EAI Endorsed Transactions
on Internet of Things
Research Article EAI.EU

IoT enabled Smart Fog Computing for Vehicular Traffic Control

Akashdeep Bhardwaj[1,*], Sam Goundar[2]

[1]University of Petroleum and Energy Studies, Dehradun, India
[2]The University of South Pacific, Suva, Fiji

Abstract

INTRODUCTION: Internet was initially designed to connect web sites and portals with data packets flowing over the networks for communications at corporate levels. Over time, live video streaming, real-time data and voice is being offered over hosted Clouds for business entertainment. Enterprise applications like Office 365, banking and e-commerce are available over smartphones. With the advent of Fog Computing and Internet of Things, corporate enterprises and non-IT industries see potential in this technology. Billions of Internet-enabled devices, globally distributed nodes, embedded sensor gateways transmit real-time generated over the internet to the cloud data centres. Cloud environments are not designed to handle this level of data that is being generated and Computing limits are being severely tested. Fog Computing has the potential to be the go-to option for Cloud service delivery.

OBJECTIVES: This paper reviewed existing research works and presents unique Smart Fog Computing based taxonomy. The authors also implemented experimental setup for Smart Cities using Smart Fog Computing for controlling Vehicular traffic.

METHODS: Smart Vehicular Management is viable use case for Fog and IoT technology. The authors designed and implemented two experimental setups. The first setup involves standard Cloud implementation and the second setup employs Fog Computing implemented using IoT Sensor nodes to compare the performance of the Vehicle Management Fog application regarding the Response time and Bandwidth Consumed. The architecture and implementation involved deploying 50 IoT sensors nodes across the university areas and routes.

RESULTS: The main results obtained in this paper are the following. As compared to Cloud computing, on deploying Fog Computing and IoT devices:

- End-to-End Processing time dropped from 29.44 to 6.7 seconds → almost 77% less
- Number of hops traversed reduced from 56 to 4 hops → almost 92% less
- Bandwidth usage dropped from 247 to 8 kbps → almost 96.7% less

CONCLUSION: From the experimental setups as compared to Cloud computing, the Fog and IoT processes the traffic data locally on the edge devices, which reduces the end-to-end time.

Keywords: Fog Computing, Edge Computing, Internet of Things, Fog Security, Cloudlets, IoT

Received on 21 November 2019, accepted on 03 December 2019, published on 12 December 2019

doi: 10.4108/_____

1. Introduction

By 2020, India is expected to have 1.9 billion IoT devices as per forecasts by Deloitte and Gartner (2018) has forecasted 21 billion IoT devices globally. Global Market Insights (2018) has forecasted that IoT will surpass a global share of US$ 700 million by 2024. This explosive,

*Corresponding author. Email:Bhrdwh@yahoo.com

impressive, unprecedented growth is unsustainable using the existing cloud approach and requires a unique Computing model, which can processes the data efficiently and effectively without delivery or security concerns. Internet of Things (IoT) based applications are generating never-before-seen volumes and variety of privacy-sensitive data from billions of end users devices. This has led to an alarming situation with concerns ranging from geographically displaced locations, high burst rates, and low latency speeds. The next generation of cloud paradigm is expected to be more energy-efficient and deliver quick services to meet the dynamic end-user expectations. Internet of Things (IoT), Web of Things (WoT) and Internet of Everything (IoE) are starting to connect everyday devices and objects to cloud-hosted service applications. Increasing data centres only cause raise in the delivery costs as well as the carbon footprints, which affects the sustainability of Cloud and Smart Fog delivery services. Cisco (2015) coined the term Fog Computing for Edge Computing.

Fog Computing technology is an emerging paradigm in IoT. As Fog nodes and IoT devices produce data logs and WoT and IoE gets every object online, centralized data processing would not be able to scale up and match the requirements of such Fog environments. Fog Computing is the proposed option by industry and research communities to address the above issues. Fog uses the network sensors of end user physical devices for collecting data and remote monitoring. This technology has gained massive traction in various spheres like healthcare, manufacturing, retail, banking, consumer goods and communication applications. Globally corporates are desperately seeking possible solutions for efficient applications to run on IoT and Fog technologies. Smart Fog Computing bridges the business gap between Cloud and IoT devices by enabling Computing, application connectivity, networking, storage, decision-making, data processing and management within close proximity of the IoT device generating the data. Other similar Computing paradigms to Smart Fog Computing like Edge Computing, Cloud of Things, Mist Computing or Cloudlets have also been proposed to address similar issues.

Traditional Cloud architectures are unable to satisfy the above-mentioned Fog Computing requirements. Existing solutions require sending data from the IoT node at the network edge to the data centre for processing. This adds latency as data streams sent from multiple IoT devices consumes the bandwidth capacity and cause service delivery issues. This is why Smart Fog Computing has emerged as the solution for IoT, Cloud Computing is extended to the edge of the network, and helps decrease the latency and network congestion. By reducing, the data volume transmitted over the Internet, the delivery and security risks can be minimized. OpenFog Consortium (2016) is involved in promoting an open architecture standard for Fog Computing. This design proposes a swarm of computational clients and edge nodes in hierarchically distributed, multi-layered Fog clusters. Each cluster processes data from a specific geographical segment of the device farm, higher-layer Fog clusters collate, and process data filtered from lower layers. These layers actually perform separate logical functions such as monitoring, storage, control, local operations and business decision processes. This system level architecture extends the Computing, storage and network to the network edge. This involves use of intelligent edge devices instead of data being sent across the Internet to Cloud data centres. This accelerates decision-making and represents a shift from traditional architecture using Internet having reliance on Cloud-based applications. To be successfully, Fog Computing architecture needs to have the below mentioned essential features.

Low Latency: Any delay caused during data transfer to the cloud data centre, data processing and then back to the application can seriously affect the performance. Applications for Health monitoring, Emergency response or Real-time production floor shutdowns or electrical service restorations in manufacturing industry require minimum latency as even milliseconds.

Conserve Bandwidth: Big data, predictive analytics and data mining require huge Computing and storage resources, which are mostly provided on the Cloud. Reduce false positives and noise for logs generated by IoT devices and real-time systems like offshore oilrigs, which can generate 500 GB of data in a week, or Boeing jets, which generate 10 TB data in just 30 minutes of flight time. It is impractical to send this amount of data from several hundreds of thousands of edge devices and nodes to the cloud.

Address Data Security: IoT data generated needs to be secure, privacy and compliant during transit and at rest. Cyber security threats like Denial of Service attacks, sniffers or man-in-the-middle attacks are major issues on the unsecured internet. Data privacy is highly regulated and legalized. Industry regulations in certain countries having laws like General Data Protection Regulation, Canada's Personal Information and Electronic Document Act or USA's Federal Information Security Management Act 2002, which forbid offsite data storage, collection or disclosure for commercial use.

Standardize Communications: Cloud devices communicate over TCP/IP Protocol using IP addressing while data transfer in IoT nodes and devices happens using 3/4G, GSM, and 6LoWPAN, Bluetooth, Wireless, ZWave or even BigZee.

Data processing location: The ability to analyse data collected close to the device node can often be the critical factor when avoiding disaster or cascading failures. IoT devices and Fog nodes, which collect data, are usually spread across a large geographic region with diverse harsh climatic conditions, so require rugged IoT devices.

Cloud Computing providers provide scalable, hosted enterprise applications over the Internet. Smart Fog Computing technology owes its explosive growth to IoT by localizing physical Computing, network and storage along

with analytics and machine learning. Cloud service providers like Amazon, Google, Amazon, IBM, Microsoft, have enabled Cloud based deliver models for SaaS, PaaS and IaaS to handle the Fog data demand and delivery. Taking the concept of Fog Computing into account, several paradigms have already been introduced in computation technology domain.

Mobile Edge Computing (MEC) and Mobile Cloud Computing (MCC) are two emerging technologies as the key enablers for 5G Mobile networks. These are regarded as the closest possible extensions for Cloud and Edge Computing capabilities. Due to the recent rise in use smart phones devices, end users deploy and run applications at the edge of the network on their handheld devices instead of using traditional Internet and Cloud data centres. Data logs are generated on the handheld devices, which often have constraints regarding computational, energy and storage or network resources. Thus, more often than not, the data processing is executed and process application data outside the mobile devices compared to execute those applications locally. MCC supports remote execution by providing necessary computational resources for the mobile applications on end user handheld devices. Therefore, the MCCC design involves Mobiles → Radio Access Network → Authorized 3rd Party applications. Use case examples include IoT applications, Video surveillance, Geolocation services, Augmented Reality, Local content distribution and Data Caching. Main feature focus for MCC are to extend the remote processing and multi tenancy capabilities to provide diverse application services, overcome mobile resource constraints and extend the battery lifetime.

Another Fog Computing alternative is the use of Cloudlets. These comprise of lightweight agents in middleware of three-tier hierarchy involving Mobile device → Cloudlet → Cloud. Cloudlets are deployed for exclusive self-management, possesses enough compute power, low end-to-end latency and builds on standard Cloud technology. Cloudlets are different from Fog Computing technology as the application virtualization is not suitable for such environments, since it consumes more resources and is energy intensive and cannot work in offline mode.

Yet another alternative is the use of Micro Data Centres. These are small yet fully functional hosting centres containing virtual machines and servers capable of providing dynamic provisioning and Computing services. Micro data centres can help Fog and other technologies by being local to the data source, reduce latency, enhances availability and service reliability. They can also be designed to be portable with built-in security protocols. These centres can help saves bandwidth consumption by data compression, local processing and analytics as well as accommodate new services applications in multi tenancy environments.

As an example, Fog environment in Smart Cities consist of distributed locations, heterogeneous networks with loosely connected IoT nodes and devices. This involves data collection, optimization and processing from IoT devices. The data is either Big Streams (data captured from IoT nodes) or Big Data (persistent data stored with decision-making archived on cloud storage). This further includes detecting real-time patterns and predictive analysis for smart and quick decision-making. This can enable real-time analysis of city infrastructure life and may well open new options for governance. Currently, data is aggregated from IoT networks, which consists of smart IoT nodes and devices. This data is sent over Internet to Cloud servers for storage and processing. Highly scalable Cloud data centres offer infrastructure and compute applications for Big Data Processing. However, when processing of large magnitude of data volume is required due to on-demand scalability and distributed across multiple locations with low latency, Cloud data processing fails to meet the IoT delivery requirements.

2. Literature Survey

For this research, the authors identified 282 research papers published from 2013 until date on Fog Computing and IoT, after a four stage selection process shortlisted 139 relevant publication works as illustrated in Figure 1 below.

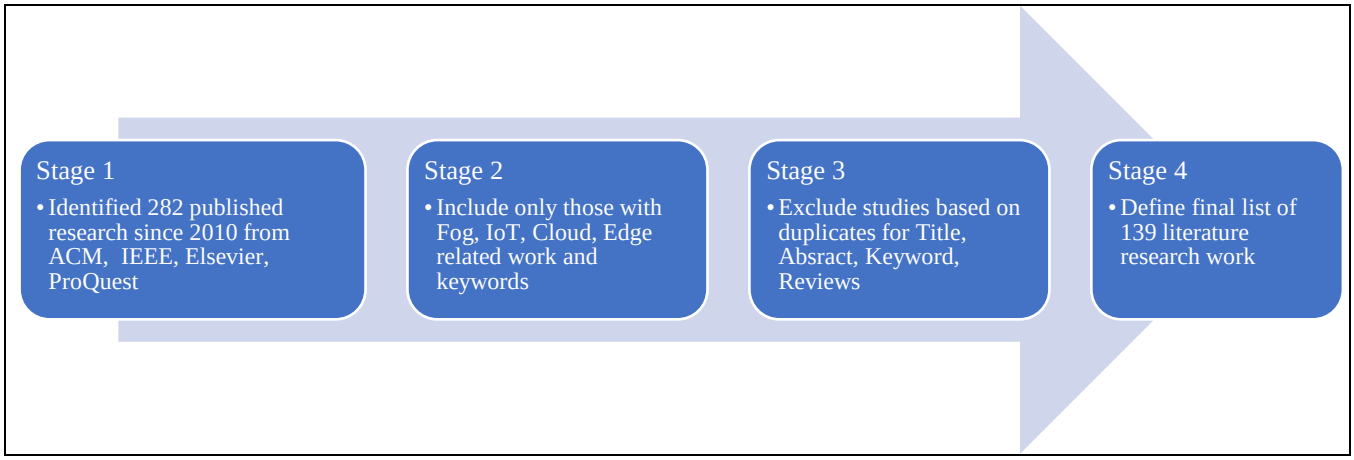

Figure 1: Four Stage Selection Criteria

Table 1 below describes the overall spread of the research papers and the subcategories that were selected. The latest reviews are presented in the section below.

Table 1: Fog Computing Literature Findings

Fog Classification	Stage 1	Stage 2	Stage 3	Stage 4	Final Review	Breakup %
Security Aspect	102	97	63	54	45	32.37%
Design Architecture	54	50	44	35	27	19.42%
Data & Capacity Control	32	28	27	25	24	17.27%
Node Management	43	40	39	32	21	15.11%
Energy Management	51	42	35	26	22	15.83%
	282	**257**	**208**	**172**	**139**	

Naha et al. (2018) presented Fog and Cloud Computing trends along with their technical differences. The authors investigated Fog Computing architectures and components in detail. This involved defining the role of each component. Fog Computing Taxonomy was also proposed in this paper as well as discussion on existing research papers and their limitations was presented. The authors also reviewed open issues and gaps about Fault Tolerance, Resource Scheduling and Allocation, Simulation of tools and Fog based micro services.

Yeow et al. (2017) proposed a thematic taxonomy about key characteristic features related to the current decentralized consensus systems. The author analyzed the common and variants features using the criteria from their literature survey. Several open issues based on decentralized consensus for edge-centric IoT and centralization risk and deficiencies in block chains were also proposed.

Anderson et al. (2017) proposed mobile cloud Computing options to enable urban renewal approach for Real Time Car Parking system (RTCPS). Unique concept of utilizing MCC and Vehicle networking (VN) has given rise to Integrated Communication Computing Platforms (ICCP). These platforms address traffic related challenges like improper parking and traffic congestion in parking lots and safety applications for vehicles. Another unique service provided is the Infrastructure-to-Vehicle (I2V) services. This provided data dissemination and content delivery services to connected Vehicular Clients (VCs). Open challenges and future research directions are discussed for an efficient VCC model, which runs on networked Fog centers using a prototype.

Wang et al. (2017) proposed a novel Fog Computing framework that utilized middleware for communicating with the information centric network and global points where data is collected, preprocessed and classed in Fog node before transmission. The advantage is reduced number of caching content in network by labeling the dynamic data and user-shareable data as well as enabling users to retrieve data from nearby nodes instead of remote servers. The authors proved that in traditional networks with limited content storage capacity, in-network caching could not be successful. The results proved the necessity of proposed framework.

Gonzalez et al. (2017) provided a wide-ranging survey of references from the academia to the Fog industry. The authors analyzed the terminology, dimensions of

performance, security and governance. A detailed analysis of Fog, Cloud and the concept of pushing data and applications to the edge of the network is presented and the future of edge Computing is discussed in detail.

Tocze et al. (2017) described the Edge Computing paradigm, architecture and the terminology associated. The authors reviewed works, elaborated specifically on taxonomy for management of edge resources, and identified the research challenges in this area.

Initial Internet architectures were based on simple standard design for communication over WAN circuits. As Voice and Data become digital, the complexity grew. With the advent of Fog, Edge and IoT, the designs become more multilayered and multifaceted. This brought about further design challenges. Aijaz et al. (2017) acknowledged that this is still in infancy stage, the authors reviewed the most complex design challenges and proposed solutions for transmit touch and actuation in real-time.

As Fog Security has now become a critical concern for IoT, Fog, 5G, AI, Tactile Internet and VR, there is an urgent need to have common industry standards for interoperability, guideline and framework for ensuring basic interoperability and security protection. OpenFog Reference Architecture for Fog Computing (2017) is the IEEE recommended baseline document to establish an open, interoperable architecture, specify APIs. The OpenFog technical community is now working on a suite of follow-on specifications, testbeds and new use cases to enable component-level interoperability. This will eventually lead to certification of industry elements and systems, based on compliance to the OpenFog Reference Architecture.

Chiang et al. (2017) discussed four specific dissimilarities between Fog and Edge technologies. As per the authors, firstly Fog is includes the Cloud Core, Edge, Metro, End Clients, and Device Things. Fog architecture helps enabling resource pooling, management, and resource security and distributed Cloud functions for supporting end-to-end services and Fog applications. Secondly, instead of handling the devices at the network edge inform of isolated Computing platforms, Fog seamlessly utilizes the Computing services from the Cloud to the edge devices. Thirdly, Fog envisions a horizontal platform that will support the common Fog Computing functions for multiple industries and application domains, including but not limited to traditional telco services. Fourthly, a major part of the edge is mobile, while the Fog Computing architecture is flexible enough to work over wireline and wireless networks.

Cloud Computing based wireless networking system utilizes unified resource pooling for improving operational efficiency. Fog based radio networking system places processing units in the network edge for reducing latency. Converging Fog and Cloud design paradigms in wireless access network can enhance support of diverse applications. Ku et al. (2017) described the recent advances in Fog radio access network research, Hybrid Fog-Cloud architecture and issues related to system designs.

Elmorth et al. (2017) illustrated the Fog Computing conceptual approach for processing data by use of virtualization, Orchestration, Networking, and Storage resources. The authors discussed opportunities, and challenges in the Fog Computing domain, offering field solutions. However, the technology is still in the initial stages and only the future can reveal which designs, solutions, proposals or applications will prove most beneficial to the society and industry.

With increase in use of new Fog applications and capabilities, cloud usage has moved closer to the end users. Chiang et al. (2017) focused on unique opportunities presented to university researchers and the industry by Fog, Internet and Networks. The authors presented overview of articles that covered the growing domain in Fog Computing and its taxonomy.

Mach et al. (2017) discussed Technological evolution, reference scenarios and use cases where mobile edge Computing is applicable. The authors surveyed existing functionalities and concepts, which integrate mobile networks and edge Computing. The survey focused on user-oriented use case in the mobile edge computation offloading. The research presented taxonomy and concentrated on three key areas – Computation offloading decisions, Computing resource allocations and Mobility management.

Mobile Edge Computing Platform Application Enablement (2017) document focused on mobile edge applications and mobile edge platform reference points. This standardizes the edge applications for interacting with mobile edge system. This includes Service related functionality, which includes registration, event notifications and discovery. Other features include traffic rules, application availability, DNS, and the time of day. The document also described the information flows, necessary operations, data model and API definitions.

Mobile Edge Computing Radio Information API (2017) document focused on Radio Network mobile-edge services. This document describes the message flows, RESTful API with the data model and the required information.

Taleb et al. (2017) presented a survey on mobile edge Computing and focuses on the fundamental key enabling technologies. This described the orchestration considering both individual services and a network of platforms supporting mobility and edge Computing, bringing light into the different orchestration deployment scenarios. The authors focused on multitenancy support for application developers, content providers, and third parties. The authors also overviewed current standardization activities and elaborated on open research challenges.

Kapsalis et al. (2017) proposed a unique Fog architecture and taxonomy. This adopted a cooperative model allowing a federation of Edge networks instead of the traditional hierarchical and centralized Fog models. Here the tasks, which the Fog nodes are required to complete were characterized according to their computational nature and are subsequently allocated to the appropriate Fog, host. The

results displayed faster real-time processing of time-sensitive data.

The interconnection of cloud and Fog infrastructures as part of different geographically dispersed environments is a key issue for the development of the Fog technology. Moreno-Vozmediano et al. (2017) presented a hybrid-interconnected framework of Fog and Cloud. This framework allowed the automatic provision of cross-site virtual networks to interconnect geographically distributed cloud and Fog infrastructures. This framework provided a scalable and multi-tenant solution, and a simple and generic interface for instantiating, configuring and deploying Layer 2 and Layer 3 overlay networks across heterogeneous Fog or cloud platforms, with abstraction from the underlying cloud/Fog technologies and network virtualization technologies.

Li et al. (2017) discussed and illustrated impacts of two recently Fog Computing coding concepts – Minimum Bandwidth Codes and Minimum Latency Codes. The authors presented a unified coding framework, which included the above two coding techniques as special cases and enabled a trade-off between computation latency and communication load to optimize system performance. Several open problems and future research directions were also discussed.

As Cloud and Fog networked sensing devices are proliferating the environment, processing and storage capabilities of the edge devices has also increased. These devices now offer low energy consumption and hardware costs. Malensek et al. (2017) presented a novel framework and taxonomy, which enabled federated query evaluations between Cloud and Fog nodes seamlessly. The framework selectively sampled data from observational streams to reduce communication and memory consumption on the Fog nodes. Over a real-world observational dataset, the proposed framework demonstrated an 89% reduction in dataset size while maintaining a mean absolute error of less than 0.25%.

Gi et al. (2017) integrated Fog computation and Medical Cyber Physical systems to build a solution for resolving Quality of Service issues unstable and long-delay links between cloud data center and medical devices. Initially the authors investigated the Fog node base station association, virtual machine placement and task distribution to provide cost-efficient solutions. This was performed by using non-linear linear program and then linearize it into a mixed integer linear programming. To address the computation complexity, linear programming based two-phase heuristic algorithm was proposed. After extensive experiment results, the authors validated the high-cost efficiency of the algorithm by the fact that the proposed algorithm produced a near optimal solution and significantly outperformed the greedy algorithm.

Live video streaming over Cloud using Fog Computing has flourished recently. This involves assorted quality and video source formats. This in turn requires huge amount of computational resources, which can transcode the various quality versions and serve viewers with distinct configurations, geographical locations and resolve delay issues. In spite of these concerns, the video streams needs to be synchronized to support live community interactions, chat and feeds. He et al. (2017) addressed these challenges by presenting a unique Fog-based transcoding framework. This offloads the transcoding workload to the network edge and viewers. The authors evaluated the proposed design using Planet Lab based experiment and real-world viewer transcoding experiments.

Tang et al. (2017) reviewed cooperative video streaming models, which pool network resources effectively in different application scenarios. The authors focused on Crowdsourced mobile streaming model. This model pools users download capacities to achieve efficient utilization of network resources and reduce the impact of channel variations. Optimum issue of efficient resource allocation and the economic issue of user cooperation was also reviewed along with novel taxonomy and future challenges and open issues in cooperative video streaming models was presented.

Fog extends the Cloud Computing model to the edge of the network until the end users. This has initiated a new class of Fog based applications and services. Fog characteristics range from Mobility, Widespread geographical distribution, Predominant role of wireless access, Strong streaming and real-time applications, Low latency and location awareness, large count of nodes and Heterogeneity. Bonomi et al. (2017) presented the Fog nomenclature and argued that the above characteristics have resulted Fog to be the appropriate platform for a number of critical Internet of Things (IoT) services and applications like Smart Cities, Smart Grid, Connected Vehicle and Wireless Sensors and Actuators Networks.

3. Unique Taxonomy & Innovation

Academic literature has already been researched and published in Fog Taxonomy considering different areas. Some of them are Application, Energy Management, Thermal Aware Scheduling, Planning Implementation, Storage Design, Renewable Energy and Waste Heat Utilization for IoT and Fog Computing devices. The proposed research and taxonomy is different from existing nomenclatures in two unique ways –

First, the taxonomy does not take into account the relative performance of Fog and IoT solutions in the industry.

Second, this taxonomy does not consider standard Fog features. Common features like Node Infrastructure and Configuration, Design and Architecture, Virtualization Design, IoT node-to-node Collaboration, Integration and Management framework, Provisioning of resources and services, Service Agreement and Objectives or Cyber security issues and challenges faced at different circumstances and node levels have been previously published like Buyya et al. (2018), Dasgupta et al. (2017) and others.

Third, this research paper presents a unique idea on use of Smart Fog Computing devices as well as proposes use of Blockchain as a future option for research.

The proposed taxonomy presents Fog Computing classification based on Fog Security and Design, Node, Energy and Capacity Management as illustrated in Figure 2 below.

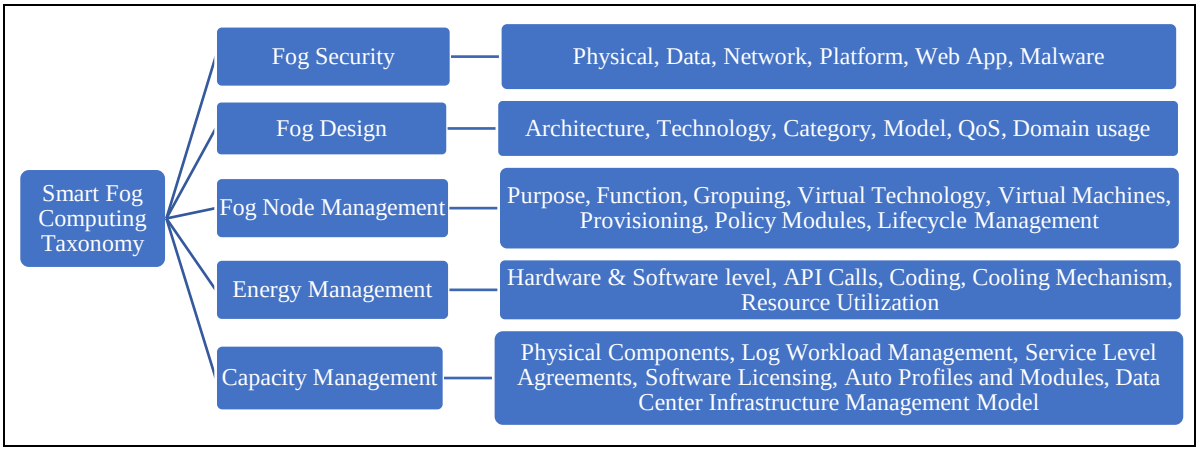

Figure 2: Proposed Taxonomy for Smart Fog Computing

The proposed Fog Computing taxonomy and examples are further described in form of the reference architecture as displayed in Figure 3 below and discussed in the section below.

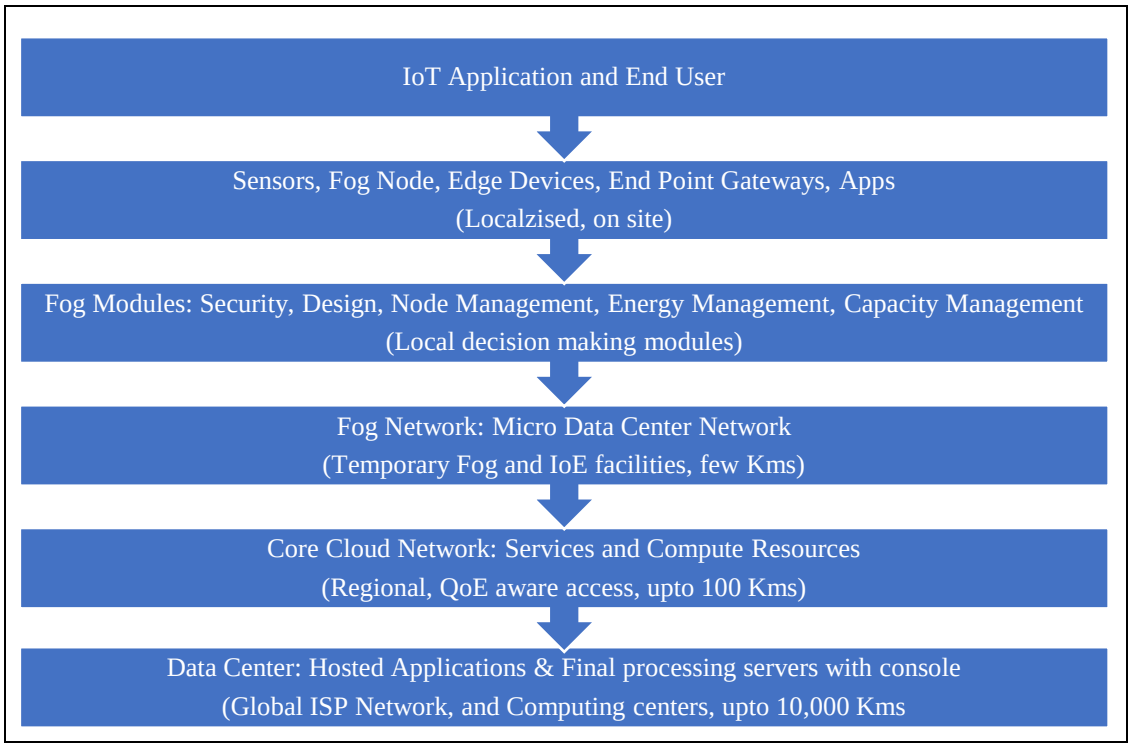

Figure 3: Proposed Reference Architecture for Smart Fog Computing

As per the proposed taxonomy, the authors recommend that the definition of Fog Computing should be redefined as "Fog Computing comprising of distributed entities of Fog nodes, which enable the deployment of Fog and IoT services comprising of at least one or more physical node and sensor device residing at the network edge with Computing, network, storage, processing and sensing capabilities".

- **Fog Security**

Fog and IoT Security breaches have become a high priority concern lately. CIA documents revealed by WikiLeaks mentioned that smart LEDs connected to Internet could secretly record conversations (Forbes Press, 2017). Smart intelligent virtual personal assistant devices can like Alexa, Google Assistant, Amazon Echo, take user input and location awareness, playing music or provide information about weather conditions or traffic and stock prices from Internet. Home gadgets like Surveillance cameras, Washing Machines, Microwave, LED TV or Mobiles are smart devices connected to Internet. These may well be inadvertently sending information from homes to hackers and cyber criminals. ISP Dyn came under DDoS attack in October 2017 (York, K. 2016) which disrupted their network operations for accessing popular websites. Cybercriminals managed to take control of large number of internet-connected cameras and DVRs and compromised the ISP DNS. Fog Security classifications are presented below.

- Physical Security: Node hardware & Chip safety, Data-at-Rest, Node Authentication
- Data Security: Data-in-Motion, Multi-Tenancy, Data ownership, Data Flow and Encryption, Access Control, Secure Key Management,
- Network Security: Insecure Wireless protocols, Sniffing, Man-in-the-Middle, Active Impersonation Message replay, Message Distortion, Illegal resource consumption
- Platform Security: Insecure APIs, Account Hijacking App Vulnerability, APTs, Malicious insiders, DDoS, Brute Force, Node & App level Vulnerabilities
- Virtual App Security: Hypervisor and Virtual Machine based attacks, No Logical Segregation, Side Channel attacks Privilege Escalation, Service Abuse, Inefficient Resource Configuration and Policies
- Web App Security: XSS (Cross Site Scripting), CSRF (Cross Site Request Forgery), Session/Account hijacking, Insecure Direct Object References, Drive-by attacks, SQL injection, Malicious redirections
- Malware Protection: Performance reduction, Infections from Bots, Ransomware, Rootkits, Virus, Worm, Trojans and Spyware

- **Fog Design**

Fog and IoT architecture with hierarchical designs in contrast to Cloud Computing are very different. Fog parallelizes data computing at the network edge instead of centralized data centre processing. This helps satisfy the location awareness, data transfer and low latency issues. This helps improve the delivery efficiency for Fog Applications. The below classification details further on the Fog design and architecture.

- Fog Architecture: Centralized, Decentralized, Distributed, Heterogeneous
- Technology: Horizontal-system, Heuristic Linear, Framework, Meta Heuristic
- Quality of Service: CPU MIPS, Throughput & Round trip, Bandwidth Consumption, Service Uptime, Data Loss, Processing Speed and Resource Utilization, Local Awareness
- Category: Academic, Research, Commercial
- Model: Simulation, Prototype, Analytical
- Domain usage: Personal Wearable, Home Domestic devices, Private and Public Sector spheres like Farming, Energy, Healthcare & Wellness, Manufacturing, Oil & Gas, Smart City, Mining, Education, Transportation

- **Fog Node Management**

This relates to end management framework for Fog nodes and sensors to enhance processing, interoperability, interaction and sharing for application resources. Fog Node Management classifications are described below.

- Purpose: reduce processing Cost, save Energy, minimize Bandwidth and Network Interference, Satisfy Service Agreements
- Function: Sensor, App Node, Base Station, Cloudlet, Server
- Grouping: Stand alone, Cluster, Client-Server, P2P
- Virtual Technology: VMware, Zen, Azure, Google, KVM
- Virtual Machine: Pre/Posy Copy for Migration, Shared/Dedicated Storage, Compression or Write Throttling
- Provisioning: Interoperability, Scalability, Configuration, Detection, Reliability, Deployment
- Policy Modules: Decision Engine, Multi Tenancy Application Administrator, Conflict Resolver, Repository Holder, Policy Enforcer
- Lifecycle Assessment: Activity monitoring, Update & Patching, Provisioning, Deployment & Version Control, Audit, Regulatory Compliance, Location Awareness and Secure Node Comm./De-Commissioning

- **Energy Management**

Energy management for smart sustainable Fog Computing is a critical component for Fog and Cloud service providers. By improving energy utilization, service provider reduces electricity and operational costs. This aspect involves optimizing environment at hardware component and application software system level as explained below.

- Hardware level: use of energy efficient transistors, logical gates, clock frequency, voltage components
- Software level: Optimize memory allocation Registers, Buffers, Kernel, Reduce CPU intensive cycles

- API Calls: Avoid high energy consuming calls Activity.FindViewByID, Broadcast.Receiver, Location.API
- Coding level: Efficient Energy Code, Energy-aware Resource Provisioning techniques like reducing the clock speed when waiting for data, reducing the processor frequency
- Cooling Mechanism: Efficient ventilation along with heating and temperature monitoring for improving energy efficiency
- Resource Utilization: optimum utilization by reserving resources in-advance for dynamic allocation

- **Capacity Management**

Fog node and IoT device capacity is calculated based on the following classifications.

- Physical components for data processing, storage, networking
- Anticipated Log Workload management: Batch, Sequential or FIFO processing
- Service Level Agreements
- Software Licensing and auto Profiling Modules to cater for dynamic or additional logs
- Data Centre Infrastructure Management Model (DCIM) tools for real-time capacity management and forecasting and trending, including the 'what if' scenarios

4. Experimental Setup

Smart Vehicular Management is viable use case for Fog and IoT technology. The authors designed and implemented two experimental setups. The first setup involving standard Cloud implementation and the second setup employing Fog Computing and IoT Sensor nodes to compare the performance of the Vehicle Management Fog application regarding the Response time and Bandwidth Consumed.

The architecture and implementation involved deploying 50 sensors nodes across the university areas and routes. Each sensor is a high gain receiver with antenna having MediaTek 3329 chipset hardware running on 5V DC interfacing with 5V microprocessors and 4GB memory chip with position accuracy of less than 3.0 meters. These sensors detected the speed of each passing vehicle along the University roads, sending data to the Cloud for query processing on the Cloud server and executing query processing engine locally for the Fog infrastructure. These sensor devices were initially setup in catch-and-forward state to send traffic data generated to the University Cloud servers connected to the Internet via MPLS and Wireless circuits, this simulated the Cloud deployment. Then the nodes were configured to store to traffic data captured and perform the queries locally and then send the processed data to the local micro data centre server, this simulated the Fog and IoT deployment.

Both deployments involved execution of multiple queries on the traffic data generated for real-time calculation for the application performance for ROUTE_PLAN, CONGESTION_FACED and TRAFFIC_ACCIDENT and TRAVEL_SPEED. Average Speed is calculated over 9-hour period. The data is then processed for Congestion Faced in each travelled lane as well as for Accident Detected based on the average time taken and level of congestion faced which indicated accidents occurred or not.

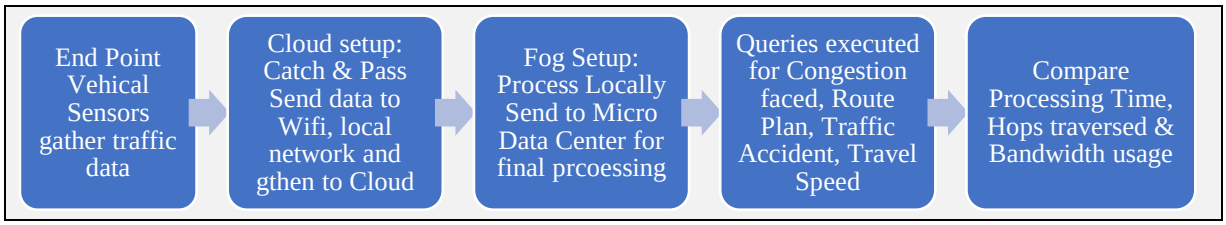

Figure 4: Fog-IoT and Cloud Computing deployment process

The traffic data was processed by the Cloud hosted servers on the University MPLS network while Fog nodes processed the traffic data locally and sent on the relevant bytes to the Fog Cloud server application console. Fog nodes dynamically connect to different places operators across fog devices when there is enough capacity to save bandwidth and minimize latency. Results obtained for both setups are compared and evaluated. After the Cloud computing data gathering is completed, the sensors are reconfigured to process the traffic data close to the source as part of the Fog infrastructure. The authors processed the data and compared it for Cloud and Fog for routing metrics as Processing Time, Hops traversed and Bandwidth usage.

4. Results Obtained

Academic researchers and the wide market growth and acceptance advocate that in near future Fog Computing enabled IoT nodes and devices will be a key enabler for Internet based IoT applications across public and private industry sectors. This research on Smart Fog Computing taxonomy has been proposed after analysing existing techniques for smart Fog Computing, taking into

Innovation and use of BLOCKCHAIN for IoT

Academic researchers and the wide market growth and acceptance advocate that in near future Fog Computing enabled IoT nodes and devices will be a key enabler for Internet based IoT applications across public and private industry sectors. This research on Smart Fog Computing taxonomy has been proposed after analysing existing techniques for smart Fog Computing, taking into consideration criteria from Fog Security, Fog Design, Fog Node Management, Energy management and Capacity Management.

Considering an IoT network having centralized authority controls for devices. The authors call through devices, treating the devices, for using the vehicular traffic data not permitted to compose protective decisions by themselves, without the availability of any central authority. Applying Blockchain to IoT and Smart Fog Computing implementation, the entire set of data is accumulated along with each tool and data also depicted and stocked. Prior to any information insertion to the network the hacker has to assemble all necessary resources for DNS attack and it must be confirmed and certified by every node present in the network. Since it, permits deposit to be completed without any bank or any negotiator (Zheng, Z. et al., 2017). A Blockchain can be owned in desperate financial benefits like electronic assets, reimbursement, and payment through online. In addition to this it can also use in other fields like IoT, smart investments and services useful for public. Apparently, an IoT (Kumar, N. M., et al., 2018) is no longer conceded to a single node.

In the universe of an IoT, an advanced and it might have imply earlier, is in the amorphous step of growth that might be a good idea for those who can see the capability in merging Blockchain security from grounded. Actually, an IoT produces a rigid threat than the Cryptocurrency in which the distributed network assigned with affecting currency from one unidentified owner to another. There is a necessary need of complex structure to authenticate, protect, and manage all the layers of an entire network. There are many frameworks are built to handle such technical issues and an appropriate framework must be able to identify illegal interruptions and to reduce the spread of malware it has to crumb hacked devices from the network. It would require a protocol to insert and delete equipment from Blockchain without bring out a protective reaction.

In addition, the Blockchain technology must beat a problem such as reasonable result is 51% of attack problem is enforced to tiny, substantially limited to an IoT networks and to obtain the control of a Blockchain expects to compromise a bulk of network equipment a complex task, when the network is spread over a globe, then it inclines and augmented easily when it is directed to a home network. Specialists have resolve to an idea of a dumped on Blockchain converge that promotes greatly more safeguard than centralized version, but does not absolutely accommodated aggregation as a developed Blockchain.

The configured Internet is currently not designed to shaft the size and difficulties occurred while handling recent transactions, because it is made up with old technologies where security issues are very huge and happens very frequently. Achieving a Blockchain technology to an IoT directly moderate and subsequently would be a great idea. Bring it to its place and then adjust it subsequently. A defeat to an address the cavernous protective space will convince a global difficulty for millions of householders later.

Conclusion

From the experimental setup and implementations, as compared to Cloud computing, Fog and IoT processes the traffic data locally on the edge devices, which reduces the end-to-end time taken for final processing and bandwidth usage reaching to the Cloud servers. Table 2 displays the huge advantage of using Fog as compared to Cloud computing.

Table 2. Comparing Fog and Cloud Computing results

Metric measured	End-to-End Process (Seconds)	Hops traversed (count)	Bandwidth Usage (Kbps)
Cloud Computing	29.44	56	247
IoT Fog Computing	6.7	4	8

As compared to Cloud computing, on deploying Fog Computing and IoT devices:

- End-to-End Processing time dropped from 29.44 to 6.7 seconds → almost 77% less
- Number of hops traversed reduced from 56 to 4 hops → almost 92% less
- Bandwidth usage dropped from 247 to 8 kbps → almost 96.7% less.

References

[1] Deloitte Report (2018). Indian IoT market value to touch $9 Billion by 2020. Retrieved May 10th 2018, from https://economictimes.indiatimes.com/tech/internet/indian-IoT-market-value-to-touch-9-bn-by-2020/articleshow/57232998.cms

[2] Gartner (2016). Forecast IoT Data Storage Capacity 2013-2018. Retrieved on June 3rd 2018, from

https://www.gartner.com/doc/3375517/forecast-IoT-data-storage-capacity

[3] Global Markets Insights (2018). Fog Computing Market Industry Reports. Retrieved April 2018, from https://www.gminsights.com/industry-analysis/Fog-Computing-market

[4] Cisco (2015). Fog Computing and the IoT: Extend the Cloud to Where the Things Are. Retrieved May 14th 2018, from https://www.cisco.com/c/dam/en_us/solutions/trends/IoT/docs/Computing-overview.pdf

[5] OpenFog Consortium (2016). OpenFog Architecture Overview. Retrieved August 10th, 2018, from https://www.openFogconsortium.org/wp-content/uploads/OpenFog-Architecture-Overview-WP-2-2016.pdf

[6] Venture Radar (2018). Top Fog Computing Companies. Retrieved September 23rd, 2018 from https://www.ventureradar.com/keyword/Fog%20Computing

[7] Naha, R., Garg, S., Georgakopoulos, D., Jayaraman, P., Gao, L. (2018). Fog Computing: Survey of Trends, Architectures, Requirements, and Research Directions. *IEEE Early Access.*

[8] Yeow, K., Gani, A., Ahmad, R., Rodrigues, J., Kwangman, K. (2017). Decentralized Consensus for Edge-Centric Internet of Things: A Review, Taxonomy, and Research Issues. *IEEE Access, Volume 6.*

[9] Anderson, E., Okafor, K., Nkwachukwu, O., Dike, D. (2017). Real time car parking system: A novel taxonomy for integrated vehicular Computing. *IEEE International Conference on Computing Networking and Informatics (ICCNI), Lagos, Nigeria.*

[10] Wang, M., Wu, J., Li, G., Li, J., Li, Q. (2017). Fog Computing based content-aware taxonomy for caching optimization in information-centric networks. *IEEE Conference on Computer Communications Workshops (INFOCOM WKSHPS), Atlanta, USA.*

[11] Gonzalez, N., Goya, W., Pereira, F., Langona, G., Silva, E. (2017). Fog Computing: Data analytics and cloud distributed processing on the network edges. *35th International Conference of the Chilean Computer Science Society (SCCC), Valparaiso, Chile.*

[12] Tocze, K., Nadjm-Tehrani, S. (2017). Where Resources Meet at the Edge. IEEE International Conference on Computer and Information Technology (CIT), Helsinki, Finland.

[13] Aijaz, A., Dohler, M., Aghvami, A., Friderikos, V., Frodigh, M. (2017). Realizing the Tactile Internet: Haptic Communications over Next Generation 5G cellular networks. *IEEE Wireless Communication, Volume 24, Issue 2, pp. 82–89.*

[14] OpenFog reference architecture for Fog Computing. (2017, February). Retrieved September 14, 2018, from https://www.openFogconsortium.org/wp-content/uploads/OpenFog_Reference_Architecture_2_09_17-FINAL.pdf

[15] Chiang, M., Ha, S., Risso, F., Zhang, T. (2017). Clarifying Fog Computing and Networking: 10 Questions and Answers. *IEEE Communications Magazine, Vol. 55, Issue 4, pp. 18–20.*

[16] Ku, Y., Lin, D., Lee, C., Hsieh, P., Wei, H., Chou, C., Pang, A. (2017). 5G Radio Access Network Design with the Fog Paradigm: Confluence of Communications and Computing. *IEEE Communications Magazine, Volume 55, Issue 4, pp. 46–52.*

[17] Elmroth, E., Leitner, P., Schulte, S., Venugopal, S. (2017). Connecting Fog and Cloud Computing. *IEEE Cloud Computing, Volume 4, Issues 2, pp. 22–25.*

[18] Schuster, R. (2017, May). About Open Edge Computing Initiative. Retrieved September 14, 2018, from http://openedgeComputing.org/lel.pdf

[19] Mach, P., Becvar, Z. (2017). Mobile Edge Computing: A Survey on Architecture and Computation Offloading. *IEEE Communications Surveys Tutorials, Volume 19, Issue 3, pp. 1628–1656.*

[20] Mobile Edge Computing. (2017). Mobile Edge Computing: Mobile Edge Platform Application Enablement. Retrieved September 10, 2018, from https://www.etsi.org/deliver/etsi_gs/MEC/001_099/011/01.01.01_60/gs_MEC011v010101p.pdf.

[21] Mobile Edge Computing. (2017). Mobile Edge Computing: Radio Network Information API, ETSI Standard. Retrieved September 10, 2018, from https://www.etsi.org/deliver/etsi_gs/MEC/001_099/012/01.01.01_60/gs_MEC012v010101p.pdf

[22] Taleb, T, Samdanis, K., Mada, B., Flinck, H, Dutta, S., Sabella, D. (2017). On Multi-access Edge Computing: A Survey of the Emerging 5G Network Edge Cloud Architecture and Orchestration. *IEEE Communications Surveys and Tutorials, Volume 19, Issue 3, pp. 1657–1681.*

[23] Kapsalis, A., Kasnesis, P., Venieris, I., Kaklamani, D., Patrikakis, C. (2017). A Cooperative Fog approach for effective workload balancing. *IEEE Cloud Computing, Volume 4, Issue 2, pp. 36–45.*

[24] Moreno-Vozmediano, R., Montero, R., Huedo, E., Llorente, I. (2017). Cross-site Virtual Network in Cloud and Fog Computing. *IEEE Cloud Computing, Volume 4, Issues 2, pp. 46–53.*

[25] Li, S., Maddah-Ali, M., Avestimehr, A. (2017). Coding for Distributed Fog Computing. *IEEE Communications Magazine, Volume 55, Issues 4, pp. 34–40.*

[26] Malensek, M., Pallickara, S. (2017). HERMES: Federating Fog and Cloud domains to support query evaluations in continuous sensing environments. *IEEE Cloud Computing, Volume 4, Issue 2, pp. 54–62.*

[27] Gu, L., Zeng, D., Guo, S., Barnawi, A., Xiang, Y. (2017). Cost efficient resource management in Fog Computing supported Medical Cyber Physical System. *IEEE Transactions on Emerging Topics in Computing, Volume 5, Issue 1, pp. 108–119.*

[28] He, Q., Zhang, C., Ma, X., Liu, J. (2017). Fog-based Transcoding for Crowdsourced Video Live Cast. IEEE Communications Magazine, Volume 55, Issue 4, pp. 28–33.

[29] Tang, M., Gao, L., Pang, H., Huang, J., Sun, L. (2017). Optimizations and Economics of Crowdsourced Mobile streaming. *IEEE Communications Magazine, Volume 55, Issues 4, pp. 21–27.*

[30] Bonomi, F., Milito, R., Zhu, J., Addepalli, S. (2017). Fog Computing and its role in the Internet of Things. *IEEE 1st Edition of MCC Workshop Mobile Cloud Computing, Helsinki, Finland, pp. 13–16.*

[31] Buyya, R., Mahmud, R., Kotagiri, R. (2018). Fog Computing: A Taxonomy, Survey and Future Directions. Internet of Everything. *Springer's Internet of Things (Technology, Communications and Computing), Singapore*

[32] Dasgupta, A., Gill, A. (2017). Fog Computing Challenges: A Systematic Review. Australasian conference on Information Systems, Hobart, Australia, pp 1-8.

[33] Forbes Press. (2017, March 20). 6 Hot Internet of Things (IoT) Security Technologies. Retrieved January 10, 2018, from https://www.forbes.com/sites/gilpress/2017/03/20/6-hot-internet-of-things-IoT-security-technologies/#403f402f1b49

[34] York, K. (2016). Dyn's Statement on the October 2016 DNS DDoS Attack – Dyn Blog. Retrieved March 5, 2018, from https://dyn.com/blog/dyn-statement-on-10212016-ddos-attack