



(A Monthly, Peer Reviewed, Refereed, Scholarly Indexed, Open Access Journal)



Impact Factor: 8.699

Volume 14, Issue 5, May 2025

⊕ www.ijirset.com 🖂 ijirset@gmail.com 🖄 +91-9940572462 🕓 +91 63819 07438





www.ijirset.com |A Monthly, Peer Reviewed & Refereed Journal| e-ISSN: 2319-8753| p-ISSN: 2347-6710|

Volume 14, Issue 5, May 2025

|DOI: 10.15680/IJIRSET.2025.1405361|

Fog Computing next to Cloud Computing

Sanket .N. Wawale¹

Department of Information Technology, Amrutvahini Polytechnic, Sangamner, India¹

ABSTRACT: Cloud computing is being used by many organizations, right from startups to MNC. Many are shifting towards it because of advantages it provides as cost deduction, low maintenance, **pay as per your usage** and the more capacity of the data with the help of servers maintained by the cloud providers. Cloud computing is typically exclusively connected to organizations and how they can maximize their operational efficiency. By introduction of Cloud computing in the real word applications is becoming beneficial to both cloud services providers and consumers. Due to the rapid development in the field of the Automation industry, human life is becoming more advanced and better in all aspects. Now a days Automated systems are being preferred over the non-automated system Increase in use of artificial intelligence and IOT devices in day to day life is also generating huge amount data that is to be stored on servers. But there are several challenges for the cloud providers to provide continuous service and data when demanded by the user. Providers has to look after zero down time to minimum latency while providing higher throughput with greater efficiency. To address this issue many technocrats are working on a middle level processing and storage of data, rather then on end server which is called as Fog Computing.

KEYWORDS: Cloud computing, grid computing, fog computing.

I. INTRODUCTION

The use of computers has drastically changed in the modern world due to the internet. People's addiction to computers extends to their online shopping and correspondence. The internet has undergone a significant transformation due to the cloud. This robust desktop application can be accessed via the internet and a database, making it accessible from any location at any time on any device. Cloud computing, sometimes called utility computing, offers customers software, platforms, and infrastructure as a service on a pay-as-you-go basis. The primary driver of cloud computing is big data. Every day, large amounts of data—enough to fill a PETA-sized disk—are uploaded to the internet, which needs a large amount of processing and storage power. Cloud Computing concept came out from the distributed computing architecture where in any computing system is divided into three layers – User Interface, Application Logic, and Data Store. Cloud computed technology is focused on providing hosted services over the distributed networks. New user communities and markets has arised in recent years, due to cloud computing and Information Technology[1]. Cloud computing services are provided from data centers located in different parts of the world. Microsoft SharePoint and Google applications are general examples of cloud computing services.

II. IOT

THE Internet of Things (IoT) is a technology used widely now and will grow in near future, in which the objects of everyday life will be equipped with microcontrollers, transceivers for digital communication, and suitable protocol stacks that will make them able to communicate with one another and with the users, becoming an integral part of the Internet [2].Furthermore, by enabling easy access and interaction with a wide variety of devices such as, for instance, home appliances, surveillance cameras, monitoring sensors, actuators, displays, vehicles, and so on, the IoT will foster the development of a number of applications that make use of the potentially enormous amount and variety of data generated by such objects to provide new services to citizens, companies, and public administrations.

However, such a heterogeneous field of application makes the identification of solutions capable of satisfying the requirements of all possible application scenarios a formidable challenge. This difficulty has led to the proliferation of different and, sometimes, incompatible proposals for the practical realization of IoT systems. Therefore, from a system perspective, the realization of an IoT network, together with the required backend network services and devices, still lacks an established best practice because of its novelty and complexity. In addition to the technical difficulties, the adoption of the IoT paradigm is also hindered by the lack of a clear and widely





www.ijirset.com |A Monthly, Peer Reviewed & Refereed Journal| e-ISSN: 2319-8753| p-ISSN: 2347-6710|

Volume 14, Issue 5, May 2025

|DOI: 10.15680/IJIRSET.2025.1405361|

accepted business model that can attract investments to promote the deployment of these technologies [3].

A "Smart Home Automation" system is a system that allows consumers to control various appliance of the different kind used and also makes controlling of home appliances a very easier and saves energy. On the other hand, they increase the comfort particularly when everyone is busy with their work. "Home automation systems" installed in houses apart from allowing centralized controlling of ventilation , heating, air condition and lighting [4], increase comfort as well. So, they provide an overall reduction in cost and also useful in saving the energy which is certainly the main problem today

The IOT can connect numerous kinds of things, for example, personal computer, tablets , and smart phones to the internet and also facilitates a new kind of communications between two or more things, or between things and people. Any object with an "IP address" can transmit data over a network successfully because of IoT. Many problems get their solution through internet, which can connect devices even in remote areas. The IoT improves the living standard of life with its inovating ideas. The development of IoT will revolutionise sectors like automation, transportation, health centre, energy and houses [5][6].



Fig 1: Connectivity for IOT devices

Waste Management: More work of ICT solutions in this domain may result insignificant savings and economical and ecological advantages. For instance, the use of intelligent waste containers, which detect the level of load and allow for an optimization of the collector trucks route, can reduce the cost of waste collection and improve the quality of recycling [8].

Structural Health of Buildings: Proper maintenance of the historical buildings of a city requires the continuous monitoring of the actual conditions of each building and identification of the areas that are most subject to the impact of external agents. The urban IoT may provide a distributed database of building structural integrity measurements, collected by suitable sensors located in the buildings, such as vibration and deformation sensors to monitor the building stress, atmospheric agent sensors in the surrounding areas to monitor pollution levels, and temperature and humidity sensors to have a complete characterization of the environmental conditions [7]. This database should reduce the need for expensive periodic structural testing by human operators and will allow targeted and proactive maintenance and restoration actions. Finally, it will be possible to combine vibration and seismic readings in order to better study and understand the impact of light earthquakes on city buildings. This database can be made publicly accessible in order to make the citizens aware of the care taken in preserving the city historical heritage.

Noise Monitoring: Noise can be seen as a form of acoustic pollution as much as carbon oxide (CO) is for air. In that sense, the city authorities have already issued specific laws to reduce the amount of noise in the city center at specific hours. An urban IoT can offer a noise monitoring service to measure the amount of noise produced at any given hour in the places that adopt the service [9]. Besides building a space-time map of the noise pollution in the area, such a service can also be used to enforce public security, by means of sound detection algorithms that can recognize, for instance, the noise of glass crashes or brawls.

Traffic Congestion: On the same line of air quality and noise monitoring, a possible Smart City service that can be





www.ijirset.com |A Monthly, Peer Reviewed & Refereed Journal| e-ISSN: 2319-8753| p-ISSN: 2347-6710|

Volume 14, Issue 5, May 2025

|DOI: 10.15680/IJIRSET.2025.1405361|

enabled by urban IoT consists in monitoring the traffic congestion in the city. Even though camera based traffic monitoring systems are already available and deployed in many cities, low-power widespread communication can provide a denser source of information.

Traffic monitoring may be realized by using the sensing capabilities and GPS installed on modern vehicles [10], and also adopting a combination of air quality and acoustic sensors along a given road. This information is of great importance for city authorities and citizens: for the former to discipline traffic and to send officers where needed and for the latter to plan in advance the route to reach the office or to better schedule a shopping trip to the city center.

Air Quality: IoT can provide means to monitor the quality of the air in crowded areas, parks, or fitness trails [8]. In addition, communication facilities can be provided to let health applications running on joggers' devices be connected to the infrastructure. In such a way, people can always find the healthiest path for outdoor activities and can be continuously connected to their preferred personal training application.

City Energy Consumption: Together with the air quality monitoring service, an urban IoT may provide a service to consumption whole monitor the energy of the city, thus enabling authorities and citizens to get a clear and detailed view of the amount of energy required by the different services (public lighting, transportation, traffic lights, control cameras, heating/ cooling of public buildings, and so on). In order to obtain such a service, power draw monitoring devices must be integrated with the power grid in the city. In addition, it will also be possible to enhance these service with active functionalities to control local power production structures (e.g., photovoltaic panels).

Smart Parking: The smart parking service is based on road sensors and intelligent displays that direct motorists along the best path for parking in the city [11]. The benefits deriving from this service are manifold: faster time to locate a means fewer emission the lesser traffic parking slot CO from car, congestion, and happier citizens. The smart parking service can be directly integrated in the urban IoT infrastructure, because many Europe providing market products companies in are for this application. Furthermore, by using short-range communication technologies, such as Radio Frequency Identifiers (RFID) or Near Field Communication (NFC).

Smart Lighting: This service can optimize the street lamp intensity according to the time of the day, the weather condition, and the presence of people. In order to properly work, such a service needs to include the street lights into the Smart City infrastructure. It is also possible to exploit the increased number of connected spots to provide WiFi connection to citizens. In addition, a fault detection system will be easily realized on top of the street light controllers.

III. FOG COMPUTING

The cloud feature of being centralized became an obstacle to latency-sensitive computations [12]. The increasing demand for cloud computing services from IoT devices is prone to the inefficiency of some basic computing and communication requirements; these include location awareness, mobility support, and low latency. The significant challenges that obstruct IoT devices' service quality today include computational energy, battery durability, storage capacity, and bandwidth. To compensate for the burden of IoT devices' limited resources, the giant became the answer—that is, employing the services of the robust, capable of dealing with the limitations. Cloud computing is thought to be the hope for service delivery with flexible resources at a low cost. However, latency, location awareness, geo-distribution, and security are some issues of disturbance that led to the introduction of fog computing.

Fog computing is a promising paradigm that provides computational services at the network edge, enabling new services and applications for the Internet's future [13]. Compared with other paradigms, such as cloudlets, mobile cloud computing (MCC), and mobile edge computing (MEC), fog computing has a better placement position as it is deployed closer to the IoT nodes. Additionally, it supports the extension of cloud-based services. Thus, it helps provide efficient services, including significant minimization of latency [14]. However, fog computing (MEC) and Mobile Cloud Computing (MCC) are examples of prospective cloud and edge computing developments. Fog computing, like MEC and MCC, can also enable edge computation. In addition to the edge network, fog computing may extend to the core





www.ijirset.com |A Monthly, Peer Reviewed & Refereed Journal| e-ISSN: 2319-8753| p-ISSN: 2347-6710|

Volume 14, Issue 5, May 2025

|DOI: 10.15680/IJIRSET.2025.1405361|

network. To be more specific, edge and core networking components may be employed as processing infrastructure in fog computing [14].

IV. FOG COMPUTING ARCHITECTURE



Fig 2: The architecture and the environment of fog computing

The fog environment comprises three layers: the terminal layer, the fog layer, and the cloud layer, while the architecture consists of combinations of fog nodes[15]. Additionally, the fog has the capacity to process data locally with a desirable latency.

4.1. Terminal layer :- This layer comprises different end devices, which are geographically distributed. These devices take the responsibility of fetching data and conveying it to a higher-level layer for data processing and storage. The devices might include wearable devices, sensors, intelligent vehicles, mobile phones, and others [15].

4.2. Fog layer:- This layer stands between the cloud and the terminal layer, situated at the network's edge. This layer device is known as a "fog node," and it is capable of data transmission, computation, and storage [16,17]. A fog node can be mobile or non-mobile and placed in a fixed, strategic location. Some examples of these devices include access points, routers, fog servers, switches, base stations, etc. The computational ability of this layer optimizes the services of latency-sensitive applications, allowing real-time processing and analysis to be realized. In addition, the fog nodes' proximity to the end devices allowed them to communicate effectively. Moreover, the extension of cloud services to the fog layer allowed the fog nodes to have increased computational, and storage power [15].

4.3. Cloud layer:- This layer comprises storage devices and servers with high performance and computational power. It is responsible for executing non-latency-sensitive jobs sent by the lower layer (fog layer) [15]. Software, platforms, and infrastructure are available as services in the cloud. Cloud services include, for instance, IaaS and PaaS-based server hosting provided by Digital Ocean, network storage provided by Apple iCloud, IaaS and PaaS-based server hosting provided by Google App Engine, and virtual IT services provided by Amazon EC2.

Fog computing is a scenario where a vast number of heterogeneous (wireless and sometimes autonomous) ubiquitous and decentralized devices communicate and potentially cooperate among themselves and with the network to perform storage and processing tasks without the intervention of third parties [16]. These tasks can support basic network functions or new services and applications that run in a sandboxed environment. Users who lease part of their devices to host these services get incentives for doing so.





www.ijirset.com |A Monthly, Peer Reviewed & Refereed Journal| e-ISSN: 2319-8753| p-ISSN: 2347-6710|

Volume 14, Issue 5, May 2025 |DOI: 10.15680/IJIRSET.2025.1405361|

V. SECURITY THREATS OF FOG COMPUTING

Most of the fog computing applications are influenced by their craving for functional services and or the user needs, ignoring security requirements, or considering them as second thoughts . The security solution implemented on cloud computing may not be effective on fog computing as they both work from different layers and their architecture differs [18]. Fog computing is prone to security attacks as it is built on a traditional network. Authentication and privacy can be troubling issues in Fog. Fog node collaboration might pose security threats on the network as an infected node can infect others [13]. The study shows that the security topic of discussion in fog computing is bending more on authentication, secured data exchange, denial of service attacks, and privacy issues [12]. Limited network visibility, ineffective way of attack detection, absence of user selective data collection, virtualization issues, multitenancy issues, and malicious fog nod issues are some of the security and privacy challenges in fog computing. Mutual authentication, secure key exchange, and anonymity must be appropriately addressed to provide adequate security and privacy in fog computing tiers. Having the fog node as the first processor that most of the time data encounter made it necessary for the nodes to have hardware root of trust implemented to avert incessant rate of attacks.

Possible Threats:-

Forgery:- It is a kind of attack where the attacker tries to emulate a particular node and fool the end-users into executing actions of his/her choice.

Tampering:- It is a type of attack where the attackers create a delay in data transmission or drop the data, or even sometimes modify it. Due to the mobility nature of fog computing, this kind of attack becomes more difficult to figure out the attack immediately, as the network itself can cause a delay and failure in the data transmission.

Spam:- Spam is often used to describe undesired, trash communications delivered to an internet user's mailbox. This attack is where the attacker fools the victim with unwanted data to seize the opportunity to use the victims network resource and expose privacy.

Furthermore spam communications use necessary storage, bandwidth, and productivity resources. Sybil:- In a Sybil attack, an attacker generates many false identities, disrupts the reputation system of network service, and exploits it disproportionately to achieve a more significant impact. The impersonating node is referred to as the malicious node or Sybil attacker, while the identity

spoofed node is referred to as the Sybil node. The harsh impact of a Sybil attack is that it creates bogus crowd sensing reports since the findings produced by these reports are untrustworthy.

Eavesdropping:- This type of attack is sometimes called snooping or sniffing, where the attacker monitors and steals the victims data over the network. Due to the open nature of the channel, data transmission in wireless mode is vulnerable to eavesdropping. As a result, the eavesdropper can decode important private information .

Denial of service:- This attack denies the rightful users the right to access the network. The attack preoccupies the network resources, which leads to the poor performance of fog computing. Because fog nodes have limited resources, they struggle to manage a high volume of concurrent queries. Fog productivity might suffer significantly in this situation.

Collusion:- This type of attack aims to cheat and or mislead a legitimate group from accessing their rightful resources by cooperating with multiple numbers of groups. Additionally, this attack can expose the victims security key for the attacker to access files and other documents.

Man-in-the-Middle As the name implies, the man-in-the-middle attack occurs when A and B nodes communicate, and another node is in between them, actively observing, recording, and exercising control of the data in communication transparently.





www.ijirset.com |A Monthly, Peer Reviewed & Refereed Journal| e-ISSN: 2319-8753| p-ISSN: 2347-6710|

Volume 14, Issue 5, May 2025

|DOI: 10.15680/IJIRSET.2025.1405361|

Impersonation:- It is a type of attack in which the attacker successfully acquires the identity of a legitimate fog node and executes the services as if it comes from the genuine node.

Identity privacy:- This type of privacy ensures the safety of the identity information of the parties in communication. On the other hand, fog authentication, which requires the users basic information, including name, address, phone number, etc., might expose the user to a particular threat.

Data privacy:- They are also referred to as information privacy. It is responsible for defining how the information can be handled appropriately. Poor data privacy on fog networks can expose the user's preferences and ideologies to nodes that are not trusted.

Usage privacy:-This refers to the model or layout in which the user uses fog services, ensuring the privacy of the user's status and operational deals on the network. One nave option would be for the fog client to create false jobs and offload them to several fog nodes, concealing its actual duties amid the dummy ones.

Location privacy:- It refers to the user's ability to control their past and present location access. As the fog supports mobility, the edge devices keep using the current or saved location, where such exposure might make the user vulnerable to some threats

VI. APPLICATION AREAS OF FOG COMPUTING

1. Healthcare management: The benefit of having multiple servers in a fog environment with the ability to run a particular application became the advantage of delivering improved healthcare services. Fog computing provides a healthcare system with many advantages, including reducing energy consumption and minimizing delays and data traffic.

2. Traffic light systems:- Fog computing and vehicular networks replaced conventional physical traffic light systems with virtual traffic light systems, which are more cost-effective. In addition, fog computing provides an easy way to reduce the traffic crowd using traffic signals adjustment based on the traffic situation or through vehicular communications guiding drivers to non-crowded routes.

3. Medical wearables: The use of these devices by healthcare providers is becoming pervasive. It is used in delivering telemedicine, monitoring the condition of patients, and directing on-site staff in surgery procedures . Fog computing does not only reduce medical expenses but has become a cornerstone of modern healthcare systems.

4. Connected vehicles: With the help of context awareness, fog computing provides a secure and efficient real-time interaction between cars, traffic lights, and access points. The vehicles in VANET's environments require services with minimal latency and short-distance domestic connections through fog computing.

5. Smart grids: Smart grids help manage the connected devices' operational activities through machine-to-machine and human-to-machine communication, leading to quality of service maximization, minimizing the rate of failure, improving the efficient use of energy, and optimizing security.

6. Smart homes and cities: The main goal of smart-city applications is to enhance the operation of the city flows and grant real-time feedback to problems that may emerge in users' operational activities. Although the intervention of fog computing extends cloud computing services close to the edge devices, which leads to the decrease in latency, improves the QoS, context awareness, load balancing, and efficient distribution of data.

7. Latency management: Latency management refers to the time taken to respond, analyze, and execute the computational request. The fog nodes' proximity with the edge devices helps in leading to faster computation tasks and analysis responses. In addition, initiating structured nodal cooperation can help provide effective latency management. The distribution of tasks and the computation between the fog and the clients are built on achieving minimal communication, and computational latency.





www.ijirset.com |A Monthly, Peer Reviewed & Refereed Journal| e-ISSN: 2319-8753| p-ISSN: 2347-6710|

Volume 14, Issue 5, May 2025

|DOI: 10.15680/IJIRSET.2025.1405361|

8. Data management: As the number of IoT nodes keeps increasing also, the volume of data keeps increasing rapidly. That made cloud computing and other previous paradigms ineffective in implementing the proper way of managing the data, making fog suitable as it is placed close to the edge devices.

9. Network management: Management of networks in fog computing encompasses Software Defined Network (SDN)/Network Function Virtualization (NFV) support, decongestion of core-network, and guaranteeing reliable network connectivity. SDN's popular function is equipping NFV. Therefore, SDN is regarded to be among the significant backbone of virtualized networks.

10. Computation management: Commitment towards managing the fog computing computational resources is an essential aspect. Resource management encompasses the estimation of resources, allocation of workload, and coordination of resources. Estimating resources tackles allocating computational resources based on some given policies to guide proper allocation and reach the desired QoS.

VII. ISSUES AND CHALLENGES

Fog computing faces structural challenges due to its heterogeneous nature. As the edge and or the core network can be used as a fog node some nodes might not be designed to serve a general-purpose computation. Therefore, integrating the general-purpose function from its traditional role might be an issue. Furthermore, in the face of service orientation, the evolution of large-scale applications might be an issue because of the limited resources of some fog nodes. Therefore there is a need for a programming platform that will help in the development of distributed applications. Even with the overwhelming features of fog computing, it still faces a shortcoming in device-to-device (D2D) communications. Many studies on fog computing concentrated on IoT to Fog and Fog to Cloud solutions. Other topics that have been discovered but need to be understood include the performance of fog ecosystems, robustness, storage, energy savings, use of distributed fog through a combination of device-to-device (D2D) and cellular network, mobility and node selection, trust and security issues at all levels of the fog paradigm Integrating IoT and fog services has started improving the quality of services in health industries.

With fog e-Health applications, the quality of service on patient management can be improved, and some medical complications that could even lead to the patient's death can be minimized. Moreover, the generated data from the applications can research and prevent epidemics and or pan-demic diseases. It is being highlighted that healthcare industries will witness the deployment of robust solutions using fog computing for quality of service delivery. However, the challenges it faces include; securing sensitive data, system failure management, the configuration of multiple systems, and the management of diverse systems having numerous dimensions.

In the smart city infrastructure, management of information and communication resources needs to increase to perform real-time analysis of big data close to the user and guarantee the security of the infrastructure and the generated information. With the function of FC of delivering application awareness to satisfy crowd-sourcing/sensing applications, FC needs to make some arrangements to set the resources that could provide mobility services. However, the challenge here is that the mobile node may experience some issues due to the variation of computation, storage, bandwidth, and latency [15].

VIII. CONCLUSION

Fog computing is a new paradigm that receives wide acceptance and recognition due to its significant contribution to modern computing technology. This paper reviews and discusses cloud computing, briefly highlighting the implemented paradigms before fog computing. These paradigms include cloudlet, mobile cloud computing, and mobile edge computing. All the paradigms targeted improving the quality of service between the end devices and the cloud itself. The standard for elucidating the taxonomy is built on the functional and vital issues in fog computing. Challenges and potential applications are identified. The paper shows that security, privacy, application, and communication challenges. Potential applications in fog computing are also identified, including healthcare applications, innovative city applications, and farm applications.





www.ijirset.com |A Monthly, Peer Reviewed & Refereed Journal| e-ISSN: 2319-8753| p-ISSN: 2347-6710|

Volume 14, Issue 5, May 2025

|DOI: 10.15680/IJIRSET.2025.1405361|

REFERENCES

[1] P. T. Jaeger, J. Lin, and J. M. Grimes, "Cloud computing and information policy: Computing in a policy cloud?" J. Inf. Technol. Politics, vol. 5, no. 3, pp. 269–283, Oct. 2008.

[2] L. Atzori, A. Iera, and G. Morabito, "The internet of things: A survey," Comput. Netw., vol. 54, no. 15, pp. 2787–2805, 2010.

[3] A. Laya, V. I. Bratu, and J. Markendahl, "Who is investing in machine-to-machine communications?" in Proc. 24th Eur. Reg. ITS Conf., Florence, Italy, Oct. 2013, pp. 20–23.

[4] Majid Al Kuwari, Abdulrahman Ramadan, et. al., "Smart-Home Automation using IOT-based Sensing and Monitoring Platform", IEEE 12th International Conference on Compatibility, Power Electronics and Power Engineering, 2018

[5] Chi Shang Shih, Jyun He Choum, Niels Reamers, "Designing CPS/IOT applications for smart buildings and cities", IET Cyber- Physical Systems: Theory& Applications, 2016

[6] Muhammad Asadullah, Ahsan Raza, "An Overview of Home Automation Systems", Transactions on Consumer Electronics IEEE, 2016

[7] J. P. Lynch and J. L. Kenneth, "A summary review of wireless sensors and sensor networks for structural health monitoring," Shock and Vibration Digest, vol. 38, no. 2, pp. 91–130, 2006.

[8] A. R. Al-Ali, I. Zualkernan, and F. Aloul, "A mobile GPRS-sensors array for air pollution monitoring," IEEE Sensors J., vol. 10, no. 10, pp. 1666–1671, Oct. 2010.

[9] N. Maisonneuve, M. Stevens, M. E. Niessen, P. Hanappe, and L. Steels, "Citizen noise pollution monitoring," in Proc. 10th Annu. Int. Conf. Digital Gov. Res.: Soc. Netw.: Making Connec. Between Citizens, Data Gov., 2009, pp. 96–103

[10] X. Li, W. Shu, M. Li, H.-Y. Huang, P.-E. Luo, and M.-Y. Wu, "Performance evaluation of vehicle based mobile sensor networks for traffic monitoring," IEEE Trans. Veh. Technol., vol. 58, no. 4, pp. 1647–1653, May 2009.

[11] S. Lee, D. Yoon, and A. Ghosh, "Intelligent parking lot application using wireless sensor networks," in Proc. Int. Symp. Collab. Technol. Syst., Chicago, May 19–23, 2008, pp. 48–57.

[12] R. Mahmud, R. Kotagiri, R. Buyya, Fog computing: a taxonomy, survey and future directions, in: B. Di Martino, K.-C. Li, L.T. Yang, A. Esposito (Eds.), Internet of Everything: Algorithms, Methodologies, Technologies and Perspectives, Springer Singapore, Singapore, 2018, pp. 103–130, doi:10.1007/978-981-10-5861-55.

[13] P. Zhang, M. Zhou, G. Fortino, Security and trust issues in fog computing: asurvey, Future Generat.Comput.Syst.88(2018)16-27,doi:10.1016/j.future.2018.05.008.https://www.sciencedirect.com/science/article/pii/S0167739X1732972

[14] R. Mahmud, R. Kotagiri, R. Buyya, Fog computing: a taxonomy, survey and future directions, in: B. Di

Martino, K.-C. Li, L.T. Yang, A. Esposito (Eds.), Internet of Everything: Algorithms, Methodologies, Technologies and Perspectives, Springer Singapore, Singapore, 2018, pp. 103–130, doi:10.1007/978-981-10-5861-5_5.

[15] P. Hu, S. Dhelim, H. Ning, T. Qiu, Survey on fog computing: architecture, key technologies, applications and open issues, J. Netw. Comput. Appl. 98 (2017) 27–42, doi:10.1016/j.jnca.2017.09.002. https://www.sciencedirect.com/science/article/ pii/S1084804517302953.

[16] F. Bonomi, R. Milito, J. Zhu, 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, in: MCC '12, Association for Computing Machinery, New York, NY, USA, 2012, pp. 13–16, doi:10.1145/2342509.2342513.

[17] A. Yousefpour, C. Fung, T. Nguyen, K. Kadiyala, F. Jalali, A. Niakanlahiji, J. Kong, J.P. Jue, All one needs to know about fog computing and related edge computing paradigms: a complete survey, J. Syst. Archit. 98 (2019) 289–330, doi:10.1016/j.sysarc.2019.02.009 https://www.sciencedirect.com/science/article/pii/S1383762118306349

[18] T. Nguyen Gia, A.M. Rahmani, T. Westerlund, P. Liljeberg, H. Tenhunen, Fog computing approach for mobility support in internet-of-things systems, IEEE Access 6 (2018) 36064–36082, doi:10.1109/ACCESS.2018.2848119. Conference Name: IEEE Access.









INTERNATIONAL JOURNAL OF INNOVATIVE RESEARCH

IN SCIENCE | ENGINEERING | TECHNOLOGY





www.ijirset.com