ISSN: 2393-8048
International Advance Journal of Engineering, Science and Management (IAJESM)
Multidisciplinary, Multilingual, Indexed, Double Blind, Open Access, Peer-Reviewed, Refereed-International Journal.
SJIF Impact Factor =8.152, July-December 2025, Submitted in September 2025

A Fog Based Data Analytics Framework Ensuring Security in Smart Home

Ms. Kanishka, Research Scholar, Nirwan University, Jaipur
Prof. (Dr.) Amit Singla, Professor, Nirwan University, Jaipur

Abstract

Fog Computing has marked an onset of appealing technology pertinent in the domain of Information Technology. Smart homes are equipped with many smart devices interacting with each other and hence generating tremendous amount of data. The increasing use of these smart homes increases thenetwork usage, energy consumption. Although there are many smart devices in smart home which generate data but CCTV is one of the main devices that contributes to a large data volume and transmission rate. The images and video streams data were sent to cloud but there is always the issue of storage and processing the data on cloud. Fog computing comes up as a solution is to improve mobility, security, and on-demand while addressing current Cloud computing problems like energy consumption, latency, and network bandwidth usage. The objective of this paper is to introduce the fog layer in smart home model which will analyse whole CCTV data here and only filtered data will be sent to cloud. This strategy lowers energy consumption, latency, and network bandwidth usage. Using the iFogSim2 network simulator, the FBSHM model shows efficiency in response time and optimization of energy use, latency, and network bandwidth usage.

Keywords: Fog Computing, Smart Home, IoT, Data Analysis, CCTV Surveillance.

1.Introduction

Our future is being shaped by innovative and disruptive concepts as the globe changes rapidly. The Internet of Things (IoT), which was first introduced many years ago but is constantly changing, is one such example. IoT is nothing but collection of physical devices connected to the internet. As devices are connected through sensors, every item we use daily gets smarter. Every gadget including actuators, mobile phones, and so forth, is a part of both our domestic and workplace lives.A vast amount of data is produced by these IoT devices since they enable new methods of device connectivity and communication. By 2025, there are expected to be over 75.44 billion IoT devices, and these gadgets will produce massive amounts of data.[1].Numerous IoT devices are installed in SH like smart door, smart kitchen, smart locks and hence they all send the data to cloud network which increases load on cloud. With the popularity of smart CCTV cameras installed in SH which generates large volume of data and traditionally the only medium to handle this data was cloud-based architecture. This has reached an epitome where it faces several challenges like high latency, energy usage and bandwidth cost [2].

Several algorithms and policies have been implemented to improve the data analysis on the cloud, but the smart cameras can generate around 400GBS of data in a month. If camera only send an alert when a threat is detected then also it can generate around 70GB of data in a month. This data is increasing substantially, so cloud network becomes inefficient in handling the real time surveillance data and becomes slower in terms of response time.

To mitigate these challenges, some mechanism is needed that can deal with few constraints like local processing of data and its storage. The challenges like increased latency, higher energy consumption and bandwidth bottlenecks due to distance between smart devices and cloud data centres need to be controlled for efficient and real time response in CCTV based smart home systems [3].To overcome these limitations, a framework is needed that integrates cloud and fog computing for smart home that can reduce latency, in other words fog layer as an intermediate layer is placed between cloud and edge devices. Thus, Fog based SH model makes data processing faster and data storage and analysis is done closer to the network. Thus, the problem is to frame a FBSHM that ensures:

- **Reduced latency** for real-time monitoring and alarm generation,
- **Optimized bandwidth usage** by processing,filtering,and cleansing raw data locally before transmitting to the Cloud,
- **Lower energy consumption** through resource-efficient allocation.

2. Literature Review

Chen et al. (2018) suggested a fog computing-based smart home model to reduce cloud load, enhance cloud performance and efficiency, and offer a real-time calculation service via Zigbee protocol. In addition to comparing cloud-only network structures and cloud-fog hybrid architectures, experiments were undertaken to measure system efficiency and latency. On the other hand, the authors did not compare the proposed model to any alternative behavioural modelling. Also, the important factors—like extensibility and availability—were not assessed, and the model that was offered was expensive.

Jha et al. (2022) recommended and implemented the fog-based architecture for real time videos in sports applications to track and improve the performance of athletes. The distributed fog computing approach is used to explore real time video data generated from elite soccer. It uses dual layer topology that integrates sensor data, video streams and analysis tools to support trainers in making quick decision. Latency is reduced to a great extent as compared to cloud centric but it lacks in stronger data privacy. So future work can be done on developing efficient encryption algorithms to secure the data

Awaisi et al. (2019) discusses the growing problem of vehicle parking in urban areas due to the rising number of personal vehicles and limited parking infrastructure. It highlights key issues such as traffic congestion, fuel waste, and pollution, all of which are intensified by inefficient parking. To resolve these concerns, the paper proposes a fog computing-based smart parking system that uses computer vision technique as cameras are installed on first layer of architecture. The architecture is simulated through iFogSim and the results shows reduced latency and network usage compared to traditional cloud-based systems. However there is a privacy breach for car owners as cameras are there in parking area and it click images which are stored in cloud.

Masip et. al. (2018) came up with a hierarchical and secure fog to cloud architecture named mF2C for efficient use of the resources at the various architecture levels is created. To collect and analyse data and guarantee resource coordination amongst the hierarchies, the designed architecture can accommodate requests from IoT applications. The mF2C architecture was tested on various applications like Emergency situation management, smart boat service and smart fog hub service. The experimental results show that by combining fog to cloud that is by using mF2C environment gives a reduction of 2.5% in latency and 15% increase in response time as compared to only cloud environment.

Mutawa and Eassa (2020) realises the dire need of security solutions in Smart homes. The author has taken into account two factors- Authorization and authentication. To prevent unwanted access, the author uses multi-factor authentication as an additional level of security. One level is facial recognition, which has gained popularity recently because of its biometric methods and ease of usage with cameras found on most popular computers and smartphones. The second level is liveness detection, these both methods are being used for log-in authentication. According to the author, these methods are never been adopted for security in smart homes.

Kanyilmazet al. (2019) presented architecture for Smart Home with private nodes at fog layer. Fog computing is essential for creating the ideal smart home since installing inexpensive wireless sensors on floors, walls, pipes, and rooms will generate a significant amount of data that must be processed locally via an edge gateway to connect the home to the cloud. This would guarantee the data's confidentiality and provide a safe environment for habitation, not just for a single home but also at the municipal level. Different fog nodes can dynamically serve smart home systems, and new fog nodes are defined. Data privacy and internet connection consumption have both decreased because of the processing of data at fog nodes. But this architecture has a disadvantage that whenever a request is made, a token must be authenticated and then send back to cloud layer.

Surantha and Wickansono (2018) explored the design and implemented smart home security system. The old-style CCTV can only capture the images and record the audio. It fails whenever there is any suspicious object. The implementations is done in Raspberry Pi and Arduino. The passive infrared sensor detects any movement around camera and it sends signals to smart webcam to click the picture. Two methods were used, they are motion detection and object recognition. If any doubtful object is detected, a warning alarm is activated to alert house owner. The results show that it takes around 2 seconds to detect an intruder with an accuracy of 89%. This system was implemented on Cloud database.

He et al. (2017) implemented a novel fog computing architecture which is multi-tier in nature and it makes use of both ad-hoc and dedicated fog nodes to perform data analytics in smart city applications. Furthermore, in order to supply computing resources for real time data analytics services, QoS based resource allocation algorithms are established.

In order to gain insight of the research published in the field of data analytics at fog layer in SH framework, we have surveyed the literature and analysed the existing techniques. The goal of this paper are:

- Analyse the environment necessary for implementation of the framework
- Implementing the Fog Based Smart Home model (FBSHM).
- Simulating the environment using iFogSim2 and setting the parameters.
- Showing the dataflow on cloud or fog by setting the flag-true or false
- Comparing the results of cloud only and hybrid fog-cloud architecture

3. Proposed Fog Based Smart Home Model (FBSHM)

This section proposes Fog based Smart Home model which is divided into three major layers. The edge layer is responsible for recording raw video data. The fog layer implements data filtering and analysis functionalities, thereby reducing dependence on cloud and ensuring faster response. The cloud layer performs long term storage and remote monitoring. The FBSHM's layered model is depicted in figure below:

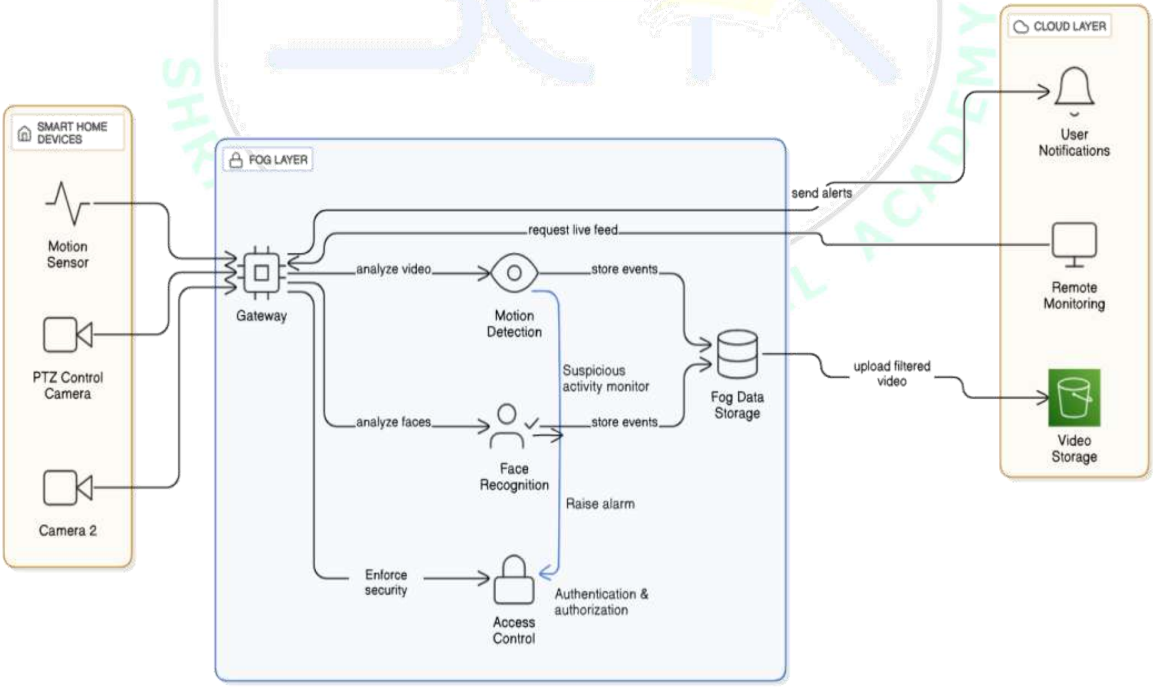


Fig 1: FBSHM Framework

The proposed framework’s first layer **EdoSH** consists of the elements which are installed at home for surveillance and sensing. The elements are motion sensor, camera and PTZ control camera. The smart CCTV camera and PTZ (pan, tilt zoom) camera are purposefully placed to cover large area. Another element install is motion sensor that monitor the movement and other changes in SH activities. The CAT-6 ethernet cable is used as a transmission medium in the edge layer for transferring raw video stream data to the gateway.

The second layer **is Fog Layer (FoSH).** The gateway act as a fog server which collects the data from CCTV and PTZ camera and sends it for real time processing. The primary goal of this layer is to do the raw video data processing here itself that is analyze the recorded data locally and make decision.

The fog layer is further divided into modules that distribute the task among themselves. These modules are motion detection, face recognition and access control.

Motion detection is responsible for analyzing raw data and to detect any suspicious activity or unusual movement. Face recognition oversees recognizing and identifying individuals. This module analyses the video frames and makes the database of authorized persons. Based on stored data, it can easily distinguish between authorize and unauthorize persons. If any unauthorize face is detected, it raises an alarm. The third module is Access control. It works when the data is provided by two modules- motion detection and face recognition, security policies are implemented that handles authentication and authorization of SH users. This allows the SH users to control the access in their home. Further, if any abnormal behavior or pattern is observed, it raises an alarm.

Fog data storageis the last module of fog layer which is accountable for storing filtered and processed video data, which is retrieved from motion detection and face recognition events results. The purpose of storing results in fog data storage (on fog layer) is to ensure when an image/video is recorded, it can be processed immediately to ensure instant notification or alert for real time security breach or any risk to SH residents.

Thus, fog-based SH solution reduces the data load before uploading on cloud layer.

Cloud Layer (CoSH) is the third layer that receives the filtered data from fog layer for further processing. It collects alert for e.g. suspicious activity, unauthorized access and sends real time notification to user of SH through connected devices like smartphone or computer. It ensures real time monitoring remotely and users can access the system via cloud. This guarantee constant monitoring even when the SH user is not at home.

4. Components of Proposed FBSHM

1. No. of Cameras installed- It represents the total count of CCTV and PTZ cameras installed in SH environment. This number directly impact the data generation rate, total region covered and network traffic in a fog based or cloud-based scenario. Also, each camera generates real time videos continuously, so increasing the number of cameras also increases network traffic to the gateway.
2. Total area or houses covered- More the number of areas covered, more cameras installed and hence more motion detection and face recognition events are store which eventually increases the load on fog devices.
3. Parameters-The proposed FBSH model worked on certain defined parameters which are improved by the implementation of this architecture. The main parameters considered are Latency, execution time and cost and the energy consumed. The large number of cameras increases bandwidth usage, FoSH supports in reducing the above parameters by processing data nearby.

5. Flowchart of Proposed model

The complete flowchart is explained in the figure below illustrating the smooth flow of data from the beginning to the end represented with the help of different symbols of the flowchart.

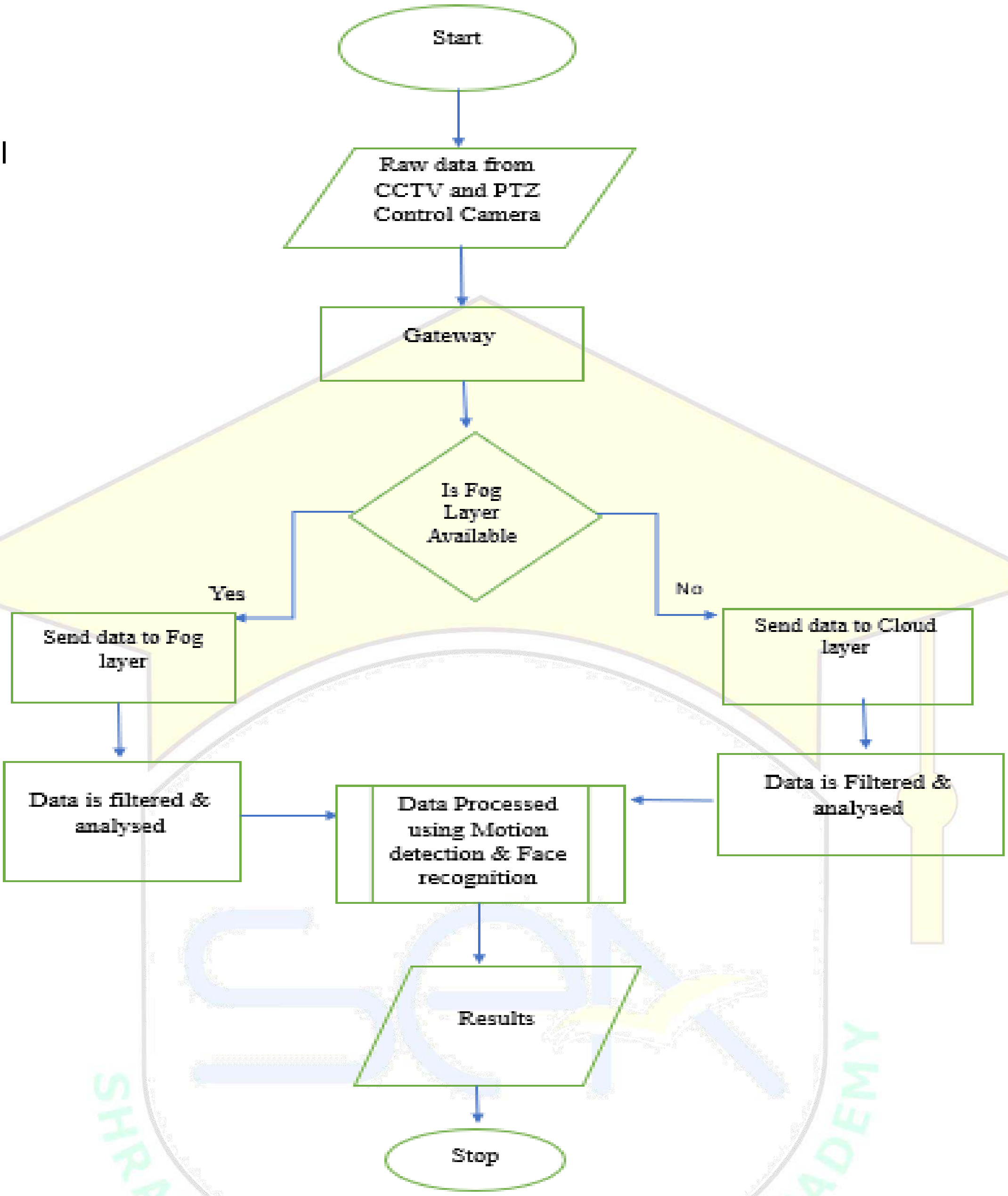

Start
Raw data from CCTV and PTZ Control Camera
Gateway
Is Fog Layer Available
Yes
No
Send data to Fog layer
Send data to Cloud layer
Data is filtered & analysed
Data is Filtered & analysed
Data Processed using Motion detection & Face recognition
Results
Stop

Fig 2: Flowchart of Proposed Model

Further, how each node is sending data to another node is explained below:

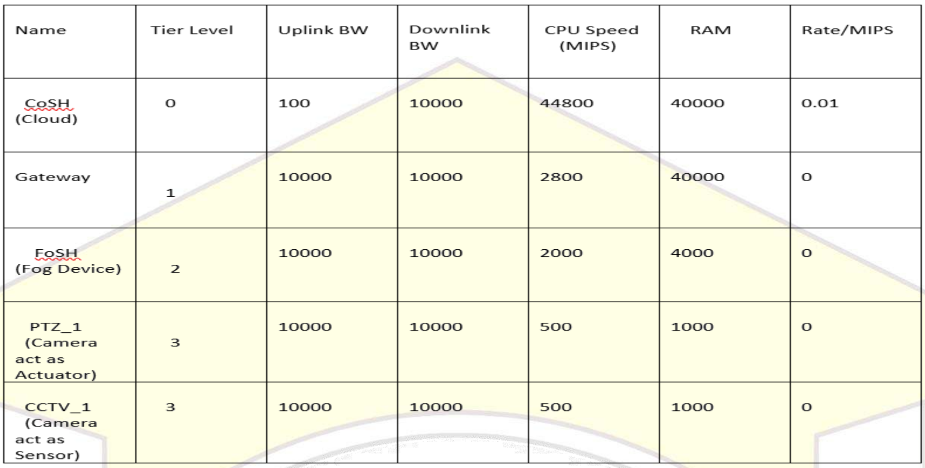
- Data is generated through CCTV cameras and PTZ control cameras installed in SH. This data is in raw form and is transferred to gateway.
- Then, to whom gateway will transfer the data depends on selected flag. A flag is a variable which is used to control the flow of program, determine a condition or a state. Its value is generally TRUE or FALSE, ON or OFF, ENABLE or DISABLE.
- If (CLOUD= false), that implies fog layer is available, then data is sent to fog layer where it does the local processing like motion detection and face recognition and send the filtered results to cloud layer.
- If (CLOUD=true) that implies fog layer is not there, so data is sent to cloud layer, here cloud layer filter and analyze the data using motion detection and face recognition and send alerts to user. It is also countable for storing the event results that can be used in future.

6. Implementation

The FBSHM is designed and simulated in iFogSim2 which is integrated in Java Based Eclipse IDE to compare the performance of Fog based SH and Cloud Based SH Model. For better comparison and accuracy check, 5 different setups have been used, in which No. of Cameras and no. of houses are progressively increased.

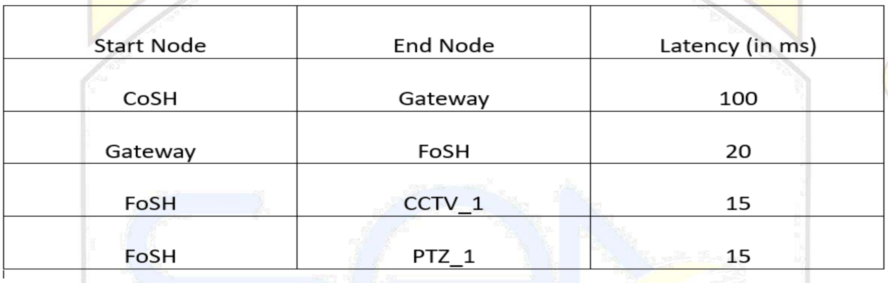
The configuration settings of each device are given in Table 1 and the latencies between various devices is listed in Table 2.

Table 1: Configuration Settings for creating Topology



Name	Tier Level	Uplink BW	Downlink BW	CPU Speed (MIPS)	RAM	Rate/MIPS
CoSH (Cloud)	0	100	10000	44800	40000	0.01
Gateway	1	10000	10000	2800	40000	0
FoSH (Fog Device)	2	10000	10000	2000	4000	0
PTZ_1 (Camera act as Actuator)	3	10000	10000	500	1000	0
CCTV_1 (Camera act as Sensor)	3	10000	10000	500	1000	0

Table 2: Latency Values between devices



Start Node	End Node	Latency (in ms)
CoSH	Gateway	100
Gateway	FoSH	20
FoSH	CCTV_1	15
FoSH	PTZ_1	15

We have taken into considerations 5 different configurations which are named as CaseNo.1,CaseNo.2, Case No.3, Case No.4 and Case No.5. In all these 5 cases, number of houses and number of cameras are increased. The details are given in the Table 3. Initially house 1 contains 1 PTZ Camera and 1 CCTV

Camera. Here CCTV camera act as sensor and PTZ Camera act as an actuator. The topology representation of Case no. 1 and Case No.4 are given in Figure 3 and 4 respectively.

Table 3: Configuration Settings of Five Different Cases

Case No.	No. of Houses	No. of Cameras	Total Cameras
1	1	2 (1-PTZ,1 CCTV)	2
2	1	4(2-PTZ,2 CCTV)	4
3	2	4 (2-PTZ,2 CCTV)	8
4	3	4 (2-PTZ,2-CCTV)	12
5	4	6 (3 PTZ,3 CCTV)	24

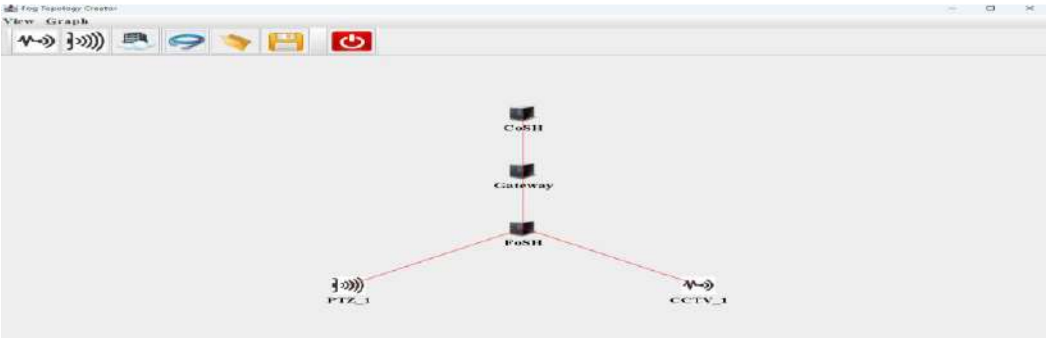


Fig 3: Topology for Case No.1

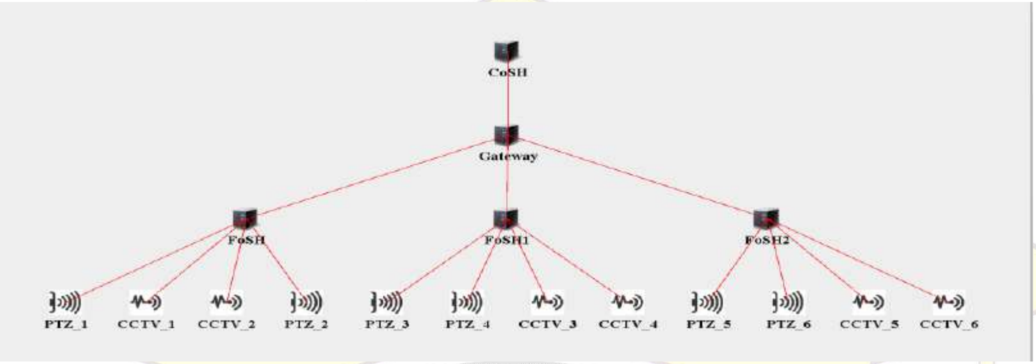


Fig 4: Topology for Case No.4

7. Results and Discussions

The simulation results summary comprises of various performance measures such as total network usage, cost of execution, energy consumption and latency. The result summary of both modes- Cloud only and Hybrid (Cloud+ Fog) are given in Table 4 and 5.

Table 4: Result Summary of Simulation Using Cloud Only Scenario

Total Cameras	Total Network Usage (KB)	Energy Consumption (KJ)	Cost of Execution	Latency (in ms)
2	81004.2	169419.7	85387.2	210.04
4	161937.0	169419.7	143121.6	210.56
8	323826.2	169419.7	259295.6	210.89
12	485768.8	169419.7	375717.6	211.54
24	970669.6	169419.7	719372.4	212.25

Table 5: Result Summary of Simulation of Hybrid (Fog + Cloud) Scenario)

Total Cameras	Total Network Usage (KB)	Energy Consumption	Cost of Execution	Latency (in ms)
2	576.6	165855.7	7317.6	6.24
4	1056.8	165855.7	10552.4	6.58
8	2346.0	165855.7	12616.11	6.89
12	3490.0	165855.7	11276.8	7.08
24	7248.0	165855.7	15354.4	7.48

The comparison of total network usage, energy consumption, cost of execution and latency of cloud and hybrid (Cloud + Fog) are given in Fig 5, 6, 7 and 8 respectively.

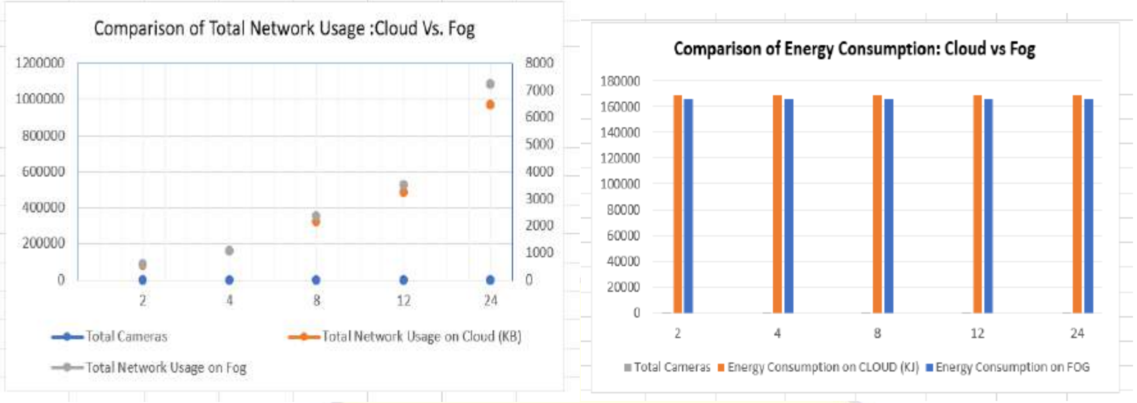


Figure 5 and 6: Comparison of total network usage and energy consumption: Cloud vs Fog

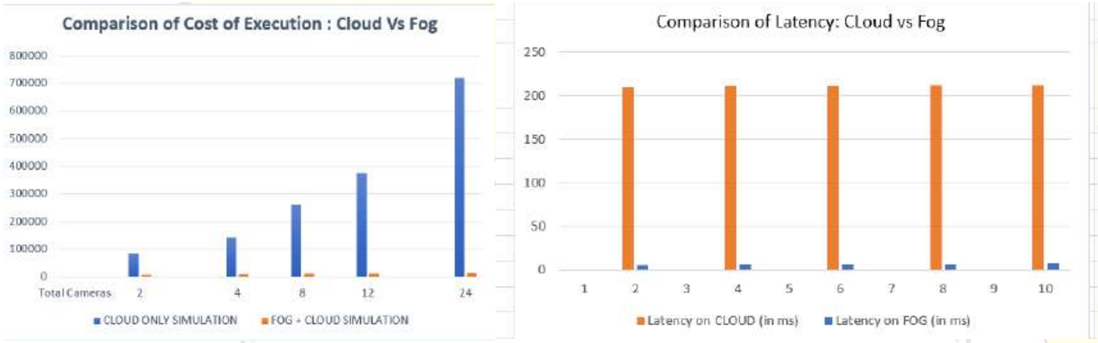


Figure 7 and 8: Comparison of Cost of Execution and Latency: Cloud vs Fog

The overall analysis shows that processing the data on fog layer considerably lowers the load on cloud and hence the network usage reduces which in turn minimize the cost of execution.

8. Conclusion and Future Scope

Fog based SH model is simulated using iFogSim2 and we have chosen CCTV data to be analysed. We have accomplished a assessment of cloud only and hybrid (fog +cloud) environment with 5 different configurations. The results of the simulation shows that all the four parameters which we have taken into consideration is lesser in hybrid mode than in the cloud only mode. This framework enhances the efficiency of data being analysed and is secure as both cameras CCTV and PTZ control camera uses motion detection and face recognition mechanism to identify any suspicious behaviour. In future, work can be carried out to further improve the security for smart home users by implementing CBE (code-based encryption technique) for providing the access.

REFERENCES

1. Alavi, A.H., Jiao, P., Buttlar, W.G. and Lajnef, N. (2018) Internet of Things-Enabled Smart Cities: State-of-the-Art and Future Trends. Measurement, 129, 589-606.
2. N. Surantha and W. R. Wicaksono, “Design of Smart Home Security System using Object Recognition and PIR Sensor,” in Procedia Computer Science, 2018, vol. 135, pp. 465–472. doi: 10.1016/j.procs.2018.08.198.
3. Fog Computing and Internet of Thins: Extend the cloud to where the things are (Cisco) [Online] https://www.cisco.com/c/dam/en_us/solutions/trends/iot/docs/computing-overview.pdf.
4. Chen, Y. D., Azhari, M. Z., & Leu, J. S. (2018, April). Design and implementation of a power consumption management system for smart home over fog-cloud computing.

In *2018 3rd International* Conference on Intelligent Green Building and Smart Grid (IGBSG) (pp. 1-5). IEEE.

5. Jha, D., Rauniyar, A., Johansen, H. D., Johansen, D., Riegler, M. A., Halvorsen, P., & Bagci, U. (2022, June). Video analytics in elite soccer: A distributed computing perspective. In *2022 IEEE 12th Sensor Array and Multichannel Signal Processing Workshop (SAM)* (pp. 221-225). IEEE.
6. Awaisi, K. S., Abbas, A., Zareei, M., Khattak, H. A., Khan, M. U. S., Ali, M., ... & Shah, S. (2019). Towards a fog enabled efficient car parking architecture. *IEEE Access*, *7*, 159100-159111
7. Masip-Bruin, X., Mar´ ın-Tordera, E., Juan-Ferrer, A., Queralt, A., Jukan, A., Garcia, J., Lezzi, D., Jensen, J., Cordeiro, C., Leckey, A., et al. (2018). “mF2C: towards a coordinated management of the IoT-fog-cloud continuum”. In Proceedings of the 4th ACM MobiHoc Workshop on Experiences with the Design and Implementation of Smart Objects, 1–8.
8. Fahd Al-Mutawa, R., &Albouraey Eassa, F. (2020). A Smart Home System based on Internet of Things. *arXiv e-prints*, arXiv-2009.
9. Kanyilmaz, A., & Cetin, A. (2019, April). Fog based architecture design for IoT with private nodes: a smart home application. In *2019 7th International Istanbul Smart Grids and Cities Congress and Fair (ICSG)* (pp. 194-198). IEEE.
10. Surantha, N., Wicaksono, W.R.: Design of smart home security system using object recognition and PIR sensor. Procedia Computer Science 135, 465–472 (2018). https://doi.org/10.1016/j.procs.2018.08.198
11. He, J., Wei, J., Chen, K., Tang, Z., Zhou, Y., and Zhang, Y. (2017). “Multitier fog computing with large-scale iot data analytics for smart cities”. IEEE Internet of Things Journal, 5(2), 677–686