Adhishwar Singh Mittal (19300379) – CS7NS1 (Data Science Strand)

Paper 1: "Mobile Edge Computing: A Survey"

DOI: "*10.1109/JIOT.2017.2750180*"

Contributions

- Presented MEC as an edge computing paradigm and highlighted focused areas of research and challenges
- Explained advantages and concerns in terms of latency, security and implementation ability
- Explained the working of MEC architecture with correlation to communication networks and cloud, and explained different configurations such as indoor, outdoor etc.
- Explained related concepts such as cloudlets, MCC and highlighted key applications such as AR and content delivery caching

Technological Insights

- Continuous connection between MEC and smart healthcare device can be used for real time mitigation of health risks
- Video analytics can be used to control traffic or control crime using face recognition through surveillance cameras
- Data from end users can be efficiently analysed by MEC which can pass only higher context information to the cloud to save communication cost and reduce lag
- There are testbeds used by created by companies such as Nokia and China mobile to test out the latest advancement in this research field

Insights on Edge/Fog Scalability

- For successful working of MEC we need to safeguard network, virtualization, computation and MEC servers using encryption techniques, dummy signals etc.
- Pricing strategy for these services need to be dynamic as it depends on a lot of components and their respective uses
- The architecture of edge computing entails entry of a lot of 3rd party service providers which has a lot of advantages but needs to carefully moderated to prevent security breaches
- MEC offers low coverage but low latency and high computation with independent powerful resources which can re-route requests and make systems robust

Paper 2: "Securing Fog Computing for Internet of Things Applications: Challenges and Solutions"

DOI: "*10.1109/COMST.2017.2762345*"

Contributions

- Reviews the features of fog computing and its architecture, along-with its role in providing services in real-time, dissemination of data, decentralized computing and transient storage
- Lists down all possible threats with respect to security and privacy of IOT devices being used in fog computing
- Reviews current solutions which are state-of-the-art in addressing and resolving security and privacy concerns in IOT applications using fog computing
- Attempts at directing future research by defining several issues which are still open

Scalability Aspects

- "Fog as a Service (FaaS)" can be the novel direction in which service providers can build up a system to cater to vertical markets by building an array of fog nodes
- In users with high-speed going across fog nodes, authentication schemes need to be designed efficiently and shared among multiple fog nodes so that user identity can verified securely.
- New devices owned by a user should be able to access the services being offered by fog network without configuration, hence dynamic device management needs to be taken care of
- With help of IOT devices close to users, smart infrastructure management, hierarchical data analytics and similar applications can be provided using fog computing methods

Technology insights

- As compared to cloud computing, fog computing is more secure because it stores data locally and it does not share data with cloud in real-time
- Along with the decrease in data traffic to the cloud of up to 90% edge computing can reduce the response time by ~20% as compared to traditional device to cloud networks
- Fog computing facilitates transient data storage, which allows users to sustain frequently accessed data and flexibly update their data in a fast manner
- Fog nodes can optimally work towards deduplication of data from IOT devices and at the same time efficiently distribute content to the IOT devices