RESEARCH ARTICLE OPEN ACCESS

Research on Edge Computing: A Detailed Study

Saptarshi Bhattacharyya
Research Associate
Department of Computer Science
St. Xavier's College (Autonomous)
30 Park Street
Kolkata - India

ABSTRACT
The success of rich cloud services has pushed the horizon of a new computing paradigm, Edge computing, which calls for processing the data at the edge of the network. Edge computing has the potential to address the concerns of response time requirement, battery life constraint, bandwidth cost saving, as well as data safety and privacy. In this paper, we introduce the definition of Edge computing, followed by several case studies as well as collaborative Edge to materialize the concept of Edge computing. Finally, we present several challenges and opportunities in the field of Edge computing.

Keywords: - *Edge Computing, Mobile Edge Computing, IoT, Computing, Cryptographic.*

I. INTRODUCTION

Edge Computing is pushing the frontier of computing applications, data, and services away from centralized nodes to the logical extremes of a network.

It enables analytics and knowledge generation to occur at the source of the data. This approach requires leveraging resources that may not be continuously connected to a network such as laptops, smart phones, tablets and sensors.

Edge Computing covers a wide range of technologies including wireless sensor networks, mobile data acquisition, mobile signature analysis, cooperative distributed peer-to-peer ad hoc networking and processing also classifiable as Local Cloud/Fog computing and Grid/Mesh Computing, dew computing, mobile edge computing, cloudlet, distributed data storage and retrieval, autonomic self-healing networks, remote cloud services, augmented reality, and more.

II. WHAT IS EDGE COMPUTING

Data is increasingly produced at the edge of the network; therefore, it would be more efficient to also process the data at the edge of the network. Previous work such as micro Data Centre, Cloudlet, and Fog Computing has been introduced to the community because Cloud Computing is not always efficient for data processing when the data is produced at the edge of the network. In this section, we list some reasons why Edge computing is more efficient than Cloud computing for some computing services, then we give our definition and understanding of Edge computing. Edge computing pushes applications, data and computing power (services) away from centralized points to the logical extremes of a network.

A. Why do we need Edge computing

i. *Push from cloud services:*

Putting all the computing tasks on the cloud has been proved to be an efficient way for data processing since the computing power on the cloud outclasses the capability of the things at the edge. However, compared to the fast-developing data processing speed, the bandwidth of the network has come to a standstill. With the growing quantity of data generated at the edge, speed of data transportation is becoming the bottleneck for the Cloud based computing paradigm.

ii. *Pull from Internet of Things:*

Almost all kinds of electrical devices will become part of IoT [The Internet of Things (IoT) is a system of interrelated computing devices, mechanical and digital machines, objects, animals or people that are provided with unique identifiers and the ability to transfer data over a network without requiring human-to-human or human-to-computer interaction.], and they will play the role of data producers as well as consumers, such as air quality sensors, LED bars, streetlights and even an Internet-connected microwave oven. It is safe to infer that the number of things at the Edge of the network will develop to more than billions in a few years. Thus, raw data produced by them will be enormous, making conventional. Cloud computing not efficient enough to handle all these data. This means most of the data produced by IoT will never be transmitted to the cloud, instead it will be consumed at the edge of the network.

III. WHAT IS MOBILE EDGE COMPUTING

Edge computing replicates fragments of information across distributed networks of web servers, which may be vast. As a topological paradigm, edge computing is also referred to as mesh computing, peer-to-peer computing, autonomic (self-healing) computing, grid computing, and other names implying non-centralized, nodeless availability.

The basic idea behind MEC is that by running applications and performing related processing tasks closer to the cellular customer, network congestion is reduced and applications perform better. MEC technology is designed to be implemented at the cellular base stations, and enables flexible and rapid deployment of new applications and services for customers. Combining elements of information technology and telecommunications networking, MEC also allows cellular operators to open their radio access network (RAN) to authorized third-parties, such as application developers and content providers. Since, MEC architecture is recently proposed, there is very few applications that had adopted this architecture. But, many case studies are proposed in recent articles. Some of the notable applications in Mobile Edge Computing are Computational Offloading, Content Delivery, Mobile Big Data Analytics, Collaborative Computing etc.

IV. FUNCTIONAL GOALS OF EDGE COMPUTING

We begin by describing the high-level features a mobile edge-cloud would aim to provide, and the accompanying security and privacy concerns users might have regarding these features when considering whether to allow their personal smartphones to be part of an mobile edge-cloud. Then, we outline the types of security and privacy guarantees users would find desirable and/or sufficient. We describe these desired features in ascending order of sophistication, and we begin with the simplest features that a mobile edge-cloud would provide.

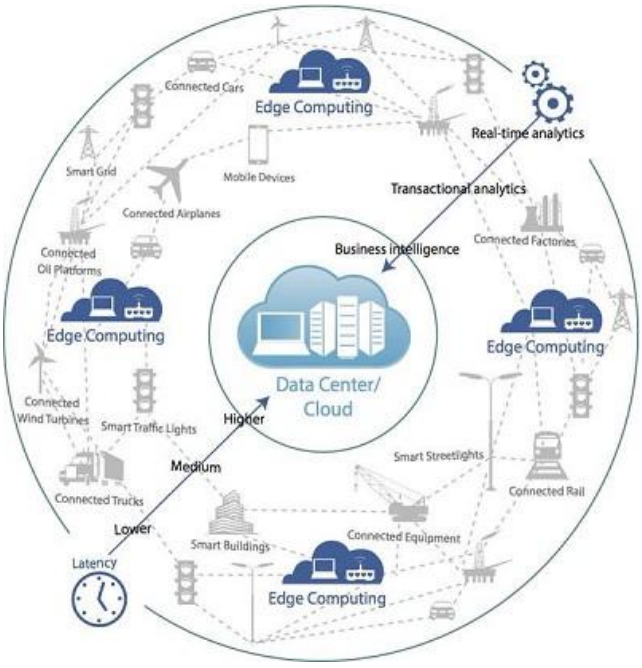

Fig. 1: Sketch Diagram Of Edge Computing

1. Remote Data Access

In its simplest form, a mobile edge-cloud can allow nodes to upload their data to a central location for some computation to process it, before each node is provided with a result aggregating the data from all the nodes in the edge-cloud. This would require nodes to either submit their own data, or allow the mobile edge-cloud to remotely access some (or all) of the data on the node. Both options would require smartphone owners to give access to some or all of the potentially private data on the node to the untrusted edge-cloud.

2.Privacy of Data

One concern edge-cloud users would have with both sending data on the node to the edge-cloud, and allowing the edge-cloud to remotely access data on the node, is that this data should not be privacy sensitive.

For instance, spectators at a ballgame may be willing to share photos and videos of the game with the edgecloud, but they not be willing to share these photos and videos if they contain images of the users themselves

in the photos and videos. Hence, users should have mechanisms available to help them decide if data being shared with an edge-cloud is privacy-sensitive.

3. Isolation of Data

Another concern edge-cloud users would have with sending or allowing remote access to data on their nodes, is whether the edge-cloud can access only data that the user

intends to share with the edge-cloud, or whether the edge-cloud can also access all other potentially private data on the node, and exfiltrate the data, leading to exposure. The edge-cloud should be able to provide users with mechanisms to ensure that only the data they intend to share with the edge-cloud is exposed, and that no other data is exfiltrated from the node. It would also be desirable for these data isolation mechanisms to be themselves trustworthy, to increase confidence in the security of the edge-cloud.

4. Remote Computation

In a mobile edge-cloud environment, network bandwidth usage can be reduced by allowing remote computation, so that small pieces of code can be sent to each node to operate on the node's data, thus eliminating the need to send all data from each node to the edge-cloud. This has two effects on the security and privacy of the edge-cloud: with remote computation, each node's data does not have to leave the node, thus improving data privacy; however, since nodes in an edge-cloud are mutually distrusting, code from other nodes is also untrusted, and running untrusted code on a node can pose security challenges.

5. Securely Executing Untrusted Code

To allow remote computation, a mobile edge-cloud must allow untrusted code from other nodes to be executed securely on the node. At a high-level, the untrusted code must not cause any harm to the node, and the untrusted code should only have behaviours necessary for completing its task.

6. Verifiable Execution

At the same time, the untrusted code in a mobile edge-cloud is also executing on a potentially hostile node. Nodes can return bogus results to avoid executing the remote code, for instance to save energy while still appearing to participate in the computation. Hence, a mobile edge-cloud should be able to verify that the remotely executed code did indeed execute correctly, and that it produced the correct results.

7. Context-aware Computing

Finally, a mobile edge-cloud can make use of the data on a node for not just computing results, but also for making scheduling and other systems decisions as part of its execution. For instance, a computation can use the location data of a node to help aggregate results, by sending a computation to nodes in the edge-cloud to instruct nodes close to each other to query each other to select the highest quality photo in that physical location. In such cases, users of nodes should be given control over whether to allow particular sensors or other data sources on the node for computation decisions. The mobile edge-cloud should also be able to identify whether contextual data on a node is being used as data in a computation, or whether it is being used as contextual data to assist the edge-cloud in making systems decisions.

8. Context Privacy

Nodes in a mobile edge-cloud should be able to provide users with controls over context data, such as location information. Users should be able to set policies on acceptable uses for this data, and the mobile edge-cloud system should then respect these policies and provide various options to users for policy violations, such as replacing context information with incorrect or less precise versions, or completely disallowing the computation.

9. Communication Substrate

Finally, the mobile edge-cloud will also require a number of auxiliary features which support the operation of the mobile edge-cloud itself. It would be challenging to implement and deploy traditional cryptographic systems in a mobile edge-cloud, such as a public-key cryptosystem. Nonetheless, a mobile edge-cloud should provide features for establishing and managing the identities of participants, and for authenticating nodes. However, it is likely that the notion of identity and authentication would be different in a mobile edge cloud with mutually distrusting participants and no pre-established cryptographic material. In addition, the mobile edge-cloud is likely to harness various protocols beneath the application-level logic for providing the mobile edge-cloud functionality. These protocols and network communications also need to be secured against malicious attackers and adversaries who may passively or actively attempt to eavesdrop on and subvert communications between edge-cloud nodes for various goals.

V. SECURITY AND PRIVACY CHALLENGES

Security and privacy concerns of users are a key obstacle deterring users from allowing their mobile devices to be participants in an edge-cloud. In this paper, we describe some of the security and privacy goals that we believe must be met for users to be convinced to participate in an edge-cloud, providing data, storage and computation on their personal mobile devices.

The first key security challenge is that all users of a mobile edge-cloud are mutually distrusting. In providing computation resources to other users, participants of a mobile edge-cloud must execute untrusted foreign code received from other users.

Allowing code from other edge-cloud participants to run on a smartphone poses a greater security risk than running third-party applications, as third-party applications downloaded through official vendor App Stores are typically subject to a vetting process to screen for malware and malicious apps, whereas mobile edge-clouds are unable to provide a central App Store nor vetting process due to the transient nature of mobile edge-clouds.

The second key challenge is that for mobile edge-cloud applications to be useful, users must be able to contribute data which they own on their mobile devices to the application. However, as mobile devices contain potentially privacy-sensitive personal data, such as contact information, photos, videos, and location information, users would be concerned about: (i) whether the data they share with the edge-cloud is privacy sensitive, and (ii) whether the edge-cloud application is able to access data on the owner's device which the owner did not intend to share with the edge-cloud application. The third key challenge is that of identity. Given that the nodes of edge-clouds are mobile devices whose owners are in close physical proximity for a short duration these mobile devices participating in the edge-cloud are likely to have never interacted with each other. In a fully mobile setting with no central processing site, it would be impossible to utilize any security mechanism which requires pre-arranged roots of trust, such as a public key cryptosystem. Hence, it would not be possible to establish identities of nodes beforehand, and it would not be possible to make use of identity-based solutions, such as message-signing or even code-signing, to gain trust in foreign code being executed.

In summary, the key security and privacy challenges facing mobile edge-clouds, are that each mobile device owner participating in the edge-cloud is an untrusted principal, there are data privacy concerns as participating devices store privacy-sensitive data, and securing communications among nodes is extremely challenging as pre-establishing identities is not possible given the transient nature of mobile edge-clouds.

VI. CONCLUSIONS

Nowadays, more and more services are pushed from the cloud to the edge of the network because processing data at the edge can ensure shorter response time and better reliability. Moreover, bandwidth could also be saved if a larger portion of data could be handled at the edge rather than uploaded to the cloud. The burgeoning of IoT and the universalized mobile devices changed the role of edge in the computing paradigm from data consumer to data producer/consumer. It would be more efficient to process or massage data at the edge of the network. In this paper, we came up with our understanding of Edge computing, with the rationale that computing should happen at the proximity of data sources. Then we list several cases whereby Edge computing could flourish from cloud offloading to a smart environment such as home and city. We also introduce Collaborative Edge, since edge can connect end user and cloud both physically and logically so not only the conventional Cloud computing paradigm is still supported, but also it can connect long distance networks together for data sharing and collaboration because of the closeness of data. At last, we put forward the challenges and opportunities that are worth working on, including programmability, naming, data abstraction, service management, privacy and security, as well as optimization metrics. Edge computing is here, and we hope this paper can bring this to the attention of the community.

VII. DECISION AND FUTURE WORK

This paper summarizes the definition of the edge computing, the outer structure of the edge computing, and the characteristics of the edge computing.

This paper also points out limitations of the current work, and also outlines directions for future research on Mobile Edge Computing.

ACKNOWLEDGMENT

The author is very much grateful to Department of Computer Science of University Of Calcutta, Kolkata for giving opportunity to work in the field of Edge Computing domain.

REFERENCES

[1] A. Khan, W. Kellerer, K. Kozu, and M. Yabusaki, "Network sharing in the next mobile network: TCO reduction, management flexibility, and operational independence," Communications Magazine, IEEE, vol. 49, no. 10, pp. 134–142, 2011.

[2] Yun Chao Hu, Milan Patel, Dario Sabella, Nurit Sprecher and Valerie Young "Mobile Edge Computing A key technology" 5th Edition

[3] M. Satyanarayanan, P. Bahl, R. Caceres, and N. Davies, "The case for vm-based cloudlets in mobile computing," Pervasive Computing, IEEE, vol. 8, no. 4, pp. 14–23, 2009.

[4] M. Hoffmann and M. Staufer, "Network virtualization for future mobile networks: General architecture and applications," in Communications Workshops (ICC), 2011 IEEE International Conference on. IEEE, 2011, p. 1–5.

[5] E. Kudoh and F. Adachi, "Power and frequency efficient virtual cellular network," in Vehicular Technology onference, 2003. VTC 2003-Spring. The 57th IEEE Semiannual, vol. 4. IEEE, 2003, pp. 2485–2489. [Online].

[6] Available: http://ieeexplore.ieee.org/xpls/abs all. jsp?arnumber=1208838

[7] Y. Zaki, L. Zhao, C. Goerg, and A. Timm-Giel, "LTE mobile network virtualization: Exploiting multiplexing and multi-user diversity gain," Mobile Networks and Applications, vol. 16, no. 4, pp. 424–432, 2011.

[8] D. Fesehaye, Y. Gao, K. Nahrstedt, and G. Wang, "Impact of cloudlets on interactive mobile cloud applications," 16th International Enterprise Distributed Object Computing Conference, pp. 123–132, Sep. 2012.

[9] A. Fischer, J. F. Botero, M. T. Beck, H. De Meer, and X. Hesselbach, "Virtual network embedding: A survey," Communications Surveys & Tutorials, IEEE, vol. 15, no. 4, pp. 1888–1906, 2013.

[10] F. Richter, A. J. Fehske, and G. P. Fettweis, "Energy efficiency aspects of base station deployment strategies for cellular networks," in Vehicular Technology Conference Fall. IEEE, 2009, p. 1–5. vol. 52, no. 1, pp. 132–139, 2014.