2017 IEEE 10th International Conference on Cloud Computing

An SDN based Framework for Guaranteeing Security and Performance in Information Centric Cloud Networks

Uttam Ghosh*, Pushpita Chatterjee†, Deepak Tosh‡, Sachin Shetty§, Kaiqi Xiong¶, Charles Kamhoua‖
Tennessee State University, TN, USA*, Old Dominion University, VA, USA†, Norfolk State University, VA, USA‡
Old Dominion University, VA, USA§, University of South Florida, USA¶, Cyber Assurance Branch, AFRL, USA‖
ughosh@tnstate.edu*, pchatter@odu.edu†, dktosh@nsu.edu‡
sshetty@odu.edu§, xiongk@usf.edu¶, charles.kamhoua.1@us.af.mil‖

***Abstract*— Cloud data centers are critical infrastructures to deliver cloud services. Although security and performance of cloud data centers have been well studied in the past, their networking aspects are overlooked. Current network infrastructures in cloud data centers limit the ability of cloud provider to offer guaranteed cloud network resources to users. In order to ensure security and performance requirements as defined in the service level agreement (SLA) between cloud user and provider, cloud providers need the ability to provision network resources dynamically and on the fly. The main challenge for cloud provider in utilizing network resource can be addressed by provisioning virtual networks that support information centric services by separating the control plane from the cloud infrastructure. In this paper, we propose an sdn based information centric cloud framework to provision network resourcesin order to support elastic demands of cloud applications depending on SLA requirements. The framework decouples the control plane and data plane wherein the conceptually centralized control plane controls and manages the fully distributed data plane. It computes the path to ensure security and performance of the network. We report initial experiment on average round-trip delay between consumers and producers.**

***Index Terms*—Network Virtualization, Information Centric Cloud Networking, Software-Defined Networking, Information Centric Networking**

I. INTRODUCTION

The evolution of cloud computing has made real time on-demand access to software, hardware platforms, and network resources feasible. The cloud technology is envisioned to sustain the explosive growth of Internet data generated by the end-users and applications provided the elastic resources are utilized efficiently and the emerging challenges related to information-centric communications are addressed. The effectiveness and usefulness of cloud technology is undoubtedly straightforward and can be inferred from the International Data Corporation (IDC)'s report that worldwide spending on public IT cloud services will leap from $70 billion in 2015 to $141 billion by 2019 [1]. Although cloud computing brings new advantages in terms of scalability, availability, resource elasticity etc., there are several downsides too. Some of the cons include: (1) resource management, (2) security and privacy concerns, (3) service quality management etc. In addition, network performance plays a key role in the successful delivery of cloud services to the end systems. Therefore, it is of utmost importance to design an efficient network service management solutions in order to sustain proliferation of cloud system users (e-businesses, public services, home network etc.) and their constantly growing content-driven demands.

Besides the intensive usage of cloud pockets across a diverse set of institutions, information has become an integral part of communication and networking between cloud entities. Cloud network traffic is mostly related to content distribution such as file handling and sharing, real time collaboration, media streaming, software services etc., which are majorly information-centric. With this vision, cloud operators are required to predict accurate performance and quality of service for the cloud enabled e-business applications based on network statistics so as to guarantee elastic demands according to service level agreement (SLA). Hence it is an urgent need to study the performance of cloud networks [2] involved in cloud data centers. Moreover, due to the variability of cloud networks, guaranteed network performance and security remain challenging, given information-centric nature of communication in the cloud domain.

Cloud computing has shown its potential in addressing scalability and adaptability to fluctuating user demands by introducing virtualization in its core. However, provisioning appropriate network support to embrace versatile group of cloud computing operators and networks remains an open question while the Internet is moving toward a content-centric direction. For these scenarios, it may be feasible to allocate computing resources but it is still unclear of how to dynamically provision network resources irrespective of the topological complexity. Therefore, in this paper we take the advantage of Information-Centric Networking (ICN) [3] and software-defined networking (SDN) [4] to develop a network virtualization framework that can guarantee stable network performance in the cloud environment as per SLA requirements. We chose ICN as a building block to our framework due to the following two reasons: (i) it can provide an efficient architecture compared to the traditional IP-based networking, (ii) by nature it replaces the current host-oriented communication model with a content-centric model. In ICN, the information can be accessed based on the identifiers (or names) of the information, instead of the identifiers of the hosts (i.e., address). Additionally, ICN also relies on location-independent naming, in-network caching,

2159-6190/17 $31.00 © 2017 IEEE
DOI 10.1109/CLOUD.2017.106

IEEE computer society

and name-based routing [5] for effective distribution of content over the network, which will definitely be a plus point to improve the cloud network performance.

Besides ICN, the other industry trend that supports flexible infrastructure and resource management for cloud operators is software-defined networking (SDN). It efficiently decouples the control plane that makes decision, including packets routing and processing, from the data plane that forwards packets to the desired destination. This separation allows network administrator to specify network services (such as routing, policy enforcement, resource management and security) using the programmable centralized control of network elements without reprogramming the underlying hardware devices individually. Altogether, these two technologies could assist in elevating the network performance according to SLA requirements. Although it is challenging to select a path that guarantees both security and performance in a large-scale cloud network, we envision that a customized network architecture should be deployed on cloud data center networks to achieve this task. The segregation of control and data planes in SDN will help to effectively integrate information-centric aspects in the cloud platform, where data flow is managed by the ICN services and is facilitated by individual providers. It could also enable provisioning different types of network services such as identification (naming), routing, in-network caching, policy enforcement and security measures for ICN. Therefore, to maintain the guaranteed network performance and security, it is of highest requirement to provide an efficient resource management and services framework by adopting the benefits of SDN and ICN technologies in cloud environment.

Motivation: Cloud users are concerned with end-to-end security and performance. However, the variability of cloud services make the performance and security metrics immeasurable. Therefore, a need for network resources provisioning in cloud data centers exists to ensure the SLA. Moreover, designing a scalable approach for selecting a user-predictable path is not an easy task. It is also a challenge to select a path for ensuring both security and performance guarantees in a large-scale cloud network. To address this, customized network protocols may be required to be deployed on cloud data center networks. Furthermore, nodes in the traditional networks are located/identified by their IP addresses, which brings serious bottleneck to the routing performance. In order to overcome this issue in cloud networks, information centric networking aspects can be applied along with virtualization. Additionally, incorporating SDN features to ICN can facilitate a centralized decision making platform for the federated cloud network, which can enable services such as identification (naming), routing, in-network caching, policy enforcement and security measures. Finally, the network virtualization provides an isolated and reliable cloud network abstracted from the underlying physical networks.

Contribution: In this paper, we propose a framework for deploying SDN enabled information centric cloud networks to efficiently handle the following:

- Decoupling of control plane and data plane.
- Cache management provides faster access to the data using in-network caching.
- Centralized routing management ensures faster, reliable, secure and bandwidth efficient route discovery.
- Network virtualization provides efficient resource abstraction and management as well as network services to ICCN customers.
- Use of ICN enables the location independent services, seamless connectivity to ICCN customers.

Paper Overview: The rest of the paper is organized as follows: the related work in the area of SDN and ICN based cloud networks are presented in Section II. In Section III, we present our proposed SDN based framework for information centric cloud networks. Section IV gives the preliminary experimental study of the proposed framework. Finally, conclusions of the paper are presented in Section V.

II. Related Works

Assessing the impact of cloud networks on the service provided to cloud users has drawn some attention from researchers in the past several years. While characterizing the impact of virtualization on network performance of Amazon EC2 cloud, [6] observed throughput instability and abnormality in delay even when the data center network is lightly utilized. This issue can be mitigated by carefully designing cloud network measurements to only use virtual instances that can at least fully utilize one CPU core. CloudCmp [7] compares the performance of different Cloud services, such as Amazon EC2, Windows Azure and Rackspace. This work focuses mostly on studying the low level performance of cloud services, such as CPU and network throughput. Some experimental platforms also have similar goals to our efforts, in terms of providing end users control over the network [8]. However, these works have not addressed the usefulness of virtualization in adapting to information-centric network requirements in the cloud computing.

To address the limitation of content-centric mobile network (CCMN), [9] discusses a cloud CCMN architecture that is aimed to serve the foreseeing multimedia traffic. They also stated that the two classical problems of content placement and request routing are yet to be addressed under the scenario of elasticity nature of cloud computing. The work presented in [10] presents a generic framework to support the information-centric Internet-of-Things (IoT) services by complementing global cloud and ICN altogether. This helped them in developing a multilayer, content- and service-centric approach to IoT data management. However, the framework has incorporated the techniques from ICN in a very loose manner which is hardly clear in the paper. In regard to cloud resource management, [2] has designed virtual network abstractions subject to QoS requirements in data center networks and [11] addresses bandwidth allocation for access networks. However, current industrial solutions focus on virtual machines rather than virtual routers and links, for example, VMware DRS clusters [12], Microsoft PRO [13], and Eucalyptus [14]. Even so, none of them can scale up to the number of hosts and VMs supported by cloud providers [15]. The existing solutions face the challenge of scaling up to the network demand of inter-cloud services. Therefore, it is of high requirement to come up with a network virtualization framework that could

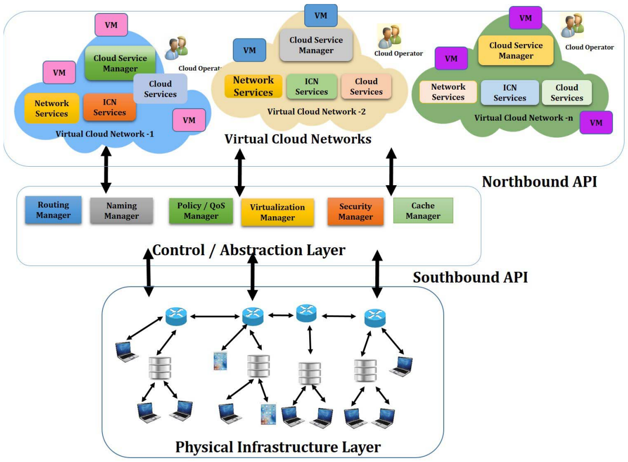

Fig. 1: The SDN based Information Centric Cloud Framework

scale up easily by migrating the control plane to a common cloud platform and provisioning ICN services on top of it. With such approach, data networking and routing across the federated cloud can be flexibly controlled without disturbing the actual physical infrastructure.

III. The Proposed Framework

The software defined networking (SDN) based framework for information centric cloud network (ICCN) is presented in Figure 1. The framework exploits the concept of SDN to separate control plane functionalities from data plane in ICCN. It mainly consists of physical cloud infrastructure layer, control / abstraction layer and virtual cloud networks.

Physical cloud infrastructure layer consists of switches (legacy or openflow), cloud servers and terminals (in information-centric networking, terminals are either consumers (cloud customers) or producers (data store)). Consumers are sending their request for any data via the Request platform API, which is responsible for interpreting the use request in ICN enabled format. Physical network consists of L2/L3 legacy and OpenFlow enabled switches (routers). When a consumer needs some data, it sends a request to Request platform which creates ICN interest packet and sends to the edge router. Upon receiving the interest packet, the router checks its content store (CS). The data is sent to the customer if it is available in CS. Otherwise the interest packet is sent to control plane and subsequently PIT is updated.

Control/Abstraction layer is a logical entity which is controlled by an SDN controller. The controller consists of security manager, policy/QoS manager, routing manager, virtualization manager, naming manager and cache manager, and resource manager.

Cache Manager keeps track of content store of each network element (routers or switches) of the ICCN infrastructure. This manager is also responsible for caching and replacement policies. It decides whether a data should be considered for caching or not. The default policy in ICCN is to cache everything. However, this may not be possible to cache everything in a large network like ICCN. In our proposed framework, cache manager can compute the frequency of use of data and cache or discard accordingly. It can be seen that if we cache the data having higher frequency of use gives lower data acquisition latency. Even though we can enforce some predefined policies to decide the content of caching. A replacement policy decides which object should be removed from the cache to accommodate new objects or data. Traditional replacement policies are FIFO, LRU and LFU.

Routing Manager is responsible for discovering routes and keeping up-to-date information of the network topology. It can efficiently locate the data and set the routes between the requested content router/switch and the content router/server which has the data.

Routing manager ensures of creating secure and performance guaranteed intra cloud end-to-end path. It creates path in the following way: Let S_j and B_j be the security level and network bandwidth of router j, where $j = 1, 2, ..., M$ and M is the number of openflow switches in the information centric cloud network. Also, let Q be a collection of the indices of all end-to-end paths in G. Denote by $D = D(b_{n_1}, ..., b_{n_K})$ and $T = T(t; b_{n_1}, ..., b_{n_K})$ the end-to-end average delay of an end-to-end service path and the percentile delay of a cloud service at time t in the path consisting of routers $n_1, n_2, ..., n_K$ for the user, respectively. Here, b_{n_j} are bandwidth allocated to router n_j and $0 \leq b_{n_j} \leq B_{n_j}$. Assume that the requirement of security, an average end-to-end delay, and a percentile delay defined in the service contractor between the user and the cloud network provider are $\hat{s}, \hat{D}$, and $(\hat{T}, \gamma\%)$, respectively. Thus, the cost efficient selection of a security and end-to-end delay-guaranteed path can be formulated as the following optimization:

$C = \min_{\forall(n_1,n_2,...,n_K)\in Q} \min_{b_{n_j},...,b_{n_K}} \sum_{j=1}^{K} c_{n_j} b_{n_j}$ subject to $min(s_{n_1}, ..., s_{n_K}) \geq \hat{s}, D \leq \hat{D}$, and $T \mid_{t=\hat{T}} \geq \gamma\%$

where c_{n_j} is a cost of per-unit bandwidth determined by the cost agreed between a user and a network provider. The challenges to solve the above optimization problem are the difficulty to calculate T and the impossibility to obtain a closed-form solution of T in general. In our proposed framework, we use SDN controller to solve the above constrained optimization problem as controller has the global view of the network.

Security Manager provides security and integrity of data in ICCN. This can be achieved by the use of public key digital signature for each data packets. Security manager is centralized and it can act as the public key infrastructure (PKI) for the key distribution in ICCN. Further, the security manager can provide authentication of consumers and producers. Therefore, it is difficult for an attacker to falsely inject any data packets in ICCN.

Policy/QoS Manager enforces policies of an ICCN for managing the network (network resources such as consumer, producer or switches). For example, a consumer can access the network resources (e.g., Internet) in a specific period of time. This type of policy can be managed by the policy manager for better utilization of network resources.

Virtualization Manager partitions the physical network resources into multiple slices (virtual network elements) which are independent and different from each other. Each slice can be assigned to different cloud operators as virtualized cloud network where cloud provider can build its own network archi-

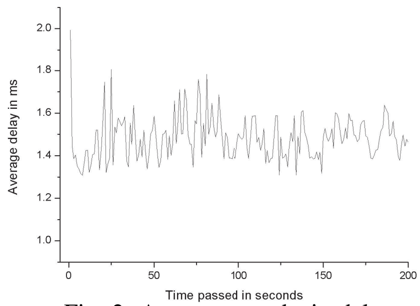

Fig. 2: Average round-trip delay

tecture with different routing, topology, caching and other ICN mechanisms. This manager further keeps up-to-date mapping information between physical and virtual network elements.

Naming Manager assigns a globally unique name to each chunk of data in ICCNs. Name consists of one or more components similar to a uniform resource locator (URL), but without any protocol, port, or host name specification. In our proposed ICCN framework, naming manager assigns and manages name spaces to the producers of the named data. Naming manager can assure the consistency and the integrity of the names published by individual producers as it is being controlled centrally.

Virtual Cloud Networks provide auto-configuration of virtual topology and network policy so that the customers can get faster cloud services. The customers can customize the size and connectivity rules of virtual cloud networks to adapt their need. The proposed framework provides ICN, network and cloud services to the customers. Cloud service manager handles basic cloud management services like managing pool of heterogeneous compute-resources, resource allocation as well as providing access to end users, security monitoring and other tracking services. Network services are specialized in coordinating, facilitating and maintaining needs and supports for different cloud users. ICN services include name resolution, seamless connectivity and faster data delivery.

IV. Initial Experimental Study

We have implemented our proposed SDN based ICCN framework in mininet emulator to conduct initial experiments. We have created openflow switches along with virtual machines (VMs). The floodlight SDN controller [16] is used to enable the content based forwarding. In order to measure the delay between requesting and receiving content we have used ccnping [17]. Ccnping is an ICN alternative to the popular application ping that can be used to confirm connectivity and measure round-trip times in IP based networks. It sends an interest packet per interval to a given destination prefix concatenated with a random value as similar to ping. It stores the time-stamp of creation when sending the packet and calculates the round-trip time on arrival of the appropriate content object (data). The ccnping servers (producers) and clients (consumers) are installed in VMs to test the connectivity and measure the round-trip delay between them.

Figure 2 shows the average round-trip delay between producers and consumers. It can be seen that the delay of first packet is around 2ms whereas the average round-trip delay is around 1.6ms. This is mainly because the first packet of every new flow with a reactive configuration takes longer delay than remaining packets. The average round-trip delay decreases once the flow rules are installed to the switches by the SDN controller.

V. Conclusions

This paper proposes an sdn based information centric cloud framework for dynamic and efficient provisioning of network resources in order to meet the dynamic demands across the federated cloud. The framework has the ability to dynamically compute the routing path to guarantee security and performance of the network. In future, we plan to perform a concrete security analysis of the architecture and implement on a real testbed. Additionally, we also aim to propose a multi-path routing scheme and cache aware routing to provide enhance network throughput and faster as well as seamless access to data for both cloud customers and service providers.

Acknowledgement

This material is based upon work supported by the NSF under award number ACI 1541348. The views and opinions of authors expressed herein do not necessarily state or reflect those of the United States Government or any agency thereof.

References

[1] "K. kelly. idc cloud research." https://www.idc.com/getdoc.jsp?containerId=prUS40960516.

[2] H. Ballani, P. Costa, T. Karagiannis, and A. Rowstron, "Towards predictable datacenter networks," in *Proceedings of the ACM SIGCOMM*, (New York, NY, USA), pp. 242–253, ACM, 2011.

[3] B. Ahlgren, C. Dannewitz, C. Imbrenda, D. Kutscher, and B. Ohlman, "A survey of information-centric networking," *IEEE Communications Magazine*, vol. 50, no. 7, pp. 26–36, 2012.

[4] D. Kreutz, F. M. Ramos, P. E. Verissimo, C. E. Rothenberg, S. Azodolmolky, and S. Uhlig, "Software-defined networking: A comprehensive survey," *Proceedings of the IEEE*, vol. 103, no. 1, pp. 14–76, 2015.

[5] M. F. Bari, S. R. Chowdhury, R. Ahmed, R. Boutaba, and B. Mathieu, "A survey of naming and routing in information-centric networks," *IEEE Communications Magazine*, vol. 50, pp. 44–53, December 2012.

[6] G. Wang and T. S. E. Ng, "The impact of virtualization on network performance of amazon ec2 data center," in *Proceedings of the INFOCOM*, (Piscataway, NJ, USA), IEEE Press, 2010.

[7] A. Li, X. Yang, S. Kandula, and M. Zhang, "Cloudcmp: Comparing public cloud providers," in *Proceedings of the 10th ACM SIGCOMM Conference on Internet Measurement*, (New York, NY, USA), 2010.

[8] "Emulab - network emulation testbed." http://www.emulab.net/.

[9] J. Tang and T. Q. Quek, "The role of cloud computing in content-centric mobile networking," *IEEE Communications Magazine*, vol. 54, no. 8, pp. 52–59, 2016.

[10] E. Borgia, R. Bruno, M. Conti, D. Mascitti, and A. Passarella, "Mobile edge clouds for information-centric iot services," in *ISCC*, IEEE, 2016.

[11] K. Xiong and H. Perros, "Service performance and analysis in cloud computing," in *2009 Congress on Services - I*, pp. 693–700, July 2009.

[12] "Resource management with vmware drs." http://www.vmware.com/pdf/vmware_drs_wp.pdf.

[13] "Microsoft performance and resource optimization." http://technet.microsoft.com/en-us/library/cc917965.aspx.

[14] D. Nurmi, R. Wolski, C. Grzegorczyk, G. Obertelli, S. Soman, L. Youseff, and D. Zagorodnov, "The eucalyptus open-source cloud-computing system," in *Proc of the CCGRID*, 2009.

[15] A. Gulati, G. Shanmuganathan, A. Holler, and I. Ahmad, "Cloud-scale resource management: Challenges and techniques," in *Proc of the HotCloud*, (Berkeley, USA), 2011.

[16] "Floodlight, an open sdn controller." http://floodlight.openflowhub.org/.

[17] "Ndn-routing/ccnping." https://github.com/NDN-Routing/ccnping.