradigm to the edge of the network, enabling the creation of refined and better applications or services. Fog is an edge computing and micro data center (MDC) paradigm for IoTs and wireless sensor networks (WSNs).

Research on fog computing is in its early stages; therefore, no standard architecture is available regarding managing resources in the fog. Very limited literature exists on fog computing and the Cloud of Things (CoT). Flavio Bonomi et al. present the basic architecture of fog computing, which does not include its practical implications and resource management for the IoT. Similarly, Salvatore J. Stolfo et al. present data protection through fog computing but do not go into resource management and related matters.

In this article, we present a description on how the fog is going to work and how is it going to help in the efficient, effective, and fair management of resources for the IoT and other underlying devices.

**The IoE brings together people, data, processes, and things, making networked connections more relevant and valuable.**

## The CoT

The future is web 3.0, the ubiquitous computing web. Since 2011, the number of people on Earth has already been outnumbered by the number of connected devices. With a high level of increase in connected devices, there is going to be a lot of data in future. Managing and storing that data locally and temporarily will not be possible anymore. Rental storage space is going to be required. Moreover, this huge amount of data must also be utilized in a more effective way, creating further services. Data must not only be formed to information, and further to knowledge, but it should be made a means of wisdom for the user. Such a type of processing is not possible at the IoT end, where devices are lightweight and not rich in resources. This implies that processing and computation must also be made available there on a rental basis. All this is possible with cloud computing. The IoT and cloud computing working in integration make a new paradigm called the CoT.

The CoT aids in managing IoT resources and provides more cost-effective and efficient ways to produce services. The portfolio of services is extended significantly with cloud–IoT integration. With the CoT, the services to be provided are in the cloud, giving ubiquitous access to the users, extending the scope of the services, and making the access of services much easier and efficient.

For the service provider, it also helps in creating cost-effective services and generates more financial gain. The CoT provides the necessary infrastructure and applications that can be reused by different stakeholders, such as end users, government organizations, health departments, emergency departments, municipal departments, and application integrators, in creating user-centric services and taking benefits from the IoT as well as the cloud. With

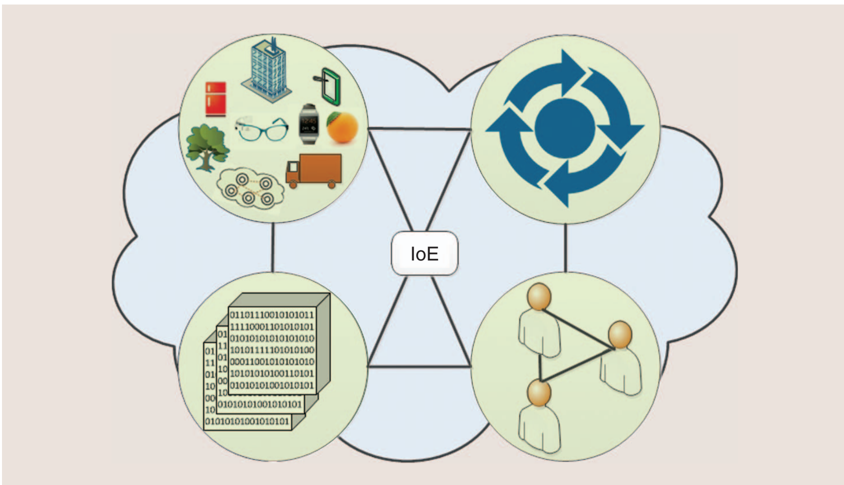

**FIG1** The IoE—connecting people, things, data, and processes.

the CoT, heterogeneous resources can be abstracted and aggregated in accordance with the semantics of the "things," thus enabling a Things as a Service (TaaS) paradigm. Data analysis also becomes more practical with the CoT.

However, there are some scenarios where the CoT also requires a middleware to handle extensive processing locally and preprocess the data before letting it go in the cloud. With the evolution of the IoT into the IoE, a lot of risks are involved. Location and personal-data privacy is going to be a main concern. For all such situations, an additional security layer and data filtration at the middleware layer are a must. That middleware is termed as "fog," as discussed in the next section. The CoT overall communication pattern is presented in Fig. 2.

## Fog computing

Fog computing, an MDC paradigm, is a highly virtualized platform, which provides computation, storage, and networking services between the end nodes in the IoT and traditional clouds. In contrast to the cloud, which is more centralized, fog computing targets the services and applications with widely distributed deployments. As shown in the overall architecture in Fig. 3, the fog will be able to deliver high-quality streaming to mobile nodes, like moving vehicles, through proxies and access points positioned accordingly, such as along highways and tracks. The fog suits applications with low latency requirements, emergency and health-care-related services, video streaming, gaming, and augmented reality, among others. For smart communication, fogs are going to play an important role. Context-aware computing can also be made possible with a fog MDC. The gateway is the device that gathers the data from the underlying nodes. There are certain situations when the gateway is required to do some sort of preprocessing- or interoperability-related tasks, which it cannot do if it is standalone. In that case, the fog is required. Therefore, the gateway has to be made smarter with fog capabilities. We call such a type of gateway a *fog smart gateway (FSG)*. An FSG is more context aware and works on the basis of the feedback from the application. In this way, it works smartly by communicating data only when needed. The extra capabilities of acting smartly are incorporated with the help of a co-located fog network.

**Fog will be able to deliver high-quality streaming to mobile nodes, like moving vehicles, through proxies and access points positioned accordingly, such as along highways and tracks.**

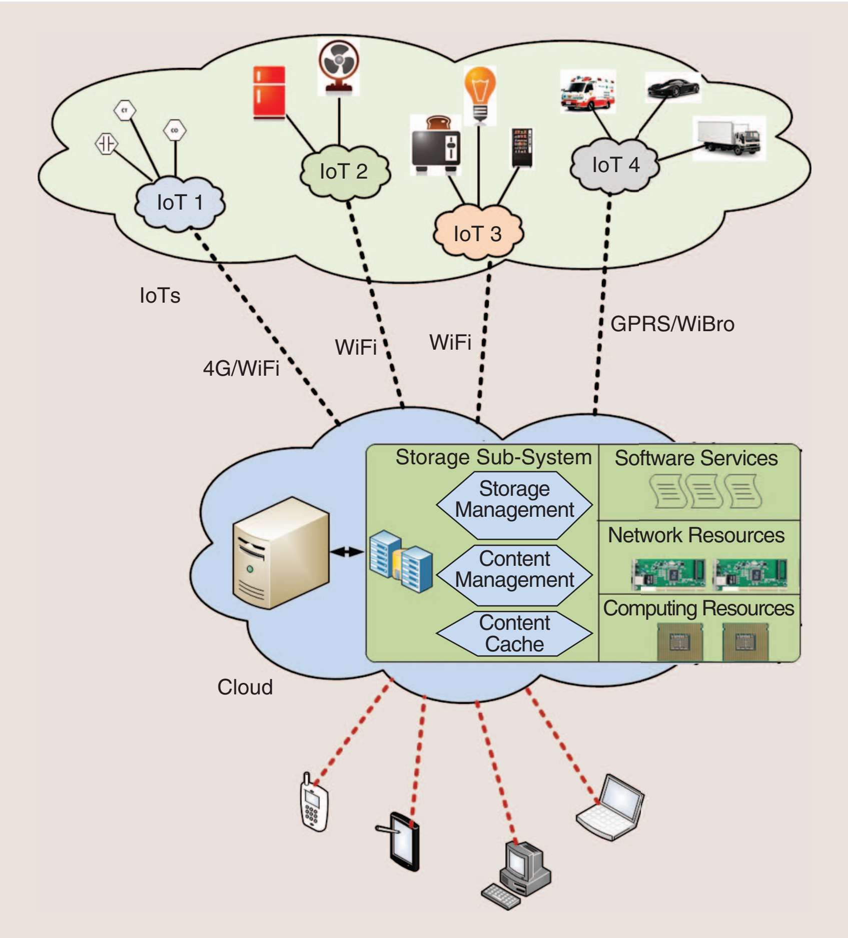


**FIG2** The CoT—data communication.

The underlying nodes and networks are not always physical. Virtual sensor nodes and virtual sensor networks are also requirements for various services. Similarly, temporary storage, preprocessing, data security and privacy, and other such tasks can be done easily and more efficiently in the presence of a fog. Based on the feedback from an application, the gateway must decide the timing and type of data to be sent. This kind of gateway would help in the better utilization of network and cloud resources. The data collected from WSNs and the IoT will be transmitted through gateways to the cloud. The received data is then stored in the cloud, and from there it is provided as a service to the users. We have presented smart gateway in detail along with its architecture in (Aazam, 2014).

Since the fog is localized, it provides low-latency communication and more context awareness. Fog computing allows for the real-time delivery of data, especially for delay sensitive and health-care-related services. It can perform preprocessing and notify the cloud, before the cloud could further adapt that data into enhanced services. With heterogeneous nodes, heterogeneous types of data would be collected. Interoperability and transcoding then becomes an issue. The fog plays a vital role in this regard. Likewise, the IoT and WSN federation, in which two or more IoTs or WSNs can be federated at one point, can be made possible through the fog. This will allow for the creation of rich services.

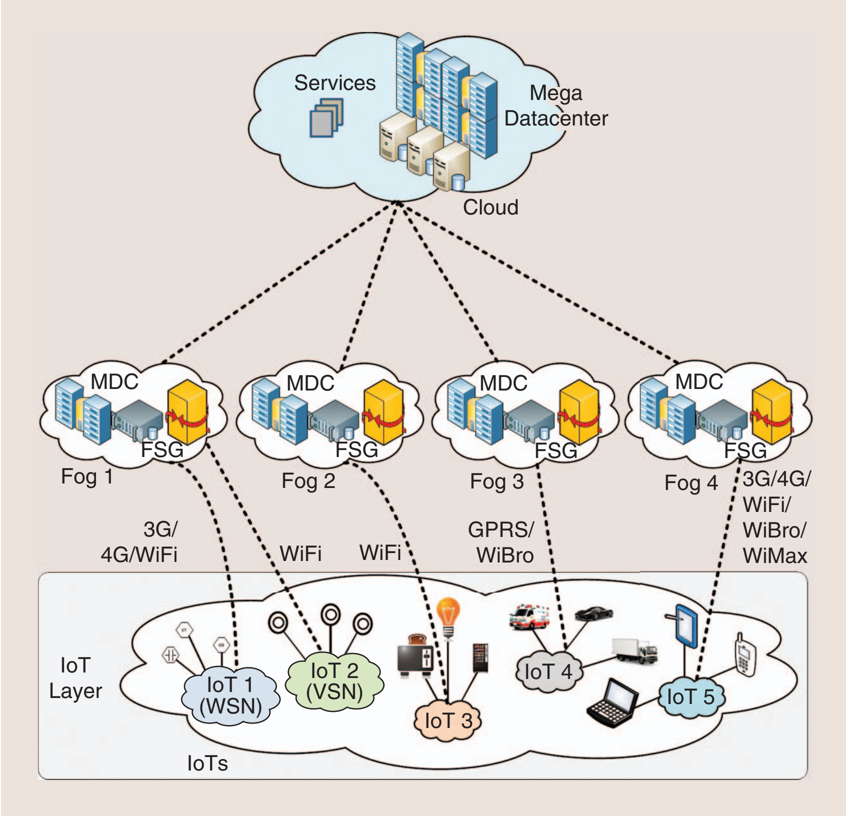


**FIG3** Smart Gateway with fog computing.

### *The difference between fog and cloud*

Both fog and cloud computing provide computation, storage, application, infrastructure, and data resources. However, they are still different from each other. The key difference is the fog's proximity to the underlying accessing nodes. The fog is localized, while the cloud is generalized. The fog extends the distant cloud to the edge of the network, closer to the accessing devices, IoTs, and WSNs. In other words, the fog is a descended cloud. Fog adds an extra layer of security to the sensitive data, including healthcare, location, metropolitan security, and other related services. The quality of cloud services, particularly multimedia, depends upon the quality of the core network. On the other hand, fog is much richer since it is available locally. Similarly, when resource-constrained devices are to be offloaded, fog is the most viable solution, rather than the cloud (or the cloud only), because it is more efficient and easy to access.

Keeping in view the basic tasks fog can provide, its overall layered architecture is presented in Fig. 4. In the physical and virtualization layer, physical nodes, WSNs, virtual nodes, and virtual sensor networks (VSNs) are managed and maintained according to the requirements. The monitoring layer watches the activities of the underlying nodes and networks. Which node is performing what task at what time and what is required from it next is monitored here. Other than this, the power-constrained devices or nodes are monitored on their energy consumption basis as well, so that effective measures can be taken in time.

The preprocessing layer performs data-management-related tasks. It analyzes the collected data, performs data filtering and trimming, and in the end, more meaningful and necessary data is generated. Data is then temporarily stored in the fog resources. Once the data is uploaded in the cloud and it is no longer required to be stored locally, that data is then removed from the storage media.

The IoT and WSNs may generate some private data as well. Ubiquitous health care and smart healthcare services generate private data of the patients. Similarly, location-aware data may also be sensitive in some cases, which should be made secure. This is where the security layer comes into play. In the end, at the transport layer, the ready-to-send data is uploaded to the cloud, burdening the core to the minimum and allowing the cloud to create more useful services.

**Fog is the most viable solution, rather than the cloud (or the cloud only), because it is more efficient and easy to access.**

## Conclusion

With rapidly increasing IoT services, service management, quality of service, efficiency, and users' satisfaction have become crucial. The future is the CoT, in which IoTs are amalgamated with cloud computing for better resource management and service provisioning. In the case of multimedia content, much resources are required. Emergency, health care, and other latency-sensitive, as

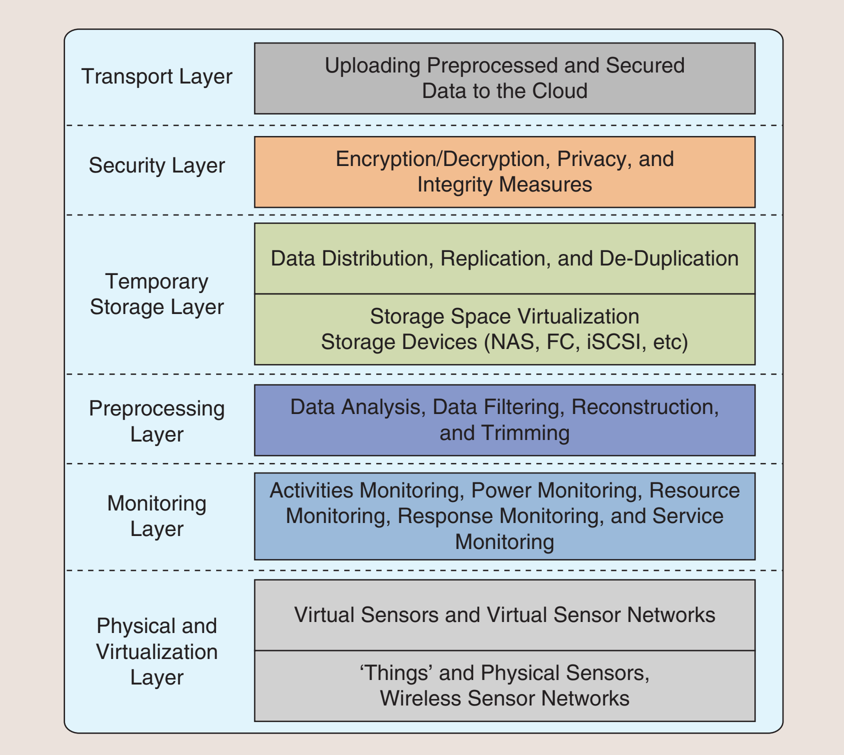


**FIG4** Layered architecture of Fog.

well as security-/privacy-sensitive services, require fog, as an MDC, to be present between the underlying nodes and the distant cloud. Efficient and in-time scheduling and management of resources allow data centers to perform according to the situation and help customer satisfaction.

## Acknowledgment


This research was supported by the Ministry of Science, ICT, and Future Planning, Korea, under the Information Technology Research Center support program [NIPA-2014 (H0301-14-1020)] supervised by the National IT Industry Promotion Agency. The corresponding author is Prof. Eui-Nam Huh.


## Read more about it


- G. Kortuem, F. Kawsar, D. Fitton, and V. Sundramoorthi, "Smart objects and building blocks of internet of things," *IEEE Internet Comput. J.*, vol. 14, no. 1, pp. 44–51, Jan.–Feb. 2010.
- D. Evans, "Internet of everything," in *Proc. Cisco IBSG*, 2012, pp. 1–9.
- J. Gubbi, R. Buyya, S. Marusic, and M. Palaniswami, "Internet of things (IoT): A vision, architectural elements, and future directions," Tech. Rep. CLOUDS-TR-2012-2, July 2012.
- M. Aazam, P. P. Hung, and E.-N. Huh, "Cloud of things: Integrating internet of things with cloud computing and the issues involved," in *Proc. 11th IEEE Int. Bhurban Conf. on Applied Sciences and Technology*, Islamabad, Pakistan, 14–18 Jan., 2014, pp. 414–419.
- M. Aazam, P. P. Hung, and E.-N. Huh, "Smart gateway based communication for cloud of things," in *Proc. 9th IEEE Int. Conf. on Intelligent Sensors, Sensor Networks, and Information Processing*, Singapore, 21–24 Apr., 2014, pp. 1–6.
- M. Aazam and E.-N. Huh, "Fog computing and smart gateway based communication for cloud of things," in *Proc. IEEE Future Internet of Things and Cloud (FiCloud)*, Barcelona, Spain, 27–29 Aug., 2014, pp. 464–470.
- F. Bonomi, R. Milito, J. Zhu, and S. Addepalli, "Fog computing and its role in the internet of things," in *Proc. ACM SIGCOMM*, Aug. 17, 2012, Helsinki, Finland, pp. 13–16.
- S. J. Stolfo, M. B. Salem, and A. D. Keromytis, "Fog computing: Mitigating insider data theft attacks in the cloud," in *Proc. 2012 IEEE Symp. Security and Privacy Workshops (SPW)*, 2012, pp. 125–128.
- [9] D. Evans, "The internet of things how the next evolution of the internet is changing everything," Whitepaper, Cisco Internet Business Solutions Group (IBSG), Apr. 2011.
- K. Tei and L. Gurgen, "ClouT: Cloud of things for empowering the citizen clout in smart cities," in *Proc. IEEE World Forum on Internet of Things (WF-IoT)*, Seoul, South Korea, 6–8 Mar., 2014, pp. 369–370.
- S. Distefano, G. Merlino, and A. Puliafito, "Enabling the cloud of things," in *Proc. 6th Int. Conf. Innovative Mobile and Internet Services in Ubiquitous Computing*, Palermo, Italy, 4–6 July, 2012, pp. 858–863.
- I. Khan, F. Belqasmi, R. Glitho, N. Crespi, M. Morrow, and P. Polakos, "Wireless sensor network virtualization: A survey," IEEE Commun. Surv. Tutorials, vol. PP, no. 99, pp. 1–1, 2015.


## About the authors


***Mohammad Aazam*** (aazam@ieee.org) is a post-doctoral fellow at the Department of Systems and Computer Engineering, Carleton University, Ottawa, Canada, since 2015. He earned his B.S. degree from Gomal University in 2006, his M.S. degree from Mohammad Ali Jinnah University in 2011, and his Ph.D. degree from the School of Computer Engineering, Kyung Hee University, Korea, in 2015. He is a Member of IEEE.

***Eui-Nam Huh*** (johnhuh@khu.ac.kr) is a professor in the School of Computer Engineering, Kyung Hee University. He is also founding director of Realtime Mobile Cloud Research Center and chair of the Internet Society Asia-Pacific Advanced Network. He earned his B.S. degree from Busan University in 1990, his M.S. degree from the University of Texas in 1995, and his Ph.D. degree from The Ohio University, in 2002. He is a Senior Member of IEEE.