Role of Fog and Cloud Computing in an IoT-based Environment

**Dr. A. Shaik Abdul Khadir**

Head and Associate Professor of Computer Science

Khadir Mohideen College

(Affliated to Bharathidasan University, Tiruchirappalli)

Adirampattinam – 614 701

Tamil Nadu, INDIA

*hiqmath4u@gmail.com*

**Dr. A. Haja Abdul Khader**

Assistnat Professor of Computer Science

Khadir Mohideen College

(Affliated to Bharathidasan University, Tiruchirappalli)

Adirampattinam – 614 701

Tamil Nadu, INDIA

*ahaja@ymail.com*

ABSTRACT

Fog computing is a distributed computing system where information, processing, storage, and applications are somewhere between the data source and the cloud. Fog computing is also known as “edge computing.” Edge computing is intended to solve challenges by storing information near the “ground.” In case of fog computing, data has been stored on local computers and storage systems instead of routing all the data to the cloud via a centralized DC. The development of fog computing structures gives organizations much more choice to process data and information where applicable. Fog computing is not a substitution for cloud computing, as it works hand in hand with cloud computing to maximize the use of available resources. The major difference between fog and cloud computing is that the cloud is a hierarchical network while fog is a decentralized distributed infrastructure. Fog computing is an intermediary between remote servers and hardware. It governs the data that should be sent to the network and can be handled locally. This chapter deals with the role of fog and cloud computing in an IoT-based environment.

Keywords— Fog computing, edge computing, cloud computing, data cloud and internet of things.

# INTRODUCTION

The internet of things (IoT) is a network of interrelated objects that can communicate with each other using the internet without any external invention. The concept connects each devices or things to the internet. The devices that are components of IoT are called smart devices or things. Sensors, vehicles, portable devices and surveillance cameras are the example of IoT devices or smart devices. Each of these smart devices has it won IP address and can send or receive data from the network.[94]

According to a recent study, many billions of objects or things will be connected to the internet of things by 2020[107]. A large number of IoT applications is being developed and used all over the world. IoT applications are available in a variety of fields including, logistics, retail market, healthcare, traffic management, home support, smart city and smart grid.

The main aim of the internet of things is to connect billions of devices together and provide internet facilities to all these smart devices. Sufficient computing and networking infrastructure need to be given to the IoT applications.

As the recent communication paradigm of IoT is growing at rapid rate, objects of day-to-day use will be connected with microcontrollers, transceivers for digital communication in the near future.

Cloud computing is considered to be suitable computing platform for the internet of things to computing and storage facilities. The important advantage of the cloud computing is that its services can be accessed by the user from anywhere in the world.

Since the cloud provides high computation power and huge storage area, it is easier for the IoT devices to send and receive data from the cloud. The IoT devices may also use the computation facility on the whenever needed.

Even though the cloud computing provides required infrastructure for the internet of things to communicate, it is not so efficient in handling IoT data. The cloud is naturally a centralized environment butt the IoT devices work in a distributed fashion. Due these reasons, the cloud computing is not able to fulfil low-latency and location-awareness demands of the IoT devices.

To overcome the drawbacks of cloud computing and satisfy the needs of the internet of things, the networking major, Cisco, introduced a new paradigm called fog computing to support the internet of things concept.

The fog computing plays an intermediary role between the cloud and the IoT devices. It brings the cloud closer to the things or smart objects. Fog computing is a fast-growing distributed computing paradigm that supports heterogeneity and high mobility of the internet of things.

In fog computing, the term ‘fog’ refers to the ‘cloud nearer to the ground’ or ‘ground-level cloud’. Fog computing connects IoT devices to the cloud and offers a number of services to the IoT devices at the network edge.

Fog computing adds a middle layer between the cloud and IoT devices in the conventional IoT architecture. In other words, it acts a bridge between the IoT layer and the cloud layer.

As per the layered model, the fog layer collects the data gathered by sensors, GPS devices, RFIDs, cameras, and other sensing devices. Then the fog node performs data pre-processing and data aggregation. Finally the resultant data are moved to the cloud layer for storage and data analytics.

Since fog computing has heterogeneity property, fog devices commonly called fog nodes are of different types. These devices include set top boxes, access points, roadside units, proxy servers and cellular base station.

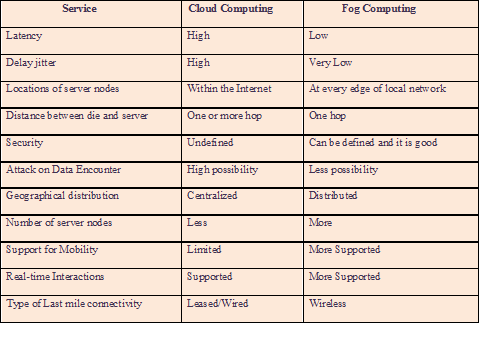
All applications of the internet of things concept are also applicable to fog computing since it is the only supporting technology for IoT. Transportation is one of the major application areas fog computing. Traffic management is also a component of transportation field.

This research work is concerned with smart railway traffic management that applies the fog computing and the internet of things technologies.

# NEED FOR FOG COMPUTING

Fog computing is also called fog networking or fogging. It is sometimes interchangeably used with edge computing because the fog services are only available at the network edge.

**Table 1: A comparison of cloud with fog**



Fogging is a decentralized platform for computing where resources for computation and application services are distributed at the end of the network. Fog computing allows various types of IoT and fog devices to interoperate with each other.

The fog network just adds another layer in the usual IoT environment. This means that fog computing supplements the cloud services in the traditional internet of things setup. However, this type of computing paradigm solves many issues that exist in the cloud-based IoT platform. Table 1 compares the cloud computing with the fog based on the services.

The main objectives of fog computing include reducing the network traffic to the cloud and minimize the response time for the IoT devices. The fog architecture does send all data generated by the sensing devices such as RFIDs, sensors, cameras. Most of the data processing operations are done in the fog layer itself. High-level sensor data analytics is only on the cloud. Thus the overall performance of the IoT applications is enhanced by the use of fog computing.

The fog computing was introduced by Cisco to support some IoT-based applications that are not suitable for the cloud computing. The application areas that need fog computing for the IoT :

* Time-sensitive applications
* Geographically distributed applications
* Application with high mobility
* Applications that require low-latency
* Large-scale distributed applications

The above applications system can be implemented with the help of the fog architecture. The internet of things based applications and services such as smart grid, smart traffic management, smart city, connected trains, gaming systems, video streaming systems, etc are well suited for fog computing.

# THE FOG MODEL

The fog computing is a newer computing paradigm based the on the capability of the cloud computing. Figure 1 shows the distributed processing of fog computing. Here, there are three layers: cloud computing layer, fog computing layer and IoT devices layer.

The fog-based model utilizes both wired and unwired transmission media for the data communication between layers and devices. The IPv6 protocol is widely used for addressing since it has 128 bits to identify each and every node in the network.

In the cloud computing layer, Provider A and Provider B are two cloud service providers. These two clouds regarded as public cloud.

In case of fog layer, each element called fog node communicates with both public and private clouds. According to the figure, two private clouds are placed within the fog limits. Fog devices such as routers, gateways, access points receive the stream data from the sensing devices.

IoT devices layer consists of end devices or smart devices including cameras, mobile phone, and sensors. Fog computing supports geographical distribution as the end devices and edge devices are naturally heterogeneous.

The distributed paradigm offers limited computing, storage, networking and management services to the clients and end users. Fog computing allows data processing locally in the fog node in order to minimize cloud-to-end data transportation. But, integrated data analytics is done only in the cloud.

Thus fog computing paradigm is ideal for applications that need high mobility, low latency, heterogeneity and geographical distribution.

.



**Figure 1: Fog computing and its distributed processing**

# THE IOT-BASED TRAFFI CONTROL

The growth of the field of IoT is very fast as the number of smart devices attached to the internet is increasing day by day. This field opens enormous opportunities for the birth of numerous distributed wireless applications.

The internet of things is fit for applications that require high mobility, geographical distribution, and quick response. Therefore, real-world applications like smart grid, smart city, and traffic management can be implanted with the help of IoT.

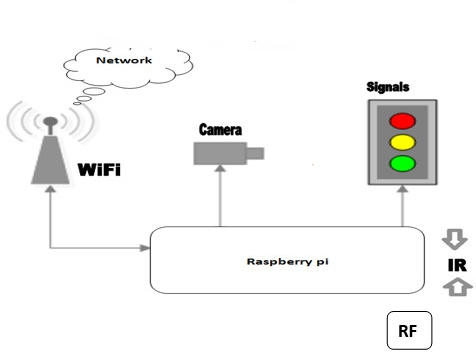
Train traffic management is highly time-sensitive problem that needs to be addressed to save lives of train passengers and the general public. It is very tedious to handle the traffic management in the railways since accidents may occur at various places in the railway transport system.

Here, an IoT-based smart traffic management system for railways is implemented. Traffic congestion is one of the issues in train traffic management. Due to traffic congestion, travel might be increased resulting difficulty to the passengers. On the other hand, a proper traffic control system has been necessitated to prevent train accidents.

Figure 2 depicts the architecture of smart train traffic control system using the concept of the internet of things. Each node of the model contains Raspberry Pi kit, signal LED board, camera, IR sensor and RFID device.

This IoT-based traffic control system has many advantages as compared to manual traffic management. This is very accurate and more reliable than human-operated traffic control in the railways.

The given model solves congestion, rail traffic clearance and signal management. With the use of IoT devices like Raspberry Pi, train traffic data will be pushed to the cloud for high level decision-making and smart traffic control. Meanwhile, local data processing and signaling are done the Python code fed into the IoT device or kit.



**Figure 2: Smart Traffic Control using IoT**

In the IoT-based smart traffic control system, a number of sensing devices can be connected to the Raspberry Pi kit. Each IoT device can communicate with the nearest one using wireless transmission technology.

The following the basic components of each node of the internet of things oriented smart train traffic control system:

1. Raspberry Pi kit
2. Wi-Fi base station
3. Pi camera
4. IR sensor
5. RFID device
6. LED lights
7. **Raspberry Pi kit**



**Figure 3: Raspberry Pi 3 – Model B**

The basic IoT device is the Raspberry Pi kit. It is a credit-card sized single board computer. It support operating systems like Debian and Raspbian and can be programmed using Python and Scratch. The device can easily be connected to monitor or TV and the standard input devices of keyboard and mouse are also supported by the device

The Raspberry has been introduced in three generations. Each generation kit is available in different models. In the IoT-based smart traffic control system, Raspberry Pi 3 Model B kit is used as the IoT device. It contains Broacom SoC (System on Chip) and GPU. Its RAM can be extended up to 1GB. Raspbian OS is running from the SD card. Figure 6.3 shows the Raspberry Pi 3 Model B kit.

1. **Wi-Fi base station**

The term Wi-Fi stands for wireless fidelity which is a popular wireless standard. The Wi-Fi base station usually refers to the wireless access point for computers. Basically, it is a low-power transmitter or wireless router that can communicate with nearby computers and other wireless devices. Here, Wi-Fi connects IoT devices with the cloud and sensors

1. **Camera**

For continuous monitoring, either conventional video camera or Pi camera can be used in the traffic management system. Pi Camera is the HD camera used for taking picture and video. This camera is attached to the Raspberry Pi kit via CSI port. Figure 6.4 shows a 5 MP Pi camera.



**Figure 4: Pi Camera**

1. **IR sensor**

****

**Figure 5: IR Sensor**

Infrared sensor simply called IR sensor is a sensing device where infrared ray is used for transmission. Figure 6.5 shows the image of an IR sensor. It consists of two elements: transmitter and receiver. Normally, IR sensors are utilized for two purposes. The sensor will measure the heart emitter by an object detect the motion. If the IR ray transmitter the transmitter will get

1. **RFID device**

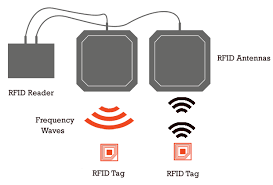
RFID is an abbreviation of radio frequency identification. It is a wireless technology through which encoded digital data in a small chip called RFID tag are recognized by its reader. This communication technology is working using electromagnetic waves.

Figure 6 shows how RFID technology functions in the IoT environment. Each RFID tag is attached to its corresponding antenna. [100] RFID tags sends data at a particular frequency. The corresponding antenna captures the data and passes it to the reader.

RFID technologies can be classified into two types namely, near and far technology. A near RFID reader uses a coil by which one has to pass AC current and generate a magnetic field.

RFID tag with smaller coil produces a potential because of the ambient changes in the magnetic field. This voltage is then coupled with a capacitor to accumulate a charge, which then powers up the tag chip. The tag can then produce a small magnetic field to the digital data. This encoded form of data is recognized by the corresponding reader.

Here radio waves with various frequencies are used for data communication between the RFID antenna and the tags. RFID tags are also of two types: active tags and passive tags. Every active tag has its own power source. But in the case of passive, there is a different phenomenon. Passive tags get power from the EM waves emitted by the nearest RFID reader [137-138]. The RFID technology can cover up to hundreds of meters.



**Figure 6: Functioning of RFID**

1. **LED lights**

Light emitting diodes are called LEDs. The smart traffic control system uses only LED lights to indicate the traffic signal to the trains. There are various types of LEDs available. To display three colors, three LED lamps need to be utilized.

The infrared sensors will give high output whenever heavy traffic and some obstacle in the track. Pi camera continuously monitoring the rail track for any toward incident. If it happens, the Python code will alert the railway authorities. RFID tags placed near tracks, in the trains, on signal poles and railway stations are used to identify the current location of the trains and other conditions in the surroundings. Thus the IoT-based system would help reduce the train traffic congestion.

By this system time management for signal lights is done which will reduce the rail traffic congestion problem.

The given IoT-based traffic control system for railways can also be implemented with fog computing concept. The proposed fog based model will add another layer between IoT devices and the cloud. The goal of using fog computing is to enhance the performance and storage cost

# THE PROPOSED FRAMEWORK FOR SMART TRAFFIC MANAGEMENT

The research work proposes a fog computing based framework for smart train traffic management for railways. The new fog-based model is applied to the train traffic management application only because the railways is highly accident prone mode of transport. Train accident may occur at any time and any place due human error.

The Figure 6.7 shows the layered model of the proposed smart train traffic management framework. It consists of four layers:

1. Cloud Layer
2. Fog Layer
3. IoT Device Layer
4. Sensor Layer

Fog Layer

Cloud Layer

IoT Device Layer

Sensor Layer

**Figure 7: The Layered Model for Proposed Framework**

1. **Cloud Layer:**

It is the uppermost layer of the model. In this layer, the cloud services are available for the user. This layer is responsible for receiving the result of the programs executing on the edge of the network (fog layer) and provides high level applications for smart traffic management.

1. **Fog Layer**

This is the new layer added in the fog computing platform for handling traffic data and ensuring smooth transportation. It gathers data from the corresponding IoT devices in the below layer.

1. **IoT Device Layer**

The third layer from the top is called the IoT device layer. It has numerous IoT devices to process the sensor data. The layer may contain any of Raspberry Pi, Arduino, Tessel, Spark and Galileo kits.

1. **Sensor Layer**

The bottommost layer of the framework will be the sensor. The sensors are tiny electronic devices that collect data from the surroundings and send it to the nearest IoT device for processing. There are various types of sensors such as temperature sensor, MEMS sensor, ultrasonic sensor, presence sensor, etc. This layer may also include actuators for traffic signaling and alarming purposes

The present model proposes the use of fog computing paradigm to support the usual cloud layer. Since the train traffic handling is highly time-sensitive application. Fog computing is needed here to reduce end-to-end data communication between the sensors and the cloud. Otherwise, the network traffic will also be high resulting time delay and poor performance of the system as mentioned in the conventional IoT-based system.

If any delay arises during data transmission, the system would not prevent the near future accidents. Train accident seems to occur in various forms and some amount of latency leads to the loss many lives. Such a viable fog computing based smart train traffic management is required by overcoming the drawbacks of the usual IoT-based model.

# CONCLUSION

The fog-based smart train traffic management systems avoids collision of trains, fatal accidents at railway crossings, derailment in the moving train and prevents fire accident both inside and outside the trains. Moreover, traffic data analytics is done in fog and cloud layers of the proposed model.

This framework can further be improved to establish communication between two trains and include other types of sensors related to intelligent train traffic management.

##### REFERENCES

[1] Aazam, M.; Hung, P.P.; Huh, E. Smart Gateway Based Communication for Cloud of Things. In Proceedings of the 2014 IEEE Ninth International Conference on Intelligent Sensors, Sensor Networks and Information Processing, Singapore, 21–24 April 2014; pp. 1–6.

[2] Aazam, M.; Huh, E.N. Fog computing and smart gateway based communication for cloud of things. In Proceedings of the 2014 International Conference on Future Internet of Things Cloud, FiCloud 2014, Barcelona, Spain, 27–29 August 2014; pp. 464–470.

[3] Aazam, M.; Huh, E.N. Fog computing micro datacenter based dynamic resource estimation and pricing model for IoT. Proc. Int. Conf. Adv. Inf. Netw. Appl. AINA 2015, 2015, 687–694.

[4] Adhatarao, S.S.; Arumaithurai, M.; Fu, X. FOGG: A Fog Computing Based Gateway to Integrate Sensor Networks to Internet. In Proceedings of the 29th International Teletraffic Congress, Genoa, Italy, 5–7 September 2017; Volume 2, pp. 42–47.

[5] Agarwal, S.; Yadav, S.; Yadav, A.K. An Efficient Architecture and Algorithm for Resource Provisioning in Fog Computing. Int. J. Inf. Eng. Electron. Bus. 2016, 8, 48–61.

[6] Ai, Y.; Peng, M.; Zhang, K. Edge cloud computing technologies for internet of things: A primer. Digit. Commun. Netw. 2017, in press.

[7] Ajith Theja, K., Kumaresan, M., Senthil Kumar, K.,Automated Unmanned Railway Level Crossing System Using WSN, International Journal of Innovative Research in Computer and Communication Engineering, Vol. 3, November 2015.

[8] Akshay Jain, Shivam Jain and Shambhu Bharadwaj, "Fog Computing," in Proceedings of ICAC-2016, pp.316-32.

[9] Alenezi, A.; Zulkipli, N.H.N.; Atlam, H.F.; Walters, R.J.; Wills, G.B. The Impact of Cloud Forensic Readiness on Security. In Proceedings of the 7th International Conference on Cloud Computing and Services Science (CLOSER 2017), Porto, Portugal, 24–26 April 2017; pp. 511–517.

[9] Alrawais, A., Alhothaily, A., Hu, C.,and Cheng, X., ``Fog computing for theInternet of Things: Security and privacy issues,'' IEEE Internet Comput., vol. 21, no. 2, pp. 34-42, Mar. 2017.

[10] Al-Doghman, F., Chaczko, A., Ajayan, A.R.,and Klempous, R., “A review on fog computing technology,” in Systems, Man, and Cybernetics (SMC), 2016 IEEE International Conference on. IEEE, 2016, pp.001 525–001 530.

[11] Amit Sangroya, Saurabh Kumar, Jaideep Dhok and Vasudeva Varma, Towards Analyzing Data Security Risks in Cloud Computing Environments, Springer-Verlag Berlin Heidelberg, pp. 255–265, (2010).

[12] Aoun, R., and M. Gagnaire, “Towards a fairer benefit distribution in Grid environments,” inProc. IEEE/ACS AICCSA Conf., 2009,pp. 21–26.

[13] Aoun, R., E. A. Doumith, and M. Gagnaire, “Resource provisioning for enriched services in Cloud environment,” in Proc. IEEE CloudCom Conf., 2010, pp. 296 –303.

[14] Ashton, K. “Internet of things,” RFID J., June 2009.

[15] Atlam, H.F.; Alenezi, A.; Walters, R.J.; Wills, G.B. An Overview of Risk Estimation Techniques in Risk-based Access Control for the Internet of Things. In Proceedings of the 2nd International Conference on Internet of Things, Big Data and Security (IoTBDS 2017), Porto, Portugal, 24–26 April 2017; pp. 254–260.

[16] Atlam, H.F.; Alenezi, A.; Walters, R.J.; Wills, G.B.; Daniel, J. Developing an adaptive Risk-based access control model for the Internet of Things. In Proceedings of the 2017 IEEE International Conference on Internet of Things (iThings) and IEEE Green Computing and Communications (GreenCom) and IEEE Cyber, Physical and Social Computing (CPSCom) and IEEE Smart Data (SmartData), Exeter, UK, 21– 23 June 2017; pp. 655–661.

[17] Atlam, H.F.; Alenezi, A.; Alharthi, A.; Walters, R.; Wills, G. Integration of cloud computing with internet of things: challenges and open issues. In Proceedings of the 2017 IEEE International Conference on Internet of Things (iThings) and IEEE Green Computing and Communications (GreenCom) and IEEE Cyber, Physical and Social Computing (CPSCom) and IEEE Smart Data (SmartData), Exeter, UK, 21–23 June 2017; pp. 670–675.

[18] Atlam, H.F.; Alassafi, M.O.; Alenezi, A.;Walters, R.J.;Wills, G.B. XACML for Building Access Control Policies in Internet of Things. In Proceedings of the 3rd International Conference on Internet of Things, Big Data and Security (IoTBDS 2018), Setúbal, Portugal, 19–21 March 2018; pp. 253–260.

[19] Atlam, H.F.; Alenezi, A.; Hussein, R.K.; Wills, G.B. Validation of an Adaptive Risk- Based Access Control Model for the Internet of Things. Int. J. Comput. Netw. Inf. Secur. 2018, 10, 26–35.

[20] Atzori, L., Iera, A., and Morabito, G., ``The Internet of Things: A survey,'' *Comput. Netw.*, vol. 54, no. 15, pp. 2787- 2805, Oct. 2010.

[21] Babaeizadeh Mahnoush, Majid Bakhtiari, and Alwuhayd Muteb Mohammed. "Authentication Methods In Cloud Computing: A Survey," Research Journal of Applied Sciences, Engineering and Technology 9.8 (2015): 655- 664.

[22] Bader, A., Ghazzai, H., Kadri, A., and Alouini, M.S., ``Front-end intelligence for large-scale application-oriented Internet-of-Things,'' IEEE Access, vol. 4, pp. 257-272, Jun. 2016.

[23] Bhagyashri Katole, Manikanta Sivapala and V. Suresh, Principle Elements and Framework of Internet of Things, Research Inventy: International Journal of Engineering and Science, vol. 3, issue 5, pp. 24–29, July (2013).

[24] Bilal Ghazal, Khaled EIKhatib, Khaled Chahine, Mohamad Kherfan, " Smart traffic Light Control System ", IEEE 2016.

[25] Bokefode, J. D., Ubale, S. A., Apte Sulabha, S., and Modani, D. G., Analysis of DAC MAC RBAC Access Control based Models for Security, International Journal of Computer Applications, vol. 104, no. 5, October (2014).

[26] Bonomi, F.; Milito, R.; Zhu, J.; Addepalli, S. Fog computing and its role in the internet of things. In Proceedings of the First Edition of the MCC Workshop on Mobile Cloud Computing-MCC ’12, Helsinki, Finland, 17 August 2012; pp. 13–15.

[27] Bonomi, F.; Milito, R.; Natarajan, P.; Zhu, J. Fog Computing: A Platform for Internet of Things and Analytics. In Big Data and Internet of Things: A Roadmap for Smart Environments; Studies in Computational Intelligence; Springer: Cham, Switzerland, 2014; Volume 546, pp. 169–186.

[28] Bonomi, F., Milito, R., Natarajan, P. and Zhu, J., “Fog computing: A platform for Internet of things and analytics”, in: N. Bessis, C. Dobre (Eds.), Big Data and Internet of Things: A Roadmap for Smart Environments, in: Studies in Computational Intelligence, vol. 546, Springer International Publishing, 2014,

[29] Buyya, R., Yeo, C. S., and Venugopal, S., “Market-oriented Cloud computing:Vision, hype, and reality for delivering IT services as computing utilities,” in Proc. IEEE/ACM Grid Conf., 2008, pp. 50–57.

[30] Chiang, M.; Zhang, T. Fog and IoT: An Overview of Research Opportunities. IEEE Internet Things J. 2016, 3,854– 864.

[31] Choi, N.; Kim, D.; Lee, S.; Yi, Y. Fog Operating System for User-Oriented IoT Services: Challenges and Research Directions. IEEE Commun. Mag. 2017, 55, 2–9.

[32] Dastjerdi, A.V.; Gupta, H.; Calheiros, R.N.; Ghosh, S.K.; Buyya, R. Fog Computing: Principles, architectures, and applications. In Internet of Things: Principles and Paradigms; Morgan Kaufmann Publishers Inc.: San Francisco, CA, USA, 2016; pp. 61–75.

[33] Dastjerdi, A.V.; Buyya, R. Fog Computing: Helping the Internet of Things Realize Its Potential. IEEE Comput. Soc. 2016, 112–116.

[34] Dodson, S, “The Net Shapes up to Get Physical”, Guardian, 2008.

[35] Dsouza, Clinton, Gail-Joon Ahn, and Marthony Taguinod. "Policy-driven security management for fog computing: Preliminary framework and a case study." Information Reuse and Integration (IRI), 2014 IEEE 15th International Conference on. IEEE, 2014.

[36] Ezechina, M. A., Okwara, K. K., Ugboaja, C. A. U., The Internet of Things (Iot): A Scalable Approach to Connecting Everything. The International Journal of Engineering and Science 4(1) (2015) 09-12.

37] Fang, W., “A paradigm shift to fog computing from cloud computing and edge computing,” Journal of Nanjing University of Information Science and Technology: Natural Science Edition, vol. 8, no. 5, pp. 404–414, 2016.

[38] Ferraiolo, D. and Kuhn, R., Role-Based Access Controls, In Proc. of the 15th NIST- NCSC National Computer Security Conference, Baltimore, MD, pp. 554–563, October (1992).

[39] Fisher, D. K., Rapid Deployment of Internet-Connected Environmental Monitoring Devices, Advances in Internet of Things, vol. 4, pp. 46–54, (2014).

[40] Garbacki P. and Naik, V. K., “Efficient Resource virtualization and sharing strategies for heterogeneous Grid environments,” in Proc. IFIP/IEEE IMSymp., 2007, pp. 40–49.

[41] Gazis, V.; Leonardi, A.; Mathioudakis, K.; Sasloglou, K.; Kikiras, P.; Sudhaakar, R. Components of fog computing in an industrial internet of things context. In Proceedings of the 12th Annual IEEE International Conference on Sensing, Communication, and Networking-Workshops, SECON Workshops 2015, Seattle,WA, USA, 22–25 June 2015; pp. 37–42.

[42] Prof. A. Haja Abdul Khader and Dr. N. Jayaveeran, ”IoT-based Collision Avoidance System for Railways using Fog Computing”, IPASJ International Journal of Computer Science (IIJCS), Volume 6, Issue 4, April 2018, Page 1-6.

[43] Prof. A. Haja Abdul Khader and Dr. N. Jayaveeran , “Cloud and Fog Computing in an IoT-Based Environment”, International Journal of Computer Engineering and Applications, Volume XII, Issue II, Feb. 2018, Page 187-194.

[44] Prof. A. Haja Abdul Khader and Dr. N. Jayaveeran, “Role of Fog Computing and IoT in Train Traffic Management”, International Journal of Electrical Electronics & Computer Science Engineering Special Issue - ICDSSI-2018 | E-ISSN : 2348- 2273 | P-ISSN :2454-1222, Page 1-5.

[45] Prof. A. Haja Abdul Khader and Dr. N. Jayaveeran, “An Overview of IoT Analytics”, International Journal of Innovative Research in Computer and Communication Engineering, Vol. 4, Special Issue 5, October 2016, Page 194-196.

\_\_\_\_\_\_\_\_