

Fog Integrated Secured and Distributed Environment for Healthcare Industry with Software Defined Networking

Jamal Kh-madhloom^{1,*} 

¹Computer Sciences and information Technology College, Wasit University, Iraq

*Corresponding Author: Jamal Kh-madhloom

DOI: <https://doi.org/10.31185/wjcm.Vol1.Iss1.5>

Received: January 2021; Accepted: February 2021; Available online: March 2021

ABSTRACT: Fog computing is a segment of cloud computing where a vast number of peripheral equipment links to the internet. The term "fog" indicates the edges of a cloud in which high performance can be achieved. Many of these devices will generate voluminous raw data as from sensors, and rather than forward all this data to cloud-based servers to be processed, the idea behind fog computing is to do as much processing as possible using computing units co-located with the data-generating devices, so that processed rather than raw data is forwarded, and bandwidth requirements are reduced. A major advantage of processing locally is that data is more often used for the same computation machine which produced the data. Also, the latency between data production and data consumption was reduced. This example is not fully original, since specially programmed hardware has long been used for signal processing. The work presents the integration of software defined networking with the association of fog environment to have the cavernous implementation patterns in the health care industry with higher degree of accuracy.

Keywords: Fog Computing, Health Care and Fog Computing, Health Care Industry and Fog Environment



1. INTRODUCTION

Fog networking embraces the internet of things (IoT) definition, in which majority of human-use computers can be linked to each other to create a network. The high performance health tracking systems include smart watches, smart glasses and smart objects with the cloud based technologies [1]. Fog networking is comprised of a control and a data plane. Fog computing allows computing resources to exist at the edge of the network. Fog computing places focus on proximity to end-users and client priorities (e.g. operating expenses, protection protocols, resource exploitation) [2], dense spatial delivery and context-awareness (for what concerns computational and IoT resources), latency reduction and backbone bandwidth savings to achieve greater quality of service (QoS) and edge analytics/stream mining, culminating in superior user-experience and redundancy in case of loss, as it is often able to be used in Assisted Living scenarios. SPAWAR, a branch of the US Navy, is developing a stable software-defined mesh network and evaluating a scalable, secure platform. Computer control applications can take over if a data communications connection is broken. These usage cases include Internet of Things systems such as smart drones. ISODE allows a means to obtain data from an object with a barcode or an RFID tag even though the tag is going from one location to another and sometimes when the barcode data does not shift. In 2011, internet of things and big data created a new collection of specifications which has necessitated a new class of hardware called fog computing [3].

In November 2015, the OpenFog Consortium was formed with Cisco, ARM, Dell, Intel, Microsoft, and Princeton University, to market fog computing. Helder Antunes was selected to become the consortium's first chairman and Intel's Chief Internet of Things Strategist Jeff Fedders was selected to become the consortium's first president [4].

Both cloud storage and fog computing enable end-users to store, execute programs, and import files online. However, fog computing can gain greater access by broad geographical distribution. In this way, we can get the role of the cloud computing [5].

Fog computing enables the usage of computing, storage [6], and networking in all commercial, public, and hybrid cloud settings. Although the edge computing is a medium level of computing power, the fog computing is a cloud form of computing power. For numerous applications, including communication, surveillance, protection, messaging, social networking, safety, smart regions, and many others, huge devices and gadgets are now linked to advanced wireless technologies.

Various paradigms, including the Internet of Things (IoT), Fog Computing, Edge Computing and Cloud Computing, are historically associated with these implementations. For better and performance-conscious communication, all of these implementations need an efficient and high-performance network environment and spawn the fields of research in the related sector [7, 8]. There are smart objects and gadgets linked to wireless technology for real-time contact and signal transmission in the case of the IoT. It is found from numerous study studies that there will be more than 30 billion connected devices using IoT by the year 2020. Moreover, by 2020, the IoT market size is expected to be over 8 trillion dollars [9, 10].

Cloud computing refers to the provision of computing services through distribution and channels centered on the Internet. In cloud computing [11], which offers services under Platform as a Service (PaaS), Infrastructure as a Service (IaaS), Software as a Service (SaaS) and many similar service delivery models, remote data centers are maintained. In the case of cloud computing, bandwidth and channels are very dependent on the Internet connection and performance. Cloud Computing relies on the speed and connection of the Internet, which might not be very successful at all places [12].

For the network-based smart world, the term Fog Computing is gaining enormous popularity these days. Cisco presented the term Fog Computing with the goal of extending cloud computing close to the end-users' control and management area. Fog Computing helps users to access resources and objects without any Internet dependence. Compared to cloud computing-based distribution, Fog Computing is closer to users accessing the services, which makes the access speed very high. The words "Fogging" and "Fog Networking" are both synonymous with Fog Computing [13, 14].

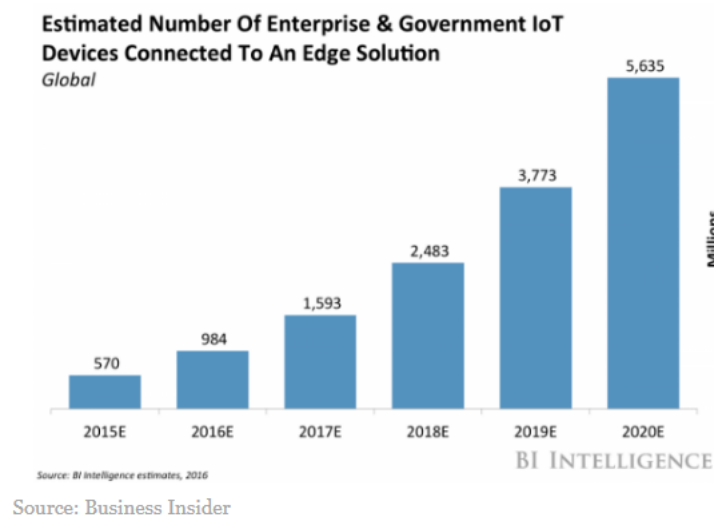


FIGURE 1. Analytics Report on Edge Systems

In Fog Computing, a decentralized environment for computing is developed. In this method, between local systems (nodes or edges) and remote data centers, resources, objects, storage, applications and data analytics are deployed. The actual tools in use are thus close to the user and there is no need to access anything through the Internet [15].

In order to prevent the problems of network bandwidth, latency, delay, jitter, Fog Computing is the intermediate layer between remote cloud and end user. This increases the overall efficiency of the network environment [16]. At the bottom, the final consumer is (On the Earth). Fog now appears close to the end user (Earth). It means that the Fog Computing layer is close to the end system where, without accessing everything using the Internet, actual services are needed [17].

Edge Computing and Mist Computing are closely connected to each other and are used synonymously several times. Mist Computing can be used between the cloud and fog or between the cloud and the edge as an intermediate layer [18]. The programmable automation controller (PAC) devices are used for edge computing, while Mist Computing uses lightweight computing objects using micro-chips and micro-controllers. At the end user site, the implementation of edge computing

or mist computing is carried out. The extension of cloud services to the edge of networks is Fog Computing. Fog Computing works efficiently and rapidly to provide cloud services, while Edge Computing can run without fog or cloud. The computing of the mist is not the obligatory layer of fog computing and can function separately. We can't see beyond 100 meters in Fog in general, but we can still see within range. The same methodology occurs in Fog Computing. We have a variety of services that we have access to the enormous dimensions [19].

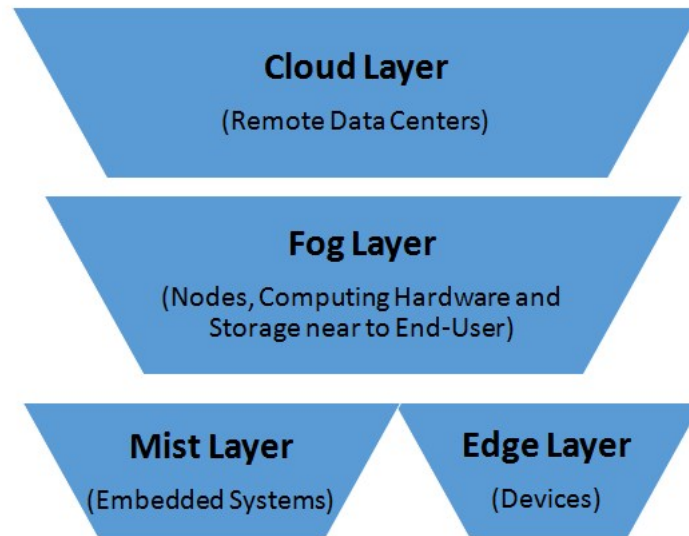


FIGURE 2. Layered Approach

Fog Computing enables the increased performance [20] on following parameters

- Capacity
- Latency
- Bandwidth
- Fault Tolerance
- Robustness
- Security
- Responsiveness
- Speed
- Data Integration
- Energy

2. FOG AND HEALTHCARE INTEGRATION

The way the world does business is evolving every day. There has been a major growth in the use of the cloud infrastructure for several other uses in the recent past. Now the cloud does not merely appeal to basic needs; the Internet of Things (IoT) is the next technical trend. Wireless sensor networks (WSN) is constantly being used to track patients in many healthcare applications. Wearable exercise systems are integrated to help users track health issues. Sensors may be of different shapes and sizes to accommodate the need [21].

This wireless sensor networks may produce a large volume of data. This network knowledge may be beneficial as well as duplicative. This massive volume of big data could overpower the data processing applications. The disposition of irrelevant data needs to be a context-specific operation. The data gathered by the sensors will have to be sent to

Table 1. Key Technologies and Simulation Platforms for Fog Simulation and IoT

URL	Title
github.com/Cloudslab/iFogSim	iFogSim
github.com/emufog/emufog	EmuFog
github.com/di-unipi-socc/FogTorch	FogTorch
clownix.net	Cloonix
imunes.net	IMUNES
contiki-os.org	Cooja
cupcarbon.com	CupCarbon
iot-dsa.org	DSA
mininet.org	Mininet
nodered.org	Node-RED
openiot.eu	OpenIoT
routereflector.com/unetlab	Unetlab
zettajs.org	Zetta
shadow.github.io	Shadow
gns3.com/	GNS3
iotivity.org	IoTivity
kaaproject.org	KAA
nrl.navy.mil/itd/ncs/products/core	CORE
nsnam.org	NS3
netkit.org	Netkit

computational machines, in order to conduct analysis, aggregation, and storage. Large amount of sensors has to be mounted to operate, and this takes up a lot of available capital. Therefore, the usage of sensor devices in a group system may be studied. This will later forward data to a cloud service from this network.

For healthcare purposes, it would not be feasible to build an infrastructure for a simple sensor-to-cloud, because hospitals may not like to keep medical information held in cloud, leading to privacy issues. There is also a real likelihood that a network breakdown or a device collapse could result in harm to the patients themselves. This is where fog computing will profoundly support healthcare systems [22].

Any of the data from the sensors cannot be fully transmitted to the cloud by using just a cloud. Cloud technologies would have tremendous effect on emergency services because of its reliability and its real-time speed. This method is not effective as it is now due to certain problems with latency and security. Intellectual property protection may often be infringed upon as well as jeopardizing the wellbeing of patients. In this scenario, decentralization of cloud computing framework can be discussed. Distributed architecture is separated and then offloaded to more than one computer [23].

The most computationally expensive activities are carried out at the edge of the network instead of in the cloud or in a consolidated data warehouse. Edge computing infrastructure utilizes the power of IoT networks to configure data for IoT local storage and preliminary computing. Cisco expects that by 2020, the amount of computers connecting to the Internet would reach 50 billion. Edge computing would be able to deal with the enormous flow of IoT computers. Edge devices are not suitable for numerous IoT applications all vying for their limited resources, which results in sluggish IoT processing and poor efficiency. A distributed function was applied to this so as to scale and minimize risk of data leakage and thereby improves protection and avoids much of the privacy issues [24].

A fog layer will be installed as an extension of existing cloud infrastructure. Patients' information and records is uploaded and shared between different applications in one single place. "infrastructure refers to points of access, gateways, and routers." The main objective of healthcare is to assist and protect the patient from harm. Implementing this fog layer would enable the effective activation of this requirement. Data is maintained and controlled in the cloud. Thus, the issue of storage, repairs, updates, and costs is solved.

EHR developers and analytics practitioners must find a way to present the data in a quick manner. It requires months, weeks, and occasionally even years to make it from source to end users [25]. We need to function in the healthcare domain in order to be noticed in the workable IoT. An ICU patient can have just minutes or even seconds until his critical state goes from a safe with unstable circumstance and may have major emotional and physical effects on his health condition. Hospitals, physicians and paramedic staff needs to be able to reach a homebound woman with heart failure displaying a dramatic decline in average move counts in case her situation unexpectedly deteriorated [26].

For healthcare organisations, cloud providers serve as a data management layer, because they're considered the data warehouse. Data is submitted wholesale to the cloud such that specific statistics are taken back down into an analytics

engine and then eventually displayed in the interface. Obviously, procedure must take a brief amount of time but sometimes "patient safety and quality care decisions cannot wait for a long time, as well." The solution isn't in the cloud, but in the haze. In this way, fog computing enables computers to make important decisions on their own without cloud storage. Pace is the core of the medical Internet of Stuff.

2.1 IFOGSIM : AN OPEN SOURCE TOOLKIT FOR FOG COMPUTING, EDGE COMPUTING AND IOT

iFogSim is a high-performance instrument package for modeling and simulating Edge Computing, Internet of Things and Fog Computing networks. iFogSim incorporates methods for resource management that can be further tailored according to the field of study.

The iFogSim simulation operates in combination with CloudSim. CloudSim is a commonly used library for simulating the management of resources and cloud-based environments. To manage the events between the components of Fog Computing using iFogSim, the CloudSim layer exists.

Key components and classes with the simulation are as follows

- Tuple
- Monitoring Edge
- Fog Device
- Actuator
- Application
- Sensor
- Resource Management Service

2.2 INSTALLATION OF IFOGSIM

You can download the iFogSim library from a URL called <https://github.com/Cloudslab/iFogSim>. The iFogSim library is written in Java, so customizing and working with the toolkit would require the Java Development Kit (JDK).

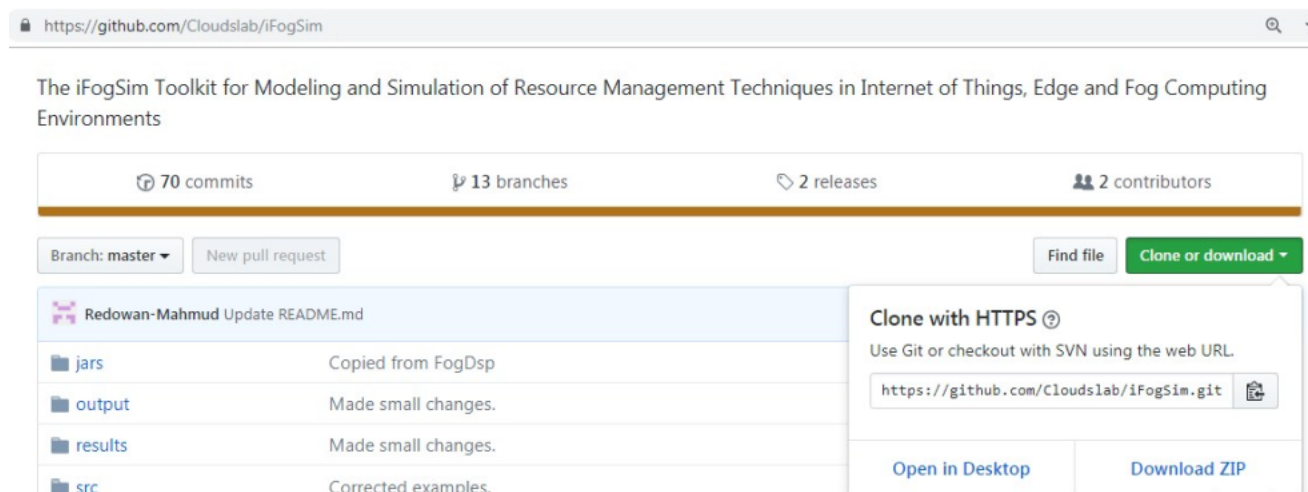


FIGURE 3. Downloading iFogSim

After extracting the toolkit, a directory called "iFogSim-master" will be created. The iFogSim library can be run on any Integrated Development Environment (IDE) focused on Java, such as Eclipse, Netbeans, JCreator, JDeveloper, jGRASP, BlueJ, IntelliJ Concept, JBuilder or any other related IDE.

We build a new project in the IDE as follows in order to incorporate iFogSim on Eclipse IDE

If the library is mounted, the directory structure of iFogSim can be seen on the Eclipse IDE. There are a lot of Java based systems for Fog, IoT and Edge Computing. In order to use iFogSim in Graphical User Interface (GUI) Mode, there

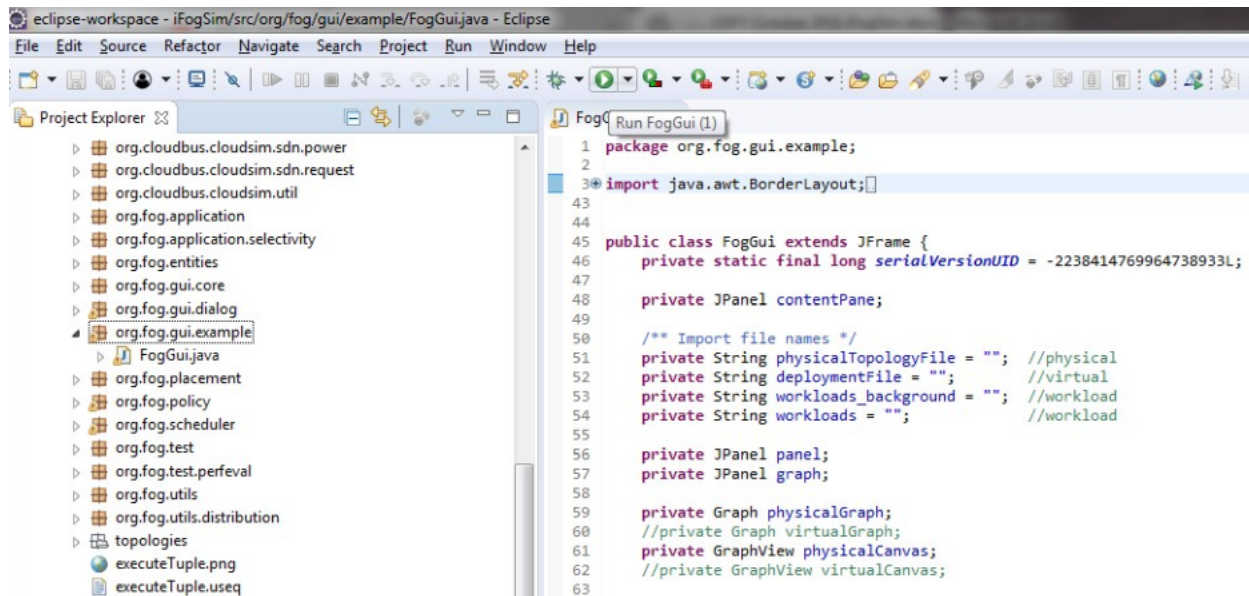


FIGURE 4. iFogSim Environment

is a file FogGUI.java under org.fog.gui.example. This file can be directly executed from the IDE and there are various forms of cloud and fog which can be imported in the simulation work field.

There is Graph Menu in Fog Topology Creator. There is an option to import topology.

The performance can be viewed in the Console of Eclipse IDE.

In iFogSim, there are possibilities for various services like Software Defined Networking (SDN) and cloud computation to be simulated.

The case studies are incorporated in the base installation of iFogSim. We provide an illustration in the analysis of smart surveillance in org.fog.test.perfeval. An overview of each requirements may be performed using criteria such as Energy, Cost Factor, Camera Efficiency and other.

```

Starting DCNS...
Placement of operator FogObject_analyzer on device d-9
successful.
Placement of operator FogObject_tracker on device d-9
successful.
Initialize user_interface on device cloud
Initialize FogObject_analyzer on device d-9
Initialize FogObject_tracker on device d-9
Initialize motion_analyzer on device m-9-9
Initialize motion_analyzer on device m-9-1
Initialize motion_analyzer on device m-9-2
Initialize motion_analyzer on device m-9-3
9.9 Submitted application dcns

```



```

=====
===== RESULTS =====
=====
EXECUTION TIME : 2583
=====
APPLICATION LOOP DELAYS
=====
[motion_analyzer, FogObject_analyzer, FogOb-
ject_tracker] ---> 5.3571428571438195
[FogObject_tracker, PTZ_CONTROL] ---> 3.119999363
=====
TUPLE CPU EXECUTION DELAY
=====
MOTION_VIDEO_STREAM ---> 2.957142857143481
DETECTED_FOGOBJECT ---> 9.1111697142865978
FOGOBJECT_LOCATION ---> 1.5285714285719128
CAMERA ---> 2.199999364
=====
cloud : Energy Dissipated = 1.3338424452551937E7
proxy-server : Energy Dissipated = 834332.999987
d-9 : Energy Dissipated = 1948835.4319992
m-9-9 : Energy Dissipated = 846391.7619942
m-9-1 : Energy Dissipated = 846391.7619942
m-9-2 : Energy Dissipated = 846391.7619942
m-9-3 : Energy Dissipated = 846391.7619942
Cost of execution in cloud = 26129.742857167836
Total network usage = 11191.12

```

Fog computing will be more dominant in 2018 and beyond ahead of 5G cell service roll out. "5G technology occasionally requires very dense antenna deployment," states CenturyLink. The maximum gap is around 20 kilometers between transmitter and receiving antennas. Fog computing infrastructure could be developed, as in a use case like this, among these stations that have a centralized controller that manages apps that are operating on the 5G network, and handles connections to back-end data centers or clouds.

Table 2. Comparison of the Results in different network ping Scenarios

Average Round Trip Time (ms)	Number of Nodes
0.319	3 (ping Forward)
0.175	3 (ping Reverse)
0.315	8 (ping Forward)
0.226	8 (ping Reverse)
0.387	10 (ping Forward)
0.229	10 (ping Reverse)
0.346	20 (ping Forward)
0.216	20 (ping Reverse)

The versatility of utilizing software based networking is rendered simpler with the technology. The history for this example is the virtualization and the remote client network. The results were proven in models with many separate situations containing different combinations of nodes, switches and controllers. In the results and simulation, it is shown that the reverse direction ping in protected shell clients requires less time to complete than safe shell streamline data transfer. Here forward link ping takes longer than the reverse connection ping.

3. CONCLUSION

SDN is a very efficient and scalable way to make up the networks. Software-defined networking is the strategy for high level network services that helps the network owner to manage and track the device and resources. The method utilizing

```

mininet@mininet-vm: ~
mininet@mininet-vm:~$
mininet@mininet-vm:~$ sudo mn --topo single,8 --mac --switch ovsk --control
ler remote
*** Creating network
*** Adding controller
Unable to contact the remote controller at 127.0.0.1:6633
*** Adding hosts:
h1 h2 h3 h4 h5 h6 h7 h8
*** Adding switches:
s1
*** Adding links:
(h1, s1) (h2, s1) (h3, s1) (h4, s1) (h5, s1) (h6, s1) (h7, s1) (h8, s1)
*** Configuring hosts
h1 h2 h3 h4 h5 h6 h7 h8
*** Starting controller
c0
*** Starting 1 switches
s1 ...
*** Starting CLI:
mininet> nodes
available nodes are:
c0 h1 h2 h3 h4 h5 h6 h7 h8 s1
mininet>

```

FIGURE 5. Software Defined Networking

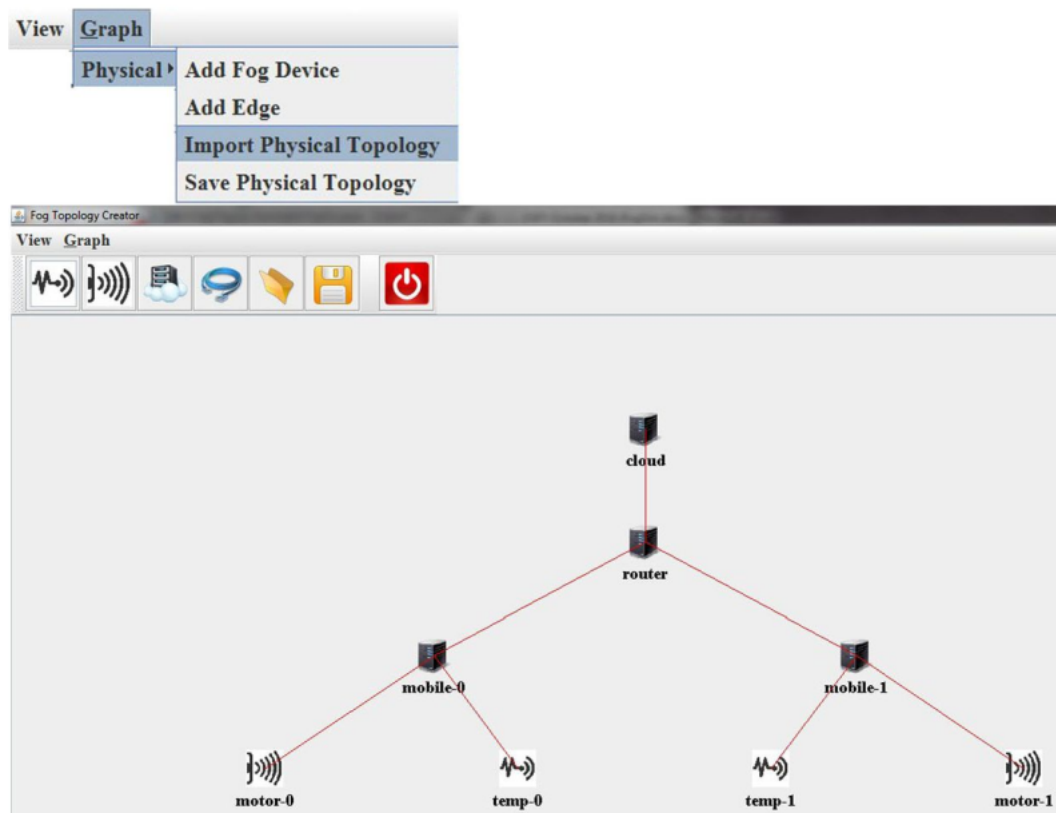


FIGURE 6. Analytics of Objects in Fog

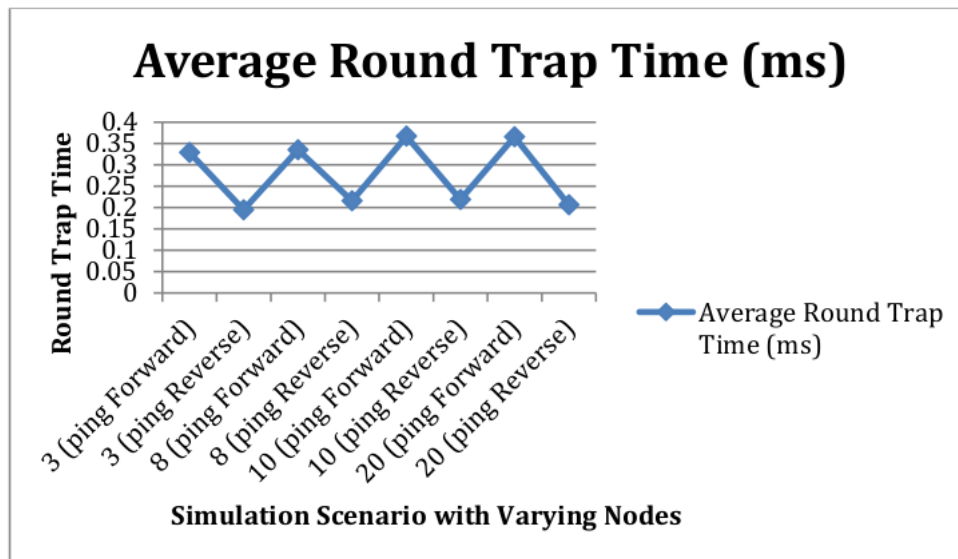


FIGURE 7. Round Trip Evaluation

```
mininet> net
h1 h1-eth0:s1-eth1
h2 h2-eth0:s1-eth2
h3 h3-eth0:s1-eth3
h4 h4-eth0:s1-eth4
h5 h5-eth0:s1-eth5
h6 h6-eth0:s1-eth6
h7 h7-eth0:s1-eth7
h8 h8-eth0:s1-eth8
s1 lo: s1-eth1:h1-eth0 s1-eth2:h2-eth0 s1-eth3:h3-eth0 s1-eth4:h4-eth0 s1-eth5:h5-eth0 s1-eth6:h6-eth0 s1-eth7:h7-eth0 s1-eth8:h8-eth0
c0
mininet>
```

FIGURE 8. Mininet based Implementations

data plane coupling and the control plane decoupling is applied for guaranteeing the protection of the device. In this current situation, OpenFlow is implemented as a software-defined networking (SDN) application Control and data planes are disconnected in SDN technology. A software controlled controller controls the forwarding of knowledge of a vast range of switches; the hardware only carries out the commands of the controller. OpenFlow is an SDN technology about control packets shared between network devices. This would be beneficial for academics to evaluate innovative concepts in a manufacturing context. New kinds of network and framework may be built using terminology such as Rime Network, Smog Network, Haze Network, Dew Network, etc.

FUNDING

None

ACKNOWLEDGEMENT

None

CONFLICTS OF INTEREST

The author declares no conflict of interest.

REFERENCES

- [1] F. C. Chang and H. C. Huang, "A survey on intelligent sensor network and its applications," *Journal of Network Intelligence*, vol. 1, no. 1, pp. 1–15, 2016.
- [2] J. S. Pan, L. Kong, T. W. Sung, P. W. Tsai, and V. Snasel, "Alpha-fraction first strategy for hierarchical wireless sensor networks," *Journal of Internet Technology*, vol. 19, no. 6, pp. 1717–1726, 2018.
- [3] J. Wang, Y. Gao, K. Wang, A. K. Sangaiah, and S. J. Lim, "An affinity propagation-based self-adaptive clustering method for wireless sensor networks," *Sensors*, vol. 19, no. 11, pp. 2579–2579, 2019.
- [4] Z. G. Du, J. S. Pan, S. C. Chu, H. J. Luo, and P. Hu, "Quasi-affine transformation evolutionary algorithm with communication schemes for application of RSSI in wireless sensor networks," *IEEE Access*, vol. 8, pp. 8583–8594, 2020.
- [5] J. Wang, Y. Gao, C. Zhou, R. S. Sherratt, and L. Wang, "Optimal coverage multi-path scheduling scheme with multiple mobile sinks for WSNs," *Computers, Materials & Continua*, vol. 62, no. 2, pp. 695–711, 2020.
- [6] H. Alemdar and C. Ersoy, "Wireless sensor networks for healthcare: a survey," *Computer Networks*, vol. 54, no. 15, pp. 2688–2710, 2010.
- [7] T. N. Gia, M. Jiang, A. M. Rahmani, T. Westerlund, P. Liljeberg, and H. Tenhunen, "Fog computing in healthcare internet of things: a case study on ECG feature extraction," in *Proceedings of the IEEE International Conference on Computer and Information Technology; Ubiquitous Computing and Communications; Dependable, Autonomic and Secure Computing; Pervasive Intelligence and Computing (CIT/IUCC/DASC/PICOM)*, pp. 356–363, IEEE, 2015.
- [8] B. Farahani, F. Firouzi, V. Chang, M. Badaroglu, N. Constant, and K. Mankodiya, "Towards fog-driven IoT ehealth: promises and challenges of IoT in medicine and healthcare," *Future Generation Computer Systems*, vol. 78, pp. 659–676, 2018.
- [9] M. Rahmani, T. N. Gia, and B. Negash, "Exploiting smart e-health gateways at the edge of healthcare internet-of-things: a fog computing approach," *Future Generation Computer Systems*, vol. 78, pp. 641–658, 2018.
- [10] F. Bonomi, R. Milito, J. Zhu, and S. Addepalli, "Fog computing and its role in the internet of things," in *Proceedings of the First Edition of the MCC Workshop on Mobile Cloud Computing ACM*, pp. 13–16, 2012.
- [11] S. Yi, Z. Qin, and Q. Li, "Security and privacy issues of fog computing: a survey," in *Wireless Algorithms, Systems, and Applications. WASA 2015. Lecture Notes in Computer Science*, K. Xu, and H. Zhu, eds., vol. 9204, pp. 685–695, Springer, 2015.
- [12] C. Huang, R. Lu, and K.-K. R. Choo, "Vehicular fog computing: architecture, use case, and security and forensic challenges," *IEEE Communications Magazine*, vol. 55, no. 11, pp. 105–111, 2017.
- [13] O. Osanaiye, S. Chen, Z. Yan, R. Lu, K.-K. R. Choo, and M. Dlodlo, "From cloud to fog computing: a review and a conceptual live vm migration framework," *IEEE Access*, vol. 5, pp. 8284–8300, 2017.
- [14] A. Alrawais, C. Alhothaily, X. Hu, and Cheng, "Fog computing for the internet of things: security and privacy issues," *IEEE Internet Computing*, vol. 21, no. 2, pp. 34–42, 2017.
- [15] H. Xiong, Y. Wu, C. Jin, and S. Kumari, "Efficient and privacy-preserving authentication protocol for heterogeneous systems in IIoT," *IEEE Internet of Things Journal*.
- [16] H. Xiong, Y. Zhao, and Y. Hou, "Heterogeneous signcryption with equality test for IIoT environment," *IEEE Internet of Things Journal*.
- [17] Z. Meng, J. S. Pan, and K. K. Tseng, "PaDE: an enhanced differential evolution algorithm with novel control parameter adaptation schemes for numerical optimization," *Knowledge-Based Systems*, vol. 168, pp. 80–99, 2019.
- [18] H. Gupta, A. V. Dastjerdi, S. K. Ghosh, and R. Buyya, *iFogSim: A Toolkit for Modeling and Simulation of Resource Management Techniques in Internet of Things, Edge and Fog Computing Environments*.
- [19] Q. Tian, S. C. Chu, J. S. Pan, H. Cui, and W. M. Zheng, "A compact pigeon-inspired optimization for maximum short-term generation mode in cascade hydroelectric power station," *Sustainability*, vol. 12, no. 3, pp. 767–767, 2020.
- [20] S. C. Chu, X. Xue, J. S. Pan, and X. Wu, "Optimizing ontology alignment in vector space," *Journal of Internet Technology*, vol. 21, no. 1, pp. 15–22, 2020.
- [21] Y. Huang, M. Hsieh, H. Chao, S. Hung, and J. Park, "Pervasive, secure access to a hierarchical sensor-based healthcare monitoring architecture in wireless heterogeneous networks," *IEEE Journal on Selected Areas in Communications*, vol. 27, no. 4, pp. 400–411, 2009.
- [22] J. S. Pan, X. X. Sun, S. C. Chu, A. Abraham, and B. Yan, "Digital watermarking with improved SMS applied for QR code," *Engineering Applications of Artificial Intelligence*, vol. 97, 2021.

- [23] R. Tso, "Two-in-one oblivious signatures," *Future Generation Computer Systems*, vol. 101, pp. 467–475, 2019.
- [24] T. Y. Wu, C. M. Chen, K. H. Wang, C. Meng, and E. K. Wang, "A provably secure certificateless public key encryption with keyword search," *Journal of the Chinese Institute of Engineers*, vol. 42, no. 1, pp. 20–28, 2019.
- [25] J. Zhang, H. Liu, and L. Ni, "A secure energy-saving communication and encrypted storage model based on RC4 for EHR," *IEEE Access*, vol. 8, pp. 38995–39012, 2020.
- [26] J. M. Wu, G. Srivastava, A. Jolfaei, P. Fournier-Viger, and J. C.-W. Lin, "Hiding sensitive information in eHealth datasets," *Future Generation Computer Systems*, vol. 117, pp. 169–180, 2021.