**INTRODUCTION:**

This is era of technology and Fog Computing is a very vast technology which is also known as Edge Computing. It is the ideal model to support those types of IoT devices which are forced by resources. Certainly, Fog Computing, which is not presume to replace the centralized Cloud but to cooperate with it. The aim of Fog Computing is to distributes the principles and technologies of Cloud Computing anywhere along the Cloud-to-Things continuity and especially at the network edge, in close proximity to the IoT devices. Instead of moving data to the cloud, it may be more efficient to move the applications and processing capabilities closer to the data produced by the IoT. Within the era of Big Data, it’s going to be disorganized to send the extraordinarily huge amount of data that swarms of IoT devices generate to the cloud. In this paper we will discuss that how Fog Computing can make better the multiple aspects in IoT applications.

**6. FOG COMPUTING AND THE INTERNET OF THINGS [6]:**

**Characterization of Fog Computing**

A high virtualized platform known as Fog Computing which provides compute, storage and networking services between Cloud Computing Data Centers and end user devices, but not specially located at the edge of network. We describe the role of Fog Computing in some scenarios which are discuss below.

**a. Connected Vehicle (CV)**

A Smart Traffic Light System illustrates the latter. This system totally interacts with a number of sensors, which detects the presence of bikers, vehicles, pedestrian bridges, zebra crossing and calculates the distance and speed of approaching vehicles. The data is collected by the Smart Traffic Light System which processed to do real-time analytics. This data is sent to the Cloud for global, long-term analytics.

**b. Wireless Sensors and Actuators Networks**

Most of the Wireless Networks involve a large number of low processing, low bandwidths, low energy, low processing power, operating system as a source of a drown, in a unidirectional fashion. TinyOS2 is a defective standard operating system. To collect environmental data, motes have proven useful in a variety of scenarios. Author stress that emergent applications demands higher bandwidth and collaborative sensing environment. Collaborative Adaptive Sensing of the Atmosphere (CASA) project, a multi-year and multi-partner initiative led by UMASS, deployed a network which is composed of small weather radars, integrated with a distributed processing and storage infrastructure in a closed-loop system to monitor the lower air for atmospheric hazards like tornados, hailstorms, etc.

**7. ISSUES AND CHALLENGES [7]**

**a. Scenarios of Mobile IoT In A Fog Environment**

In this era of technology, very large number of mobile devices connected to all over the world. It is increasing every day at an unprecedented rate. According to this research there were 7.6 billion global mobile devices in 2015, 8.0 billion in 2016 and our prediction says that it will reach up to 11.6 billion by 2021. Our ambition is to focus on a specific subset of mobile devices which are the IoT ones.

Mobile IoT is ever increasing phenomenon and are definitely impressive. This research report says that smart phones and wearable devices, which are probably the best- and well-known example of mobile IoT devices. In 2016, there were 325 million devices all over the world and according to our prediction and expectations it will become up to 929 million by 2021. This amount of increasing in mobile IoT devices may take advantage of Fog Computing to enable services that can completely improve people’s lives. Now we discus some scenarios where there is a combination of IoT and Fog Computing, and in which mobility support is necessary.

**b. Citizen's healthcare:**

All the devices are connected to the patient’s smartphone wirelessly, which always runs the frontend application component. The backend component is deployed at the Fog layer instead. It receives the data and perform initiative computations to extract important information from them and determine the actions to be performed. In hurry situation these actions are dynamic is of most important and can make the difference between life and death. The Fog application component is emigrated to the patient’s smartphone, when she crossed the town. Finally, when the patient reaches the hospital, the Fog service is emigrated to a Fog node which is installed in a nearby cellular base station.

**c. Drones for smart urban surveillance:**

The Unnamed Aerial Vehicles (UAVs) namely Drones, can be hired in plenty of situations and it is very dangerous in some cases especially for humans (for e.g. searching for a missing person, for some disaster and some emergency management). While drones don’t have a pilot on board and are very cheap as compare to aircrafts. Many companies are investing much amount in drones. Hence the market for them is expected to reach up to $21.23 billion by 2022. Now adays, drones have been remotely controlled by humans.

But in upcoming generation of drones, they will be going to be completely autonomous, which means that they are able to operate without any control by human or without any human intervention. All types of processing required to analyze the collected data and information and make decisions which may be actually performed onboard, but this would become a negative affect at the drone battery life and all over the duration of flight. These computations are extremely resource intensive. They are also usually use for video streams. They have some sensors which sense the human interaction while the actions to be performed are the drone and camera control.

**d. Problem Description:**

As we discus in this paper, the problem is to provide mobility support in a Fog-IoT environment which means to save the Fog Computing merits and also when the mobile IoT nodes move away from Fog application component. As above mentioned, advantages are all made possible by Fog to end devices, what to do for moving Fog application component from one node to another, keep it close it is enough to the related mobile IoT nodes. Actually, when the Fog service is stateless, there is no need to move it from one node to another, as there is no state o be maintained. Thus, the Fog service can be instantiated on the target Fog node and the related mobile nodes be redirected to it. At a first look, the Fog component topologically close to the related IoT nodes might seem such a hard job.

Actually, the problem is the migration of Fog service which can be defined as the issue of decisive Where, When and How to move the service in order to obtain the aim and compromising among all the factors under the consideration. As for where to move, it would be ideal and deploy the Fog component to the Fog node which is topologically closest to the mobile IoT devices.

**8. Vehicular Fog Computing [8]**

**a. System Architecture**

The system architecture of vehicular Fog Computing is presented in Fig.1, which contain three types of entities, which are Smart Vehicles, Roadside units or fog nodes and Cloud Servers. Smart Vehicles as the data generation layer, Roadside units or fog nodes as the Fog layer, and cloud servers as the Cloud layer.

City-level decision

Fog layer

Data generation layer

Cloud Layer

Area-level decision

Data exploitation and analysis

Data fusion and Pre-processing

Data gathering and Pre-processing

Vehicle-level decision

Cloud servers

Roadside units/ fog nodes

Smart Vehicles

Figure 1. Architecture of vehicular fog computing.

**b. Cloud Servers**

Those servers which provide city-level monitoring and centralized control from a distant location are known as Cloud Servers. These servers will get the data uploaded by the fog nodes while performing computationally intensive analytics to make optimal decisions from a holistic perspective (e.g., city-level decision).

**c. Smart Vehicles**

In Vehicular Fog Computing system, Smart vehicles play an important role as the key data generator, due to their real-time computing, sensing (e.g., radars, cameras and GPS), communication, and storage capabilities. The amount of data collected by the various sensors in a smart vehicle has been estimated to be around 25 GB/h in a single day (e.g., 20–60 MB/s for cameras, 10 kB/s for radar, and 50 kB/s for GPS). Some of these data can be processed by the smart vehicle itself, in order to inform real time decision making (i.e., vehicle-level decision).

**d. Roadside Units/Fog Nodes**

Roadside units, generally deployed in different areas of a city, can easily be upgraded to act as fog nodes. This will allow the collection of data sent by smart vehicles, processing of the collected data, and reporting of the (processed) data to the cloud servers. These units/nodes also act as the middleware/intermediate devices on the function of a connecting link between the cloud servers and the smart vehicles in a vehicular fog computing system. Vehicular networks will have more functions and provide more distinct services for smart vehicles, such as video streaming, navigation, and smart traffic lights.

|  |  |  |
| --- | --- | --- |
| Application Type | Service | Description |
| Traffic Control | Smart navigation | Plan optimal routes for smart vehicles |
| Smart traffic lights | Schedule traffic lights of each intersection in the city to control traffic flows |
| Driving Safety | Road condition detection | Detect environment information of smart vehicles and make adjustments accordingly |
| Emergency warning | Broadcast emergency warning information to nearby smart vehicles, such as car accidents and work zones |
| Entertainment | Commercial advertisement | Publish advertisements of public interest (e.g., Amber alerts) to nearby smart vehicles |
| Multimedia | Provide multimedia services for smart vehicles, such as music and video |

Table 1. Application examples of vehicular fog computing.

**e. A Fog-Assisted Traffic Control System**

A fog-assisted traffic management system is designed to deliver benefits such as reducing road traffic congestion and car accidents. A typical implementation will consist of two subsystems: one responsible for the local area and one responsible for the global area.

**f.** **Security and Forensic Challenges in Vehicular Fog Computing**

Our Existing security researches mainly target on the identification of potential attacks, threats, and hazards of fog-assisted vehicular applications.  A passive attack does not destroy the functionality of a vehicular fog computing system but attempts to disclose private information. An active attack is an attempt to deliberately disrupt the operations of a vehicular fog computing system.

**9.** **FOG COMPUTING: TOWARDS MINIMIZING DELAY IN THE INTERNET OF THINGS [9]**

Fig. 1 illustrates a general framework for an IoT-fog-cloud architecture that is considered in this work. There are three layers in this architecture: things layer, where the “things” and end-users are located, fog layer, where fog nodes are placed, and cloud layer, where distributed cloud servers are located. A cloud server contains several processing units, such as a server with multiple processing cores or a rack of physical servers.

In each layer, these nodes are divided into domains where a single application of IoT and Fog-Cloud is implemented. For example, in fig 1; a domain of IoT nodes is shown in dark green, and they communicate with a domain of fog nodes associated with the application. A domain of IoT nodes could comprise things in a smart home, temperature sensors in a factory, or soil humidity sensors in a farm where all the things in the vicinity are considered to be in a single domain. Normally in one domain these fog nodes are placed in close proximity to each other, for example, in a single zip-code. Each domain of fog nodes is combine with a set of cloud servers for a single application. The given below diagram explains the basic way in which IoT nodes, fog nodes, and cloud nodes operate and interact is as follows. Cloud nodes process requests and send the response back to the IoT nodes.

4

4

3

2

1

Distributed Cloud layer (core)

Cloud

Cloud Domain 1

Aggregation

4

Fog Layer (Edge)

Fog

Fog Domain 2

Fog Domain 1

Server Rack

Things Layer

Fog Node

Generated Data by Things

Server Rack

Fig. 1. General framework for IoT-fog-cloud architecture. Each layer is partitioned into domains where a single application is implemented

**10. FOG COMPUTING FOR THE INTERNET OF THINGS: SECURITY AND PRIVACY ISSUES [10]**

**Security and Privacy Challenges in IoT**

IoT plays a central role in this era of technology, and it gives services more effectively and efficiently to end users. It has also facing many security and privacy problems and compose them. We summarize all the major security and privacy challenges in IoT environments.

**a. Authentication**

These resource-constrained devices can outsource expensive computations and storage to a fog device which will execute this protocol. This model is based on public-key infrastructure using multicast authentication for secure communications.

**b. Trust**

“Trust” models which are totally based on reputation which have been successfully deployed in many scenarios like online social networks. Kai Hwang and colleagues proposed such a new point of view to improve the trust in clouds, which combines security-reinforced data centers, data access, and virtual clusters directed by reputation systems. To design a trust model based on reputation in the IoT, we need to deal with that how to maintain the service reliability and prevent accidental failures, identify misbehavior issues.

**c. Privacy**

The Big issue of privacy leakage of user information and data in IoT environments such as the data, location and usage are attracting the attention of research community. The second privacy issue is the location privacy that can be used to infer the IoT device’s location. The third privacy issue is the protection of a user’s usage pattern of some generated data by IoT devices, such as smart grids, healthcare systems, and vehicle ad hoc networks. IoT devices limit the techniques that can be used to deliver efficient and effective privacy-preserving schemes.

**REFRENCES:**

[6]Bonomi, Flavio, Rodolfo Milito, Jiang Zhu, and Sateesh 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*, pp. 13-16. 2012.

[7] Puliafito, Carlo, Enzo Mingozzi, and Giuseppe Anastasi. "Fog computing for the internet of mobile things: issues and challenges." In *2017 IEEE International Conference on Smart Computing (SMARTCOMP)*, pp. 1-6. IEEE, 2017.

[8] Huang, Cheng, Rongxing Lu, and Kim-Kwang Raymond Choo. "Vehicular fog computing: architecture, use case, and security and forensic challenges." *IEEE Communications Magazine* 55, no. 11 (2017): 105-111.

[9] Yousefpour, Ashkan, Genya Ishigaki, and Jason P. Jue. "Fog computing: Towards minimizing delay in the internet of things." In *2017 IEEE international conference on edge computing (EDGE)*, pp. 17-24. IEEE, 2017.

[10] Alrawais, Arwa, Abdulrahman Alhothaily, Chunqiang Hu, and Xiuzhen Cheng. "Fog computing for the internet of things: Security and privacy issues." *IEEE Internet Computing* 21, no. 2 (2017): 34-42.