iJRASET
International Journal For Research in Applied Science and Engineering Technology



# INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

**Volume:** 10 **Issue:** VII **Month of publication:** July 2022

**DOI:** https://doi.org/10.22214/ijraset.2022.45952

www.ijraset.com

Call: 08813907089 | E-mail ID: ijraset@gmail.com

International Journal for Research in Applied Science & Engineering Technology (IJRASET)
*ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor: 7.538*
*Volume 10 Issue VII July 2022- Available at www.ijraset.com*

# Fog Computing: A Review

Monika Gautam[1], Jyoti[2]
[1, 2]*Department of Computer Science, Puran Murti College of Engineering, DCRUST, Murthal*

***Abstract:*** ***Fog computing provides different types of services & all these services are accessed through different AP (access points) or STB (set top boxes). The fog computing infrastructure provides different services close to client or user. In some way fog computing behaves similar to cloud computing. Both computing technologies provide application, storage, data and computing services to their registered clients. But fog computing provides services close to its end users as compared to cloud computing that provides services remotely. Also fog computing provides thick geographical distribution and having support for mobility. This paper provides literature review on Fog Computing Techniques.***
***Keywords: Fog computing, edge computing, mobile cloud computing, cloud computing***

## I. INTRODUCTION

In Fog computing [1], services can be hosted at end devices such as set-top-boxes or access points. The infrastructure of this new distributed computing allows applications to run as close as possible to sensed actionable and massive data, coming out of people, processes and thing. Such Fog computing concept, actually a Cloud computing close to the 'ground', creates automated response that drives the value.

In some way fog computing behaves similar to cloud computing. Both computing technologies provide application, storage, data and computing services to their registered clients. But fog computing provides services close to its end users as compared to cloud computing that provides services remotely.

Both Cloud and Fog provide data, computation, storage and application services to end-users. However, Fog can be distinguished from Cloud by its proximity to end-users, the dense geographical distribution and its support for mobility.

We adopt a simple three level hierarchy as in Figure 1.

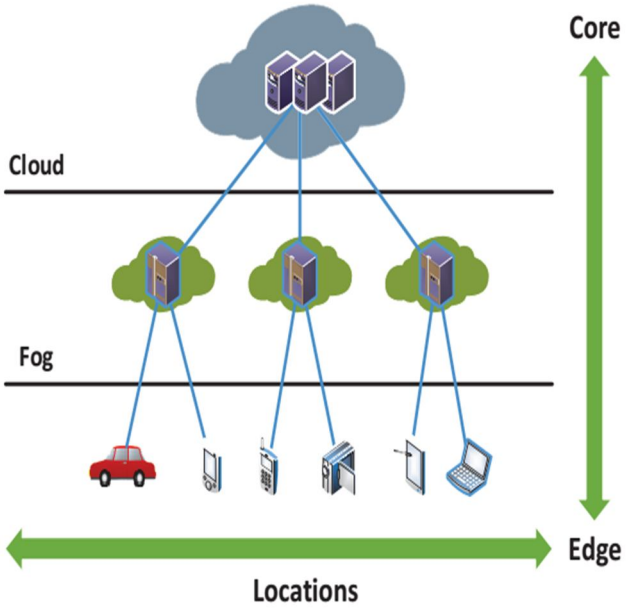



Fig 1: Fog between edge and cloud.

In this framework, each smart thing is attached to one of Fog devices. Fog devices could be interconnected and each of them is linked to the Cloud.

This paper provides literature review on Fog Computing Techniques.

*ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor: 7.538*
*Volume 10 Issue VII July 2022- Available at www.ijraset.com*

## II. NEED FOR FOG COMPUTING

In the past few years, Cloud computing has provided many opportunities for enterprises by offering their customers a range of computing services. Current "pay-as-you-go" Cloud computing model becomes an efficient alternative to owning and managing private data centres for customers facing Web applications and batch processing. Cloud computing frees the enterprises and their end users from the specification of many details, such as storage resources, computation limitation and network communication cost. However, this bliss becomes a problem for latency-sensitive applications, which require nodes in the vicinity to meet their delay requirements . When techniques and devices of IoT are getting more involved in people's life, current Cloud computing paradigm can hardly satisfy their requirements of mobility support, location awareness and low latency [2].

Fog computing is proposed to address the above problem . As Fog computing is implemented at the edge of the network, it provides low latency, location awareness, and improves quality-of-services (QoS) for streaming and real time applications. Typical examples include industrial automation, transportation, and networks of sensors and actuators. Moreover, this new infrastructure supports heterogeneity as Fog devices include end-user devices, access points, edge routers and switches. The Fog paradigm is well positioned for real time big data analytics, supports densely distributed data collection points, and provides advantages in entertainment, advertising, personal computing and other applications.

Figure 2 below shows the position of fog in the client server communication.

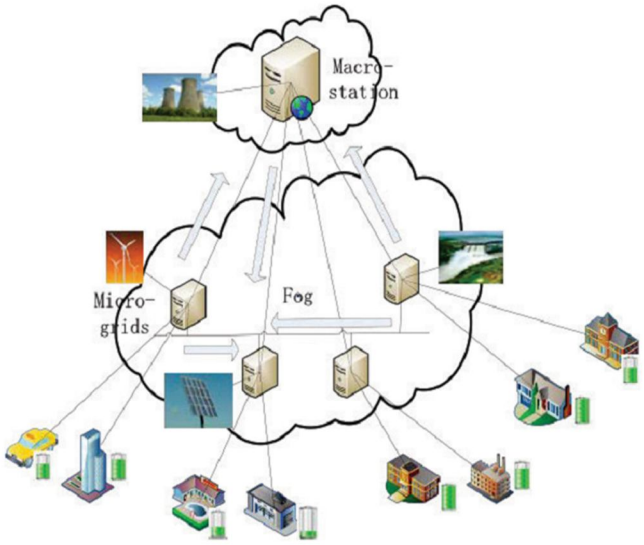



Figure 2: Fog computing in client server communication

## III. LITERATURE REVIEW

Several works related to our work, which presents the concepts of fog computing are explained below:

Pearson, Siani, et al. (2010) [4] wrote a paper. In this paper authors described that "cloud computing is an emerging paradigm for large scale infrastructures. It has the advantage of reducing cost by sharing computing and storage resources, combined with an on-demand provisioning mechanism relying on a pay-per-use business model. These new features have a direct impact on the budgeting of IT budgeting but also affect traditional security, trust and privacy mechanisms. Many of these mechanisms are no longer adequate, but need to be rethought to fit this new paradigm. In this paper they assessed how security, trust and privacy issues occur in the context of cloud computing and discuss ways in which they may be addressed".

Dlamini, M. T. et al. (2011) [5] wrote a paper. In this paper authors described that "cloud computing is a new computing paradigm for the provisioning, delivery and consumption of IT resources and services on the Internet. This computing paradigm comes with huge benefits such as cost savings, increased resilience and service availability, improved IT operations efficiency and flexibility. However, most research cites security concerns as one of the biggest challenges for most of these organizations. This has led to fallacy or misconception about security challenges of the 'cloud' which needs to be clarified. This is a call for more research to separate reality from the hype. Hence, this paper aims to separate justified security concerns from the hype, fear of the unknown and confusion that currently prevails within cloud computing. This paper aims to advance the current discussions on cloud computing security in order to clear the 'foggy cloud' hovering over such a promising technology development. It seeks to inform and make decision makers aware of the real pertinent and justified security issues within cloud computing".

©IJRASET: All Rights are Reserved 

Stolfo, Salvatore J., et al. (2012) [6] described in their paper that "cloud computing promises to significantly change the way we use computers and access and store our personal and business information. With these new computing and communications paradigms arise new data security challenges. Existing data protection mechanisms such as encryption have failed in preventing data theft attacks, especially those perpetrated by an insider to the cloud provider. They proposed a different approach for securing data in the cloud using offensive decoy technology. They monitored data access in the cloud and detect abnormal data access patterns. When unauthorized access is suspected and then verified using challenge questions, we launch a disinformation attack by returning large amounts of decoy information to the attacker. This protects against the misuse of the user's real data. Experiments conducted in a local file setting provide evidence that this approach may provide unprecedented levels of user data security in a Cloud environment".

Madsen, Henrik, et al. (2013) [7] considered "current paradigms in computing and outlines the most important aspects concerning their reliability. The Fog computing paradigm as a non-trivial extension of the Cloud is considered and the reliability of the networks of smart devices are discussed. Combining the reliability requirements of grid and cloud paradigms with the reliability requirements of networks of sensor and actuators it follows that designing a reliable Fog computing platform is feasible".

Hong, Kirak et al. (2013) [8] in their paper described that "the ubiquitous deployment of mobile and sensor devices is creating a new environment, namely the Internet of Things (IoT), that enables a wide range of future Internet applications. In this work, they presented Mobile Fog, a high level programming model for the future Internet applications that are geospatially distributed, large-scale, and latency-sensitive. They analyzed use cases for the programming model with camera network and connected vehicle applications to show the efficacy of Mobile Fog. They also evaluated application performance through simulation".

Chou, Te-Shun et al. (2013) [9] In this paper, "clouds provide a powerful computing platform that enables individuals and organizations to perform variety levels of tasks such as: use of online storage space, adoption of business applications, development of customized computer software, and creation of a realistic network environment. In this paper, three cloud service models were compared; cloud security risks and threats were investigated based on the nature of the cloud service models. Real world cloud attacks were included to demonstrate the techniques that hackers used against cloud computing systems. In addition, countermeasures to cloud security breaches are presented".

Modi, Chirag et al. (2013) [10] described that "cloud computing offers scalable on-demand services to consumers with greater flexibility and lesser infrastructure investment. Since Cloud services are delivered using classical network protocols and formats over the Internet, implicit vulnerabilities existing in these protocols as well as threats introduced by newer architectures raise many security and privacy concerns. In this paper, they surveyed the factors affecting Cloud computing adoption, vulnerabilities and attacks, and identify relevant solution directives to strengthen security and privacy in the Cloud environment".

Stojmenovic, Ivan et al. (2014) [11] described that "fog Computing is a paradigm that extends Cloud computing and services to the edge of the network. Similar to Cloud, Fog provides data, compute, storage, and application services to end-users. In this article, they elaborated the motivation and advantages of Fog computing, and analyse its applications in a series of real scenarios, such as Smart Grid, smart traffic lights in vehicular networks and software defined networks. Security and privacy issues are further disclosed according to current Fog computing paradigm."

Shankarwar, Mahesh U., et al. (2014) [12] described that "cloud Computing is continuously evolving and showing consistent growth in the field of computing. It is getting popularity by providing different computing services as cloud storage, cloud hosting, and cloud servers etc. for different types of industries as well as in academics. On the other side there are lots of issues related to the cloud security and privacy. Security is still critical challenge in the cloud computing paradigm. These challenges include user's secret data loss, data leakage and disclosing of the personal data privacy. Considering the security and privacy within the cloud there are various threats to the user's sensitive data on cloud storage. This paper is survey on the security and privacy issues and available solutions. Also present different opportunities in security and privacy in cloud environment".

Firdhous, Mohamed et al. (2014) [13] described that "cloud computing is the newest computing paradigm that makes computing resources available over the Internet on a utility costing basis. Cloud computing offers many advantages to users in terms of reduced cost, elimination of system administrative functions, increased flexibility, better reliability and location independence. Though these are definite advantages, cloud computing also suffers from certain limitations. These limitations arise from the very same reason that is considered an advantage too. Hosting of cloud data centres in the Internet creates large and unpredictable network latencies and undefined security issues as sensitive data is now entrusted to a third party. Also location independence of processing in cloud computing may also not desirable for certain types of networks such as sensor networks and Internet of Things. These services are known as location aware services and require location dependent fast processing.

In order to overcome these limitations, researchers have proposed a new cloud computing model called fog computing where the cloud system is located either at the edge of the private network or very close to it."

Loke, Seng W et al. (2015) [14] described that "focuses on services and applications provided to mobile users using airborne computing infrastructure. We present concepts such as drones-as-a-service and fly-in,fly-out infrastructure, and note data management and system design issues that arise in these scenarios. Issues of Big Data arising from such applications, optimising the configuration of airborne and ground infrastructure to provide the best QoS and QoE, situation-awareness, scalability, reliability, scheduling for efficiency, interaction with users and drones using physical annotations are outlined".

Bitam, Salim et al. (2015) [15] described that "cloud computing is a network access model that aims to transparently and ubiquitously share a large number of computing resources. These are leased by a service provider to digital customers, usually through the Internet. Due to the increasing number of traffic accidents and dissatisfaction of road users in vehicular networks, the major focus of current solutions provided by intelligent transportation systems is on improving road safety and ensuring passenger comfort. Various transportation services provided by VANET-Cloud are reviewed, and some future research directions are highlighted, including security and privacy, data aggregation, energy efficiency, interoperability, and resource management".

Roman, Rodrigo et al. (2016) [16] described that "cloud computing paradigm is unable to meet certain requirements (e.g. low latency and jitter, context awareness, mobility support) that are crucial for several applications (e.g. vehicular networks, augmented reality). To fulfill these requirements, various paradigms, such as fog computing, mobile edge computing, and mobile cloud computing, have emerged in recent years. While these edge paradigms share several features, most of the existing research is compartmentalized; no synergies have been explored. This is especially true in the field of security, where most analyses focus only on one edge paradigm, while ignoring the others. The main goal of this study is to holistically analyze the security threats, challenges, and mechanisms inherent in all edge paradigms, while highlighting potential synergies and venues of collaboration. In our results, we will show that all edge paradigms should consider the advances in other paradigms".

Saad Khan et. al. (2017) [17] described that "Fog computing is a new paradigm that extends the Cloud platform model by providing computing resources on the edges of a network. It can be described as a cloud-like platform having similar data, computation, storage and application services, but is fundamentally different in that it is decentralized. In addition, Fog systems are capable of processing large amounts of data locally, operate on-premise, are fully portable, and can be installed on heterogeneous hardware. These features make the Fog platform highly suitable for time and location-sensitive applications. For example, Internet of Things (IoT) devices are required to quickly process a large amount of data. This wide range of functionality driven applications intensifies many security issues regarding data, virtualization, segregation, network, malware and monitoring. This paper surveys existing literature on Fog computing applications to identify common security gaps. Similar technologies like Edge computing, Cloudlets and Micro-data centres have also been included to provide a holistic review process. The majority of Fog applications are motivated by the desire for functionality and end-user requirements, while the security aspects are often ignored or considered as an afterthought. This paper also determines the impact of those security issues and possible solutions, providing future security-relevant directions to those responsible for designing, developing, and maintaining Fog systems".

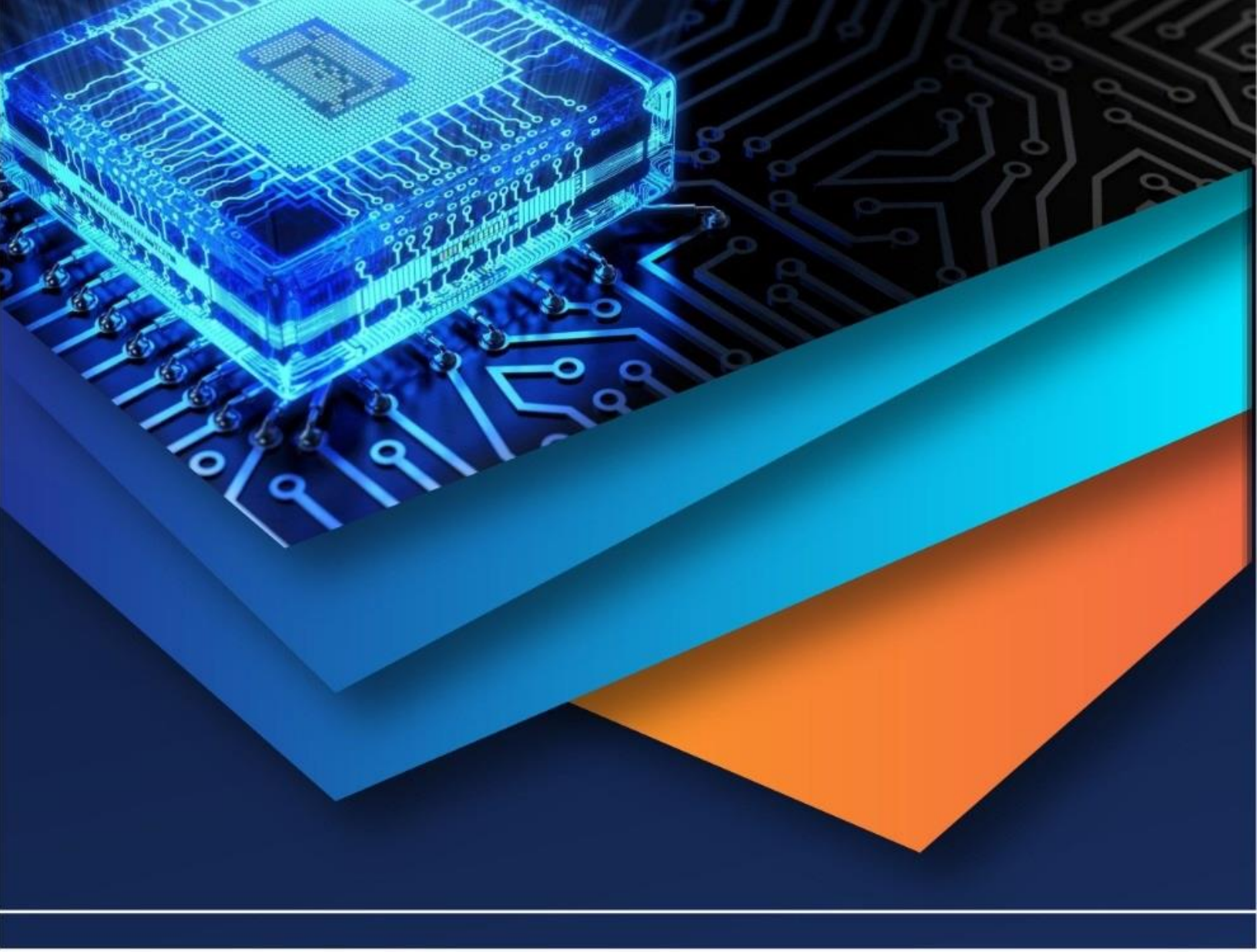
Hany F. Atlam et. al. (2018) [18] described that "With the rapid growth of Internet of Things (IoT) applications, the classic centralized cloud computing paradigm faces several challenges such as high latency, low capacity and network failure. To address these challenges, fog computing brings the cloud closer to IoT devices. The fog provides IoT data processing and storage locally at IoT devices instead of sending them to the cloud. In contrast to the cloud, the fog provides services with faster response and greater quality. Therefore, fog computing may be considered the best choice to enable the IoT to provide efficient and secure services for many IoT users. This paper presents the state-of-the-art of fog computing and its integration with the IoT by highlighting the benefits and implementation challenges. This review will also focus on the architecture of the fog and emerging IoT applications that will be improved by using the fog model. Finally, open issues and future research directions regarding fog computing and the IoT are discussed".

## IV. CONCLUSION

In Fog computing, services can be hosted at end devices such as set-top-boxes or access points. The infrastructure of this new distributed computing allows applications to run as close as possible to sensed actionable and massive data, coming out of people, processes and thing. Such Fog computing concept, actually a Cloud computing close to the 'ground', creates automated response that drives the value. Both Cloud and Fog provide data, computation, storage and application services to end-users. However, Fog can be distinguished from Cloud by its proximity to end-users, the dense geographical distribution and its support for mobility. This paper provides literature review on Fog Computing Techniques.

## REFERENCES

[1] Sarkar, S., Misra, S., “Theoretical modelling of fog computing: a green computing paradigm to support iot applications”, IET Networks 5(2) (2016) 23–29
[2] Peter, Nisha, "Fog computing and its real time applications." International Journal of Emerging Technology and Advanced Engineering (IJETAE) 5, no. 6 (2015): 266-269.
[3] Wang, Yifan, TetsutaroUehara, and Ryoichi Sasaki, "Fog computing: issues and challenges in security and forensics." In Computer Software and Applications Conference (COMPSAC), 2015 IEEE 39th Annual, vol. 3, pp. 53-59. IEEE, 2015.
[4] Pearson, Siani, and AzzedineBenameur. "Privacy, security and trust issues arising from cloud computing." In Cloud Computing Technology and Science (CloudCom), 2010 IEEE Second International Conference on, pp. 693-702. IEEE, 2010.
[5] Dlamini, M. T., et al. "Security of Cloud Computing: Seeing Through the Fog." computing 2 (2011): 3.
[6] Stolfo, Salvatore J., Malek Ben Salem, and Angelos D. Keromytis. "Fog computing: Mitigating insider data theft attacks in the cloud." In Security and Privacy Workshops (SPW), 2012 IEEE Symposium on, pp. 125-128. IEEE, 2012.
[7] Madsen, Henrik, Bernard Burtschy, G. Albeanu, and F. L. Popentiu-Vladicescu. "Reliability in the utility computing era: Towards reliable fog computing." In Systems, Signals and Image Processing (IWSSIP), 2013 20th International Conference on, pp. 43-46. IEEE, 2013.
[8] Hong, Kirak, David Lillethun, UmakishoreRamachandran, BeateOttenwälder, and Boris Koldehofe. "Mobile fog: A programming model for large-scale applications on the internet of things." In Proceedings of the second ACM SIGCOMM workshop on Mobile cloud computing, pp. 15-20. ACM, 2013.
[9] Chou, Te-Shun. "Security threats on cloud computing vulnerabilities." International Journal of Computer Science & Information Technology 5, no. 3 (2013): 79.
[10] Modi, Chirag, Dhiren Patel, BhaveshBorisaniya, Avi Patel, and MuttukrishnanRajarajan. "A survey on security issues and solutions at different layers of Cloud computing." The Journal of Supercomputing 63, no. 2 (2013): 561-592.
[11] Stojmenovic, Ivan, and Sheng Wen. "The fog computing paradigm: Scenarios and security issues." In Computer Science and Information Systems (FedCSIS), 2014 Federated Conference on, pp. 1-8. IEEE, 2014.
[12] Shankarwar, Mahesh U., and Ambika V. Pawar. "Security and Privacy in Cloud Computing: A Survey." In FICTA (2), pp. 1-11. 2014.
[13] Firdhous, Mohamed, Osman Ghazali, and Suhaidi Hassan. "Fog computing: Will it be the future of cloud computing?." In Third International Conference on Informatics & Applications, Kuala Terengganu, Malaysia, pp. 8-15. 2014.
[14] Loke, Seng W. "The internet of flying-things: Opportunities and challenges with airborne fog computing and mobile cloud in the clouds." arXiv preprint arXiv:1507.04492 (2015).
[15] Bitam, Salim, AbdelhamidMellouk, and SheraliZeadally. "VANET-cloud: a generic cloud computing model for vehicular Ad Hoc networks." IEEE Wireless Communications 22, no. 1 (2015): 96-102.
[16] Roman, Rodrigo, Javier Lopez, and Masahiro Mambo. "Mobile edge computing, fog et al.: A survey and analysis of security threats and challenges." Future Generation Computer Systems (2016).
[17] Saad Khan, Simon Parkinson† and Yongrui Qin, “Fog computing security: a review of current applications and security solutions”,Khan et al. Journal of Cloud Computing: Advances, Systems and Applications (2017)
[18] Hany F. Atlam, Robert J. Walters and Gary B. Wills, “Fog Computing and the Internet of Things: A Review”, Big Data Cogn. Comput. 2018.



10.22214/IJRASET

45.98

IMPACT FACTOR: 7.129

IMPACT FACTOR: 7.429

# INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

Call : 08813907089 (24*7 Support on Whatsapp)