iJRASET
International Journal For Research in Applied Science and Engineering Technology

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

Volume: 7 **Issue:** VI **Month of publication:** June 2019

DOI: http://doi.org/10.22214/ijraset.2019.6306

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: 7.177
Volume 7 Issue VI, June 2019- Available at www.ijraset.com

IoT, Fog Computing with AI Possibility

Dhananjay Yadav[1], Bharat Chilampuram[2]

Abstract: ***During the development of technology, we are facing many challenges and responsibility of better solution driven architecture for internet of things. Fog Computing vs edge computing try to solve many issues in internet of things but artificial intelligence making more advanced solution of that, which will help to generate robust emerging option. To applying AI will require strong solution-based architecture with highly trained system, it's now possible by large collection of data and computing power. Now we are generalizing and filter best solution available in IOT fog scenario using AI.***

Keywords: Fog Computing, Internet of Thing, Artificial Intelligence, Edge Computing, Distributed AI, Cloud.

I. INTRODUCTION

Fog and edge which is the same functionalities in terms of publishing both data and intelligence to analytic platforms in cloud that are situated either on near place or close to where the data originated from. “Fog computing && edge computing are work as the same thing. Both are trying to accomplish to leveraging the computing capabilities within near a local network to carry out computation workflow that would generally have been carried out in the different cloud station. These technologies can help organizations reduce their overall reliance on cloud-based architecture to analyze data, which generally leads to major latency issues, and instead be able to make data-driven decisions faster. The main difference between both technologies comes down to where the processing or computing of that data takes place. So, with Fog computing, the information is processed within a fog edge node or IoT gateway which is situated within the local LAN. As for edge computing, the data is processed on the device or machine itself without being sending anywhere.

Cloud computing is a technique for businesses to use the internet to connect to off-premise storage unit and processing computing infrastructure. In the era of the Internet of Things, the cloud provides a very large scalable way for businesses enterprises to manage all aspects of an IoT deployment including device place and management, billing, protocols, security protocols, data mining etc. Cloud services also make developers friendly breakthrough for leveraging powerful tools to create IoT applications and deliver different aspect of services quickly. On-demand scalability is main feature here given the grand vision of IoT; a world saturated with smart, interconnected things.

Many big enterprise players have brought cloud-as-a-service offerings to market for IoT. Microsoft has its Azure suite, amazon have Amazon Web Services, a giant in cloud services, has an IoT-specific play, google offer cloud service GCP, IBM offers access to the Watson platform via its Bluemix cloud, and the list of that type are more.

However, for services and applications that require very low network latency or have a very limited resource “pipe” through which to pump the data, there are some downsides to the cloud that are better to we have addressed at the edge device.

Fog is the main extension of cloud processing that have multiple of multiple edge nodes which are directly connected to physical end devices.

Such nodes are generally much closer to devices if we compared to centralized architecture data centers, which is why they are make possible to provide instant connections. The considerable some part of processing power of edge nodes allows them to perform many processing computations of a great amount of data on their own near place, without sending or pushing it to cloud servers.

Fog can also have cloudlets — small-scale and but powerful data centers located at the edge of the network in near device. Their purpose is to support resource and intensive IoT apps that require very low latency. The main difference between fog computing or edge computing and cloud computing is that cloud is a mainly centralized system, while fog is a distributed decentralized network of infrastructure.

Fog computing is a working between hardware and remote servers. It regulates which information or data should be sent to the cloud server and which can be processed locally in edge. In this way, fog is a make intelligent gateway of system that offloads clouds enabling more efficient data, storage, processing and analysis the information. One should note that fog computing is not a separate architecture and it doesn’t replace any cloud computing infrastructure but rather complements it, getting as close to the source of information as possible to push through the cloud. The Internet of Things (IoT), as an option which can potentially have a double meaning. Naturally, while the term came to pass and be accepted widely to define the overall process of connecting things in physical devices to wireless or local networks, the company trying continues to get to best grips with the coming together of

information technology and cloud technology. An engaging panel debate at IoT Tech conferences today explored the future of company in an IoT-enabled world, the data challenges of market, and examples of innovation.

One of the key discussion topics at the all event, across all the conference talks, has been around the use of data to generate knowledge from it. company who have spent the past many years making out data breach now realize, to continue the nautical analogy, that they have missed the starting journey. the vast majority of enterprise are using data to inform their options, rather than power them. Yet data mining and analysis in itself is not the goal. "You can have all the related solution-oriented algorithms from machine learning or deep learning, but for an industry like not interested in processing large data sets. They're interested in searching solutions,

"Most companies have tried into the concept of AI will solve their problems. They store their data into a big cloud or storage structure and try it will solve everything for you, “The reality is very different. Data needs to go through many layers and layers of processing and computing; all those mini layers have to be work done before it can bring value to you and your enterprises; and also, it could be of no business value at the end of it.

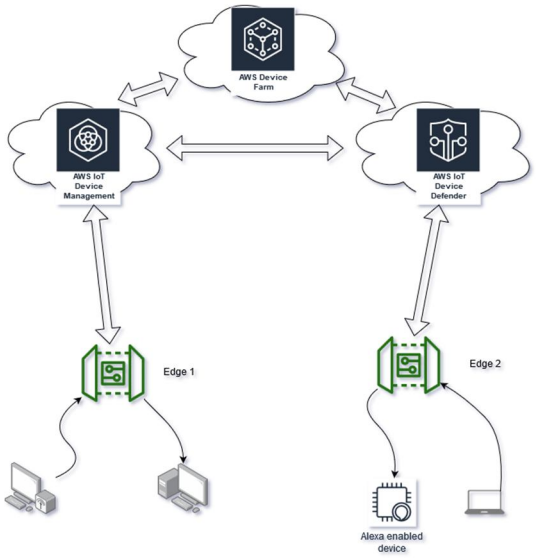


Fig. 1 Example of Fog edge computing using AWS

AI, on the other hand, is the analytical engine or “processing brain” that will allow the knowledge discovery and decision-making based on the data collected by the IoT devices. In other words, the IoT collects and store the data in cloud infrastructure and the AI processes the data to give them meaningful value. You can observe the many operation of these systems on a personal level in many tracking devices and in Google Home, Amazon ‘s Alexa or Apple ‘s Siri, Samsung Bixby etc. More connected devices come to generate more data that has the potential to provide many incredible knowledges for business, although this presents a new aspect of challenge: how to analyses them all. The collection of these large data does not make benefit anyone unless there is a system of interpretation to understand the data. That’s where the AI comes into picture. Making huge amounts of data relevant and important for the knowledge discovery role of Artificial Intelligence.

When the different data collected from the Internet of Things is analyzed using Artificial Intelligence, software developers and organization can make useful informed decisions by the identification and understanding of patterns in the big analyzed data. This will create many benefits, both for end consumers and software developers. It allows software developers to search solutions to their IoT products and innovations in the IT industry

IoT machine will generate large set of data, then artificial intelligence will be main work necessary to deal with these large volumes if we’re to have any option of making usedness of the data. Data is only work full if it makes any kind of action. To make data workable, it needs to be join with context and creativity. IoT and AI work together is this context, i.e. ‘connected and think’ and not just connected working devices. Traditional option of analyzing structured or unstructured data and making action are not designed to flow process the vast amounts of real-time data that stream from IoT devices. This is where AI-based system analysis and response becomes must require for extracting optimal value from that data.

AI is beneficial for both real-time and post event scenario

Post Event Search and identifying patterns in data and running in predictive analytics, e.g. the correlation showcases between traffic congestion, air pollution and chronic respiratory illnesses within a city center

Real-time– actioning fast to conditions and making up knowledge of decisions about those actions, e.g. remote video camera read license plates for parking payments to be more accurate when I say AI,really mean machine learning. It is machine learning that gives the power to detect patterns in data presented. It learns from these patterns in that manner which will make actionable event for more sensible events.

II. CHALLENGES

1) *Cost:* Connecting devices and operations takes much time, lots of it, and it's a very common problem to overcome. sometimes it taking two times longer? That's based on that in 2018 data, 75 per cent of IoT projects will take up to thrice as long as initially planned. The pure upcoming of IoT sensors takes two to five years. Especially in the beginning, when only a less amount of resources is equipped with IoT sensors, there are very low benefits. Projects with a two-to-five-year horizon aren't great in terms of business." the cost. of IoT deployments can involve costs of between 600 Rs and 3000 Rs a sensor, with mounting prices and many researchers estimates that most large-scale infrastructure project require budgets of 10lakh or above for IoT projects. that type of budgets require major approval and this involves an entirely different type of IoT challenges, but the lack of expertise and confidence among business executives and board members when it comes to complex deployments of machine or IoT technologies.
2) *Business Transformation Potential:* Its common thought while thinking about iot projects, because IoT is still a new to many enterprises, teams. often see uncertainty among many leaders when implementing new tech architecture, especially when supporting big-scale business transformation.
3) *Security and Privacy:* It's a top priority While IoT challenges for enterprise are largely separate to consumer smart-home-tech. major area drawing customer, concerns are data integrity. Data is the main blood of IoT events operations and it's critical its integrity is robust. All enterprise involved must ensure their data or information has not been changed or tampered with while at-rest, in-transfer or in-use cases.

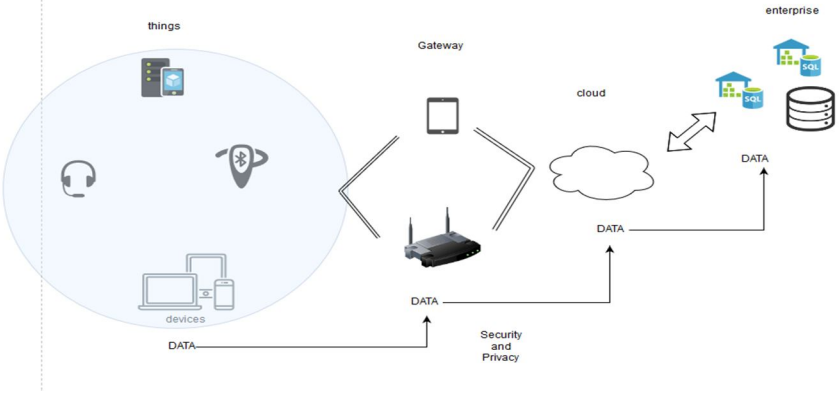


Fig. 2 security And Privacy in terms of Data

Personal information, as well as any generated by an IoT sensor device must be protected & secure whether it is in-transfer state or at-rest. Organizations should encrypt their data to protect when it arrives unaltered, where it's needed.

Enterprises user and other users must be able to trust their network. This means not only making a system that is as secure and protected as possible, but one that's also robust enough a security. Reliability is must. They must find ways to offer uninterrupted user experience and functionality, even if a part of the network infrastructure is under attack.

No person is capable of managing large set of iot sensors device. The continuous addition of devices sensor and network infrastructure means there will constant introduction of new type of vulnerabilities and points where attach chances are high. This means that processes and sensor management become automated and the same time the new threat security have be to added for secure the system.

IoT will always continue to progress stage. resources, sensors, applications and other technologies will come and go over the cycle of an ecosystem. Tools that provide end-to-end proven security and privacy protection management of all entities are imperative.

ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor: 7.177
Volume 7 Issue VI, June 2019- Available at www.ijraset.com

4) *Latency:* Its only matter if occurred otherwise it not effect some type of operation. Internet of things (IoT) applications, example its going to always to check someone when some fraction of temperature changes in thermostat in 1 milliseconds vs 50 milliseconds' really effect in automated car engine managements. Real-time image processing for manufacturing errors on an assembly line may affect some latency where checking is done as fast as possible? Robotic arms performing surgery on a live patient in network? In these use cases and others latency is everywhere. So 40 times benefits in latency. However, that's just the recommendation at this time -- it's unclear as of yet where 5g really provide that or not this in the real word, especially at the launch of 5G.

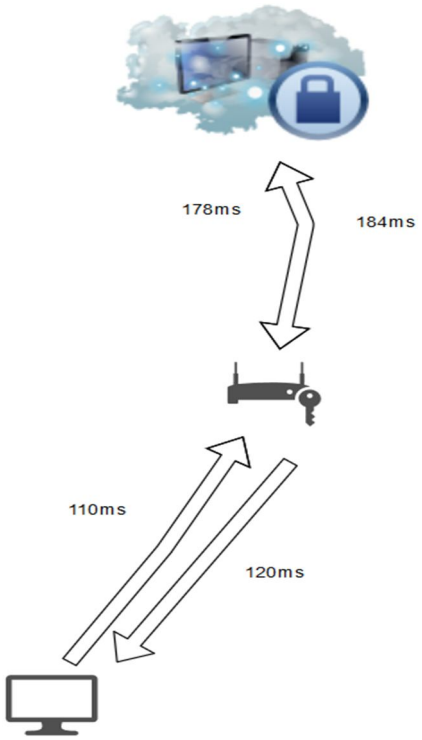


Fig 3. Latency between sending and receiving

But if it does end up being this significant, report like this. it will help to reach new milestone in iot field in next few years.

III.SOLUTION APPROACH USING AI

AI is specially adopting at finding and established solution patterns. Especially when there is huge amount of data. now in terms of data availability iot never lacking in ever. there are already many proofed strategy cases where machine learning which are ai part help to improve iot.

A. Network-Based

Instead of looking for single device security, network-based architecture solution can help secure iot machine by making shield of home network. This will have registered new devices in network and allowed access to device .ai will order to prevent intruders from iot networks by using algorithms of intrusion detection system but every device must have access to and be accessed from outside third parties like cloud and other devices. machine learning engine can help to monitor every device incoming and outgoing traffic to create individual device-based profile. That will help to determine the normal behavior of iot devices in infrastructure. Detecting threat will easy by monitoring and send to warn message to owners of device about that device potential risk and their suspicious behavior.

Machine learning already used in many fields of corporate and enterprise network to help detect threats. But the main problem is attack are happening in generally in the form of legitimate request and normal process. fortunately, in iot functionality and action are very limited, its hard to detect malicious request in that rule and much easy to follow finite rule and an make them normal profile in the system.

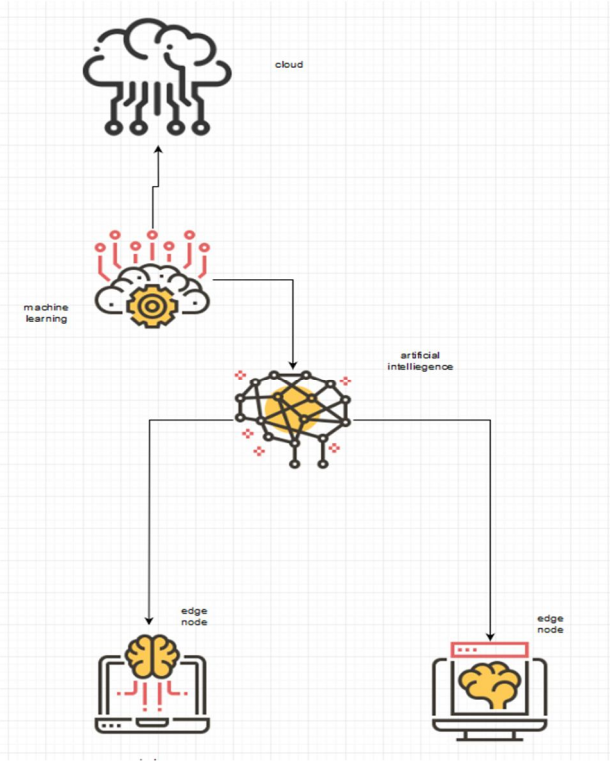


Fig 4. Artificial intelligence in Iot

B. Device-Based Solutions

One of the problems with a many number of IoT sensors is that they don't have the processing power and storage capacity to run security solutions and store huge databases of threat and malware signatures to protect them against threats. Again, machine learning can help bring lightweight endpoint protection to IoT devices. Instead of signature-based protection (which can easily be circumvented with trivial techniques), behavior-based solutions can be developed as thin solutions that are less resource-demanding and can run without bogging down small processors. I've already discussed such solutions in an article I wrote for TechCrunch that was focused on AI-based endpoint solutions that can outsmart malware. The common denominator of all of the mentioned products is that they were very lightweight and they use pattern-based approaches to deal with threats. Though they're made for workstations and not IoT devices, but the concept can easily be ported to the IoT space.

There's also a good post on Network World that presents some nice AI-based solutions to IoT security. Although I favor network-based solutions, I wouldn't say that any of the two are complete per se and I would recommend to opt for both as layers upon layers of protection for your IoT devices.

C. Security Based

One of the biggest challenges in the IoT network security is classifying the type of data to look for anomalies, which are significant deviations in the way data usually behaves over the network. For enterprises and businesses, this poses a huge threat because it means their data on an IoT device–that might be running on any of the several non-standardized wireless protocols–is not secure.

Bob walks us through how this problem is currently tackled, and how IoT security could be improved in the future using deep learning and machine learning applications, such as TensorFlow. Below are some of the important points Bob covers in this particular section Machine-learning tools are already getting more accurate at classifying image categories with only a 3% error-rate as opposed to human error-rate of 5-10%. This is because they get trained on copious amounts of data and become better at identifying categories over time. In the near future, this capability could be extended to the cyberspace for classifying data threats. Currently, there is a significant lack of labeled data in the cyberspace from which the machine learning applications can learn. Therefore, identifying anomalies and monitoring cybersecurity involve hours of manual work and effort. Bob explains how the learnings from image classification can be applied to cybersecurity and how machine learning tools can better identify anomalies in IoT network traffic that could constitute as threats.

IV. FUTURE SCOPE

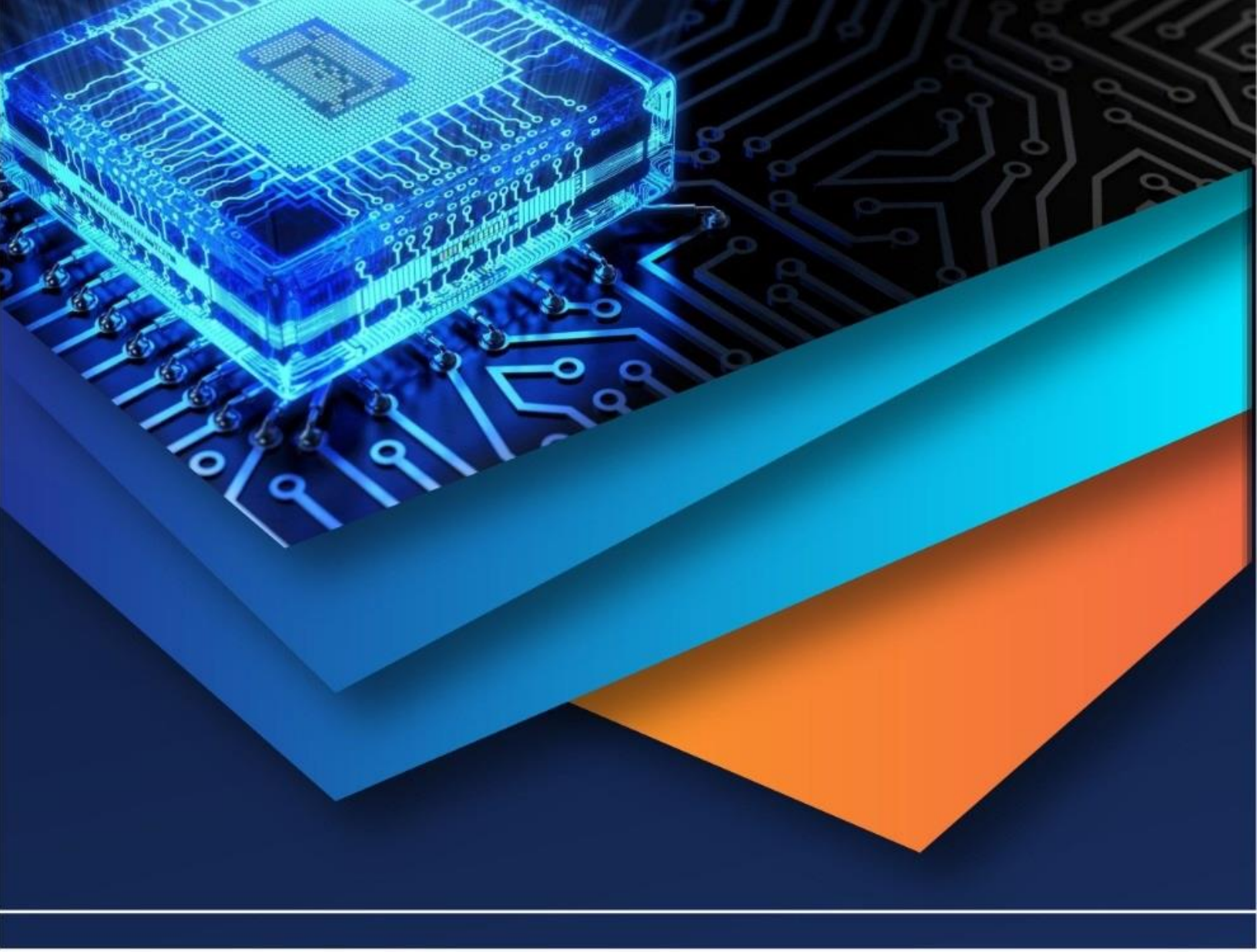
In other scenario what will happen when iot using artificial intelligence. in near future we try to established some statistics which will provide better understanding of more outcome related result. Many fields already try to use in iot edge computing, accessing their data also help to provide better decision support.

V. ACKNOWLEDGMENT

This work was supported by Institute for Information & Management studies, imcost thane(w). under the guide of many professor which help to establish better understanding of many things.

REFERENCES

[1] S. Sarkar, S. Chatterjee, and S. Misra, "Assessment of the suitability of fog computing in the context of internet of things," *IEEE Trans. Cloud Comput.*, vol. 6, no. 1, pp. 46–59, Jan 2018.
[2] S. J. Russell and P. Norvig, *Artificial intelligence: a modern approach*. Malaysia; Pearson Education Limited, 2016.
[3] A. V. Dastjerdi, H. Gupta *et al.*, "Fog computing: Principles, architectures, and applications," in *Internet of Things*. Elsevier, 2016, pp. 61–75.
[4] M. R. Palattella et al., "Internet of Things in the 5G era: Enablers, architecture, and business models," IEEE J. on Sel. Areas in Commun., vol. 34, pp. 510–527, Mar. 2016.
[5] R. Inam et al., "5G network programmability for mission-critical applications," Ericsson Tech. Review, pp. 2–11, Jan. 2018. [4] V. Petrov et al., "Achieving end-to-end reliability of mission-critical traffic in softwarized 5G networks," IEEE J. on Sel. Areas in Commun., vol. 36, pp. 485–501, Mar. 2018.
[6] A. V. Dastjerdi and R. Buyya, "Fog computing: Helping the Internet of Things realize its potential," Computer, vol. 49, pp. 112–116, Aug. 2016.
[7] Y. Mao et al., "A survey on mobile edge computing: The communication perspective," IEEE Commun. Surveys & Tutorials, vol. 19, pp. 2322– 2358, Aug. 2017. [6] S.Andreevetal.,"Exploringsynergybetweencommunications,caching, andcomputingin5G-gradedeployments,"IEEECommun.Mag.,vol.54, pp. 60–69, Aug. 2016.
[8] P. Yang et al., "Catalyzing cloud-fog interoperation in 5G wireless networks: An SDN approach," IEEE Network, vol. 31, pp. 14–20, Sep. 2017.
[9] J. Choi et al., "Millimeter-wave vehicular communication to support massive automotive sensing," IEEE Commun. Mag., vol. 54, pp. 160– 167, Dec. 2016. [9] J. Xu et al., "Cooperative distributed optimization for the hyper-dense small cell deployment," IEEE Commun. Mag., vol. 52, pp. 61–67, May
[10] Y. Yang, "Multi-tier computing networks for intelligent iot," *Nature Electronics*, vol. 2, no. 1, p. 4, 2019.
[11] A. V. Dastjerdi and R. Buyya, "Fog computing: Helping the internet of things realize its potential," *Computer*, vol. 49, no. 8, pp. 112–116, Aug 2016.
[12] N. Abbas, Y. Zhang *et al.*, "Mobile edge computing: A survey," *IEEE Internet Things J.*, vol. 5, no. 1, pp. 450–465, 2018.
[13] N. Chen, Y. Yang *et al.*, "Fog as a service technology," *IEEE Commun. Mag.*, vol. 56, no. 11, pp. 95–101, 2018.
[14] B. Tang, Z. Chen *et al.*, "Incorporating intelligence in fog computing for big data analysis in smart cities," *IEEE Trans. Ind. Informat.*, vol. 13, no. 5, pp. 2140–2150, 2017.
[15] P. O'Donovan, C. Gallagher *et al.*, "A fog computing industrial cyber-physical system for embedded low-latency machine learning industry 4.0 applications," *Manufacturing Letters*, vol. 15, pp. 139–142, 2018.
[16] Y. He, F. R. Yu *et al.*, "Software-defined networks with mobile edge computing and caching for smart cities: A big data deep reinforcement learning approach," *IEEE Commun. Mag.*, vol. 55, no. 12, pp. 31–37, 2017.
[17] C. Perera, Y. Qin *et al.*, "Fog computing for sustainable smart cities: A survey," *ACM Comput. Surveys (CSUR)*, vol. 50, no. 3, p. 32, 2017.
[18] T. Ouyang, Z. Zhou, and X. Chen, "Follow me at the edge: Mobility-aware dynamic service placement for mobile edge computing," *IEEE J. Sel. Areas Commun*, vol. 36, no. 10, pp. 2333–2345, Oct 2018.
[19] T. Taleb, S. Dutta *et al.*, "Mobile edge computing potential in making cities smarter," *IEEE Commun. Mag.*, vol. 55, no. 3, pp. 38–43, March 2017.
[20] A. I. Maarala, X. Su, and J. Riekki, "Semantic reasoning for context-aware internet of things applications," *IEEE Internet Things J.*, vol. 4, no. 2, pp. 461–473, 2017.
[21] S. Husain, A. Kunz *et al.*, "Mobile edge computing with network resource slicing for internet-of-things," in *Internet of Things (WF-IoT), 2018 IEEE 4th World Forum on*. IEEE, 2018, pp.



10.22214/IJRASET

45.98

IMPACT FACTOR: 7.129

IMPACT FACTOR: 7.429

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY