2019 IEEE 43rd Annual Computer Software and Applications Conference (COMPSAC)

Hybrid approach for enabling hierarchical Fog Networks in an IoT deployment

Nuwan Jayawardene
Department of Computer Science
Informatics Institute of Technology
Colombo, Sri Lanka
nsgaj12@gmail.com

Pumudu Fernando
Department of Computer Science
Informatics Institute of Technology
Colombo, Sri Lanka
pumudu.f@iit.ac.lk

***Abstract*— More and more "Smart Devices" are coming online every year. These Smart Devices have the ability to communicate with other Smart Devices across the web, exchange information and make intelligent decisions. This influx of new devices and connections has caused the central servers that manage those Smart Devices to come under heavy load. Measures to combat this have inadvertently resulted in increased network complexity. This paper considers a use-case where such complexity might arise and points out why addressing that complexity is necessary. The paper also considers existing IoT products and how network complexity is handled in them. The paper concludes by proposing a hybrid approach that would enable a central server to understand complex IoT networks especially ones with devices arranged in a hierarchical manner. It should be noted that this research is still ongoing and under development.**

Keywords—Fog Networks, Edge Computing, Edge Gateways, Smart City

I. INTRODUCTION

Before the advent of the Technological Revolution, household items simply performed the tasks they were built for. They were known as "dumb" things. Then a concept known as the "Internet of Things" (IoT) came along which made it possible for any end user device to have Internet connectivity. This allowed devices to connect to other devices and services for extended functionality [1].

In traditional IoT architectures, all data generated from connected devices are sent to a central server for storage and further analysis [2]. With added complexity brought on from new devices that are connecting to the network, additional load has been applied on the central servers orchestrating the communication between those devices. A new concept known as "Edge Computing" aims to combat this. It refers to the computational logic that is done close to or at the source of the generated data to alleviate the need for all data gathered to be sent to the central cloud [3].

The best way to understand how Edge Computing and the central cloud servers work in tandem is to study a Smart City scenario [4]. When taken in the urban context there are several instances where authorities have decided to use connected devices to observe the state of public services. Some of the notable situations among those being; Building Monitoring, Waste Management, Smart Parking and Autonomous Driving [5]. In the case of Building Monitoring, Smart Parking and Autonomous Driving there can be instances where these services function simultaneously to provide better value to residents. For example; an autonomous car can be instructed to travel to an apartment complex with a building monitoring service. Upon arrival the car would connect to the apartment building's central monitoring service wirelessly. This monitoring service could be paired with others as in the case of several apartment complexes in close vicinity, each with their own monitoring system. Finally, all the apartment complexes can be monitored and maintained through a central server located offsite.

This Smart City example shows that there can be real-world instances where multiple layers of devices (arranged in a sort of multi-level-hierarchy) come together to form a complex Fog enabled IoT Network [6]. Typically, Fog enabled IoT Networks are formed by Fog Nodes [7], small pockets of "mini-networks" comprising of a main Edge Gateway to which child Edge Devices would be connected. In this instance, a Fog Node would be formed between a single apartment building's central monitoring service and the connected series of autonomous cars.

Good governance within a complex system is maintained by trust among its participants [8]. If not for this, participants would refrain from participating in the system, making the system a failure. This applies for IoT Networks as well [8]. In any IoT Network this governance is upheld by several fundamental characteristics [9]. Those characteristics include; Dynamic nature, Heterogeneity, Safety, Connectivity etc. These characteristics combine together to create several crucial umbrella factors such as;

- Security – The security risk of a network goes up significantly with the increase in the number of devices and in turn, the network complexity [10].
- Analytics – Knowledge of the devices within a network gives context to the type of data being transferred. This further aids in functions such as Edge analytics [2].
- Diagnostics – Device actions within a network provide insight into what each of their functions are. Device Management services are used in such instances [11].

It is by adhering to these factors that good governance within an IoT Network and by extension, its longevity is

978-1-7281-2607-4/19/$31.00 ©2019 IEEE
DOI 10.1109/COMPSAC.2019.10258