Edge-centric Computing: Vision and Challenges

Pedro Garcia Lopez
Universitat Rovira i Virgili

Alberto Montresor
University of Trento

Dick Epema
Delft University of Technology

Anwitaman Datta
Nanyang Technological University

Teruo Higashino
Osaka University

Adriana Iamnitchi
University of South Florida

Marinho Barcellos
Universidade do Vale do Rio dos Sinos

Pascal Felber
University of Neuchatel

Etienne Riviere
University of Neuchatel

This article is an editorial note submitted to CCR. It has NOT been peer reviewed.
The authors take full responsibility for this article's technical content. Comments can be posted through CCR Online.

ABSTRACT

In many aspects of human activity, there has been a continuous struggle between the forces of centralization and decentralization. Computing exhibits the same phenomenon; we have gone from mainframes to PCs and local networks in the past, and over the last decade we have seen a centralization and consolidation of services and applications in data centers and clouds. We position that a new shift is necessary. Technological advances such as powerful dedicated connection boxes deployed in most homes, high capacity mobile end-user devices and powerful wireless networks, along with growing user concerns about trust, privacy, and autonomy requires taking the control of computing applications, data, and services away from some central nodes (the "core") to the other logical extreme (the "edge") of the Internet. We also position that this development can help blurring the boundary between man and machine, and embrace social computing in which humans are part of the computation and decision making loop, resulting in a human-centered system design. We refer to this vision of human-centered edge-device based computing as *Edge-centric Computing*. We elaborate in this position paper on this vision and present the research challenges associated with its implementation.

1. INTRODUCTION

In many areas of human society, there is a recurrent struggle between the forces of centralization and the forces of decentralization. In federal states, power may shift back and forth between the federal government and the constituent states. Energy generation was first concentrated in large power plants but is now moving to decentralized power grids.

In computing, we have witnessed similar shifts between centralized and decentralized control. In the 1980s a wave of decentralization led to a shift away from centralized mainframes to PCs and local networks, which culminated in fully decentralized systems using peer-to-peer and autonomous computing approaches.

Recent years have seen a proliferation of powerful computing devices at the user-facing end of the Internet. High capacity mobile devices, always-on and dedicated Internet connection boxes and home routers, or high-bandwidth pervasive wireless networks are prominent examples. We also faced simultaneously an important wave of centralization. The control, data and intelligence of computing systems moved back to the cloud, dematerialized but nonetheless centralized computing systems.

Clearly, cloud computing with the enormous capacities of its dedicated data centers and the use of simple centralized architectures creates effective economies of scale. However, we believe that when pushed to such a logical extreme, full centralization brings more harm than good in several ways. The first fundamental problem is the loss of privacy by releasing personal and social data to centralized services such as e-commerce sites, rating services, search engines, social networks, and location services. A second fundamental problem is the complete delegation of the applications and systems control from the users to the cloud, which requires unilateral trust from clients to the clouds and prevents establishing finer grain trust between users. Third, there is the missed opportunity of exploiting the enormous amount of computational, communication, and storage power of modern personal devices. Finally, centralization hampers novel human-centered designs that would allow blurring the boundaries between man and machine and emerge novel applications.

We position in this paper that the advent of clouds should not be the final paradigm shift, and that a new decentralization wave is necessary. We advocate for *Edge-centric Computing* as a novel paradigm that will push the frontier of computing applications, data, and services away from centralized nodes to the periphery of the network. We position that this paradigm will retain core advantages of using clouds as a support infrastructure but will put back the control and trust decisions to the edges and allow for novel, human-centered computing applications.

We consider a node-oriented view of the Internet consisting of data centers and clouds at the *core* as illustrated in Figure 1. Surrounding this core are smaller web servers and content distribution networks as the next layer, which is in turn followed by the "edge" consisting of individual human-controlled devices such as desktop PCs, tablets, smart phones, and nano data centers (stable computing devices such as routers or media centers). The next layer of IP-enabled sensors and embedded processors is ignored in the context of this paper, as we focus on human-operated devices. Note that this view of the Internet stands in contrast to a network-oriented view in which the network itself is regarded as the core, and all computing devices and systems small and large are considered to be edge devices.

Edge-centric Computing encompasses the following ele-

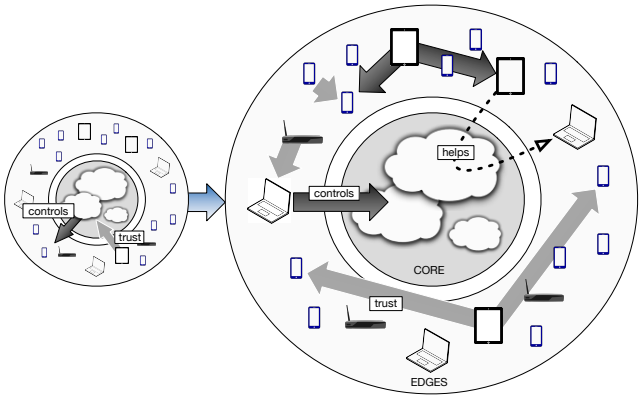

Figure 1: Centralized cloud model (left) versus Edge-centric Computing (right).

ments:

- *Proximity is in the edge*: This is the old but still valid argument of peer-to-peer (P2P) systems and content distribution networks (CDNs). It is more efficient to communicate and distribute information between close-by nodes than to use far-away centralized intermediaries. Here, "close-by" can be understood both in a physical and a logical sense.
- *Intelligence is in the edge*: As miniaturization still continues and computing capacity still increases, edge sensors and devices become more powerful. This opens the way to autonomous decision-making in the edge such as novel distributed crowdsensing applications, but also human-controlled actuators or agents reacting to the incoming information flows.
- *Trust is in the edge*: Personal and social sensitive data is clearly located in the edge. The control of trust relation and the management of sensitive information flows in a secure and private way must therefore also belong to the edges.
- *Control is in the edge* The management of the application and the coordination also comes from the edge machines that can assign or delegate computation, synchronization or storage to other nodes or to the core selectively.
- *Humans are in the edge*: Human-centered designs should put humans in the control loop, so that users can retake control of their information. This should lead to the design of novel crowdsourced and socially informed architectures where users control the links of their networks. Finally, is also opens opportunities for novel and innovative forms of human-centered applications.

We do not see Edge-centric Computing as only implying purely decentralized or P2P systems. An Edge-centric Computing architecture may consist of a federation of edge-centric distributed services deployed across data centers and nano data centers, and accessible from edge devices. Furthermore, following the decentralized nature of Internet services such as e-mail, hybrid edge services may be deployed by different vendors and be able to talk to each other. We foresee interesting scenarios where Edge-centric Computing services may be the natural decentralized evolution of a variety of Personal and Social communication and storage services.

2. RELATED FIELDS

Content Delivery Networks: The term Edge Computing was coined around 2002 and it was mainly associated with the deployment of applications over CDNs, when some large companies announced deals to distribute software through CDN edge servers. The main objective of this approach was to benefit from the proximity and resources of CDN edge servers to achieve massive scalability. In this early flavor of Edge Computing, the "edge" was restricted to CDN servers distributed around the world. This architectural model was studied and extended by several researchers, notably for deploying and replicating applications in CDNs [8].

Our vision of Edge-centric Computing goes far beyond this initial approach linked to CDNs. In our view, the edge is not restricted to CDN nodes but it can also include the myriad of user devices and sensors that are at the periphery of the network. Furthermore, we consider additional aspects beyond just proximity, by also taking into account trust, intelligence, and humans.

P2P: P2P computing is not only a field closely related to edge computing, it is also its main precursor. The term P2P was first introduced around 2000 with the appearance of popular file-sharing systems such as Napster and Kazaa. Since then, it has grown to be an important subfield of distributed systems, where decentralization, extreme scalability, tolerance to high levels of churn, and protection against malicious behavior have been major topics of research. Among the main achievements of the field one can mention *distributed hash tables* that later evolved in the more general paradigm of distributed key-value store in cloud computing; *generalized gossip protocols* that have been successfully used for complex tasks beyond simple information diffusion, e.g., data aggregation and topology management; or *multimedia streaming*, in the form of video on-demand, live TV, person-to-person communication, etc.

Unfortunately, the P2P term has always been tainted by its use for illegal file sharing and the wide media coverage of the associated prosecution and lawsuits. As a consequence, a number of commercial technologies that are actually based on the P2P paradigm do not acknowledge it (e.g., Akamai's NetSession interface).

The edge-centric computing paradigm originates from P2P but expands to new avenues. It avoids the naive pursuit of the "decentralization myth" that considers decentralization as a cure-all. Instead, it extends the concept of peer to all the devices at the edge of the Internet, and blends P2P computing with the cloud.

Decentralized Cloud Architectures: Cloud computing is a naturally centralized paradigm, with storage and processing resources hosted within large data centers. Nevertheless, there have been many efforts in recent years to combine P2P and Cloud computing architectures. On the one hand, Cloud services can strengthen P2P systems by providing them with stable resources when necessary, e.g., when facing high churn or sub-critical peer populations. On the other hand, P2P can reduce the operating costs of Cloud services by contributing additional resources, and they can enhance them by providing geographical diversity and proximity to customers.

Along these lines, various peer-assisted [10] services have recently emerged, combining peer and cloud resources in hybrid architectures. For example, researchers have shown that a hybrid architecture where resources at the peers (band-

width, storage) are complemented with temporary usage of Cloud storage services can perform comparably to traditional client-server architectures but at a fraction of the costs [10].

Another interesting line of research is the use of relatively stable peer resources to build nano data centers [5], micro clouds, community clouds, or edge clouds [9]. For example, in [5] all the home appliances are controlled and managed centrally by the telecommunication provider. In contrast, our vision of edge-centric computing systems is user-centric and the control comes from the edges towards the core, not the other way around.

Fog Computing: Fog Computing is a recent research field that has substantial overlap with Edge-centric Computing. As defined by CISCO [2], *"Fog Computing is a paradigm that extends Cloud computing and services to the edge of the network."* Proximity to end-users, dense geographical distribution, and support for mobility are the main distinguishing characteristics of Fog Computing.

Fog Services [1] may be hosted by the network, or even in end devices such as set-top-boxes or access points. The major benefit is the combination of proximity with intelligence in the edge to obtain real-time or predictable latency for a number of applications. Fog Computing is thus well positioned for real time data processing and analytics.

Finally, in the same line that Fog Computing, [7] propose an open application model based on swarmlets to bridge the gap between cyber-physical systems (sensors, actuators) and the Cloud benefiting from proximity and intelligence in the edge. Again, our vision of edge-centric computing is more focused on human-driven applications controlled from the edges of the network.

3. RESEARCH CHALLENGES

3.1 Human-driven distributed systems

The defining aspect of Edge-centric Computing is the key role of humans. Human-centered designs should put users in the control loop, so that they can retake control of their information. The massive proliferation of personal computing devices is opening new human-centered designs that blur the boundaries between man and machine.

Employing powerful capability of mobile devices such as smartphones has become a promising approach for large-scale environmental and human-behavioral sensing. Several techniques for mobile phone sensing [6] and opportunistic sensing [3, 4] have been proposed.

This should lead to the design of novel socially-informed architectures where users control the information provided or aggregated in a secure way. There is an important research challenge in designing novel safe methods for including humans in the data-analysis loop through means such as crowdsensing.

Users acting as sensors may create enormous flows of useful information in the context of the Internet of Things. Humans then become an important source of training data for learning algorithms, data analytics and visualization tools.

Classical centralized architectures to such crowd-sensing and crowdsourcing information may entail strong privacy risks. An important challenge is thus to design secure and sensitivity-aware edge big data analytics systems respecting users privacy. There are strong ethical issues related to centrally monitoring edge users. Edge-centric Computing can provide the platform to get the services without paying the costs for aggregated personal information.

Finally, the analysis of human activity and their interactions with physical and digital artifacts will also be extremely useful for closing the control loop of adaptive distributed systems. This may open a new research playground for distributed systems that adapt to user behaviors in different contexts.

3.2 Edge Architectures and Middleware

An important difference with P2P approaches is that these new architectures may rely on novel edge-centric distributed services deployed in data centers. Novel standard distributed services must be created for rendezvous, communication, computation, content distribution and storage for edge nodes. These services should enable the distribution of applications across datacenters and edge devices, while ensuring end-user control and privacy. Novel programming abstractions and middleware for Edge-centric Computing applications and services will be required as well.

Edge-centric Computing goes beyond the hybrid cloud model where one part is trusted and the public one is not. Edge-centric Computing is based on a decentralized model that interconnects heterogeneous cloud resources controlled by a variety of entities. Novel combinations of overlay technologies with cloud resources may open new research possibilities.

Another important difference is that the inherent nature of churn and transient availability of P2P may be overcome by the reliance on stable resources for edge applications. This will naturally allow for novel design alternatives that have not been previously addressed in the P2P community.

Finally, an important challenge for edge architectures will be to find the correct tradeoffs between mobile terminals and cloud servers. Minimizing computation and battery exhaustion in mobile terminals while ensuring privacy and security will represent novel and interesting research challenges.

3.3 Security and Privacy

Edge-centric Computing goes beyond previous attempts on using E2E (End-to-End) encryption and user-centric privacy systems that try to protect users information in the cloud. Edge-centric architectures will challenge researchers in new ways. Beyond encryption to protect private information, more secure proxies will be needed for rendezvous, communication, and access control using different techniques like re-encryption or attribute-based encryption among others. Furthermore, novel secure middleware for privacy-aware information sharing must be created to boost edge-centric systems.

Many existing works on cloud security such as encrypted data stores, queries over encrypted data, homomorphic systems could contribute to the creation of novel edge-centric services. An important difference with traditional cloud security research is that Edge-centric Computing may assume the existence of trusted, or partially trusted, stable resources performing some communication, persistence, queries, and even computation for applications deployed and controlled in the edges. Edge-centric computing may also consider the coexistence of trusted nodes with malicious ones in distributed edge-based overlays. This will again require secure routing, redundant routing, trust topologies and previous P2P research applied to this novel setting.

Finally, another key difference is that Edge-centric Com-

puting prevents the concentration of information as compared to centralized computing. Previous cloud security research on fragmentation of information combined with encryption may converge with decentralized overlay technologies to ensure appropriate data protection for sensitive data. Furthermore, secure cloud queries and computation over fragmented data and indexes in overlay networks may create entirely new models respecting the privacy of sensitive information.

3.4 Scalability

Scalability is a recurring research challenge both in peer-to-peer and cloud computing settings. The design of architectures that scale to millions of users must take into account issues like fault-tolerance, churn, elasticity and many others. In P2P, churn and dynamism complicate the feasibility of these architectures and their overall service availability. In cloud computing, scaling and elasticity are recurrent topics, and even major cloud providers may be overcome by massive denial of service attacks.

Edge-centric Computing, however, changes completely the scalability challenges presented before. Churn is not such a limiting factor anymore, thanks to the use of stable cloud resources. A major challenge is the correct tradeoff between computing and communication responsibilities between edge devices, trusted servers and untrusted services.

Given that the control is in the edges, scaling problems are still very relevant. Building massive overlays combining mobile devices with limited batteries with stable cloud resources require special attention for communication protocols among nodes. Furthermore, cloud edge services must also be efficient and take into account the heterogeneous nodes they must be serving.

Another research challenge is the combination of scalability with security in massive overlays. Edge architectures requiring security will impose non-negligible overheads due to encryption, that must be dealt with to provide scalability.

4. SCENARIOS

4.1 Personal Spaces in the Edge

Our digital life is now scattered among a myriad of devices and applications in the Cloud. We have files in Dropbox, our email in Gmail, selected photos in Instagram, our work contacts in LinkedIn, and our social network in Facebook. And the rest of our information, such as work data and personal data (photos, videos, finance data, and health data), is spread on hard disks and a variety of user devices.

In the next years, Personal Information Spaces will emerge to unify the multiple flows of our entire digital life. All our personal information will be stored in the Cloud, and we will have mechanisms to let third-party applications access part of our data repositories. In this context, Edge-centric Computing can offer:

Trust and Control: A strong challenge of future Personal Information Spaces is privacy and user-control of their own information. In the next years, Edge-centric Computing will enable a novel generation of user-centric Personal Spaces where users will be able to decide which parts of their information silos can be accessed by third-party applications, but also by third-party users. This requires the design of novel architectures offering controlled privacy-aware data sharing and advanced access control mechanisms.

User information may be stored in Cloud providers, but with encryption and privacy guarantees that will ensure that the Cloud provider cannot access users data without permission. Furthermore, secure queries should enable users to look for data in their Personal Information Spaces without the cloud provider being able to infer information about them (blind servers).

Another key aspect is trust in other users or entities that may establish different kinds of social links. This is essential for sharing information with others and for collaborative interactions between participants. These connections can be permanent or spontaneous. An example of permanent connection is members of a family sharing their photos, videos, songs, books, apps and other purchased digital content. An example of spontaneous collaboration is for example the transient overlapping of two Personal Spaces to share some information at some time.

Humans: Human-centered Personal computing is here to stay since we are surrounded by connected devices. This is in line with existing research efforts in Pervasive Computing, invisible computing, ubiquitous systems and augmented reality interfaces.

Edge-centric Computing architectures will produce distributed systems that adapt to user behaviors depending on their location or context. It will also handle the interaction with other humans through their available connected devices. Every human will carry multiple mobile devices (phones and wristwatches) and sensors (such as bands and implanted devices). These devices may obtain information from their owner (health, sensory), from other close-by devices in their location, from other close-by devices from other users, and from remote links through the Internet.

Furthermore, users may participate in secure distributed crowdsourcing platforms where they provide part of their selected personal data to external analytic systems. Imagine a user letting a third company access their energy usage at home to optimize her bill. The design of such infrastructures will pose serious challenges to distributed systems and security researchers.

Proximity and Intelligence: Our Personal Space must adapt to our current location: at home, at work, in the car, walking in the street, in a mall, in an airport, etc. An important aspect of the design of these edge distributed architectures is that they will be decentralized, and that the different information flows will belong to heterogeneous services and entities. Interaction, synchronization and content distribution that benefit from proximity will play important roles in the design of such systems.

Edge-centric Computing may also become a key facilitator for the deployment of personal agents and multi-agent systems in a variety of scenarios. Agents may receive flows of information from external entities and even react to these flows. Edge-centric Computing platforms may provide the needed communication, discovery and trust platforms for the deployment of agents.

There are a lot of research challenges involved in the paradigm shift towards more edge-centric autonomous agents. Whereas current centralized models limit the possibilities of agents, placing trust in the edges may facilitate the necessary peer interactions among agents.

4.2 Social Spaces in the Edge

Most current online social networks (OSNs) such as Facebook and LinkedIn impose a centralized model with a datas-

tore owned by the company that maintains all their data and that is accessed by the users. Of course, users are aware of the business model behind such OSNs, based on advertising or paid premium services.

Like in many previous works we argue that this centralized model is a serious danger to the privacy of users. But decentralized OSNs such as Diaspora do not have enough traction since they imply costly installations for the users. Semi-decentralized or federated alternatives such as Quitter also imply trust in the federated server which in fact follows a centralized data store model for their own users.

We argue that Edge-centric Computing hybrid architectures may be an adequate solution for OSNs for the following reasons:

Trust and Control: Privacy in these novel architectures may be achieved combining end-to-end security with semi-trusted data center support for Edge-centric Computing. Secure and sensitive information such as friend lists, online social profiles, log of computer-mediated social interactions should be carefully protected and controlled by the users.

On the one hand, users will not be forced to install and administer complex server software, which will reduce the barrier for entering the network. Data center support for Edge-centric Computing will offer the necessary secure infrastructure for social interactions. Such technologies should be open and standardized such as open Internet protocols in order to reach traction as OSN communication means between users.

On the other hand, the combination of cloud security and P2P technologies may create novel systems where even compromised servers may not imply a leakage of users sensitive data. A lot of research challenges emerge here to make feasible this kind of networks. Since any mobile device or even server may be compromised by attacks, such system will in the end have to reach a trade-off between affordable security and users interaction. What privacy guarantees can be given assuming some inevitable leakages to edge nodes?

Humans: Social networks are at the heart of human-driven distributed systems where connections are established between human (and their associated devices). When the underlying connection architecture reflects those human connections, many research challenges may arise in distributed systems. For example, previous P2P research on secure routing, reputation and trust may be applied to this new setting where the edge topology is driven by human interactions.

Another critical issue is social networks as valuable sensors of human activity. When information is not centralized, the access and aggregation of social information may be extremely useful for a number of applications.

There are important research challenges to create open platforms that permit third-party applications access to selected information in their social networks in a privacy-sensitive way. What protocols need to be in place for social apps to work? How to protect data from such applications reporting it to a third party? What new social activity would be enabled by edge-based OSNs?

Another important challenge is human collaboration (Computer Supported Cooperative Work) thanks to Edge-centric Computing platforms. Social Networks may evolve to provide human participation in heterogeneous groups. For example, new edge platforms may facilitate citizen participation and the reinforcement of social links in local communities. Novel distributed services may be designed for this kind of services addressing the participation of mobile devices and server resources from adhoc or permanent collaborative groups.

Proximity and Intelligence: Location or physical proximity may be also relevant for the interactions in close-by social spaces such as companies, universities, neighborhoods or even bars and pubs among others. In this case, direct connections using Bluetooth, Wifi Direct, and short range technologies may be key to establish close-by communications between social spaces. This involves a combination of direct connections between mobile devices and connections between server edge resources. Proximity in these cases should be key to provide the correct tradeoffs that minimize the computational and battery costs of mobile devices involved in these communications.

When the information of these massive social networks is not controlled by a single centralized entity a wealth of information is then accessible to authorized third parties. Mining the deep social web creates interesting opportunities to intelligent agents, crawlers, and authorized applications. Matching and searching applications such as Dating, Work, Reputation, or even sales can then be controlled by the own users.

Previous work on recommender systems could now be applied to this massive edge social networks. But novel intelligent agents and assistants may benefit from this source of knowledge to extract useful information for groups or users. In this field we can also consider data sensitivity agents that may help users to simplify the protection and exposure of their own information in these networks.

4.3 Public Spaces in the Edge

Public Spaces are the more challenging and complicated scenarios for the next generation of distributed systems. They can include Smart Cities, Smart Grids, Smart Transportation Systems, IoT (Internet of Things), or IoE (Internet of Everything).

The public space is also the confluence of a myriad of Personal and Social Spaces that interact in public locations such as streets, roads, buildings or stadiums. For this reason, many of the aforementioned challenges in the two previous sections may partially overlap with the challenges of the public space.

Another important reason is efficiency and real-time interactions. Support for mobility and proximity implies that fast responses to users or devices (cars, M2M) are much more efficient if they do not require the intervention of a central party. The IoE implies a variety of heterogeneous mobile and fixed computing devices interacting with each other in different ways. This clearly precludes centralized designs and favors Edge-centric Computing hybrid architectures.

Trust and Control: Every end-user participates in the public space through its own mobile devices and sensors. A mobile user in the public space may switch between different service providers and contexts that may compromise its security and privacy.

When users (and their devices) are exposed to a huge variety of different interactions with service providers and sensors, novel technologies are required to preserve their security and privacy across domains. In particular, novel edge distributed technologies should help end-users to perform threat analysis and to protect (or be aware) accordingly to close-by risky interactions.

Again, edge technologies should seamlessly integrate with

their own cloud-based security/privacy schemes. As the user moves in the public space, she may generate flows of information that may compromise her own privacy. The interactions of the user that requires access to Cloud technologies should guarantee the confidentiality and security of users content and sensitive information.

Finally, Edge-centric Computing trust mechanisms should make end-users active participants of the public space. Instead of the passive citizen as a sensor of the centralized smart city, Edge-centric Computing can promote the active participation of users in their local communities.

Open research issues include reputation systems in the public space, trusted interaction between users and sensors, or anonymous participation mechanisms, among others.

Humans: Humans are the most important factor to take into account in these novel distributed systems. Human behavior is of paramount importance as a valuable information for adaptive distributed systems.

For example, one goal of the Smart City may be to optimize energy usage, but another key goal is to improve the quality of life of its citizens. Edge distributed systems may even use personal information to provide personalized advice to some citizens. For example, if one is allergic to some specific plants, she could receive different path recommendations that avoid risky zones.

Here the information flows are bidirectional between humans and platforms. On the one hand, users generate their own flows of information that may share with the IoE environment. They can make public some personal information, or they can even capture and contribute information with their own devices (user's sensors).

On the other hand, the public space and their different service providers (advertising, entertainment, social, public institutions, sensors) may also generate information flows that may be of interest for humans and their devices. In this case, the user's intelligent agent may receive these information flows and react to them according to their user's interests.

Proximity and Intelligence: In the public space, proximity is very relevant both for analyzing close-by information and for storing local information. Like in Fog Computing [1], one of the key characteristics of Edge-centric Computing is its proximity to end-users and its support for mobility.

With the progress of M2M and IoT, the amount of data generated from Giga-ordered sensors in urban areas might become Exabyte order. In such huge data, it is difficult to store all of the data in remote cloud servers with reasonable costs. In general, neighboring geospatial data might have strong correlation not present in distant geospatial data.

Thus, it might be suitable for storing neighboring geospatial data in local edge servers (controlled by community networks, users or institutions) and providing local dependent services using those data. Since such geospatial data are welled out continuously everywhere, all of such big data cannot be stored in the cloud. Thus, we need to study about (i) what information processing are needed for treating such huge data, (ii) what analytic mechanisms are useful for those geospatial data, (iii) how and when we can discard sensing data welled out continuously and (iv) how to protect user's data obtained from user edge sensors. The solutions for such questions can really provide future safe and smart urban life to people.

5. CONCLUSIONS

Edge-centric Computing is a novel paradigm that moves the locus of control of Cloud Computing applications and services to the edges of the network. An edge may be a mobile device, a wearable device but also a nano-data center or a user-controlled device. While the fundamental reason is privacy, since Edge-centric Computing allows users to retake control of their information, leveraging user's resources and even reducing response times make edge-centric computing appealing to novel personal and social online services.

The distinguishing characteristics that we find in the edges of the network are: (i) Humans: indistinguishable from their devices in many cases, (ii) Trust: based on edge encryption under user's control, (iii) Control: coordination from trusted edges (iv) Intelligence: leveraging the resources of edge devices and (v) Proximity: edge location and support for mobility.

Edge-centric Computing is the natural confluence of peer-to-peer and cloud computing to create hybrid architectures that combine stable resources with mobile terminals. It overcomes the limitations of P2P models (churn, availability) while providing security and privacy to hybrid Edge services.

6. REFERENCES

[1] F. Bonomi, R. Milito, J. Zhu, and S. Addepalli. Fog computing and its role in the internet of things. In *Proc. of the 2nd Workshop on Mobile Cloud Computing (MCC)*, pages 13–16. ACM, 2012.

[2] Cisco Research Center Requests for Proposals (RFPs). Fog computing, ecosystem, architecture and applications. `http://www.cisco.com/web/about/ac50/ac207/crc_new/university/RFP/rfp13078.html`.

[3] R. Ganti, F. Ye, and H. Lei. Mobile crowdsensing: Current state and future challenges. *IEEE Communications Magazine*, 49(11):32—39, 2011.

[4] T. Higuchi, H. Yamaguchi, and T. Higashino. Mobile devices as an infrastructure: A survey of opportunistic sensing technology. *Journal of Information Processing*, 23(2):94—104, 2015.

[5] I. P. Kurniawan, H. Febiansyah, and J. B. Kwon. Cost-effective content delivery networks using clouds and nano data centers. In *Ubiquitous Information Technologies and Applications*, pages 417–424. Springer, 2014.

[6] N. Lane, E. Miluzzo, H. Lu, D. Peebles, T. Choudhury, and A. Campbell. A survey of mobile phone sensing. *Communications Magazine*, 48(9):140–150, 2010.

[7] E. Lee et al. The swarm at the edge of the cloud. *Journal of Design & Test*, 31:8–20, 2014.

[8] M. Rabinovich, Z. Xiao, and A. Aggarwal. Computing on the edge: A platform for replicating internet applications. In *Web content caching and distribution*, pages 57–77. Springer, 2004.

[9] M. Ryden, K. Oh, A. Chandra, and J. Weissman. Nebula: Distributed edge cloud for data intensive computing. In *Proc. of the 2nd Int. Conf. on Cloud Engineering (IC2E)*, pages 57–66. IEEE, 2014.

[10] L. Toka, M. Dell'Amico, and P. Michiardi. Online data backup: A peer-assisted approach. In *Proc. of the 10th Int. Conf. on Peer-to-Peer Computing (P2P)*, pages 1–10. IEEE, 2010.