Computational Viability of Fog Methodologies in IoT Enabled Smart City Architectures-A Smart Grid Case Study

Md. Muzakkir Hussain[1,*], Mohammad Saad Alam[2], M.M. Sufyan Beg[1]

[1]Department of Computer Engineering, Aligarh Muslim University
[2]Department of Electrical Engineering, Aligarh Muslim University

Abstract

The gradual evolution in the Information Communication Technology (ICT) support of Smart City (SC) architecture leveraged with meshes of Internet of Things (IoT) creates and welcomes research and investment efforts from academia, R&Ds and policymakers. The IoT utilities are being deployed at every layers of a typical SG backbone namely Application layer, Energy layer and Communication layer. The geo-distributed clusters of IoT "objects" produce galactic volume of data that exacerbates the need to make a paradigm shift from centralized data center based processing to a hybrid model that supports both in situ as well as cloud based storage and computational resources. To combat such SC issues, Fog Computing (FC) emerges as a promising solution, which pushes the computation resources onto the network edge nodes. This work investigates the high performance of Fog Computing over generic cloud computing in terms of metrics viz. latencies, power consumption etc, through a Smart Grid (SG) use-case. Through an operational cost optimization framework, the work comprehends the suitability of fog methodologies to make a synergistic interplay with the core centered clouds thus empowering a wide breed of real-time and latency free services. Finally, an overview of the core orchestration issues, challenges, and future research directions are presented for FC enabled SCs.

1. Introduction

Smart city vision brings emerging heterogeneous communication technologies such as Fog Computing (FC) together to substantially reduce the latency and energy consumption of Internet of Everything (IoE) devices running various applications. The key feature that distinguishes the FC paradigm for smart cities is that it spreads communication and computing resources over the wired/wireless access network (e.g., proximate access points and base stations) to provide resource augmentation (e.g., cyber-foraging) for resource- and energy-limited wired/wireless (possibly mobile) things. Moreover, smart city applications are developed with the goal of improving the management of urban flows and allowing real-time responses to challenges that can arise in users' transactional relationships.

The notion of smart city (SC) arises from the concept of efficient utilization of city resources for enhancing quality of life of inhabiting citizens, leading to acceleration of urban penetration. For ensuring an enhanced standard of living, utilities should focus on improvement of services and infrastructure in such cities. Thanks to the revolution in Information and Communication Technology (ICT) and the power of the Internet, the contemporary infrastructures and public services are expected to be more interactive, more accessible, and more efficient while stepping towards the realization of smart cities. In lieu of such domains, the emergence of the Internet of Things (IoT) paradigm strongly encourages utilization of the IoT's potential to support the smart city vision around the globe. As a consequence, the smart city has emerged as one of the important application drivers for IoT aided services. IoT enabled SC architectures promote the concept of interrelated physical objects (things), uniquely identified and distributed over broad physical areas covering entire city geography.

Recently, the IoT technologies have stepped forward towards connecting five pillars viz. "things", data, process, energy and people, forming the Internet of Everything (IoE) environments. From one perspective, cities can be regarded as an aggregation of interconnected networks that make up the IoE. Hence, the IoE pillars play a significant role and work together toward the promise of our smart city vision for the

*Corresponding author. Email: md.muzakkirhussain@zhcet.ac.in

future. The IoE's creation of data deluge synonymously Big Data (BD) over a distributed environment has the potential to create processing as well as storage concerns for such data-streams. Although, Cloud Computing posits to address such problems providing virtually unlimited and flexible resource pools but cannot work efficiently for mission critical Smart City applications due to its inherent problems. For instance, smart city applications like health monitoring, traffic monitoring, power transmission networks of smart grid systems etc, cannot tolerate the delay and latency incurred when transferring a massive amount of data to the remote Cloud Computing center and then back to the application.

The concept of Fog Computing (FC) had recently been proposed here, as an architectural set-up that extends Cloud services to the edge of the network, closer to the end user, which reduces data processing time and network traffic overhead. The primary definition of FC was introduced by Cisco as "*an architecture that uses one or a collaborative multitude of end-user clients or near-user edge devices to carry out a substantial amount of storage (rather than stored primarily in cloud data centers), communication (rather than routed over the internet backbone), and control, configuration, measurement and management (rather than controlled primarily by network gateways such as those in the LTE (telecommunication) core)*". The most fundamental entity in FC, called a Fog Computing Node (FCN), facilitates the execution of IoT applications. Basically, FC can act as an interface layer between end users end devices and distant Cloud data centers, with the aim of satisfying mobility support, locational awareness, geo distribution, and low latency requirements for IoT applications.

In future SCs, the SG will be critical in ensuring reliability, availability, and efficiency in city-wide electricity management. Figure 6 demonstrates an example future smart grid system, where Fog/Cloud computing can play a significant role. A successful smart grid system will be able to help improve transmission efficiency of electricity, react and restore timely after power disturbances, reduce operation and management costs, better integrate renewable energy systems, effectively save electricity for future usage, and so on. It will also be critical in building better electricity networks to help bring down electricity bills and balance the whole electricity system. In addition, the smart power grid system should monitor power generation, power demands and help make storage decisions. In terms of security, a smarter grid will also add resiliency to large-scale electric power systems so as to help governments react promptly to emergencies or natural disasters, e.g., severe storms, earthquakes, large solar flares, and even terrorist attacks, etc.

Motivated by those considerations, we present FC supported Smart Grid (SG) use-case to investigate the expediencies of FC paradigms towards fulfilling store and compute requirements of emerging SC services. A multitier FC structure in SG supports the applications running on things to jointly compute, route, and communicate with one another through the IoE environment to decrease latency and improve energy provisioning and the efficiency of services among things of varying computational capabilities. The FOG (From cOre to edGe) paradigm will potentially abridge the silos between personalized and bulk level analytics in SG informatics. A robust fog topology allows dynamic augmentation of associated fog nodes, thus significantly improvising the elasticity and scalability profiles of mission critical infrastructures. This work outlines the fog computing paradigm and examines its primacy over the cloud computing counterpart that became ubiquitous in fulfilling the computational and analytics needs of a reliable, robust, resilient and sustainable SG.

The argument here is not to cannibalize the existing cloud support for SG, but to comprehend the applicability of fog computing algorithms to interplay with the core centered cloud computing support leveraged with a new breed of real-time and latency free utilities. The objective is to assess the computational viability of FC for SC services (taking smart grid as use-case) in the realm of IoT space, through proper orchestration and assignment of compute and storage resources to the endpoints and where the cloud and fog technologies tuned to interplay and assist each other in a synergistic way.

The key contributions of the work are outlined as:

I. Proposed a fog processing architecture customized to mission critical requirements of Smart Grid.

II. A cost effective resource provisioning optimization model is proposed to guarantee computational QoS in emerging Smart Grid.

III. A modified differential evolution (DE) enhanced by fitness sharing is used for solving the proposed optimization model.

IV. A comparative analysis of both cloud and fog execution framework is performed to assess and unveil the suitability a fog aware cloud computing platform over generic cloud framework.

V. The Significant issues, challenges, and future research prospects towards fog orchestration of IoT application in Smart City domains are highlighted.

2. Fog Computing in Smart Grid-A Case Study

There exist relentless economic as well as environmental arguments in the academia, industries, R&Ds and legislative bodies for the overhaul of the contemporary power grid comprehended by a full Smart Grid rollout [1]. The latter integrates green cum renewable energy production utilities, robust power monitoring schemes, adapts and evolves with the consumption behavior and requirements. However, the unique feature that overlays on the heap of a SG amenities is connectivity and real-time analytics [2]. The recent advancements in information and communication infrastructures in general and Internet of Things (IoT) utilities in specific redefine the notion of "SMART" in current SG architectures. This work outlines the fog computing paradigm and examines its primacy over the cloud computing counterpart that became ubiquitous in fulfilling the computational and analytics needs of a reliable, robust, resilient and sustainable SG.

The notion of smartness has been introduced into the contemporary SG architectures where the local nodes will be leveraged with computational capabilities. They will no longer remains a "thing" rather will be transformed into active

computing nodes or "objects". Every component of SG network whether it is at the generation, transmission or service level, will act as active nodes in the entire transportation web. They are now called object in the sense that they will be having attributes, gateways, states etc. The whole transportation system can be encapsulated as a network of active nodes having deterministic state transitions. This is achieved through the notion of internet of thing (IoT). IoT will ensure real-time transport of information to and from the utilities, smart grid system and other components in the power system and charging infrastructure in a way that the current as well as future needs of these entities along with dedicated business engagement can be determined [3].

Such technologies are enabled by the recent developments in RFID, smart sensors, communication standards, and Internet protocols [4]. The basic principle is to have an environment where smart sensors collaborate directly with the "objects" without human involvement aiming to deliver multitudes of applications and services [5], [6]. It is a consensus belief by industries as well as research giants that down the line, in near future IoT will emerge as a technology enabler for smart transport, X2X (where X may be any of but not necessarily same from entities like Vehicles, Grids, Homes, Micro-grid etc.) data and energy exchange topologies, optimal renewable integration and intelligent charging infrastructures [7].

However, it is obvious that in the IoT architecture the population of connected entities will overshoot the current growth drift and will jeopardize the normal computing configurations [8]. This will in turn cause an exponential escalation in data generation, handling of which is key task to ensure viable implementation any data aware infrastructure. Connecting the objects through edge networks and technologies such as Wireless Sensor Networks (WSN), Zigbee, bluetooth, RFID, WiFi, 3G, and 4G etc. will increase the complexity of underlying communication architectures. Efficient and robust data analytics setup that can establish a real-time cum intelligent decision making atmosphere at every edge services becomes the need of hour. An exhaustive review of existing control paradigms reveal the presence centralized coordination strategies such as cloud computing, grid computing etc [8],[9]. However the service demands of IoT architecture reflect that there needs computing schemes that can execute locally at the edge itself. The prevalent cloud models are not intended to handle the seven unprecedented V's (Volume, Velocity, Variety, Variability, Veracity, Visualization and Value) in the data generated by IoT architectures and coupling the whole universe of "things" or "objects" directly to the cloud is nearly unfeasible [10]. Fog computing approaches seem to be the preeminent preference for computations at the extreme edges such as vehicles, roadways, charging station etc [10]–[13].

However installation of fogs (mini data centers) everywhere across the edges of the networks and entities may not be cost productive. The infrastructure demands varying levels of services which in turn have specified QoS requirements. Transporting tera-peta bytes of data from millions of edge devices to the central cloud in real-time is quite infeasible and even unessential, as a significant percentage of data are passive and don't contribute to any decision making process.

Furthermore, there exist several tasks that don't even entail storage, processing and analytics at cloud scale. Such requirements motivate the need of a hybrid control architecture where the mining and analytics activities are intelligently dispersed.

The smart grid applications require location aware geodistributed intelligency in services such as metering information updates, power thefts, distribution outages, network intrusions etc, and require prompt and reflex actions to evolve and organize according to the adversaries. However, the current smart grid is under immense pressure owing to its sullen response to the abovementioned computational demands. Also, due to its fragility concerns in SG control and coordination sub-systems, repercussions of power outages, resiliency and reliability issues are growing ever more serious. Upgrading to a computationally smarter, reliable and resilient grid has escalated from being a desirable vision, to an urgent imperative. Here we itemize few but not the least, of some of the mission critical requirements of an ideal SG infrastructure plus the sombre experiences encountered while going for pure cloud computing deployment.

1.1 *Support for scalable real-time services:*

The need of real-time analytics and decisions is being emerged as the need for the hour to carry up the timing requirements of mission critical SG utilities [14]. Even if some servers' fiascos occur, the system should heal itself with just graceful degradation in latency services. The current cloud models support for SGs can provide rapid response mechanisms but adversaries still pose threats to responsiveness.

1.2 *Support for scalable, consistency guaranteed, fault-tolerant services:*

Consistency for cloud-hosted utilities is a broad term associated with ACID (Atomicity, Consistency, Isolation and Durability) guarantees, support for state machine replication, virtual synchrony, and support for only limited count of node failures [1]. Today's smart grid cloud infrastructures often "embrace inconsistency", thus implementing consistency preserving computational structures constitute a nascent thrust domain for the research & development sector.

1.3 *Privacy and security:*

The woeful protection services of current cloud deployments often stimulate the cloud vendors to recapitulate their security management folks to "not be evil". Stern efforts are in progress across the power system and transportation communities to come up with SG cloud utilities and platforms leveraged with robust protective contrivances where the stakeholders could entrust the storage of sensitive and critical data even under concurrent share and access architectures [15], [16].

1.4 *Highly Assured Connectivity:*

Added with power outages, the smart grid consumers also experience intermittence in data connectivity. Projects for establishing mechanisms dedicated to support secured multipath data routing from user edges to cloud services are on headway [17],[18]. Critical components of the future smart grid applications demand better quality of service (QoS) and quality of experience (QoE) from the data routing backbone that underlie the cloud-hosted utilities.
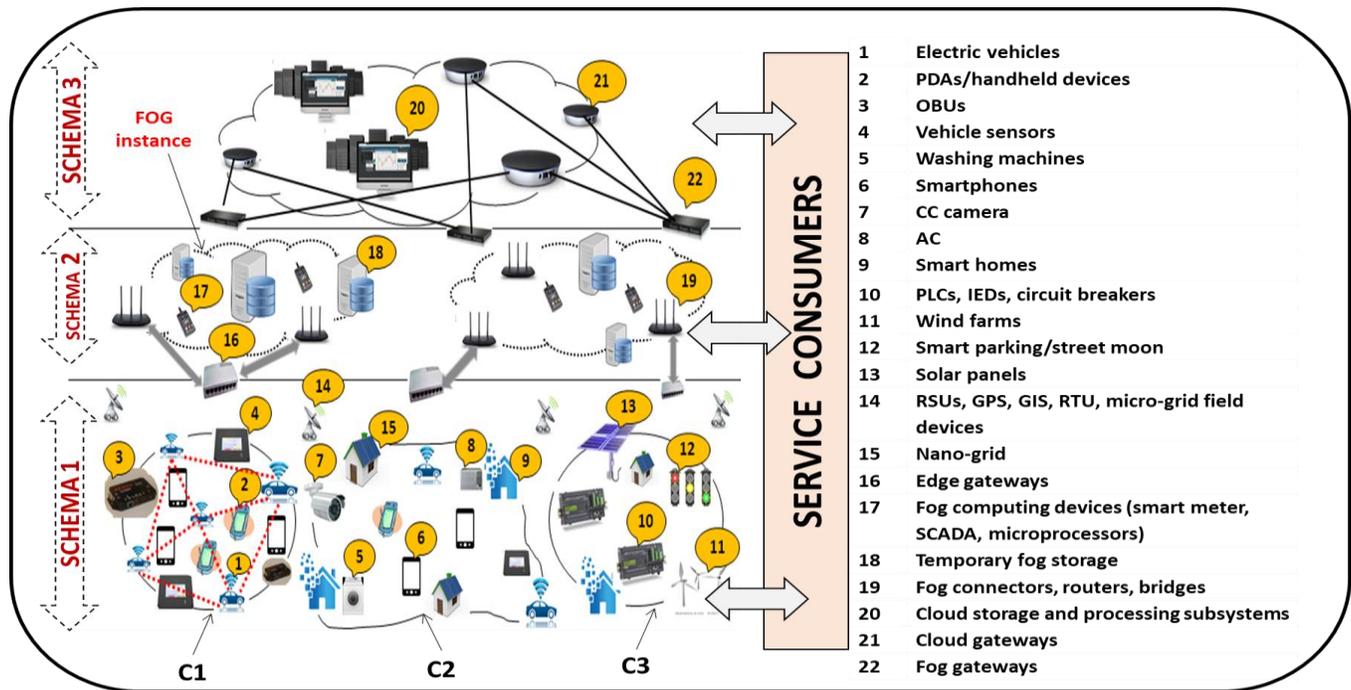
Figure 1: Topology of FOG computing paradigm in a Smart Grid

Legend for Figure 1:

1. Electric vehicles
2. PDAs/handheld devices
3. OBUs
4. Vehicle sensors
5. Washing machines
6. Smartphones
7. CC camera
8. AC
9. Smart homes
10. PLCs, IEDs, circuit breakers
11. Wind farms
12. Smart parking/street moon
13. Solar panels
14. RSUs, GPS, GIS, RTU, micro-grid field devices
15. Nano-grid
16. Edge gateways
17. Fog computing devices (smart meter, SCADA, microprocessors)
18. Temporary fog storage
19. Fog connectors, routers, bridges
20. Cloud storage and processing subsystems
21. Cloud gateways
22. Fog gateways

1.5 *Need for risk management modules:*

Switching from traditional power grid to multi-tenant SG subsystems introduce substantial risks to power sector, an issue that need to get fixed in inception phase. The penetration of autonomous EVs into modern road transport manifolds such concerns. The EVs are becoming a basin for multi-dimensional data production, an asset if mishandled, may befool the execution of whole systems. Moreover, the data generated due to Cloud-IoT integrated transportation telematics coupled with advanced metering infrastructures (AMI) can prove to be harmful to its stakeholders, specifically for privacy and security [19]. Thus, it's an earnest need for the stakeholders to be assured with stringent protection protocols and be inert from the vulnerabilities. Such scenario necessitates incorporating robust risk analysis procedures that will evaluate and quantify the computational and business risks that persist in such critical infrastructures [20]. Selection followed by implementation of proper risk analysis paradigms is itself a full-fledged realm to dwell on. Risks perceived to be minor in inception phase, later elicits tougher public concerns. Though the "pay-for-usage" protocols of cloud computing business models are efficient in satisfying the bulky analytics and computational tasks, the bliss transforms into worries when the applications demand null-latency services and when the data stream chokes the bandwidth restricted communication buses [21]. The emerging wave IoT based transportation telematics can prove potentially astonishing in fulfilling the mobility requirements of contemporary smart grid architectures [21], [22].

Motivated by the above mentioned mission critical Smart Grid requirements, the pitfalls associated with current cloud computing infrastructures to meet such needs, and having the assumption that the smart grid community is not in a position to reinvent a remotely owned Internet infrastructure or to develop computing platforms and elements from scratch, this work presents a fog computing framework whose principle underlie on offloading the time and resource critical operations From cOre to edGe. The argument here is not to cannibalize the existing cloud support for SG, but to comprehend the applicability of fog computing algorithms to interplay with the core centred cloud computing support leveraged with a new breed of real-time and latency free utilities.

3. Fog Computing Architecture for Smart Grid

This section presents a three schema computing architecture where the significant portions of smart grid control and computations are non-trivially hybridized alongside the cloud computing support. The objective is to overcome the disruption caused by the development of IoT utilities where the control, storage, networking and computational needs are actively proliferated across the edges or end-points.

The lowermost schema namely physical schema or data generator layer primarily comprises of a wide range of smart IoT enabled devices which come within the SG domain. For simplicity, the entities are abstracted into logical clusters of applications, directly or indirectly influenced by the expediency of SG operations. The first cluster (C1) represents vehicular applications where the intelligent vehicles are arranged to form vehicular fogs. The existing transportation telematics support such as cellular telephony, on-board sensors (OBS), roadside units (RSU), and smart wearable devices will uncover the computational as well as networking capabilities latent in the underutilized vehicular resources. The notion is to employ the underutilized vehicular resources into

communicational and analytics use, where a collaborative multitude of end-user clients or near-user edge devices carry out communication and computation, based on better utilization of individual storage, communication and computational resources of each vehicle [5]. Similarly, similar presence of clusters (C2) could also be traced in smart home networks that have a noteworthy contribution in consistent operations of the backend SG support. The intelligent IoT equipped home gadgets such as washing machines, AC, freezes, parking lots, CC camera etc, are also potentially active to provide storage, analysis and computational support for satisfying the prompt and local decision making services. The third but not the least, cluster C3 depicts similar structure that can be constituted by utilities involved at the extreme ends of a SG infrastructure viz. micro-nano grid, PLCs, (HAN, MAN etc) automated circuit breakers and other entities associated to diverse range of SG generation, transmission and distribution services.

The smart nodes within such clusters sense and cultivate the heterogeneous physical attributes and transmit it to the upper layers through dedicated edge gateways. However, the whole or a portion of data generated within these physical clusters are accumulated at the interim across access points such as global positioning (GPS), GIS, road-side units (RSU),remote terminal units (RTU), intelligent electronic devices (IED), phasor data concentrators (PDC), and other field arrays.

The next tier constitutes the fog computing layer comprising of intelligent fog devices such as SCADA, smart meters, routers, switches high-end proxy servers, intelligent agent and commodity hardware etc, having peculiar ability of storage, computation and packet routing. The software defined networking (SDN) assembles the physical clusters to form virtualized inter cluster private networks (ICPN) that route the generated data to the fog devices spanned across the fog computing layer The fog devices and its corresponding utilities form geographically distributed virtual computing snapshots or instances that are mapped to lower layer devices in order serve the processing and computing demands of SG.

4. Networking and System Formulation

In a cloud computing model the mega data center (MDC) provides sharable resource pool available for on demand use. Since the MDC are far remote from the generation and query sites, data migration and service latency gives rise to infeasibilities for real-time and interactive SG applications and services. However, in a fog architecture, low power fog computing nodes (FCN) are deployed at the dedicated edges of the network to provide platform for SG mobility, real-time response and geo-distributed intelligence.

Consider a fog architecture customized for SG services which supports both cloud as well as local fog processing, in which data and computation are selectively offloaded to either cloud or fog scale processing guided by an application specific logic. Without loss of generality, let us assume the sets D , F , and N represents the set of data centers, fog nodes and number of consumers having cardinality D, F and N respectively. An instance of Smart Grid (SG) network can be modeled as a connected cellular graph of order (N +F) whose

vertices are constituted by data consumer set (N) and FCN set (F). Let (r_i^a) be the frequency of workload arrival on fog node *i*. The FCNs are equipped with set of processing elements (E) each having service rate r_i^s . An FCN *j* is reachable from query source node *k* if the former is in the preference list L.

For demonstrating the feasibility of a customized fog computing architecture in smart grid sub-systems proposed in section 3, the work utilizes metrics that correlates the performance of fog computing services to that of traditional cloud computing paradigms. The geo-distributed micro datacenters in a typical fog model performs a significant proportion of local computations on the data produced by data generators at the schema 1. However, the devices are leveraged with distributed intelligence, in that depending upon the degree of services criticality and the types of data, the righteous decision of whether to offload the data to the cloud or to the local micro-data centers can be undertaken. For SG applications, the fog computing framework outperforms its pure cloud counterparts in respect to metrics like power consumption, latency and carbon footprint (emission) etc [25].
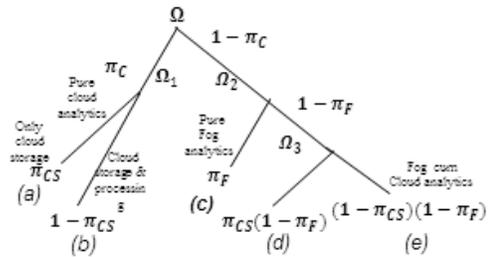

Figure 2: Probabilistic decision tree depicting the workload offloading strategy

Consider a pilot SG analytics service to be delivered from the three tier fog architecture devised in section 3 over a 24 hour time horizon. Out of volume Ω of data generated in the whole day, the pre-processing and decision modules deployed in the first tier offloads Ω_1 into the mega datacenters for cloud level analytics while distributes Ω_2 to the micro datacenters for local and instant scale processing and computations. The uncertainty in the data distributions across multiple schemas is captured by probability tree depicted in Figure 2. An ideal fog-cloud framework is leveraged with robust inferencing logic and intelligent filtering devices to undertake instant decisions on where to distribute the produced datasets. The objective of the proposed framework is to minimize the cost encountered due to power consumption, latency and emission issues. In case of fog computing approach, an additional cost term needs to be added due to communication among the IoT enabled sensors as well as micro datacenters.

1. **Cost profile for Generic Cloud processing:**

$$F_c(x) = C_c(v) + C_c(w) + C_c(c) \qquad (1)$$

Where $F_c(x)$, $C_c(v)$, $C_c(w)$ and $C_c(c)$ represent the overall cost function, power consumption cost (incurred due to

storage and execution of the data at the mega datacenters), cost due to latency terms and the cost due to carbon footprint at the data centers respectively.

$$C_c(v) = \begin{bmatrix} V_1.\Pi_C\{\Pi_{CS}.(\alpha_{CS}) + (1-\Pi_{CS}).(\alpha_{CA})\} + \\ (1-\Pi_C).(1-\Pi_F).(\alpha_{CA}).V_3 \end{bmatrix}.\lambda_E \quad (2)$$

Where, α_{CS}, α_{CA} and V_3 represent the power consumed in cloud storage, cloud storage cum processing and amount of data that is migrated to the cloud layer through cloud-fog gateway interface (21-22 in fig 1). λ_E ((USD/KWh)) is the energy to cost conversion factor.

$$C_c(w) = \begin{bmatrix} \left(\Pi_C.\dfrac{V_1}{w_{DC}} + (1-\Pi_C).(1-\Pi_F).V_3\right) \\ .\left(\dfrac{1}{w_{DE}} + \dfrac{1}{w_{EF}} \dfrac{1}{w_{FC}}\right) \end{bmatrix}.\lambda_L \quad (3)$$

λ_L (USD/Minutes) is the delay to cost conversion factor.

$$C_C(c) = \chi.\{V_1.\Pi_C + V.(1-\Pi_C)\}.\lambda_G \quad (4)$$

χ and λ_G represents the gas emissions rate from the data centers and emission to cost conversion factor.

2. Cost Profile for Fog aware Cloud processing:

$$F_F(x) = C_F(v) + C_F(w) + C_F(c) \quad (5)$$

Where $F_F(\ )$, $C_F(\ )$, $C_F(\ )$ and $C_F(\ )$ represent the overall cost function, power consumption cost (incurred due to storage and execution of the data at the micro datacenters), cost due to latency terms and the cost due to carbon footprint at the local data centers respectively.

$$C_F(v) = \begin{bmatrix} (V_2 - \ ).(1-\Pi_C).\{\Pi_F.(\alpha_{FA}) + \\ (1-\Pi_C).(1-\Pi_F).(\alpha_{FS}).V_3 \end{bmatrix}.\lambda \quad (6)$$

where, α_{FA} and α_{FS} represent the energy consumed in fog processing, fog processing plus cloud storage respectively.

$$C_F(w) = \begin{bmatrix} (1-\Pi).\Pi_F.(V_2 - V_3).\dfrac{1}{w_{DE}} + \\ (1-\Pi_C).(1-\Pi_F).V_3.\left(\dfrac{1}{w_{EF}} + \dfrac{1}{w_{FC}}\right) \end{bmatrix}.\lambda_L \quad (7)$$

$$C_F(c) = \chi.\begin{cases} (V_2 - V).(1-\Pi_C) \\ +V_3.(1-\Pi_C).(1-\Pi) \end{cases}.\lambda \quad (8)$$

w_{DC}, w_{DE}, w_{EF} and w_{FC} represent the bandwidth of the channel linking generators to mega datacenters (when data demands pure cloud storage or computations), generators to edge routers, edge routers to fog gateways and fog gateways to cloud gateways respectively.

3. Optimization model:

In order to assess the viability of proposed fog computing framework, in this subsection a cost optimization model is proposed. The objective is to reveal the fact that, if properly designed, a fog computing framework can circumvent intricacies prevalent in contemporary cloud computing paradigms. The following optimization framework captures the scenario where former outperforms the later in terms overall performance.

$$Maximize\ \{\min F_F(x) - \min F(x)\} \quad (9)$$

Subject to:

$$V = V_1 + V \quad (10)$$

$$C_F(c) < C(c) \quad (11)$$

$$C_F(w) < C(w) \quad (12)$$

5. Simulations and Results

For simulating the topology, the 100 most populated cities around the world are considered for representing the number of IoT users and the corresponding geographical coordinates are used to determine the relative Euclidian distance. The number of application consumers and the potential data traffic is assumed to be proportional to the population of Internet users of the city. The user to fog links allows transmission of packets of 34 to 64K bytes following Poisson arrival pattern having 8 byte instruction size. The capacity of user to fog links and fog to cloud links is assumed as 1Gbps and 10Gbps respectively. For assessment of system performance against the network parameters the total population of consumers is captured in a variable in the range [10000, 100000]. The number of data centers is considered to be 8 and the pairwise Euclidian distance is stored in 2D variable $D_E[\ ][\ ]$.

For cost analysis, the cost of 1Gbps and 10Gbps Gateway router port is kept USD50 each per year while cost of server is USD 4000 per year. These routers are assumed to consume electricity at 20W and 40W respectively. Upload rate is USD 12 per byte while storage cost is kept in the range of USD 0.45-0.55 per hour. The penalty corresponding to CO_2 emission is kept USD 1000 per tons of CO_2 emitted.

The formulated optimization model is a multistage, discrete, nonlinear, constrained mixed-integer programming problem (MINLP). Usually classical mathematical programming techniques fail to provide tractable solutions to such problems. Evolutionary optimization algorithms specifically meta-heuristic methods such as differential evolution (DE) [price] are promising approach to solve an MINLP. DE is a population-based evolutionary optimization method which had proven to be very simple yet powerful to solve minimization problems with nonlinear and multi-modal objective functions. It differs from conventional evolutionary

algorithms in that instead of having a predefined probability distribution function (pdf) for mutation process, it utilizes the differences of randomly sampled pairs of objective vectors for its mutation process [6]. Such variations will ensemble the topology of the objective function towards optimization procedure thus providing more efficacious global optimization capability. We employed, a modified version of differential evolution with fitness sharing function of niche radius () in order to reduce the fitness of similar offspring's. The fitness function is given by

$$Ff(\varphi, \kappa) = 1 - \left(\frac{\kappa}{\rho}\right)^{\varphi} \Big| \qquad 0 \leq \kappa < \rho \qquad (13)$$
$$0 \qquad\qquad otherwise$$

As in DE the evolution strategy is focused to obtain minimal optimal value, of the shared fitness is obtained from

$$S_f = f \cdot \sum_{j=1}^{PS} Ff^{j}(\varphi, \kappa) \qquad (14)$$

Where, f_j controls the crossover constant commonly determined on a case to case basis. In order to guarantee the fact that the best offspring always appear for next generation, elitism is employed. Further details are beyond the objective of this paper. In this section we presented the comparative result analysis of cloud and fog execution in terms of performance metrics namely response times (service delay), electricity consumption and cost of architecture.

We depict the overall latency profile of a fog aware cloud architecture with a generic cloud execution scenario. The upload latency, inter-fog communication delay and delay due to fog to cloud dispatch is abstracted in transmission latency while the delay caused due to computations and analytics at VM fog nodes and data center servers is accumulated to processing latency term. The overall service delay is the linear sum of transmission and processing latency. For a parameter $\Re$ defined to be the ratio of data packets dispatched to cloud core to the number of packets entering into the fog network through consumer to fog gateways.

$$\Re = \frac{\mathbb{N}_C}{\mathbb{N}_F} = \frac{\mathbb{N}_F - \mathbb{N}}{\mathbb{N}_F} \qquad (15)$$

The fog-cloud comparison delay statistics is shown in Fig. 3 for $\Re = .25$ (three fourth of requests are served within fog alone). It can be observed that for both the fog as well as cloud platforms the latency is proportional to the population of data generators (traffic) and performance of fog aware execution outperforms the cloud counterparts for every volume of traffic.

In Fig. 4 the electricity consumption pattern in transmission/dispatch of data bytes, computation (at both fog and cloud servers) is analysed. It can be observed that with the rise in the population of service consumers the overall power consumption show linear growth and is significantly lower than the conventional cloud framework. The fog aware

framework betters the aggregated electricity consumption over the cloud computing paradigm by more than 40%.
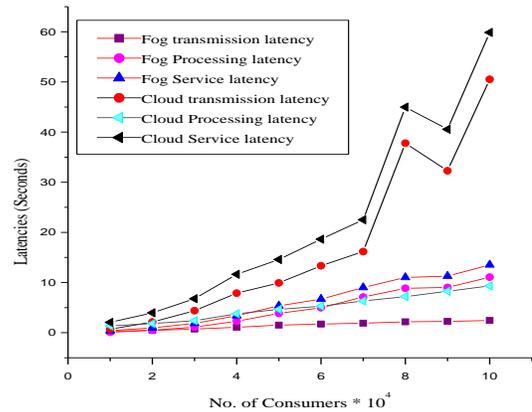

Figure 3: Comparison of Latency Metrics between generic cloud Vs Fog Assisted Cloud Platforms
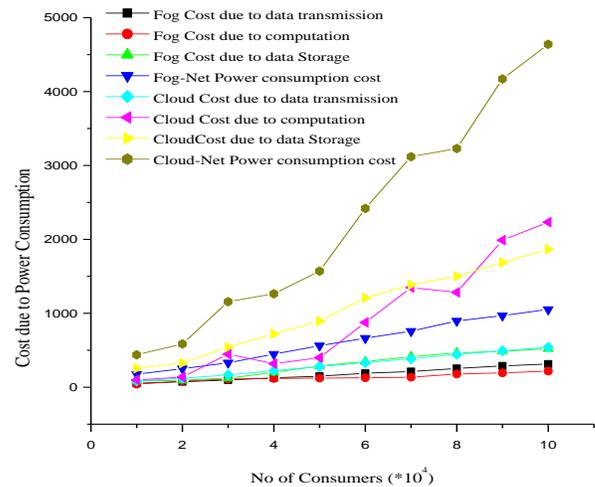

Figure 4: Comparison of various cost parameters

6. Fog Enabled Smart Cities-Challenges and Future Directions

A typical fog platform is driven by key technology enablers, for its successful deployment. Since, the field is relatively immature [23], a large amount of experimentation needs to be done. The FC platform should be able to provide a framework that others can use it to test different approaches, techniques, and algorithms. For instance, there are many ways to autonomously annotate data with semantics within a fog gateway. It is not possible to develop one universal approach or algorithm to annotate data. Thus, a FC platform should be provide flexibility to the developers to write exertions, support new ways of annotating data [24].

Also, FC should provide built-in supports for varying communication standards and application level protocols [21]. Further, providing support for existing data analytics frameworks is also important. Due to low computational

resources of FC gateways, it is important that these plugins can be easily removed to avoid resource wastage when not required in a given fog gateway. Despite we see a large number IoT cloud platforms in the market in both academia (e.g., OpenIoT) and industry (e.g., IBM Bluemix, Microsoft Azure IoT), a fog computing platform that supports all the those features are yet to be researched and developed [25]. We believe such fog platforms would be greatly beneficial to the research and industrial communities once available as by then people can easily test new fog computing related approaches, techniques and algorithms.

Distributed intelligence will be very critical in making fog computing platforms successful in building future smart cities. The main reason is that prompt reactions and best possible decisions should be achieved in a timely manner to make future cities smarter, safer and more living-enjoyable. This requires a large amount of research efforts in putting distributed intelligence in place properly across smart things, buildings, fog devices/gateways, and cloud computing infrastructure in a city. This process will involve many important aspects, such as available domain-dependent knowledge/ intelligence, combination of business logic, engineering processes and government policies, cost-efficient and computation-efficient and context-/semantics-aware computing models for real-time decision making, etc [26].

High paced R&D and investments efforts since past decade have led to the maturity of the cloud based techniques having efficient frameworks, deployment platforms, simulation toolkits and business models. However, in context of fog deployments such efforts though on pace, but still near its infancy [21], [26]. There may be plenty of literatures hypothesizing the execution scenario of fog platforms but are still in concept and simulation phase. Roll-out of fog services needs to inherit many of the properties of cloud counterparts and the requirement of deploying computational workloads on fog computing nodes (FCN) need to be demystified properly [27]. In addition fog comes with its inherent silos and raises many questions asking for right and consensus answer. Some of them may be, where to place a workload, what are the connection policies, protocols and standards, how to model/interpret the interaction of/among fog nodes, how to route the workload etc.

Since IoT enabled smart city services are pervasive in cyber-physical environments and the complex IoT services are increasingly composed of sensors, devices, and compute resources within FC infrastructures, orchestrating such applications can simplify maintenance and enhance data security and system reliability [28]. However, efficiently dealing with dynamic variations and transient operational behavior of such SC services is a crucial challenge. This section provides an overview of the core issues, challenges, and future research directions in orchestration for IoT services in FC enabled smart cities. In the next sub-section we highlight the key orchestration challenges in fog-enabled orchestration for SC applications. Following this, the nascent research avenues envisioned by such issues and challenges are also explored.

A. Fog orchestration Challenges for Intelligent Transportation Applications in IoT space

1. Scalability

Since the heterogeneous sensors and smart devices employed in SC are designed from multiple IoT manufacturers and vendors, selecting an optimal device becomes increasingly intricate while considering customized hardware configurations and personalized SC requirements. Moreover, there may be applications can only operate with specific hardware architectures viz. ARM or Intel etc, and through wide range of operating systems [29]. Additionally, the SC applications with stringent security requirements might require specific hardware and protocols to function. An orchestration framework need not only to cater to such functional requirements, it must scale efficiently in the face of increasingly larger workflows that change dynamically [23], [30]. The orchestrator must assess whether the assembled systems, comprised of cloud resources, sensors, and fog computing nodes (FCN), coupled with geographic distributions and constraints are capable of provisioning complex services correctly and efficiently. In particular, the orchestrator must be able to automatically predict, detect, and resolve issues pertaining to scalability bottlenecks that could arise from increased application scale in a customized SC architecture.

2. Privacy and Security

Security is also a critical issue in building future smart cities. This mainly refers to security of fog computing platforms, including potential cyber-attacks to smart things, fog devices/gateways, and trust and authentication, network security, and data security, etc [31]. For example, cyber-attacks to smart things, fog devices/gateways can dysfunction smart things, fog devices/gateways and pose risks in failure of providing proper services to the city and making wrong decisions in reaction to emergencies and disasters. Failure of ensuring trust and authentication will also put any large-scale fog computing platforms at risk, potentially leading to intentional and accidental misbehaviour, criminal activities and so on. Network security is also of great importance since network attacks such as jamming attacks, sniffer attacks and so on can create huge risks in fog computing systems, potentially leading to chaos of the whole fog computing systems. Data security will also be critical. Sensitive and/or valuable data generated from any fog computing platforms should be kept secure [32].

Since in IoT aided SC like use-cases such as Smart Grid, smart parking etc, a specific application is composed of multiple sensors, computer chips and devices, their deployment in varying different geographic locations result in increased attack vector of involved objects. Examples of attack vector may be human-caused sabotage of network infrastructure, malicious programs provoking data leakage, or even physical access to devices [33]. Holistic security and risk assessment procedures are needed to effectively and dynamically evaluate the security and measure risks, as evaluating the security of dynamic IoT based application orchestration become increasingly critical for secure data

placement and processing. The IoT integrated devices for fog support such as switches, routers and base stations etc, if are brought to be used as publicly accessible computing edge nodes, the risk associated by public and private vendors that own these devices as well as those that will employ these devices will need revised articulation. Also, the intended objective of such devices, e.g. an internet router for handling network traffic, cannot be compromised just because it is being used as fog node. The fog can be made multi-tenant only when stringent security protocols are enforced.

3. Dynamic Workflows

Another significant characteristic and challenge for IoT enabled SC applications is their ability to evolve and dynamically change their workflow composition. This problem, in the context of software upgrades through FCNs or the frequent join-leave behavior of network objects, will change the internal properties and performance, potentially altering the overall workflow execution pattern. Moreover, handheld devices used by SC stakeholders inevitably suffer from software and hardware aging, which will invariably result in changing workflow behavior and its device properties (for example, low-battery devices will degrade the data transmission rate). Furthermore, performance of transportation applications will change owing to their transient and/or short-lived behavior within the SC subsystem, including spikes in resource consumption or big data generation. This leads to a strong requirement for automatic and intelligent reconfiguration of the topological structure and assigned resources within the workflow, and importantly, that of FCNs.

4. Tolerance

Scaling a fog computing framework in proportion to SC application demands increases the probability of failure. Some rare software bugs or hardware faults that don't manifest at small scale or in testing environments, such as stragglers, can have a debilitating effect on system performance and reliability. At the scale, heterogeneity, and complexity we're anticipating, different fault combinations will likely occur. To address these system failures, developers should incorporate redundant replications and user-transparent, fault-tolerant deployment and execution techniques in orchestration design.

B. Future Research Directions

The challenges outlined in the above sub-section unlock several key research directions for successful deployment of fog supported SC architectures. The research prospects defined for fog life cycle management can be executed in three broad phases. In deployment phase, research opportunities include optimal node selection and routing, parallel algorithms to handle scalability issues, etc. In runtime phase, incremental design and analytics, re-engineering, dynamic orchestration etc, are potential research thrusts for supporting dynamic QoS monitoring and providing guaranteed QoE [34]. In the evaluation phase, Big-Data-Driven analytics (BD^{2}A) and Optimization Algorithms are prime avenues that need to be explored to improve orchestration quality and accelerate optimization for problem solving.
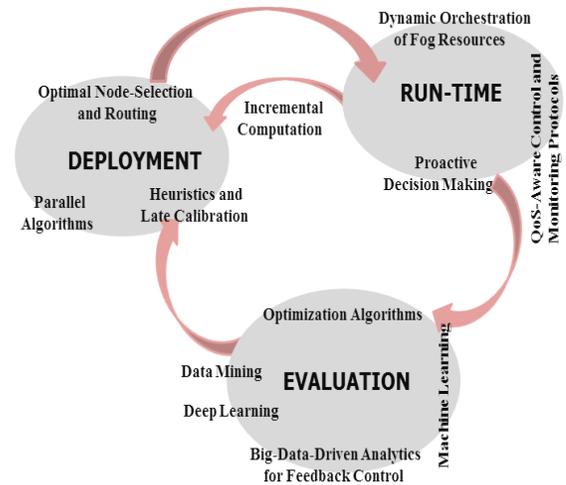

Figure 5: Functional elements of a typical fog Orchestrator

1. Opportunities in Deployment Phase:
i) Optimal Node-Selection and Routing:

Determining resources and services in cloud paradigms is a well explored area and easily understood, but exploiting network edges in decentralized fog settings call for discovery mechanisms to associate optimal nodes [5],[34],[35]. Resource discovery in fog computing is not as easy as in both tightly and loosely coupled distributed environments, and manual mechanisms are not feasible because of sheer volume of FCNs available at fog layer. If the SC utility needs to execute machine learning or Big-Data tasks, resource allocation strategies also need to cater for datastream of heterogeneous devices from multiple generations as well as online workloads. Benchmark algorithms need to be developed for efficient estimation of FCN's availability and capability [4]. These algorithms must allow for seamless augmentation (and release) of FCNs in the computational workflow at varying hierarchical levels without added latencies or compromised QoE. Autonomic node recovery mechanisms needs to be devised to ensure consistency and reliability in in fault detection in FCN networked architectures, as existing cloud based solutions don't fit to them. Besides, the most potential research aspect to ponder is workflow partitioning in fog computing environments. Though numerous task partitioning techniques, languages and tools have been successfully implemented for cloud data centers, but research regarding work apportioning among FCNs is still in concept phase. Without specifying the capabilities and geo-distribution of candidate FCNs, automated mechanism for realizing computation offloading among those nodes is challenging. Maintaining a ranked list of associated host nodes through priority aware resource management policies, making hierarchies or pipelines for sequential offloading of workloads, developing schedulers for dynamically deploying segregated tasks to a multiple nodes, algorithms for parallelization and multitasking of only FCNs, FCNs and data centers or only data enters etc, are rigorous research hypes in academia as well as R&D community [35].

ii) Parallelization Approaches to Manage Scale and Complexity:

Optimization algorithms or graph-based approaches are typically time and resource-consuming when applied on a large scale, and necessitate parallel approaches to accelerate the optimization process. Recent work provides possible solutions to leverage an in-memory computing framework to execute tasks in a cloud infrastructure in parallel. However, realizing dynamic graph generation and partitioning at runtime to adapt to the shifting space of possible solutions stemming from the scale and dynamicity of IoT components remains an unsolved problem.

iii) Heuristics and Late Calibration:

To ensure near-real-time intervention during IoT application development, one approach is to use correction mechanisms

that could be applied even when suboptimal solutions are deployed initially.

To ensure near-real-time intervention during IoT application development, one approach is to use correction mechanisms that could be applied even when suboptimal solutions are deployed initially. For example, in some cases, if the orchestrator finds a candidate solution that approximately satisfies the reliability and data transmission requirements, it can temporarily suspend the search for further optimal solutions. At runtime, the orchestrator can then continue to improve decision results with new information and a re-evaluation of constraints, and use task- and data-migration approaches to realize workflow redeployment.
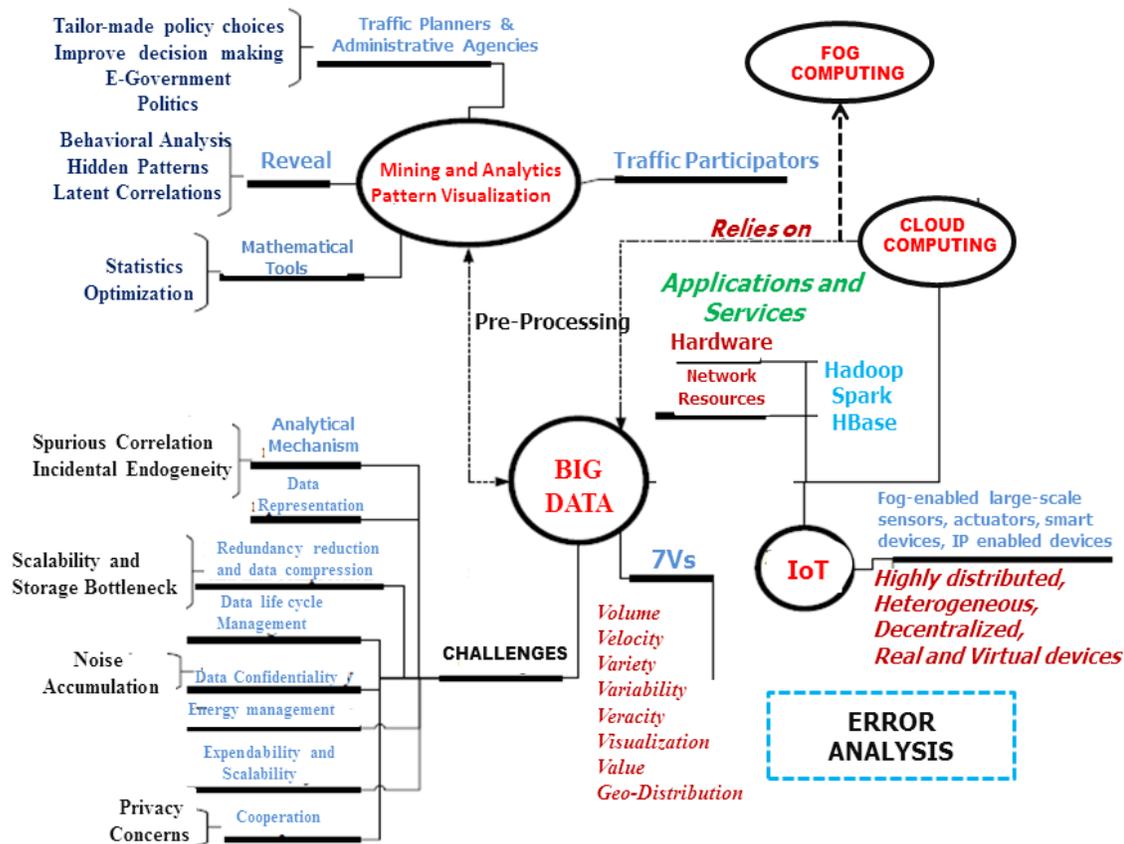

Figure 6: The conceptual Framework for Big Data-Driven Analytics and Optimization of Smart City based on Cloud and Fog Platforms

2. Opportunities in Runtime Phase

i) Dynamic Orchestration of Fog Resources:

Apart from the initial placement, all workflow components dynamically change in response to internal transformations or abnormal system behavior. IoT applications are exposed to uncertain environments where execution variations are commonplace. Because of the degradation of consumable devices and sensors, capabilities such as security and reliability that initially were guaranteed will vary, resulting in the initial workflow being no longer optimal or

even totally invalid. Furthermore, the structural topology might change according to the task execution progress (that is, a computation task is finished or evicted) or will be affected by the execution environment's evolution. Abnormalities might occur owing to the variability of combinations of hardware and software crashes, or data skew across different management domains of devices due to abnormal data and request bursting. This will result in unbalanced data communication and subsequent reduction of application

reliability. Therefore, dynamically orchestrating task execution and resource reallocation is essential.

ii) Incremental Computation Strategies:

The SC applications may often be choreographed through workflow or task graphs to assemble different IoT applications. In some domains, the orchestration is supplied with a plethora of candidate devices with different geographical locations and attributes. In some cases, orchestration would typically be considered too computationally intensive, as it's extremely time-consuming to perform operations including pre-filtering, candidate selection, and combination calculation while considering all specified constraints and objectives. Static models and methods become viable when the application workload and parallel tasks are known at design time. In contrast, in the presence of variations and disturbances, orchestration methods typically rely on incremental scheduling at runtime (rather than straightforward complete recalculation by rerunning static methods) to decrease unnecessary computation and minimize schedule makespan.

iii) QoS-Aware Control and Monitoring Protocols:

To capture the dynamic evolution and variables (such as dynamic evolution, state transition, and new IoT operations), we should predefine the quantitative criteria and measuring approach of dynamic QoS thresholds in terms of latency, availability, throughput, and so on. These thresholds usually dictate upper and lower bounds on the metrics as desired at runtime. In normal setting, complex QoS information processing methods such as hyper-scale matrix update and calculation would lead to many scalability issues.

iv) Proactive Decision Making:

Localized regions of self-updates become ubiquitous within fog environments. The orchestrator should record staged states and data produced by fog components periodically or in an event-based manner. This information will form a set of time series of graphs and facilitate the analysis and proactive recognition of anomalous events to dynamically determine such hotspots [36].The data and event streams should be efficiently transmitted among fog components, so system outage, appliance failure, or load spikes will rapidly feed back to the central orchestrator for decision making.

3. Opportunities in Evaluation Phase: Big-Data-Driven analytics (BD²A) and Optimization

A typical SC framework congregates the diverse smart entities into a clique like structure in IoT realm and enables a bidirectional flow of energy and data among the stakeholders in order to facilitate the assets optimization. The major data sources for a data driven SC include SC sensing objects such as SG, SCADA, Connected Vehicles, On-Board Sensors (OBS), Road-Side Units (RSU), Traffic sensors and actuators, GPS devices, smart traffic lights and the web data from recommender systems, crowdsourcing, feedback modules.

Furthermore, the domain of IoT in SC applications is extended to numerous geographically distributed devices that produce multidimensional, high-volume dynamic data streams requiring a noble mix of real-time analytics and data aggregation. Figure 15.6 depicts the conceptual framework for Big Data-Driven Analytics (BD2A) and Optimization of an intelligent traffic management use-case based on Cloud and

Fog Platforms. The fog orchestration module should employ efficient data-driven optimization and planning algorithms for reliable data management across complex IoT aided SC endpoints. While developing SC applications adhered to fog computing and making proper trade of such applications across different layers in the fog environment, the developers should employ robust optimization procedures that stabilizes the schema definitions, mappings, all overlapping, interconnection between layers (if any). In order to reduce data transmission latencies data processing activities and the database services may be pipelined. Rather than frequent triggering of Move-Data actions, use of multiple data- locality principles (e.g. temporal, spatial etc.) and efficient caching techniques can distribute or reschedule the computation tasks of FCNs near the sensors thereby improving the delays. The data relevant attributes related to QoS parameters such as the data-generation rate or data-compression ratio can be customized to adapt to the desired degree of performance and assigned resources to strike a balance between data quality and specified response-time targets.

A major challenge is that decision operators are still computationally time consuming. To tackle this problem, online machine learning can provision several online training (such as classification and clustering) and prediction models to capture the constant evolutionary behavior of each system element, producing time series of trends to intelligently predict the required system resource usage, failure occurrence, and straggler compute tasks, all of which can be learned from historical data and a history-based optimization (HBO) procedure. Researchers or developers should investigate these smart techniques, with corresponding heuristics applied in an existing decision-making framework to create a continuous feedback loop. Cloud machine learning offers analysts a set of data exploration tools and a variety of choices for using machine learning models and algorithms.

7. Conclusions

Due to the improvements in sensing technology and reduction in costs, sensing capabilities are expected to be integrated into everyday objects around us. There is a natural tendency that smart city applications are being built in a centralized manner. That means all the data collected by sensors are transferred to a cloud node for knowledge discovery. However, this is a very inefficient approach from both computational and communication perspectives. To address such issues, the FC paradigm has been proposed, as it brings sustainability to the smart city computations. In this work, high performance of Fog Computing over generic cloud computing is evaluated, in terms of metrics viz. latencies, power consumption etc, through a Smart Grid (SG) use-case. This paper also provides an overview of the core issues, challenges, and future research directions in fog-enabled orchestration for IoT enabled SC applications.

References

[1] L. Da Xu, S. Member, W. He, and S. Li, "Internet of Things in Industries : A Survey Internet of Things in Industries : A Survey," *IEEE Trans, Industrial informatics*, vol. 10, no. November, pp. 2233–2243, 2014.

[2] I. Technology, "Key ingredients in an IoT recipe : Fog Computing , Cloud Computing , and more Fog Computing," *IEEE 19th International Workshop on Computer Aided Modeling and Design*

of Communication Links and Networks (CAMAD), Athens, 1-3 Dec. 2014, pp. 325–329.

[3] Z. Lv *et al.*, "Next-Generation Big Data Analytics : State of the Art, Challenges, and Future Research Topics", *IEEE Trans, Industrial informatics*, vol. 13, no. 4, pp. 1891–1899, 2017.

[4] R. Deng, R. Lu, S. Member, C. Lai, T. H. Luan, and H. Liang, "Optimal Workload Allocation in Fog-Cloud Computing Toward Balanced Delay and Power Consumption," IEEE Internet of Things Journal , vol. 3, no. 6, pp. 1171–1181, 2016.

[5] D. Alahakoon and X. Yu, "Smart Electricity Meter Data Intelligence for Future Energy Systems: A Survey," *IEEE Trans, Industrial informatics*, vol. 12, no. 1, pp. 425–436, 2016.

[6] V. C. Güngör *et al.*, "Smart grid technologies: Communication technologies and standards," *IEEE Trans, Industrial informatics*, vol. 7, no. 4, pp. 529–539, 2011.

[7] H. Zhang, Y. Xiao, S. Bu, D. Niyato, R. Yu, and Z. Han, "Computing Resource Allocation in Three-Tier IoT Fog Networks : a Joint Optimization Approach Combining Stackelberg Game and Matching," arXiv:1701.03922v1 [cs.GT] 14 Jan 2017, pp. 1–10.

[8] S. Sarkar, S. Member, S. Chatterjee, and S. Member, "Assessment of the Suitability of Fog Computing in the Context of Internet of Things," *IEEE Trans, Cloud Computing, (to be published)*.

[9] M. Chiang and T. Zhang, "Fog and IoT: An Overview of Research Opportunities," *IEEE Internet of Things Journal.*, vol. 3, no. 6, pp. 854–864, 2016.

[10] A. Pang, W. Chung, T. Chiu, and J. Zhang, "Latency-Driven Cooperative Task Computing in Multi-User Fog-Radio Access Networks," I*EEE 37th International Conference on Distributed Computing Systems (ICDCS)* , Atlanta, GA, USA , pp. 1647–1656, 2017.

[11] H. Gupta, A. V. Dastjerdi, S. K. Ghosh, and R. Buyya, "iFogSim: A Toolkit for Modeling and Simulation of Resource Management Techniques in Internet of Things, Edge and Fog Computing Environments " arXiv:1606.02007 , Tech. report CLOUDS-TR-2016-2, Cloud Comput- ing and Distributed Systems Labora- tory, Univ. of Melbourne, 2016 pp. 1–22, 2016.

[12] D. Kwon and M. R. Hodkiewicz, "IoT-Based Prognostics and Systems Health Management for Industrial Applications," Special section on trends and advances for Ambient Intelligence with Internet of Things (IoT) systems, *IEEE Access,* pp. 3659–3670, 2016.

[13] C. Perera, Y. Qin, J. C. Estrella, S. Reiff-Marganiec, and A. V. Vasilakos, "Fog Computing for Sustainable Smart Cities: A Survey," ACM Computing Surveys 2017 (to be published).

[14] K. Birman, L. Ganesh, and R. Renesse, "Running smart grid control software on cloud computing architectures," *Proc. Work. Comput. Needs Next Gener. Electr. Grid*, pp. 1–28, 2011.

[15] O. Osanaiye, S. Chen, Z. Yan, R. Lu, K.-K. R. Choo, and M. Dlodlo, "From Cloud to Fog Computing: A Review and a Conceptual Live VM Migration Framework," *IEEE Access*, vol. 5, pp. 8284–8300, 2017.

[16] S. Yi, C. Li, and Q. Li, "A Survey of Fog Computing : Concepts , Applications and Issues," Proceedings of the 2015 Workshop on Mobile Big Data, pp 37-42, Hangzhou, China — June 21 - 21, 2015.

[17] M. Taneja and A. Davy, "Resource Aware Placement of Data Analytics Platform in Fog Computing," *Procedia Comput. Sci.*, vol. 97, pp. 153–156, 2016.

[18] L. Jiang, L. Da Xu, H. Cai, Z. Jiang, F. Bu, and B. Xu, "An IoT-Oriented Data Storage Framework in Cloud Computing Platform," *IEEE Trans, Industrial informatics*, vol. 10, no. 2, pp. 1443–1451, 2014.

[19] A Zanella, N. Bui, a Castellani, L. Vangelista, and M. Zorzi, "Internet of Things for Smart Cities," *IEEE Internet Things Journal.*, vol. 1, no. 1, pp. 22–32, 2014.

[20] F. Tao, Y. Cheng, L. Da Xu, L. Zhang, and B. H. Li, "CCIoT-CMfg: Cloud computing and internet of things-based cloud manufacturing service system," *IEEE Trans, Industrial informatics*, vol. 10, no. 2, pp. 1435–1442, 2014.

[21] Ye Yan, Yi Qian, Hamid Sharif, and David Tipper, "A Survey on Smart Grid Communication Infrastructures : Motivations , Requirements and Challenges A Survey on Smart Grid Communication Infrastructures : Motivations , Requirements and Challenges," *IEEE Coomunication Surveys & tutorials*, vol. 15, no.1, first2013 pp. 1–16, 2013.

[22] K. Akkaya, A. S. Uluagac, A. Aydeger, and A. Mohan, "Secure Software Defined Networking Architectures for The Smart Grid."

[23] F. A. Kraemer, A. E. Braten, N. Tamkittikhun, and D. Palma, "Fog Computing in Healthcare–A Review and Discussion," *IEEE Access*, vol. 5, pp. 9206–9222, 2017.

[24] V. C. Gungor *et al.*, "A Survey on smart grid potential applications and communication requirements," *IEEE Trans, Industrial informatics,* vol. 9, no. 1, pp. 28–42, 2013.

[25] X. Fang, S. Misra, G. Xue, and D. Yang, "Smart Grid — The New and Improved Power Grid: A Survey," *IEEE Coomunication Surveys & tutorials*, vol. 14, no. 4, pp. 944–980, 2012.

[26] A. R. Al-Ali and R. Aburukba, "Role of Internet of Things in the Smart Grid Technology," *Journal of Computer and Communications.*, vol. 3 no. 5 May, pp. 229–233, 2015.

[27] B. Alohali, M. Merabti, and K. Kifayat, "A secure scheme for a smart house based on Cloud of Things (CoT)," *6th Comput. Sci. Electron. Eng. Conf. CEEC 2014 - Conf. Proc.*, pp. 115–120, 2014.

[28] N. B. Truong, G. M. Lee, A. M. Crépeau, and R. Cedex, "Software Defined Networking-based Vehicular Adhoc Network with Fog Computing," IFIP/IEEE International Symposium on Integrated Network Management (IM) , pp. 1202–1207, Ottawa, Canada 2015.

[29] A. Khalid and M. Shahbaz, "Service Architecture Models For Fog Computing : A Remedy for Latency Issues in Data Access from Clouds," KSII Transactions on Internet & Information Systems , vol. 11, no. 4, pp. 2310–2345, 2017.

30. Yu, B.X., Ieee, F., Xue, Y., and Ieee, M. (2016) Smart Grids : A Cyber – Physical Systems Perspective", Proceedings of the IEEE , pp-1–13, 2016.

31. He, W., Yan, G., Xu, L. Da, and Member, S. (2014) Developing Vehicular Data Cloud Services in the IoT Environment", *IEEE Trans. Indus. Informatics,* **10** (2), 1587–1595.

32. Hou, X., Li, Y., Chen, M., Wu, D., Jin, D., and Chen, S. (2016) Vehicular Fog Computing: A Viewpoint of Vehicles as the Infrastructures. *IEEE Trans. Veh. Technol.*, **65** (6), 3860–3873.

33. Garraghan, P., Lin, T., and Rovatsos, M. "Fog Orchestration for Internet of Things Services", *IEEE Internet Computing*, (2017) .

34. Zhang, H., Xiao, Y., Bu, S., Niyato, D., Yu, R., and Han, Z. Computing Resource Allocation in Three-Tier IoT Fog Networks : a Joint Optimization Approach Combining Stackelberg Game and Matching", *IEEE Internet of Things Journal*, 1–10, 2017.

35. Okafor, K.C., Achumba, I.E., Chukwudebe, G.A., and Ononiwu, G.C. (2017) Leveraging Fog Computing for Scalable IoT Datacenter Using Spine-Leaf Network Topology. Hindawi Journal of Electrical and Computer Engineering Volume pp-1-11, 2017,

36. Gubbi, J., Buyya, R., Marusic, S., and Palaniswami, M. (2013) Internet of Things (IoT): A vision, architectural elements, and future directions. *Futur. Gener. Comput. Syst.*, **29** (7), 1645–1660.