Available online at : http://www.advancedscientificjournal.com
http://www.krishmapublication.com
IJMASRI, Vol. 3, issue 1, pp. 899- 903, Jan. -2023
https://doi.org/10.53633/ijmasri

INTERNATIONAL JOURNAL OF MULTIDISCIPLINARY ADVANCED SCIENTIFIC RESEARCH AND INNOVATION (IJMASRI)

ISSN: 2582-9130 **IBI IMPACT FACTOR 1.5** **DOI: 10.53633/IJMASRI**

RESEARCH ARTICLE

SIMULATING AI BIAS IN INDUSTRIAL IOT DEVICES

Deepak Sangwan[1], Karan Goyal[2] and Ajay Kumar Kaushik[3]
[1,2,3,] *Department of Information Technology, Maharaja Agrasen Institute of Technology, Delhi, India.*

Abstract

In recent years, the Internet of Things has reached the height of popularity because of its widespread applications ranging from hospitals, agriculture, homes, and whatnot. This growth has led to an increase in the number of IoT devices as well as our dependence on them. This has led to increased concerns about their ethical/unethical usage. This paper simulates one of these ethical issues i.e. biases in IoT devices. We consider the bias in Smart parking system and then go on to apply certain techniques to remove the bias.

Keywords: IoT, Smart Parking, Bias, ethical

Introduction

Defines IoT as. IoT has applications in healthcare (Patel Keyur *et al.*, 2016; Kashani and Mostafa Haghi 2021) education (Al-Emran *et al.*, 2020), agriculture (Shenoy *et al.*, 2016) and many other fields. With the growing use of AI in IoT (Sivaganesan 2019) there has been increasing concerns regarding the ethical issues in IoT devices. One of the important ethical issues is bias in AI powered IoT devices (Seng and Loke 2021).). AI bias can occur when the data used to train a machine learning model is not representative of the population it is intended to serve. This can lead to AI systems making unfair or discriminatory decisions. In the context of industrial IoT devices, AI bias could potentially lead to unequal treatment of workers or customers, or to the deployment of faulty or unreliable systems. It's important for companies to be aware of this issue and to take steps to prevent AI bias in their systems. This can include carefully selecting and cleaning the data used to train the model, as well as regularly testing and evaluating the performance of the AI system to ensure it is making fair and accurate decisions. This research aims at simulating an IoT based smart parking system in iFogSim, comparing the latency of cloud and fog technologies and detecting the bias in working of smart parking systems.

A. Research Field

A smart parking IoT system is a network of sensors, cameras, and other technologies that are used to monitor and manage parking spaces. The

system collects data on the availability of parking spaces, and can use this information to direct drivers to available spots, or to help city planners and traffic managers make decisions about parking infrastructure. Smart parking systems can also use machine learning algorithms to improve their accuracy and efficiency over time. Some potential benefits of a smart parking IoT system include:

- Improved convenience and accessibility for drivers, who can easily find available parking spaces and avoid spending time searching fora spot.
- Reduced congestion and emissions, as drivers are able to find parking spots more quicklyand efficiently.
- Increased revenue for cities and parking operators, as the system can help optimize the use of existing parking spaces and potentially reduce the need for new construction.
- Enhanced safety, as the system can help prevent accidents and incidents in parking lots by providing real-time information on the availability of spaces and other factors.
- Overall, a smart parking IoT system can help improve the efficiency and effectiveness of parking management, and provide benefits for drivers, cities, and parking operators.

This research paper simulates a smart parking system on an iFogSim platform. This would then use the data collected on iFogSim to calculate bias and remove that bias using AI methodologies.

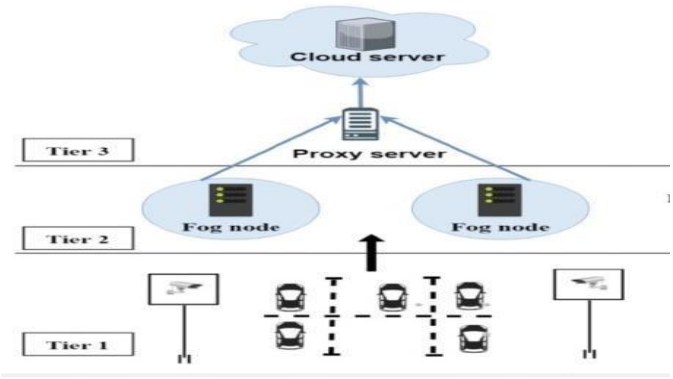

Fig 1. Various tiers of Smart Parking System.

Fig 1 shows how the smart parking system collects data. The system can be divided into 3 tiers.

Tier 1: Tier 1 consists of the actual cars and the camera sensors. There may be any number of cameras. The number of cameras will impact the latency of the fog system.

Tier 2: Tier 2 consists of the fog nodes which act as the link between the cloud and the cameras. To process the real-time data of parking slots, the fog computing infrastructure is enabled as a supporting middle layer in between edge nodes and the cloud to collect, process, and analyze the data at the edge.

Tier 3: The role of cloud in the proposed framework is that it stores the image data in its storage when it is no longer needed by the fog node. The communication between the fog and the cloud is enabled through a proxy server. The fog node passes the images data to the cloud after a specific time period, and if the fog needs some image data, then thedata is provided by the cloud.

B. *Research Motivation*

The literature review before the research suggested the following loopholes in researches done so far:

1. Although a wide range of application areas have been discovered for AI enabled IoT (Song and Hao. (2020), there is a general scarcity of measurements of impacts of bias on the working of such devices. Given the vast range of applications of IoT (Kashani and Mostafa Haghi 2021; Al-Emran *et al.*, 2020; Shenoy 2016; Sivaganesan 2019) it is important to properly assess the working bias in the working of IoT devices as it can have drastic impacts on the lives of people.
2. Almost every AI enabled device might have the possibility of odd behaviour mainly because of improper training models/wrong training sets/biased training data etc. It is important to identify such biases.

Based on the above 2 findings from the literature review, it becomes essential to do this research using available resources.

Literature Review

Researchers around the world have confirmed the various ethical issues including AI can occur in IoT devices. Seng (Seng and Loke 2021) reviews the ethical algorithmic behaviour in IoT. Danks (Danks and London 2017) highlights that algorithmic bias can arise in Autonomous Systems. With the increasing data-driven nature of IoT devices, a number of possible opportunities for discrimination can arise as noted in (Tschider 2018) the examples given include an IoT gaming console and neighbourhood advisor that advises avoiding certain areas. Additionally, such an algorithmic bias can occur in machine-learning algorithms used for autonomous vehicles, where large volumes of data over time frames of minutes to days are analysed. iFogSim has been used for simulating IoT environments as in the case of (Tariq Ahamed Ahanger 2020) where an intruder detection system was simulated in iFogSim. Similar simulations were done in other application areas like CO2 level detection in rooms (Kairong Duan 2018) etc. Although there have been many examples of AI applications in IoT devices as well as simulations of IoT devices on simulators like iFogSim, there has not been much research on detecting the bias of IoT devices and further correcting these biases. This paper aims at focussing on detecting the bias in decisions made by IoT devices.

Proposed Methodology

A. Simulating the working of the IoT parking system on iFogSim

iFogSim is a JAVA based simulator based on the Fog technology. Fog just like the cloud is a technology that provides data, compute, and storage and application services (Gupta 2017). The difference between fog and cloud is that fog is an extension of cloud and brings services to the edge of cloud These features of fog help reduce latency caused in cloud computing and helps make faster decision making possible. iFogSim, as proposed in is a simulator to model IoT and Fog environments and measure the impact of resource management techniques in latency, network congestion, energy consumption, and cost.

Following is the topology for the iFogSim network of a parking system with 12 cameras:

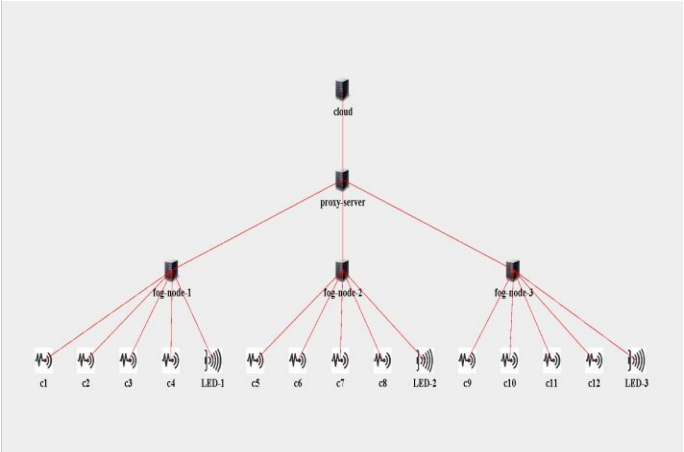

Fig. 2: Topology for iFogSim setup

We used 12 cameras as sensors, 3 fog nodes, Proxy to establish connection between fog node and cloud. The cameras clicked the images of the parking lot from various directions and sent these to the fog nodes. The fog nodes would then assess those images and detect the empty parking spaces. The empty parking spaces would then be displayed on the LED in the parking lot displaying the positions of the empty parking slots. Different parameters such as RAM, CPU Length, UPLINK, DOWNLINK etc have to be defined in iFogSim.

Experimental implementation and Results

The values for the various parameters stated in the previous section have been given in the following table:

Parameters	Cloud	Fog	proxy
Level	0	2	1
CPU Length (MIPS)	448000	2800	2800

RatePerMIPS	0.01	0.0	0.0
UPLINK (MB)	100	10000	10000

Table 1: Various Parameter values in Ifogsim

where α is the Tuple CPU Execution Delay for capturing pictures and μis the time to upload pictures on fog nodes for processing and storage. Finally, φ is the time taken to display the information to the LED after processing at the Fog node.

From the table, it is clear that the latency drops substantially when a fog node is used as compared to direct usage of cloud.

Based on these parameters and the above given topology of a 6-camera network, the latency and network usage of a cloud and fog network were compared. The following were the results obtained:

S.No	No. of fog devices	No. of cameras per fog devices	Latency in fog(ms)	Network Usage in fog(kb)	Latency in cloud (ms)	Network Usage in the cloud(k b)
1.	1	4	135	760	335	778
2.	2	4	212	1520	424	1556
3.	3	4	258	2280	553	2334
4.	4	4	324	3040	652	3112
5.	5	4	572	3800	764	3890

Table 2: Latency and Network Usage comparison forFog and Cloud

A. Latency

The latency is computed using

$$Latency=\alpha+\mu+\varphi \quad \ldots\ldots 1$$

compared to when the data goes to fog. The reason as given in (Gupta 2017) is that the processing of images in case of fog is limited to the fog node of

B. Network Usage

When the traffic increases on cloud servers then, only the cloud resources are used. Increase of traffic on the cloud server results in increased network usage. Consequently, the data rates on the network decrease due to the increased traffic. For geographically distributed servers, one fog node is dedicated for one geographical area to deal with the request of that area. Consequently, the network usage in that case decreases and the transmission rate for therest of the traffic increases.

The network usage is calculated using which is derived from (Tariq Ahamed Ahanger 2020).

$$Network usage=Latency*\partial \quad \ldots\ldots 2,$$

where ∂ = tupleNWSize

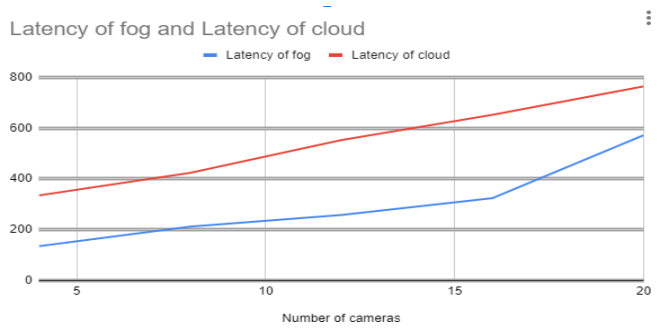

Fig. 3: Effect of increase in cameras on latency

From figure 3 it can also be observed that as the number of cameras increases, the latency of the network greatly increases. But this increase in latency varies differently for fog and cloud. The increase in latency is more in case when the data goes to cloud

as that specific area only. However, in the case of cloud, the single cloud processes images from all the sensors.

Conclusion

Based on the values of network usage and latency achieved in table II, it can be concluded that Fog Nodes greatly improve the speed and performance of a network as compared to direct usage of cloud. The average latency in cloud system was 99.45% more than fog. Similarly, in case of network usage, Fog system clearly outperforms cloud. Cloud network had 2.36% more network usage than fog. Further detection of bias in the network as well as its correction can be done in the future course of action.

Acknowledgment

We wish to express our gratitude to Mr. Ajay Kaushik, our mentor at MAIT for assisting us with the research paper. We would like to thank him for his doubt clearing sessions throughout the course of this research paper. Under his guidance we have completed our research and tried our best to implement what we had learnt till now.

Reference

1. Patel Keyur K., Sunil, M. Patel and Scholar, P. (2016). "Internet of things-IOT: definition, characteristics, architecture, enabling technologies, application & future challenges." International journal of engineering science and computing 6.5 (2016).
2. Kashani and Mostafa Haghi. (2021). "A systematic review of IoT in healthcare: Applications, techniques, and trends." Journal of Network and Computer Applications 192 (2021): 103164.
3. Al-Emran., Mostafa, Sohail Iqbal Malik and Mohammed, N. (2020). Al-Kabi. "A survey of Internet of Things (IoT) in education: Opportunities and challenges." Toward social internet of things (SIoT): enabling technologies, architectures and applications (2020): 197-209.
4. Shenoy, Jeetendra and Yogesh Pingle. (2016). "IOT in agriculture." 2016 3rd International Conference on Computing for Sustainable Global Development (INDIACom). IEEE, 2016.
5. Sivaganesan, D. (2019). "Design and development ai-enabled edge computing for intelligent-iot applications." Journal of trends in Computer Science and Smart technology (TCSST) 1.02 (2019): 84-94.
6. Seng and Loke, W. (2021). Achieving Ethical Algorithmic Behaviour in the Internet of Things: A Review School of Information Technology, Deakin University, Geelong 3217, Australia;July 2021.
7. Danks, D and London, A. J. (2017). Algorithmic Bias in Autonomous Systems. In Proceedings of the 26th International Joint Conference on Artificial Intelligence, Melbourne, Australia, 19–25 August 2017; pp. 4691–4697.
8. Tschider, C.A. (2018). Regulating the IoT: Discrimination, Privacy, and Cybersecurity in the Artificial Intelligence Age. Denver Univ. Law Rev. 2018.
9. Tariq Ahamed Ahanger., Usman Tariq. Atef Ibrahim. Imdad Ullah and Yassine Bouteraa. (2020). “IoT-Inspired Framework of Intruder Detection for Smart Home Security Systems”, Aug. 2020.
10. Kairong Duan. Simon Fong and Yan Zhuang. (2018).“Carbon Oxides Gases for Occupancy Counting and Emergency Control in Fog Environment” Feb 2018.
11. Gupta, H., Dastjerdi, A.V. Ghosh, S. K and Buyya, R. (2017). "iFogSim: A toolkit for modeling and simulation of resource management techniques in the Internet of Things edge and fog computing environments", Softw. Pract. Exper., vol. 47, no. 9, pp. 1275-1296, 2017.
12. Song and Hao. (2020). "Artificial intelligence enabled Internet of Things: Network architecture and spectrum access." IEEE Computational Intelligence Magazine 15.1 (2020): 44-51.

*****