Proceedings of the APAN – Research Workshop 2016
ISBN 978-4-9905448-6-7

Deploying and Evaluating OF@TEIN Access Center and Its Feasibility for Access Federation

Aris Cahyadi Risdianto[1], Phyo May Thet[2], Azeem Iqbal[3], Nurul Ainaa Binti Muhamad Shaari[4], Hari Krishna Atluri[5], Galih Nugraha Nurkahfi[6], Apichart Wantamanee[2], Rifqy Hakimi[6], Uzzam Javed[3], Muneeb Ahmad[3], Chaodit Aswakul[2], Muhammad U. Ilyas[3], Teck Chaw Ling[4], Arumugam Paventhan[5], Eueung Mulyana[6], and JongWon Kim[1]

1) Gwangju Institute of Science and Technology (GIST), Korea.
Email: jongwon@nm.gist.ac.kr
2) Chulalongkorn University, Thailand.
3) National University of Sciences and Technology (NUST), Pakistan.
4) University of Malaya, Malaysia.
5) ERNET (Education and Research Network) India, India.
6) Institut Teknologi Bandung (ITB), Indonesia.

***Abstract* – For the emerging software-defined infrastructure, to be orchestrated from so-called logically centralized DevOps Tower, the shared accessibility of distributed playground resources and the timely interaction among operators and developers are highly required. In this paper, by taking OF@TEIN SDN-Cloud playground as a target environment, we discuss an access center effort to address the above requirements. In providing the developer presence via the proposed access center, the inherent heterogeneity of internationally dispersed OF@TEIN resources is setting a unique challenge to cope with the broad spectrum of link bandwidths and round-trip delays. The access capability of deployed access center is experimentally verified against a wide range of access network conditions, which would be extended for futuristic access federation with appropriate identity management and resources abstraction for multiple developers and operators.**

***Index Terms* — DevOps-based automation, SDN-Cloud playground, software-defined infrastructure, multi-domain resource federation, and federated resource access.**

I. INTRODUCTION

SINCE launched in 2012, OF@TEIN has extended its capability from OpenFlow-enabled into SDN-Cloud-enabled playground[1]. As shown in Fig. 1 [1], the playground resources are deployed on the top of underlay network infrastructure that is distributed over multiple international sites and is involved with multiple network administrator domains. The playground resources are managed by logically-centralized DevOps (i.e., Development and Operations) Tower, which allows both developers and operators to perform various developments and resource management.

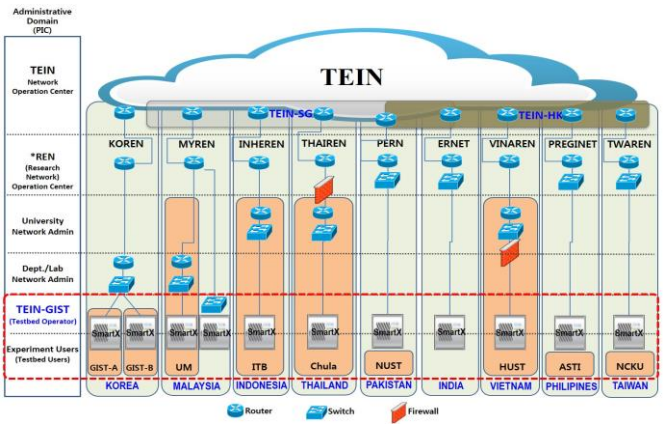

Figure 1: OF@TEIN Playground: A multi-domain SDN-Cloud testbed environment.

All authors are member of OF@TEIN Community (website: http://oftein.net).

[1] Note that we intentionally use the term 'playground' instead of 'testbed' to highlight the software-driven flexibility of shared resource pools.

In order to allow developers to perform diverse experiments, we need to provide a systematic access to the shared resources of OF@TEIN playground directly from the different access networks of all developers. Since each access network can belong to different administrative domain, we need to apply a different set of rules to manage (i.e., allow and restrict) the playground access. In order to allow the playground access, the playground operators are required to identify the diverse reachability between OF@TEIN playground and developer access networks. However, the reachability can be still limited due to bandwidth availability, routing configuration, and firewall policy of underlying access networks. Considering these limitations (or difficulties), so-called access center deployment is needed to support multiple access methods by leveraging well-known protocol/port combinations, secure access scheme, and remote desktop access scheme. This access center may be able to help the developers to utilize the playground resources, overcoming several access limitations, without the burden of additional configuration.

II. Access Center: Requirements and Related Work

There are several access requirements and related efforts that motivated the deployment of OF@TEIN access center.

A. Access Center: Requirements

The developers may need full access to the playground for playground customization and experiment execution. The access should be open any time and any location regardless of developer's sites with different time zones, institutions, and access networks. The common access hurdles are troublesome IPAM (IP address allocation and management including firewall blocking) issues and protocol-/time-of-day-based bandwidth limitations. The access may not be restricted in the sense of remote visualization. For example, the developer of video streaming experiments may want faster GUI-based access. Furthermore, remote access from different types of devices needs to be considered. Also, flexible configuration to support interactive and programmable access is required to help developers with different remote access needs.

The other access hurdles are unified (i.e., federated) authentication and heterogeneous resource abstraction with extended/expanded capability. The unified identity federation is required for centralized, policy-driven authentication to assign different levels of privileges. A simplified abstraction for heterogeneous resources is also required so that it can facilitate resource pooling by integration dispersed resources at specific locations (e.g., Chulalongkorn University Thailand, UNINET Thailand, and ERNET India).

B. Related Work

Akarsu and others discuss about gateways for seamless desktop access to high performance resources [2]. The gateway will retrieve data from different resources and allocate computational resources to process data. Thus, it hides system management and coordination from the developers. Treder et al. discuss about desktop applications for both remote and local accesses that support flexible access and remote desktop capability according to user requirements [3]. BonFire provides centralized broker service that interfaces users and federated resources of heterogeneous cloud and network testbeds. It offers user's access to resources through SSH gateway by VPN [4]. Also, Wahle et al. propose a reference-point gateway concept to federate independent testbed islands [5]. They provide web services to query and request the testbed resources.

From another perspective, Leandro et al. discuss about identity federation for access control in multi-tenancy cloud environment using Shibboleth, an authentication and authorization infrastructure based on SAML [6]. SAML standard assertion carries credentials across trusted domain boundaries, also known as tokens. Furthermore, Bhatt et al. try to maintain the confidentiality, integrity, and authentication over insecure internet connection [7]. As the communication was secured by SSLv3 and TLSv1 with CA server and Smart card client, the overall authentication time will be doubled.

III. OF@TEIN Access Center: Design

This section discusses about the design issues for access center. It includes access parameters to be considered, solution candidates, and the selection flexibility of users.

A. Key Design Issues

There are two aspects for OF@TEIN access center design. They are developer and access network requirements, respectively.

1) Developer Requirement

As discussed above, user's (developer's) requirements are important to be considered as the developers need to do experiments without constraints. The developer's access should be provided regardless the access locations (e.g., campus network, dormitory, or internet) as they may be wired and wireless connected. The access should be flexible with different access methods such as CLI-based, web-based GUI, and remote display for their specific visual experiment and verification.

2) Access Network Requirement

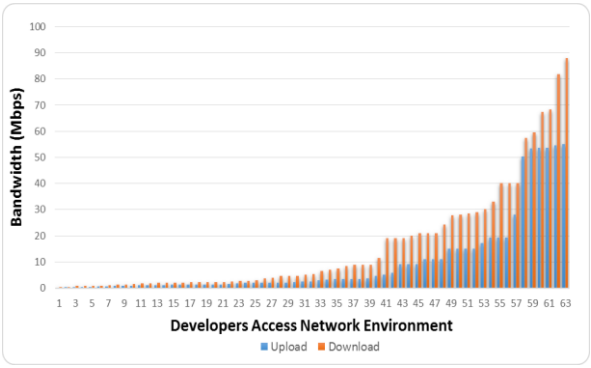

Figure 2: Developer access network: available bandwidth.

In order to provide the developer access from diverse network environments, several network parameters are considered between the developer's access network and the access center, such as *i)* basic connectivity/reachability to verify the routing configuration, *ii)* access limitations or firewall policies to ensure access scheme provided, and *iii)* the available bandwidth to predict the access responsiveness. As depicted in Fig. 2, OF@TEIN access center is tested to provide multiple access schemes from various network environments (i.e., 21 networks with 3 different access times).

B. Design for Access Center

By considering many aspects of access center design and requirements, several access solutions or approaches have been selected such as *i)* multiple points of entry for access center, *ii)* multiple access schemes with different solutions, and *iii)* access center components for deployments. The detailed design of OF@TEIN access center is shown in Fig. 3.

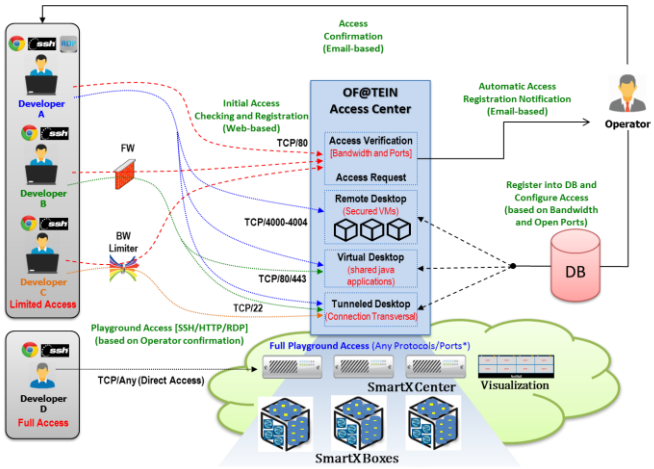

Figure 3: OF@TEIN Access Center: Design.

1) Multiple Points of Entry

Point of entry is a point where all the playground's resources/services are accessible from the developers. Currently, the design considers entry from the R&E (research and education) network with unlimited access and from internet with some selected access schemes only. It is decided to provide developer's access from their campus network as well as external network.

2) Multiple Access Methods

The script-/program-based and GUI-based accesses are required for the developers for their experiments. Several protocols or ports are however blocked/filtered due to their security performance policies. For this, the designed access center provides several access schemes such as using well-known application protocols and ports (e.g., HTTP web browsing), encrypted protocols communications (e.g., SSH remote access, HTTPs secure socket layer, or trusted Java web application), and/or remote pre-configured secured desktops (e.g., VRDP – virtual remote desktop protocol).

3) Selected Components

Several components are selected to provide the flexible access that satisfies all the considerations and requirements. The selected components for preliminary access center are:

- *Web-based portal* to verify the connectivity from developer's access network and for online access registration.
- *Bandwidth measurement web applications* to verify the available bandwidth from developer's access network.
- *Port scanner web applications* to check the access list applied in the developer's access network.
- *Connection transversal (tunneled desktop)* to provide access by translating into well-known protocol and ports.
- *Secure access for shared (virtual desktop) web application* to provide access through secure communication protocols (e.g., HTTPS).
- *Remote access to secured desktop or workstation (remote desktop)* to provide the accesses to secure dedicated virtual machine for each developers.

IV. OF@TEIN Access Center: Deployment and Verification

A. Deployment

The main task of the access center deployment is a physical box that is accessible from R&E networks (and Internet). This box is running on Ubuntu Linux OS with additional software and services (i.e., Open SSH server for secure remote access and Apache web server for web portal interface). For bandwidth measurement, we utilize *Ookla* Speedtest Mini [8] and *jnetscan* [9] port scan (as a java application). Three different access schemes are utilizing different software combinations: *i) Open SSH server* for tunneled desktop access through well-known ports, ii) Community version of *Ulteo Virtual Desktop* [10] for java-based shared virtual desktop web application, and iii) *Oracle Virtual Box* [11] for remote desktop to secure pre-configured virtual machines.

B. Measurement

In order to measure the quality of service (QoS) and quality of experience (QoE) of this preliminary access center deployment, several developers are tested and measured the access performance through several different access networks. In total, it is involved with 6 different countries (i.e., Korea, Thailand, Pakistan, Indonesia, Malaysia, and India), 10 developers, and 21 networks including R&E and public networks. The QoS measurement calculates the access setup time duration and number of packets or bytes required for the access. It simply utilizes *Wireshark* [12] network analyzer to capture all access related packets from developer's terminal to the access center. Based on the captured (*pcap* formatted) file, the traffic statistic (e.g., number of packets, number of bytes, duration between first packet and last packet, and average rate) for specific access scheme can be analyzed. The QoE measurements polled the developer's experiences during testing and measurements for different access schemes and quick feedbacks to match with their requirements.

C. *Result and Analysis*

As mentioned above, two different measurements are completed (i.e., QoS and QoE) and analyzed for further improvements in next deployment.

1) *Quality of Service based on Pcap Packet Analysis*

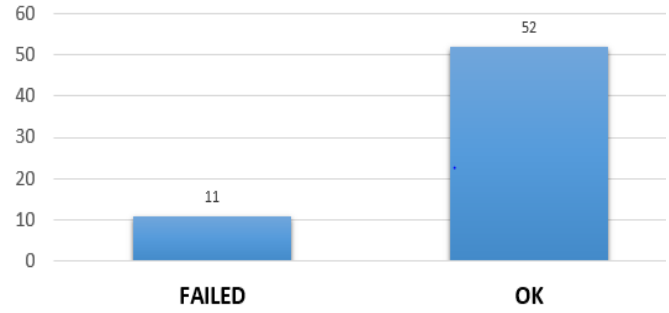

Figure 4: Access status result.

The overall testing result of all access schemes is acceptable, because approximately 83 % of accesses are successful, as depicted in Fig. 4. Less than ~17 % access problems are caused by several different aspects (e.g., developer's operating system issue, java/browser compatibility issue, and some unknown reasons), which may not be directly related with current access center deployment. However, it still needs to be considered for future work extension.

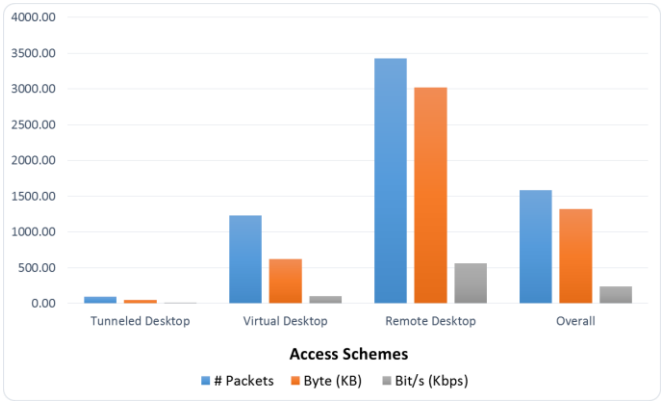

Figure 5: QoS comparison for all access schemes.

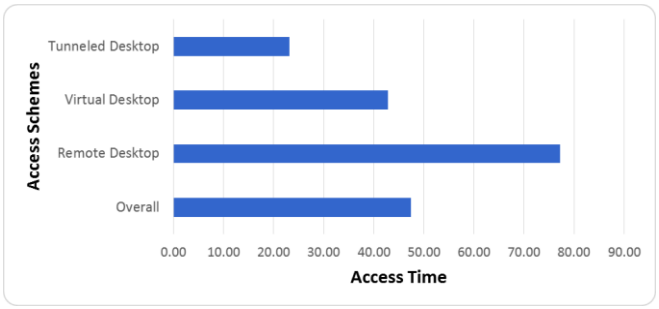

Figure 6: Access time comparison for all access schemes.

Fig. 5 and Fig. 6 show the comparison between the access schemes based on the measured access parameters. As expected, the tunneled desktop requires smallest number of packets and number of bytes, and also with fastest access setup time. It is then followed by virtual desktop and remote desktop accesses that require more packets and bytes and longer access setup time. However, tunneled desktops are only suitable for well-known applications and static TCP ports (e.g., web page, remote access, and others). Also it is required for specific configuration (e.g., TCP port translation, Linux scripting, and unique access links). Virtual and remote desktops are more useful for GUI-based experiments such as video or java-based applications.

2) *Quality of Experience based on Developers Polling*

As QoE verification from the developers, MOS-like (similar with "*mean opinion score*") value is one representative parameter for this purpose. In order to get the developer's opinion score about their access experiences, simple polling method is selected for 10 developers from different countries and access networks. The result is shown in Table 1, where the highest score for tunneled desktop followed by remote desktop and virtual desktop. However, note that overall the score is around 3.57, which are in between *"Fair"* and *"Good"* quality [13].

TABLE 1: DEVELOPERS ACCESS QUALITY OF EXPERIENCE (QOE)

NO	ACCESS SCHEMES	QOE (MOS)
1	Tunneled Desktop	4.43
2	Virtual Desktop	2.86
3	Remote Desktop	3.43
	Overall	**3.57**

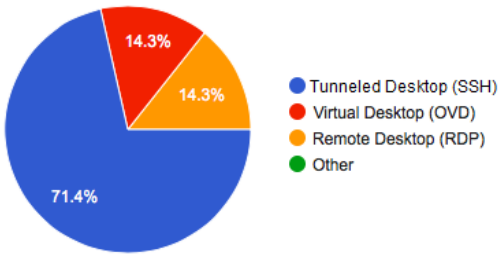

Figure 7: Preferred access schemes based on developer's experiences.

With this simple polling method, the developers also select the most preferred access *"anonymously"* in order to ensure independency. As depicted in Fig. 7, surprisingly that most all the developers are preferred tunneled desktop (based on connection transversal) access scheme than the other schemes. It is concluded that tunneled desktop is "lighter" and "faster" for accessing some specific resources in OF@TEIN playground. However, it needs to be verified continuously by observing and measuring *"real"* playground accesses during developer's experiments.

V. Feasibility Of Access Center For Access Federation

Since 2015, the focus of OF@TEIN collaboration is shifted into establishing an open collaboration consortium amongst existing and new potential collaborators, and developing a reference model to build and operate SDN-Cloud-leveraged open/shared infrastructure. Also, it hopes to establish a federation-based multi-domain SDN-Cloud playground and also a distributed support center to provide technical guide for all collaborators. Aligned with this transition, more playground resources, network domains, and developers are expected to increase and federate, while simple access and strong authentication/authorization are still needed to be considered. This section discusses more about the challenges of current work to be leveraged in the federation environment.

A. Access Federation Challenges

This work mainly focuses on "successful" access schemes to the playground for all developers and operators if required. Currently, it is not covering *authentication* and *authorization*, which defines the portions of playground resources accessible to different developers. Another important aspect for access federation is an abstraction for all federated resources into logical entities that are accessible from the access center. Additionally, the favorable access should give less resource requirements (e.g., terminal specification, bandwidth, software installation, etc.). In summary, access federation needs to solve following challenges:

- *Single identity management* to provide single-sign-on with group-based access control for multi-tenancy environment. It is possible to build trust relationships between institutions (as identity providers) and OF@TEIN playground (as resource provider).
- *Resources authorization* to provide OF@TEIN playground access policies for developers, operators to avoid resource monopoly or collision.
- *Playground abstractions* to present overlay entities of OF@TEIN playground over underlying multi-domain federated resources.
- *Access offload or network-style proxy* to minimize developer terminal requirements and speed-up the developer access to the playground resources.

B. Access Center for Access Federation

Based on the analysis on the requirements and current work results, the important items to extend in near future are:

a) *Access center (deployment enhancement)*: This is the main piece of access federation as it will federate (i.e., aggregate) all types of access (e.g., GUI or CLI) from the developers to the playground resources. But, improvements are required based on current measurement results and developer's experiences feedbacks. It also needs enhancements to provide an overlaid playground abstraction on top of underlay playground infrastructure.

b) *ID Federation:* This is an important component to provide single-sign-on authentication and resources authorization for different developers/operators. It should cover both SDN and Cloud resources. Several approaches are evaluated such as keystone federation and slice-based federation architecture (SFA).

c) *Access Box:* This additional deployment is required for access offload or network-style proxy to solve the current access limitations to the resources (e.g., low bandwidth, public IP address limitation, lack of graphical interface). It can be implemented as lightweight physical box (Pi or NUC) or virtual box (VM or container) with pre-configured operating systems and additional software.

VI. Conclusion

In this paper, OF@TEIN access center deployment is preliminary verified to provide multiple access schemes for OF@TEIN developers from multiple countries with different types of access networks. Based on QoS and QoE measurements, the preferred access scheme is tunneled desktop (based on connection transversal) access, preferred over virtual/remote desktop accesses. However, current deployment needs to be improved by considering other aspects such as single authentication and authorization, resource abstraction, and access offload, in order to provide the complete design of access federation for overlaid OF@TEIN playground over OF@TEIN underlay infrastructure.

Acknowledgement

This research was supported by 'Software Convergence Technology Development Program', through the Ministry of Science, ICT and Future Planning (S1004-14-1045). We also thank all OF@TEIN collaborators who are involved with open collaboration around OF@TEIN playground.

References

[1] Risdianto, Aris Cahyadi, et al. "OF@ TEIN: A Community Effort towards Open/Shared SDN-Cloud Virtual Playground." Proceedings of the Asia-Pacific Advanced Network 40 (2015), pp. 22-28.

[2] E. Akarsu et al., "Using Gateway system to provide a desktop access to high performance computational resources," High Performance Distributed Computing, 1999. Proceedings. The Eighth International Symposium on, Redondo Beach, CA, 1999, pp. 294-298. doi: 10.1109/HPDC.1999.805309

[3] Treder, Terry Noel, Christopher Fleck, Adam Marano, Anil Roychoudhry, and Richard James Mazzaferri. "Methods and systems for maintaining desktop environments providing integrated access to remote and local resources." U.S. Patent 9,239,666, issued January 19, 2016.

[4] David Garcia-Perez, Juan Angel Lorenzo Del Castillo, Yahya Al-Hazmi, Josep Martrat, Kon-stantinos Kavoussanakis, et al.. Cloud and Network facilities federation in BonFIRE. Federative and interoperable cloud infrastructures, August 2013, Aachen, Germany. Euro-Par 2013: Parallel Processing Workshops, 8374, Lecture Notes in Computer Science.

[5] Sebastian Wahle et al., "Technical Infrastructure for a Pan-European Federation of Testbeds", 5th International Conference on Testbeds and Research Infrastructures for the Development of Networks & Communities and Workshops, 2009. TridentCom 2009, pp. 1-8, doi: 10.1109/TRIDENTCOM.2009.4976205

[6] Leandro, M. A., Nascimento, T. J., dos Santos, D. R., Westphall, C. M., & Westphall, C. B. (2012). Multi-tenancy authorization system with federated identity for cloud-based environments using shibboleth. In Proceedings of the Eleventh International Conference on Networks, pp. 88-93.

[7] Bhatt, Deep Vardhan, Stefan Schulze, and Gerhard P. Hancke. "Secure Internet access to gateway using secure socket layer." IEEE Transactions on Instrumentation and Measurement, 55.3 (2006), pp. 793-800.

[8] "OOKLA Speedtest Mini." [Online]. Available: http://www.speedtest.net/mini.php

[9] "jnetscan." [Online]. Available: https://code.google.com/archive/p/jnetscan/

[10] "Open virtual Desktop Community Edition." [Online]. Available: http://www.ulteo.com/get-it/

[11] "Oracle Virtual Box". [Online]. Available: https://www.virtualbox.org

[12] "Wireshark." [Online]. Available: https://www.wireshark.org

[13] "Wikipedia: Mean opinion score." [Online]. Available: https://en.wikipedia.org/wiki/Mean_opinion_score

Aris Cahyadi Risdianto received the B.S. degree from Telkom University and M.S. degree from Institut Teknologi Bandung (ITB) in Telecommunication Engineering. He is currently pursuing the Ph.D. degree in School of Information and Communication at Gwangju Institute of Science and Technology (GIST), South Korea. His research interests include Cloud-Computing, Software-Defined Networking and Future Internet Architecture.

Phyo May Thet received B.Eng degree in Electronic Engineering from Technological University (Thanlyin), Myanmar, in 2011. From 2012 to 2014, she worked as a telecommunication engineer in Thailand and Myanmar. She is currently a Master student in the field of Wireless Network & Future Internet (STAR) Research Group at Department of Electrical Engineering, Chulalongkorn University, Thailand. From 2014 to present, she is a recipient of scholarship for International Graduate Students in ASEAN countries, Chulalongkorn University, Thailand. Her research interests include Cloud Computing, Future Internet Technology and Software Defined Networking.

Azeem Iqbal received the B.S. degree from University of Management and Technology (UMT), Pakistan in Electrical Engineering. He is currently pursuing the M.S. degree in School of Electrical Engineering and Computer Science at National University of Sciences & Technology (NUST), Pakistan. His research interests include Software Defined Networking, Data Analytics and Cloud Computing.

Nurul Ainaa Binti Muhamad Shaari received her B. Sc. degree from University of Technology MARA (UiTM) and MCS degree from University of Malaya (UM) in Data Communication and Computer Network. She is a lecturer at a private college and currently pursuing the Ph.D. degree in Faculty of Computer Science and Information Technology at University of Malaya (UM), Malaysia. Her research interests include Cloud-Computing, Software-Defined Networking and Future Internet Architecture.

Hari Krishna Atluri is working as a Project Engineer at ERNET, India's national education and research network (NREN). He has worked on R&D projects on the topics of "Mobile IPv6 testbed for mobility management over heterogeneous access networks", "Managing 6LoWPAN wireless sensor networks" and "Cloud computing based Educational Services". Prior to working at ERNET, Hari spent 2 years working for Supercomputer Education and Research Center (SERC), Indian Institute of Science. His current research interests are in areas of Internet protocols, software defined networking, cloud computing and future internet.

Galih Nugraha Nurkahfi received his B.S from physics and M.S degree in Telecommunication Engineering from Institut Teknologi Bandung (ITB), Indonesia. He is lecturer in School of Computing, Telkom University (Tel-U), and also IT consultant. His research interests are in Software Defined Networking, data science and big data.

Apichart Wantamanee received B.Eng in Telecommunication Engineering from King Mongkut's Institute of Technology Ladkrabang, Thailand, in 2010. Currently, he is a master student in the field of Wireless Network & Future Internet (STAR) Research Group at Department of Electrical Engineering, Chulalongkorn University, Thailand and works as senior engineer at Thaicom, satellite operator. His research interests include Cloud platform and Future Internet Technology.

Rifqy Hakimi received his B.S and M.S degree in Telecommunication Engineering from Institut Teknologi Bandung (ITB), Indonesia. He is a junior lecturer in School of Electrical Engineering & Informatics, Institut Teknologi Bandung (ITB) since 2015. His research interests are in Computer Networking field such as Internet Technologies and Software Defined Networking.

Uzzam Javed received his B.S. degree in Electrical Engineering from National University of Computer and Emerging Sciences (FAST-NUCES) Islamabad, Pakistan in 2013, and his M.S. degree in Electrical Engineering from School of Electrical Engineering and Computer Sciences (SEECS) of National University of Science and Technology (NUST), Islamabad, Pakistan in 2016. His research interest includes Software-Defined Networking, Data Science and Cloud Computing.

Muneeb Ahmad received his B.S. degree in Electrical Engineering from Air University (AU) Islamabad, Pakistan in 2013, and is currently pursuing his M.S. degree in Electrical Engineering from School of Electrical Engineering and Computer Sciences (SEECS) of National University of

Sciences & Technology (NUST), Islamabad, Pakistan. His research interests include Software-Defined Networking, Network Function Virtualization and Cloud Computing.

Chaodit Aswakul received the B.Eng. degree (1st class honor) in Electrical Engineering from Chulalongkorn University, Thailand, in 1994. In 2000, he received Ph.D. in Communications Networking from the Imperial College of Science, Technology and Medicine, University of London, U.K. He is currently an associate professor at Department of Electrical Engineering, Chulalongkorn University, Thailand, and head of the university's Wireless Network & Future Internet (STAR) Research Group. Chaodit was a recipient of the Ananda Mahidol Foundation Scholarship, Thailand.

Muhammad Usman Ilyas is currently appointed Assistant Professor of Electrical Engineering at the School of Electrical Engineering and Computer Science (SEECS) of the National University of Sciences and Technology (NUST), Islamabad, Pakistan. Prior to that he was a Post-doctoral Research Associate appointed jointly by the Electrical & Computer Engineering (ECE) department and the Computer Science & Engineering (CSE) department at Michigan State University (MSU). He worked under the joint supervision of Dr. Hayder Radha (IEEE Fellow) and Dr. Alex Liu at East Lansing, MI. Dr. Ilyas received his Ph.D. and MS degrees in Electrical Engineering from Michigan State University in 2009 and 2007, an MS in Computer Engineering from the Lahore University of Management Sciences (LUMS) at Lahore, Pakistan in 2004, and a BE (Honors) in Electrical Engineering from NUST, Pakistan in 1999. He is interested in network science, future Internet architectures and social networks.

Teck Chaw Ling is an Associate Professor at the Faculty of Computer Science and Information Technology, University of Malaya and also the chairperson of Malaysia Research and Education Network-MYREN Network & Distributed Systems Working Group. His research areas include Software Defined Networking, Green computing, Core network research, inter-domain Quality of Service (QoS), Voice over IP (VoIP), Cloud computing, and network security.

Arumugam Paventhan is Additional Director (R&D) with ERNET (India's national research education network) At ERNET, he has handled R&D projects, in the domains of Internet of Things, Mobile IPv6, EU funded MyFIRE Future Internet and Educational Cloud. Prior to joining ERNET, he held scientific and research positions at National Informatics Centre (HQ), New Delhi, C-DAC, Bangalore and Rutherford Appleton Laboratory (RAL), Oxford, UK. He has received M.Tech Computer Applications from IIT Delhi and PhD in the field of Gridcomputing from the University of Southampton, UK under the research scholarship award within the School of Engineering Sciences. He is a Senior Member of IEEE, and member of Internet Society (ISOC) and ACM. His current research interests include protocols and standards for Internet of Things (IoT), Cloudcomputing and Software Defined Networking.

Eueung Mulyana is an Assistant Professor in the School of EE and Informatics at Institut Teknologi Bandung (ITB), Indonesia. He received a Bachelor in EE from ITB, M.Sc. in Communication Channels Modeling from Universitatet zu Karlsruhe (now Karlsruhe Institute of Technology, KIT Germany) in 2001. He received his PhD (Dr.-Ing.) degree in Communication Networks from TUHH (Technische Universitaet Hamburg-Harburg), Germany in 2006. His current research focuses on Advanced Networking Technology and Services, including SDN, NFV and other emerging cloud-related infrastructure and applications.

JongWon Kim received the B.S., M.S. and Ph.D. degrees from Seoul National University (Seoul, Korea), in 1987, 1989 and 1994, respectively, all in Control and Instrumentation Engineering. In 1994–2001, he was a faculty member of KongJu National University (KongJu, Korea) and University of Southern California (Los Angeles, USA). From September 2001, he has joined Gwangju Institute of Science & Technology (Gwangju, Korea), where he is now a full Professor. Since April 2008, he is leading GIST SCENT (Super Computing & Collaboration Environment Technology) Center as a director. He is also leading Networked Computing Systems Lab. (recently renamed from Networked Media Lab.) which focuses on Dynamic & Resource-aware Composition of Media-centric Services employing Programmable/Virtualized Computing/Networking Resources. His recent research interests cover topics such as software defined networking (SDN)/cloud computing for Future Internet testbed and smart media-centric services employing heterogeneous SmartX nodes.