Innovations in the Industrial Internet of Things (IIoT) and Smart Factory

Sam Goundar
The University of the South Pacific, Fiji

J. Avanija
Sree Vidyanikethan Engineering College, India

Gurram Sunitha
Sree Vidyanikethan Engineering College, India

K. Reddy Madhavi
Sree Vidyanikethan Engineering College, India

S. Bharath Bhushan
VIT Bhopal University, India

IGI Global
PUBLISHER of TIMELY KNOWLEDGE

A volume in the Advances in Computer and
Electrical Engineering (ACEE) Book Series

Published in the United States of America by
IGI Global
Engineering Science Reference (an imprint of IGI Global)
701 E. Chocolate Avenue
Hershey PA, USA 17033
Tel: 717-533-8845
Fax: 717-533-8661
E-mail: cust@igi-global.com
Web site: http://www.igi-global.com

Library of Congress Cataloging-in-Publication Data

Names: Goundar, Sam, 1967- editor.
Title: Innovations in the industrial internet of things (IIoT) and smart factory / Sam Goundar, J. Avanija, Gurram Sunitha, K Reddy Madhavi, S. Bharath Bhushan, editors.
Description: Hershey, PA : Engineering Science Reference, 2020. | Includes bibliographical references and index. | Summary: “This book discusses the development of models and algorithms for predictive control of industrial operations and focuses on optimization of industrial operational efficiency, rationalization, automation, and maintenance”-- Provided by publisher.
Identifiers: LCCN 2019051895 (print) | LCCN 2019051896 (ebook) | ISBN 9781799833758 (h/c) | ISBN 9781799833765 (s/c) | ISBN 9781799833772 (eISBN)
Subjects: LCSH: Automation. | Internet of things--Industrial applications. | Cloud computing--Industrial applications. | Operations research.
Classification: LCC T59.5 .I48 2020 (print) | LCC T59.5 (ebook) | DDC 658.5/14--dc23
LC record available at https://lccn.loc.gov/2019051895
LC ebook record available at https://lccn.loc.gov/2019051896

This book is published in the IGI Global book series Advances in Computer and Electrical Engineering (ACEE) (ISSN: 2327-039X; eISSN: 2327-0403)

British Cataloguing in Publication Data
A Cataloguing in Publication record for this book is available from the British Library.

Chapter 1

The Challenges, Technologies, and Role of Fog Computing in the Context of Industrial Internet of Things

Sasikala Chinthakunta
Srinivasa Ramanujan Institute of Technology, Anantapuramu, India

Shoba Bindu Chigarapalle
https://orcid.org/0000-0002-3637-507X
Jawaharlala Nehru Technological University, Anantapur, India

Sudheer Kumar E.
https://orcid.org/0000-0003-2752-0711
Jawaharlala Nehru Technological University, Anantapur, India

ABSTRACT

Typically, the analysis of the industrial big data is done at the cloud. If the technology of IIoT is relying on cloud, data from the billions of internet-connected devices are voluminous and demand to be processed within the cloud DCs. Most of the IoT infrastructures—smart driving and car parking systems, smart vehicular traffic management systems, and smart grids—are observed to demand low-latency, real-time services from the service providers. Since cloud includes data storage, processing, and computation only within DCs, huge data traffic generated from the IoT devices probably experience a network bottleneck, high service latency, and poor quality of service (QoS). Hence, the placement of an intermediary node that can perform tasks efficiently and effectively is an unavoidable requirement of IIoT. Fog can be such an intermediary node because of its ability and location to perform tasks at the premise of an industry in a timely manner. This chapter discusses challenges, need, and framework of fog computing, security issues, and solutions of fog computing for IIoT.

DOI: 10.4018/978-1-7998-3375-8.ch001

INTRODUCTION

The “Internet of Things (IoT) refers to embodiment of the continuous convergence between the physical aspects of human activities and its reflection on the data world “ (Puliafito et al., 2019). The fast technological advancements have remodeled the industrial sector. They extended the industrial business to the automation of industrial processes by avoiding man power interaction in the industry. In the framework of IIoT, the operation of complex physical machines are interconnected with networked sensors and software applications. It is the technological enabler of significant improvements in the efficiency of modern industrial processes. It consist of sensor networks, machines, robots, actuators, machines, appliances and personnel. Here, the data acquired from the sensors and machines are analyzed to get the valuable data to run factory operations. Generally, industrial big data analysis is performed at the Cloud end.

Generally, Cloud involves Data-Centric Network’s (DCNs), which provides resources for storage and computation to the clients. So every service request and demands of the customers are analyzed and processed within the remotely located DC’s . However, with the increased number of devices associated with the internet and growing technological advances of the IoT, the data handled by the cloud DCs is significant.Both cloud computing and IoT have a gratuitous working relationship.The IoT produces large quantities of data while cloud computing provides a way for that data to reach its destination, thus it helps to make the work more effective (Xu, 2012).

Technological development in manufacturing refers to an advanced manufacturing model enabled by IoT,cloud computing, service-oriented technologies and virtualization that convert manufacturing resources into services that can be accessed and distributed extensively. Even though cloud computing offers several advantages for IoT, its approach normally disputes with

the framework of IIoT. Most often cloud DCs are remote, it may leads to undesirable latency on transmission when the network traffic is heavy. Another limitation of cloud computing is implicit dependency, also known as “vendor lock-in” from the book *Enterprise cloud computing for non-engineer*.

If the technology of IoT depends on cloud (Atlam et al., 2018)collected data from the trillions of devices in the network are enormous and the data should be processed within the cloud DCs for analysis or visualization.Because the IoT devices don’t have enough storage,compute and networking resourcesand they are battery powered.Hence IoT uses powerful resources provided by the cloud for storage and computation(Ramli et al.,2019).

The heterogeneous devices on the IoT network may produces numerous data traffic, it leads to high service latency, network bottleneck and poor Quality.Because in the cloud environment computation,data storage and processing done within DCs,they are available remotely to the end users.

Moreover, in order to process many user requests, the DCs must be up and working 24x7 without fail, which eventually result in a huge amount of energy being used.The IIOT includes various sensor devicesd and machines, they produce the large volumes of data for analysis.The data may be time-dependent or sensitive. Therefore, to take some decisions very quickly the data should be processed locally rather than DCs. Machines in the IIoT scenario require a timely response, unwanted delays can result in severe catastrophic failures.

Bonomi et al. proposed the Fog Computing (FC) model as a way of expanding cloudbased technologies to the network edge, sharing processing, storage, and networking resources and services along the CloudtoThings continuum, closer to IoT devices’ topological proximity.So, the placement of a special node called fog node as an intermediate node to perform tasks efficiently and effectively is a crucial need in IIoT. Due to its placement and ability to do tasks fog is an intermediary node to perform specific timely manner tasks at the premises of an industry.This chapter discusses about fog computing, layered structure of fog computing and key technologies for fog computing, Industrial Internet of Things and its components, role of fog computing in IIoT and its applications, challenges in IIoT, finally conclusion of the work.

LITERATURE SURVEY

Several researchers were published their work in the field of Fog Computing. This section briefly discusses some of the important works related to Fog Computing. Bonomi et al. talked about the importance of FC in the domain of IoT. Yi et al. focused on FC under "seven themes, namely, fog networking, quality of service (QoS), interfacing and programming model, computation offloading, accounting, billing and monitoring, provisioning and resource management, security and privacy". LM Vaquero et al. explained about the "concept of fog computing in terms of emerging trends and enabling technologies and in usage patterns. They also briefly discuss the challenges ahead". Yannuzzi et al. explained " some of the challenges in IoT scenarios and demonstrate that fog computing is a promising enabler for IoT applications". Dasterji et al. discusses "an overview of fog computing along with its characteristics. They introduce various applications that benefit from fog and present several challenges". More recently, Chiang *et al.* given a tutorial on fog computing. "They discuss at a very high level the differences between fog computing, edge computing, and cloud computing. They also present the advantages of fog computing and discuss the research challenges". Many studies have been published on fog computing in depth (Stojmenovic & Wen,2014)and (Chiang et al.,2017) also in the context of particular application domains, i.e., " vehicular Ad-hoc NETworks (VANETs) (Kai et al.,2016), Radio Access Networks (RAN) (Ku et al.,2017,Peng et al.,2016) and Internet of Things (Chiang et al.,2016)".

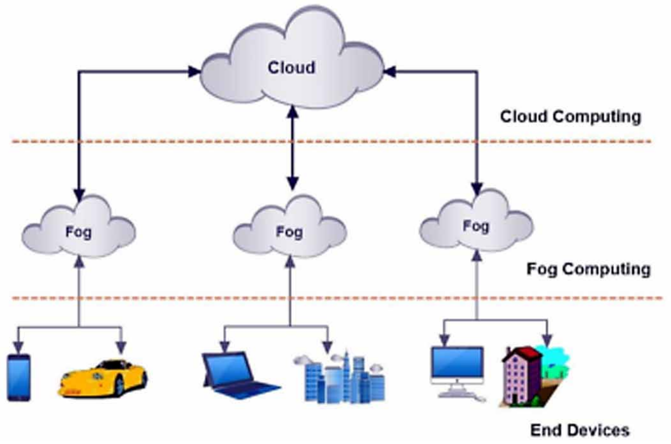
FOG COMPUTING

FC is a distributed computing paradigm between traditional cloud computing and various end devices with limited capabilities i.e. storing, computing and networking services (Mahmud et al.,2018). This type of computing suitable for IoT applications that are latency-sensitive. FC is an extension of the cloud but much relevant to the things that operates on IoTdata. As depicted in Fig 1, It works as an interface between DCs and end devices for getting networking, storage and processing resources closer to the end devices.Usually, those devices referred as "fog nodes". With a network link, those nodes can be deployed anywhere.Any device with access to the network, storage and processing will act as a fog node.For example, "industrial controllers, embedded servers, switches, routers and video surveillance cameras". Even though fog and cloud uses the same resources and similar methodologies and attributes such as virtualization and multi-tenancy, FC offers several advantages for IoT devices like scalability, Low latency, geographical and large-scale distribution and reduced operating costs.

Layered Architecture of Fog Computing

Fog computing is a computing paradigm, that brings the execution of some of the DCs operations at the "edge" of the network. The main objective of fog computing is to provide low and predictable latency

Figure 1. Fog Computing
(Alrawais et al.,2017)



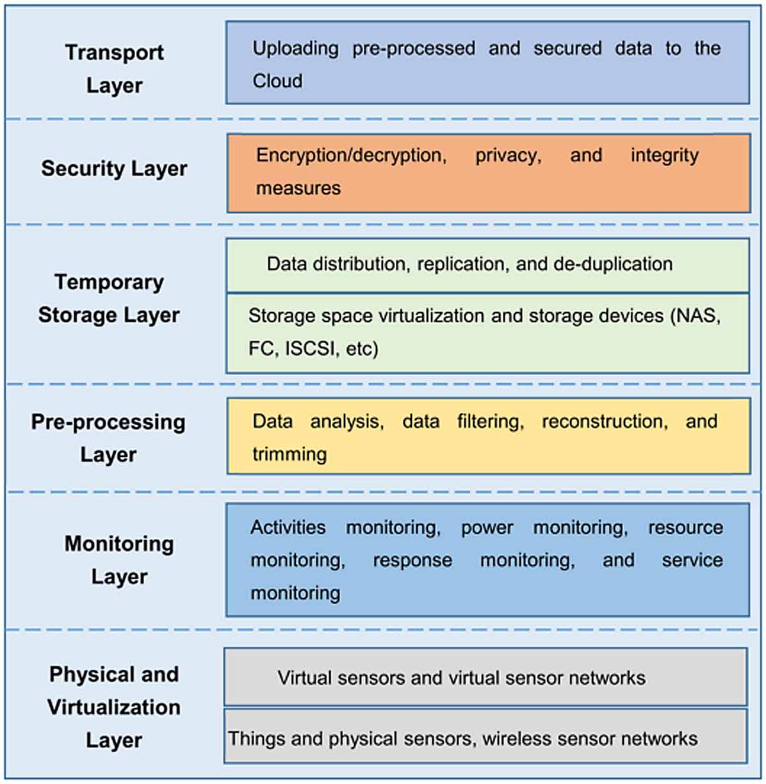
for time-dependent IoT applications(Shi et al.,2015). Figure 2, shows the layered architecture of Fog computing.The architecture of fog computing (Ni et al.,2017)includes six layers from bottom to top: "physical and virtualization layer, monitoring layer, pre-processing layer, temporary storage layer, security and transport layer". The layer of physical and virtualization consists of multiple nodes such as physical nodes,virtual nodes and virtual sensor networks. In this layer, nodes are maintained and managed depending on their service demands and types. The monitoring layer is responsible for monitoring the availability of fog nodes, resource utilization, and sensors nodes and network elements. Hence, through this layer it is possible to moniter the work performed by the particnode in the network. It is also able to know about at what time particular node is executed what task, and what will be needed from it next.

The responsibility for conducting data management activities rests with the pre-processing layer. Throughout this step, the analysis of the collected data, data filtering and trimming will be performed to extract the required information from the collected data.After the data is processed the datais temporarily stored in the temporary storage layer.Data encryption / decryption should be done in the protection layer. This layer can also uses integrity techniques to protect the data from tampering. The preprocessed data is submitted to the cloud in the transport layer, allowing the cloud to retrieve and provide more useful services for the end users (Aazam et al.,2018).

Key Technologies for Fog Computing

The key technologies to implement FC are deterministic virtualization and deterministic networking. Deterministic virtualization enables a fog node to perform functions with various levels of security, time, safety -criticality. For example, "a real-time control function can run on a real-time operating system side by side with a data analytics application on a standard operating system" (Steiner and Poledna,2016).On the other hand, to increase the special distance between physical process and the fog node that controls the process is enabled in deterministic communication. So, control functions are implemented remotely on the fog node.

Figure 2. The layered architecture of Fog Computing
(Aazam et al.,2018)

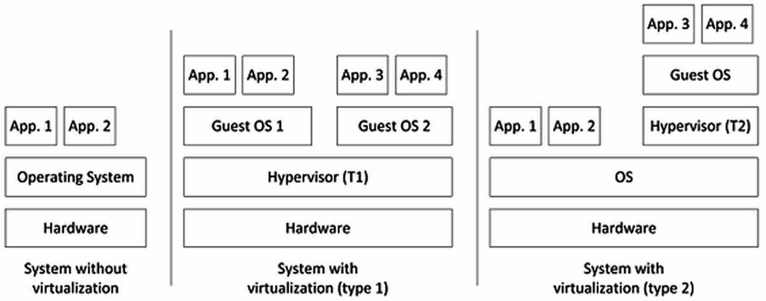


Deterministic Virtualization

Virtualization has been developed as a technique for sharing hardware among many applications, ensuring minimal interference between various applications on each other(Sandstrom et al.,2013) . Fig.3 shows the two types of virtualizations.Generally,Type 1 hypervisors is also known as “bare-metal” or “native” hypervisors. Its implementation allows one or more Operating Systems known as guest OS.Its implementation involves a software layer that is directly executed on the underlyinghardware. It also shares hardware resources, like CPU,memory among different guest OSs, by giving scheduled accessto the resources However, the major drawback with type 1 hypervisor is, it gives limited access to the hardware resources for each guest OS. Hence, in this scenario, each guestOS will not be aware of the existence of the hypervisor. Type 2 hypervisors also known as “hosted” hypervisors.They form a software layer located at the top of an operating system (OS). The structure of a system with type 2 hypervisor is depicted in Figure 3.

Even though Type 1 supervisors are essential for fog computing, type 2 hypervisors also suitable for some applications of FC. However, only the technique of virtualization cannot reduce the limitations of the underlying hardware layer which would depend on the quality of the nonfunctional properties. On the other hand, to know more about the non-functional properties of a layered system that involves virtualization, must know about each layer. For example, Unless the hardware layer provides the capabili-

Figure 3. System structure with and without virtualization
(Barham et al.,2003)



ties to ensure a real-time response, it cannot be retrieved by higher layers, e.g. App, with a comparable level of quality(Barham et al.,2003)

Deterministic Networking

Ethernet has been increasing in market share in industrial automation over the decades. However, because of the consideration of reliability capabilities and lack of real time response as non-functional properties the IEEE 802 set of standards is not efficient.Hence, the industry has developed a lot of real-time variants for Ethernet. Examples are TTEthernet, Profinet, EtherCAT, Ethernet Powerlink and Ethernet/IP. Some of the improvements in industrial Ethernet are discussed in the following sections.

Time Synchronization

The distributed systems includesIEEE has standardized protocols for the synchronization of local clocks in the nodes (e.g., fog nodes). IEEE 1588 was standardized in 2002 with a revision of standards published in 2008.These protocols dynamically elect a grandmaster clock in the distributed system which acts as a time master for other nodes. When the grandmaster is disconnected or fails, the protocols elect a new grandmaster in another way and time synchronization is re-stored.Both IEEE 1588 and IEEE 802.1AS are being updated. The newly added functionality will allow the co-existence of multiple operational grandmasters as well as their time distribution information on standalone network routes.

Schedule Traffic

One way of using synchronized time is to make broadcasting and forwarding decisions over the network. The basic functionality of time-triggered communication is standardized in IEEE 802.1Qbv. Here, the nodes will send the data in accordance with the repetitive communication schedule and the messages will be sent over the network as scheduled.As nodes and switches synchronously process their schedules, they ensure the minimal message queuing delays and guaranteed real-time transmission guarantees are required.

Frame Preemption

IEEE 802.1Qbu standardizes the ability to preempt ongoing frame transmissions. Usually,it is used in networks carrying a limited number of small-complex messages like alarms and long low-critical data messages. In this environment, queuing delays among high-complex messages on each other is acceptable, but queuing delays among high-complex and low-complex messaging may result in the loss of its real-time transmission delay. Therefore,with IEEE 802.1Qbu, the ongoing lower-critical message can preempted by the higher- critical message in the transmission. As a second advantage, when using scheduled traffic (IEEE 802.1Qbv) frame preemption may increase bandwidth utilization of low-complexity messages.

INDUSTRIAL INTERNET OF THINGS

IoT connects essential devices such as sensors in the infrastructure of industries and integrates the instances with current IoT applications.By deploying IIoT, both users and organizations get valuable insights in industrial processes.Therefore,they achieve high IIoT interconnects critical devices and sensors in industries' infrastructure and integrates scenarios with existing IoT applications. With the deployment of IIoT, organizations, as well as users, gain invaluable i nsights into industrial processes. So, they can obtain high productivity along with reliability with reduced cost. In IIoT, machine-to-machine interaction is provided through communication links are. They must satisfy the strict requirements regarding reliability.

Elements of Industrial Internet of Things

The IIoT implementation strategies depends on the components that are required by an IIoT. This section briefly explains the components of IIoT as follows.

Localization of Wireless Sensor and Actuator Networks(WSANs)

With the help of WSANs, different actions are executed depending on sensed data that needs highly reliable and quality data. To convert the data produced from sensors i.e. electrical signal into certain physical action Actuators are used. By using one or more actuators an actor acts on the field. Actor is one of the very important network entity that performs networking responsibilities such as receive,process, transmit and relay the data. In an IIoT environment, WSANs are controlled through over the internet through a remote application over the internet.Actors typically have much more resources compared to sensors such as longer battery life and higher data transmission rate. Nevertheless, the sensed data on the basis of which the actions performed must still be relevant by the time an action is initiated.The actors in IIoT may be Unmanned Aerial Vehicles (UAVs) they are usually known as drones. Furthermore, the sensor and actor environment in IIoT may be complex and hierarchical with the layout of master and slave nodes(Jazdi et al.,2014). A rich middleware can be feasible anchor node like a fog micro-datacenter. Fog can take local actions very fastly and it helps to achieve a cohesive interface with remote application with heterogeneous actors and sensors. In addition, WSANs have many open up privacy and securitychallenges, so there is a need for appropriate solutions for fog environment such as middleware in a strong IIoT environment.

Controlling and Managing Cyber-Physical Systems(CPS)

“A Cyber-Physical System (CPS) allows the networking oftraditional embedded systems and devices in the cyber world” (Gazis et al.,2015).It is a sub-set of IoT that interfaces machines and devices either directly or via remote application. A CPS allows control and remote access to embedded systems and devices.Therefore, it supports numerous flexible services such as remotely turning on the cooling/heating system which is critical to an industrial environment.

Figure 4. CPS Architecture
(Azam et al.,2016)

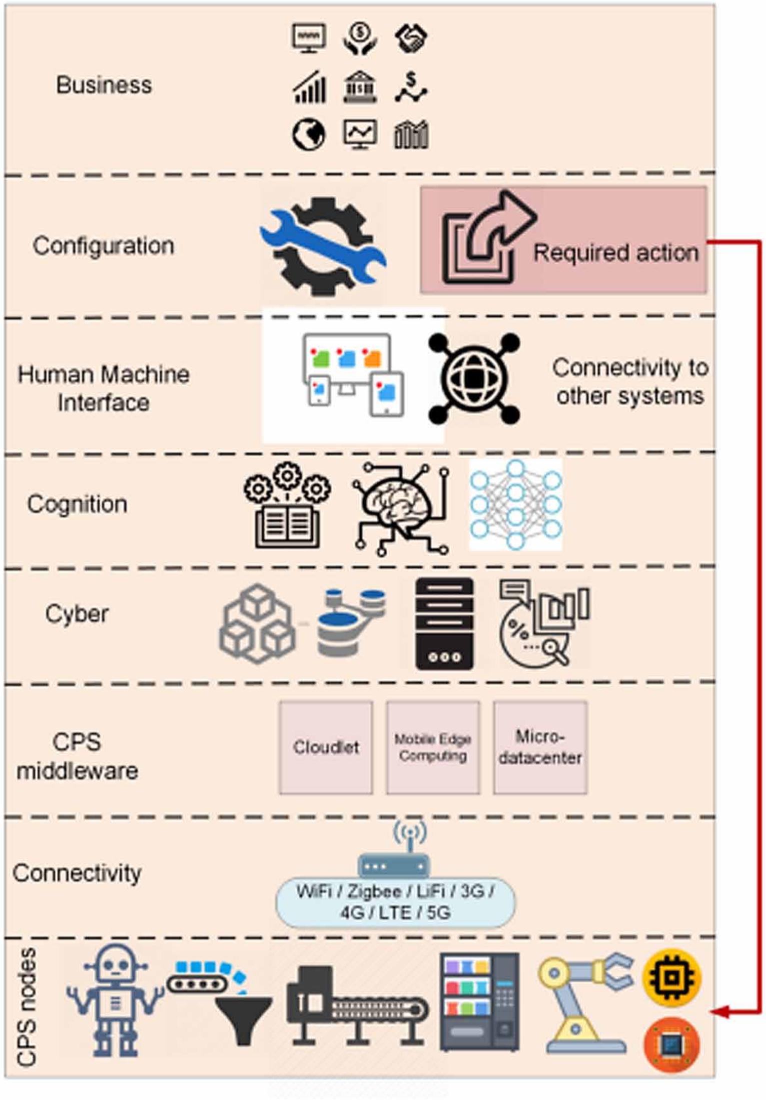


Figure 4 shows the overall layered architecture of CPS.A CPS provides the communications between machines, humans and products. CPS can play vital role in a cost-effective manner in the automation system of industrial process such as maintenance, control, diagnostics, and assistance.Further,business models can also be created using CPS. “A CPS has a control unit which is responsible for controlling sensors, machines, actuators and devices. The entities in a CPS communicate with the real world, gather the data, and process the data inorder to contribute to the industrial process. The CPS nodes requires a communication interface to share the data with several embedded systems, over-the Internet applications, and the cloud. The data sharing is the valuable function of a CPS,since the obtained data may be processed centrally. CPS interacts with machines, actuators and devises,it is extreamely crucial in the

Manufacturing processes processes and thus within the framework of the Industry 4.0 definition. Smart manufacturing, robotic surgery, smart grid, automotive manufacturing are all good examples of CPS based an industrial environment” (Azam et al.,2016).

Industrial Big Data Analytics

When an industrial system is automated and to a certain degree, they may be autonomous, large quantities of data will be involved.By deploying WSANs, WSNs, Virtual Sensor Networks (VSNs), linked machines, devices and appliances continuously generates large volumes of data. The data provide a means to build tailor-made services when the data analytics needed are applied(Salman et al.,2015).

An IIoT without extensive data processing on the sensed data would be incomplete. Information analytics helps in: predictive maintenance, improved fault tolerance, error avoidance, detection and cost-efficiency, etc.

Virtual Sensing and Virtual Sensor Networking(VSN)

A smart system requires multiple sensors to challenge the environment and products to satisfy the the requirements of the system.In this case the deployment of physical sensors is very costly. Virtual Sensors (VSs) are therefore the feasible solution that allows a nearby fog to easily provide the data. Construction of VSNs(Lee et al., 2016)Sensing devices and customisation of virtual sensing devices are used according to the requirements. For example, it is possible to configure VSs for industrial environments,different goods, manufacturing, etc. and machine learning techniques can be applied in the cloud. The program running on the user’s mobile device would then provide the service provider with feedback. Different sensors may be needed within an agricultural area to monitor the development of various plants within various environments or maybe even various times of the day.Interactive sensing capabilities by fog can fulfill the standards for customisable and scalable sensornetworking. Through this way, cost savings can be made and more tailor-made programs can be offered.

Web of Things for the Industry

“When actuators and sensors integrated up with the applications and services available on the web, it is called a web ofthings (WoT) - a refinement of IoT” (Bonomi et al.,2012). Many services would be provided over the web in the IIoT environment.Furthermore,the interconnection of sensors, robots and devices needs integration with third-party web-services. For example, data from a recycling firm is integrated with the sensors and devices of a waste management company to build adaptable and enhanced services(Aazam et al.,2016). Therefore in IIoT, WoT would be a major element.

FOG WITH IIOT

This section describes the scope of the current IIoT with the support of FC. Fog is a middleware,that handles the resources, communication among nodes in the network and local processing of the data. The solution provided by an IIoT may have various entities like actuators, devices andsensors etc. Most of the sensors and devices are small in size and have minimal resources example, sensors embedded on the door. So, this type of devices is inefficient to execute large computations like context-awareness and data analytics. In addition to this, the devices are battery powered so energy consumption is also an important challenge. Hence, to do tasks like complex data analysis and management a middleware i.e. fog is useful for IIoT. Figure 5, shows the fog based architecture for IIoT. In the IIoT environment, the fog can act as an edge, cloudlet, an edge device, a nano-datacenter or a micro-datacenter(Tang et al.,2017).. Fog performs complex tasks on behalf of the devices. It also monitors the sensors energy consumption of each sensor and then changes the data generation frequency respectively. It also analyses and maintains other energy sources i.e. thermal, solar etc. Most of the service providers of IIoT possesses proprietary systems, they need better interoperability approaches with multi-protocol translation, functions and API's to solve issues occurred in interoperability. In IIoT, the major task of fog is to design short-range protocols to communicate with the sensor nodes in the network. Example (Sivashanmugam et al.,2003) if a sensor node is working using Bluetooth it may need to communicate to the IIoT node located at long distance in the network. In this environment, the publish/subscribe paradigm (Depuru et al.,2011) is used, here publishers are the information producer's and subscribers are the information receivers. It provides a better way to distribute information among multiple consumers and producers. In the IIoT environment, fog enables pub/sub service provisioning to enhance business processes.

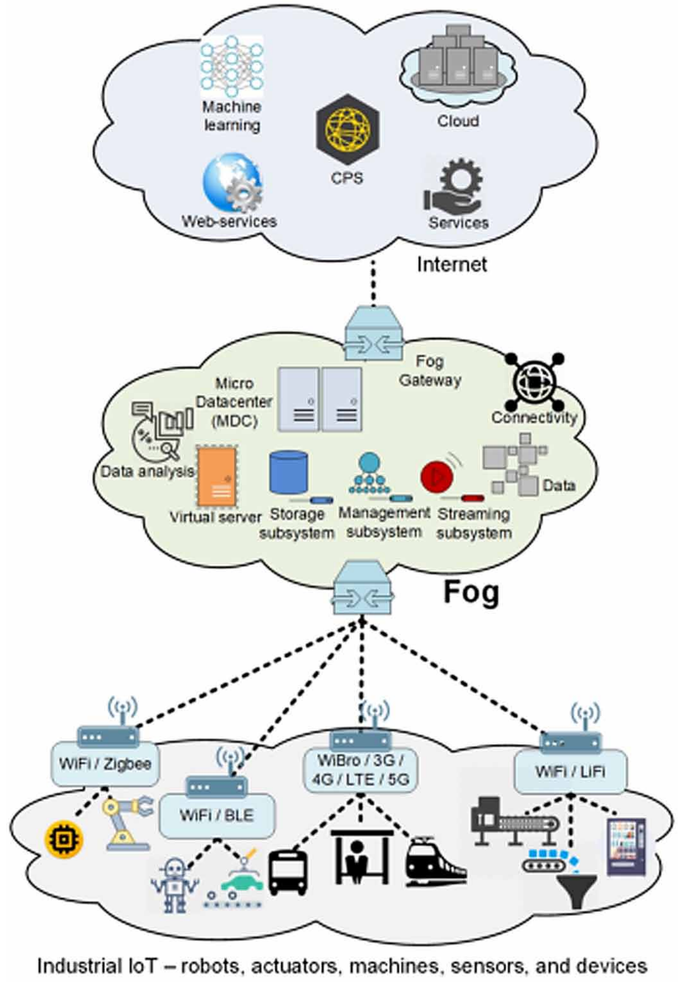
Role of Fog in Industry

Fog computing nowadays plays a critical role in all fields of industry. The whole industry is divided into three sectors: i)extraction, such as mining ii) manufacturing, such as automobiles and iii) services, such as transportation. Each industry have the ability in becoming part of the IoT or the IIoT vision. This section presents some of the areas of industry where IoT can be implemented with the help of fog, to achieve the goals of future smart industries.

Mining

Mining is one of the primary industries that need data analysis. This also increases the scale of the mining sector with the increasing population. Mining entails some risks and is too costly too. Based on IBM surveys, every person needs about 3.11 million pounds of metals, fuel and minerals in his or her lifetime. By using sensors and technologies related to sensors, efficiency would be increased by avoiding excessive waste and costs. In addition, maintenance costs and system failures can be calculated accurately. Before the actual digging process starts, the collected data will save time and money. Therefore, autonomous drilling system or digging, self-driving cars using IIoT standards can be some of the examples of mining

Figure 5. Fog computing in IIoT
(Tang et al.,2017)



industry modernisation. Mining has many challenges and is one of the most dangerous forms of industry. The autonomous drilling method, driverless vehicles may also be some of the examples of modernizing the mining industry using IIoT standards. Mining is one of the toughest kinds of business with many dangers. In the case of mineral and coal mining for example, suffocation, rock sliding and other risks are typical. Besides, certain methods of mining can have dangerous chemical reactions and gas emissions.

Therefore, the use of sensor networks is very useful for capturing data and communication. Additionally, accuracy can also be improved with sensor networking and especially with FC, since extensive processing of data is applied through the co-existing fog. There are also significant concerns for the maintenance and energy efficiency for the mining industry, as it includes heavy machinery and requires a lot of time to manage the entire mining and collection process. With IIoT, mining can lead to better management of machinery and energy-efficiency.

Smart Grid and Power Industry

The smart grid is the latest electrical infrastructure that has grown continuously over the last ten years.

The smart grid comprises renewable energy infrastructure, energy-efficient smart meters (Farhangi, 2010) and smart appliances. In the conventional electric grid scheme, customers are provided with electricity services and billed once a month (Depur et al., 2011). Nowadays, however, the demands are very complex with the technological advancement of automation and autonomous lifestyle, with various electrical machines and appliances. Hence, there is a need for two-way relationship between a consumer and a manufacturer of electrical power, which is the fundamental concept behind the smart grid. "The power resource is distributed in a smart grid to local distribution companies (LDCs), which operate as a micro grid and provide the end-users with electricity" (Chekired et al., 2017). Since the whole concept of a smart grid is not confined to electrical suppliers only, telecommunications operators should also be interested in designing the smart grid. Telecom operators thus sign agreements with local electrical utilities to provide two-way contact between service providers and smart meters through the "Advanced Metering Network" (AMI) (Gungor et al .,2011).

Transportation

"Transport is a key industry and every country's backbone".The transport sector includes commercial public transit buses, metro and subway trains, private cars and cargoes. Intelligent Transportation Systems (ITS) is a transport-related subset of IoT, ITS and the Road Side Unit (RSU) may be fitted with a fog. For example, fog can allow the Internet of Vehicles (IoV), provide location-aware and context-aware services, support in-vehicle entertainment, smart parking and smart traffic lighting management on the basis of road conditions, detours, traffic load these are all examples of ITS allowed by fog computing.

CHALLENGES IN IIOT

To understand the scope of IIoT in the real world, we need to address several challenge, some of them are discussed in this section.

Dynamic Energy Consumption Management

Generally, the industries consume the largest amount of power, so they need to do power management dynamically. The consumption of energy varies based on the industry type even it may vary depending on the season. Thus, consumption of energy affects the lifetime of the network. Hence, energy consumption is a crucial factor in IIoT. It includes not only robotics but also have sensors and actuators. The transition of a large number of data packets continuously in IIoT leads to the consumption of a lot of energy in the network. The energy consumption also affects the time of synchronization. To address this issue, we need algorithms that can solve both time synchronization and energy consumption issues in the IIoT environment. Dynamic management of energy consumption is an important requirement of IIoT.

Interoperability Issues of Devices

Since IIoT involves several subsystems, devices, machines, and external systems, all of them are working together to perform a task. Therefore, integration of the sensors with the system and interoperability techniques becomes a challenge in IIoT.

Security and Privacy

With the progressive increment of the device connectivity to the network large volumes of data are producedwhich may be liable to misuse or theft because most of the industrial applications are deployed on external resources. Hence, IIoT data may be in the risk,that can affect the confidentiality, availability and integrity of the data. So, developing new techniques to ensure security objectives in the IIoT environment is a challenging task.

Fault Detection and Recovery

The IIoT systems highly automated and they have heterogeneous entities. Hence the chance of failures also increases in this environment such as delayed communication, device malfunction, and connectivity failures. An efficient IIoT system must have the capability to detect and rectify common faults in time. Therefore, efficient fault detection algorithms have to be employed at the gateway, middleware or hub or that coordinates different machines and devices.

Service Provisioning Based on Context-Aware

The ability to discover web-services based on the requirement is essential to support a dynamic environment in the industry.In the IIoT environment, the major objective of context awareness is to get contextual information without having existing contextual information or gather contextual information from an existing information. Both cases have different complexities and outcomes, hence context-awareness requires more intelligence and efficiency.

CONCLUSION

The technological advances in the industry introduce the automation of business processes. To provide the support for automation a middleware fog is used in IIoT. This chapter describes the structure of fog computing,IIoT and need of fog in the IIoT environment. Finally, it discusses some of the challenges such as dynamic power management, security and privacy issues, interoperability, and context awareness in the IIoT environment.

REFERENCES

Aazam, M., St-Hilaire, M., Lung, C. H., & Lambadaris, I. (2016, October). Cloud-based smart waste management for smart cities. In *2016 IEEE 21st International Workshop on Computer Aided Modelling and Design of Communication Links and Networks (CAMAD)* (pp. 188-193). IEEE. 10.1109/CAMAD.2016.7790356

Aazam, M., Zeadally, S., & Harras, K. A. (2018). Deploying fog computing in industrial internet of things and industry 4.0. *IEEE Transactions on Industrial Informatics*, *14*(10), 4674–4682. doi:10.1109/TII.2018.2855198

Alrawais, A., Alhothaily, A., Hu, C., & Cheng, X. (2017). Fog computing for the internet of things: Security and privacy issues. *IEEE Internet Computing*, *21*(2), 34–42. doi:10.1109/MIC.2017.37

Atlam, H. F., Walters, R. J., & Wills, G. B. (2018). Fog computing and the internet of things: a review. *Big Data and Cognitive Computing, 2*(2), 10.

Barham, P., Dragovic, B., Fraser, K., Hand, S., Harris, T., Ho, A., Neugebauer, R., Pratt, I., & Warfield, A. (2003). Xen and the art of virtualization. *Operating Systems Review*, *37*(5), 164–177. doi:10.1145/1165389.945462

Bonomi, F., Milito, R., Zhu, J., & Addepalli, S. (2012, August). Fog computing and its role in the internet of things. In *Proceedings of the first edition of the MCC workshop on Mobile cloud computing* (pp. 13-16). 10.1145/2342509.2342513

Chekired, D. A., Khoukhi, L., & Mouftah, H. T. (2017). Decentralized cloud-SDN architecture in smart grid: A dynamic pricing model. *IEEE Transactions on Industrial Informatics*, *14*(3), 1220–1231. doi:10.1109/TII.2017.2742147

Chiang, M., Ha, S., Risso, F., Zhang, T., & Chih-Lin, I. (2017). Clarifying fog computing and networking: 10 questions and answers. *IEEE Communications Magazine*, *55*(4), 18–20. doi:10.1109/MCOM.2017.7901470

Dastjerdi, A. V., & Buyya, R. (2016). Fog computing: Helping the Internet of Things realize its potential. *Computer*, *49*(8), 112–116. doi:10.1109/MC.2016.245

Depuru, S. S. S. R., Wang, L., Devabhaktuni, V., & Gudi, N. (2011, March). *Smart meters for power grid—Challenges, issues, advantages and status. In 2011 IEEE/PES Power Systems Conference and Exposition*. IEEE.

Farhangi, H. (2010). The path of the smart grid. *Power and Energy Magazine, 8*(1), 18-28.

Gazis, V., Leonardi, A., Mathioudakis, K., Sasloglou, K., Kikiras, P., & Sudhaakar, R. (2015, June). Components of fog computing in an industrial internet of things context. In *2015 12th Annual IEEE International Conference on Sensing, Communication, and Networking-Workshops (SECON Workshops)* (pp. 1-6). IEEE. 10.1109/SECONW.2015.7328144

Groom, F. M., & Jones, S. S. (Eds.). (2018). *Enterprise cloud computing for non-engineers*. CRC Press. doi:10.1201/9781351049221

Gungor, V. C., Sahin, D., Kocak, T., Ergut, S., Buccella, C., Cecati, C., & Hancke, G. P. (2011). Smart grid technologies: Communication technologies and standards. *IEEE Transactions on Industrial Informatics*, *7*(4), 529–539. doi:10.1109/TII.2011.2166794

Jazdi, N. (2014, May). *Cyber physical systems in the context of Industry 4.0. In 2014 IEEE international conference on automation, quality and testing, robotics*. IEEE.

Kai, K., Cong, W., & Tao, L. (2016). Fog computing for vehicular ad-hoc networks: paradigms, scenarios, and issues. *The Journal of China Universities of Posts and Telecommunications, 23*(2), 56-96.

Lee, W., Nam, K., Roh, H. G., & Kim, S. H. (2016, January). A gateway based fog computing architecture for wireless sensors and actuator networks. In *2016 18th International Conference on Advanced Communication Technology (ICACT)* (pp. 210-213). IEEE.

Mahmud, R., Kotagiri, R., & Buyya, R. (2018). Fog computing: A taxonomy, survey and future directions. In *Internet of everything* (pp. 103–130). Springer. doi:10.1007/978-981-10-5861-5_5

Ni, J., Zhang, K., Lin, X., & Shen, X. S. (2017). Securing fog computing for internet of things applications: Challenges and solutions. *IEEE Communications Surveys and Tutorials*, *20*(1), 601–628. doi:10.1109/COMST.2017.2762345

Peng, M., Yan, S., Zhang, K., & Wang, C. (2016). Fog-computing-based radio access networks: Issues and challenges. *IEEE Network*, *30*(4), 46–53. doi:10.1109/MNET.2016.7513863

Puliafito, C., Mingozzi, E., Longo, F., Puliafito, A., & Rana, O. (2019). Fog computing for the internet of things: A Survey. *ACM Transactions on Internet Technology*, *19*(2), 1–41. doi:10.1145/3301443

Ramli, M. R., Bhardwaj, S., & Kim, D. S. (2019). *Toward Reliable Fog Computing Architecture for Industrial Internet of Things*. Academic Press.

Salman, O., Elhajj, I., Kayssi, A., & Chehab, A. (2015, December). Edge computing enabling the Internet of Things. In *2015 IEEE 2nd World Forum on Internet of Things (WF-IoT)* (pp. 603-608). IEEE. 10.1109/WF-IoT.2015.7389122

Sandström, K., Vulgarakis, A., Lindgren, M., & Nolte, T. (2013): Virtualization technologies in embedded real-time systems. In *2013 IEEE 18th conference on emerging technologiesand factory automation (ETFA)* (pp. 1–8). Los Alamitos: IEEE Press. 10.1109/ETFA.2013.6648012

Shi, Y., Ding, G., Wang, H., Roman, H. E., & Lu, S. (2015, May). The fog computing service for healthcare. In *2015 2nd International Symposium on Future Information and Communication Technologies for Ubiquitous HealthCare (Ubi-HealthTech)* (pp. 1-5). IEEE. 10.1109/Ubi-HealthTech.2015.7203325

Sivashanmugam, K., Verma, K., Sheth, A. P., & Miller, J. (2003). *Adding semantics to web services standards*. Academic Press.

Steiner & Poledna.(2016). Fog computing as an enabler for the Industrial Internet of Things. *e &iElektrotechnik und Informationstechnik, 133*(7), 310-314.

Stojmenovic, I., & Wen, S. (2014, September). *The fog computing paradigm: Scenarios and security issues. In 2014 federated conference on computer science and information systems*. IEEE.

Tang, B., Chen, Z., Hefferman, G., Pei, S., Wei, T., He, H., & Yang, Q. (2017). Incorporating intelligence in fog computing for big data analysis in smart cities. *IEEE Transactions on Industrial Informatics*, *13*(5), 2140–2150. doi:10.1109/TII.2017.2679740

Vaquero, L. M., & Rodero-Merino, L. (2014). Finding your way in the fog: Towards a comprehensive definition of fog computing. *Computer Communication Review*, *44*(5), 27–32. doi:10.1145/2677046.2677052

Xu, X. (2012). From cloud computing to cloud manufacturing. *Robotics and Computer-integrated Manufacturing*, *28*(1), 75–86. doi:10.1016/j.rcim.2011.07.002

Yannuzzi, M., Milito, R., Serral-Gracià, R., Montero, D., & Nemirovsky, M. (2014, December). Key ingredients in an IoT recipe: Fog Computing, Cloud computing, and more Fog Computing. In *2014 IEEE 19th International Workshop on Computer Aided Modeling and Design of Communication Links and Networks (CAMAD)* (pp. 325-329). IEEE.

Yi, S., Li, C., & Li, Q. (2015, June). A survey of fog computing: concepts, applications and issues. In *Proceedings of the 2015 workshop on mobile big data* (pp. 37-42). 10.1145/2757384.2757397