2014 IEEE/ACM 7th International Conference on Utility and Cloud Computing

Analysis of SDN contributions for Cloud Computing Security

Wanderson Paim de Jesus
National Education and Research Network
wanderson.jesus@rnp.br
Brasília, Brazil

Daniel Alves da Silva, Rafael T. de Sousa Júnior
Francisco Vitor Lopes da Frota
Electrical Engineering Department
University of Brasília
daniel.alves@redes.unb.br, desousa@unb.br, vitor.lopes@latitude.unb.br
Brasília, Brazil

***Abstract*—Cloud infrastructures are composed fundamentally of computing, storage, and networking resources. In regards to network, Software-Defined Networking (SDN) has become one of the most important architectures for the management of networks that require frequent re-policing or re-configurations. Considering the already known security issues of Cloud Computing, SDN helps to give fast answers to emerging threats, but also introduces new vulnerabilities related to its own architecture. In this paper, we analyze recent security proposals derived from the use of SDN, and elaborate on whether it helps to improve trust, security and privacy in Cloud Computing. Moreover, we discuss security concerns introduced by the SDN architecture and how they could compromise Cloud services. Finally, we explore future security perspectives with regard to leveraging SDN benefits and mitigating its security issues.**

I. Introduction

According to the National Institute of Standards and Technology (NIST) [1] Cloud Computing comprises on-demand self-service, broad network access, resource pooling, rapid elasticity, and measured service as essential characteristics. Also, NIST identified four deployment models, namely: Private, Community, Public, and Hybrid cloud. Regardless of the adopted deployment model, it will be dependent on hardware and software infrastructure, usually spread over multiple Data Centers (DC). These computing resources can be dynamically allocated so the service capacity is able to shrink or grow according to client demand.

Data Centers are composed fundamentally of computing, storage, and networking resources. In this scenario, flexibility is the key to address the challenge of planning and managing systems whose characteristics, workloads, performance, availability, and reliability goals change rapidly. Concerning networking resources, Software-Defined Networking (SDN) [2] became one of the most important architectures for the management of large-scale and complex networks, which may require frequent re-policing or re-configurations [3]. Considering the already known security issues of Cloud Computing [4], SDN helps to give fast answers to emerging threats, but also introduces new vulnerabilities related to its own architecture.

SDN defines the decoupling of the control plane and the data plane that share the traditional network equipment. On one hand, such decoupling is beneficial as it enables centralized decisions about data traffic in networks. This way, policies can be enforced quickly in response to emerging network requirements, as well as to network threats. On the other hand, SDN Security issues [5], such as fraudulent rule insertion, controller-switch communication flood, unauthorized controller access, and controller hijacking, could be explored in Cloud environments to harm client applications and network performance. In face of this, from the security point of view, it is relevant to investigate whether SDN constitutes a solution or a problem for Cloud Computing environments, since the answers to this question are important indicators of the trust that a costumer can place in SDN and SDN based cloud computing services.

There are several proposals in the literature that address SDN security. Some of them show how to use SDN as an additional defense measure to tackle security threats, due to the SDN support to new IDS [6][7], IPS [8], and DPI [9] solutions. Other proposals focus on analyzing SDN architectural vulnerabilities and proposing solutions [10][11].

In this paper, we discuss recent security proposals arising from SDN, and analyze whether SDN helps to improve trust, security and privacy in Cloud Computing. We also present security challenges introduced by SDN and how they could compromise Cloud services. Moreover, we explore security perspectives related to leveraging SDN benefits and mitigating its security issues.

The rest of the paper is structured as follows. In Section II, we give our understanding about trust, privacy and security in cloud and outline related papers in this area. In Section III we discuss the role of the SDN architecture in Cloud Computing environments. Then, in Section IV, we point out the main SDN contributions to improve Cloud security, privacy and trust. In Section V we discuss the additional concerns consequent to the use of SDN. Finally, in section VI, we conclude the paper with our impressions about the counterbalance of using or not SDN as part of a cloud network solution.

II. Trust, Security and Privacy

The new model of service provisioning introduced by Cloud Computing, which reduces costs by sharing resources among applications, impacts directly information technology (IT) budget [12]. Conversely, while usually providing worldwide availability, resource sharing affects trust, security, and privacy.

978-1-4799-7881-6/14 $31.00 © 2014 IEEE
DOI

Recently, large enterprises described security concerns as the main reason to avoiding the public cloud model [13]. In this model, the physical infrastructure is owned and managed by the service provider. Cloud trustiness and mainly privacy have also been affected by the Patriot Act, a US federal law, which compels companies to provide private information to government in legal requests.

Due to the different interpretations given to trust, security and privacy throughout scientific papers, it is worth discussing our understanding of these terms. Trust refers to the confidence that people, data, entities, information, or processes, will behave or function in expected ways. Security concerns the confidentiality, availability and integrity of data or information. Security may also include authentication and non-repudiation. Privacy is related with the private life and is usually defined and regulated by regional, national or global laws. Some privacy principles are described in [14], including consent, purpose restriction, legitimacy, transparency, data security and data subject participation.

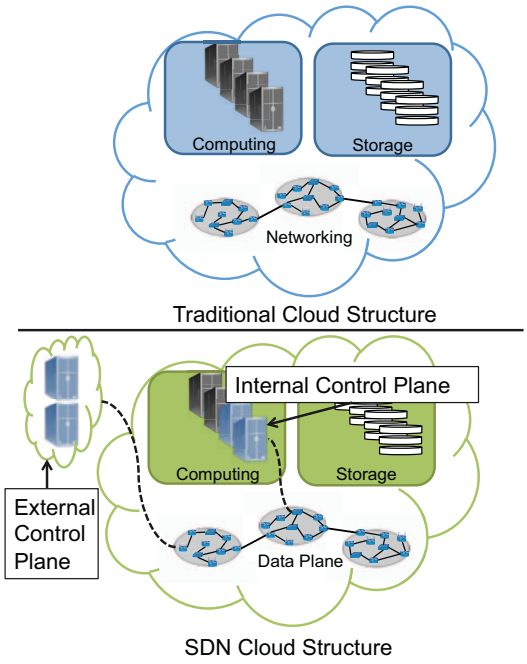

Figure 1. Traditional and SDN Cloud Structures

Cloud security issues are present in several parts of data centers, such as computing infrastructure, including physical components as cable links and hardware, client or control applications, interfacing and networking. The deployment of SDN in such environment requires architectural, management and policy adaptations. It is possible to use SDN in place of regular network technologies, keeping protocols and functions. Notwithstanding, in order to leverage SDN benefits, a new arrangement of network resources is required. To start with, planning the merge of SDN architecture (application, control and data plane) to the data center?s infrastructure must receive most attention. Defining the control plane location [15][16], the distribution mode [17], and communication policies [18] are examples of possible concerns. Figure 1 illustrates the basic changes from a traditional cloud structure to a possible SDN based cloud structure. Regular network devices are replaced by SDN forwarding equipment forming the Data Plane.

With the decoupling of control and data planes in SDN architecture, routing decisions and control functions must run on servers that might be in different physical locations from the forwarding elements. In [19], the authors proposed to use the cloud computing resources themselves to deploy the SDN control plane. Such possibility is described as Internal Control Plane in Figure 1. This approach is beneficial to SDN because it leverage resource availability and elasticity, – intrinsic to the cloud model – becoming more resilient to attacks such as Distributed Denial of Service (DDoS). Furthermore, the cloud supports live migration of Virtual Machines (VMs) from one physical machine to another.

It is also possible to use SDN to address cloud security concerns. The employment of software to control network behavior, as enabled by SDN, permits centralized decisions, analysis of multiple parameters and quick response and propagation of forwarding policies. These function are more valuable to security than to trust and privacy, since these two are more general properties and depend not only on computing resources, but also on laws and utilization policies.

III. SDN in Cloud Computing Era

In general, cloud models are deployed in Data Centers due to the lower unitary cost achieved by sharing computing resources. There are in the literature several studies about data center network (DCN) structures [20][21][22], which falls basically into two categories: switch-centric and server-centric. Whilst the former concentrate the interconnection intelligence on switches, the last concentrate this intelligence in servers. In server-centric structures, switches are used just as crossbar channels. Although the use of SDN is a viable means to implement a switch-centric structure, adapting SDN components to a DCN structure represents itself a great challenge. Although the control plane of SDN runs in servers, it is not to be confused with a server-centric structure. The control plane is part of the SDN architecture and has no interference in client application servers.

In the categorization presented in [5], the authors have classified SDN security issues according to the affected SDN layer. This paper also presents a discussion about the possible benefits of using SDN. A similar study has been provided by in [4], a paper arguing that cloud computing security related issues comprise five categories, namely, Security Standards, Network, Access Control, Cloud infrastructure, and Data. In Table I, we synthesize from [4] some indicators on whether SDN helps or hinders to solve the cloud network and infrastructure issues.

It is worth mentioning that there are other works in the literature that analyze cloud issues and provide different

Cloud Networking Issues [4]	Helpers	Impediments
Proper installation of network firewalls	With the logically centralized intelligence and global topology overview, SDN helps identifying threats and giving more efficient and rapid answers with the deployment of firewall rules [23]	
Network security configurations	Even with orchestration solutions, traditional networks still keep many configuration aspects dependent on specific proprietary commands. In SDN, security configurations are resumed in the control plane and have flexibility enough to address special security policies	In order to enable communication between data, control and application planes, switches and control plane devices must be synchronized, requiring some security configurations, such as cryptographic algorithm, certification policy, and strategy in case of control-plane unavailability
Internet protocol vulnerabilities	With the emergence of SDN, traditional protocols executed switch-by-switch have become outdated. In SDN, packets are forwarded according to centralized decisions diminishing Internet protocols inconsistencies	Instead of one-by-one traditional protocols, SDN defines network behaviors in software modules, which are also prone to errors and vulnerabilities
Internet Dependence	External access is crucial to cloud services. SDN does not change this fact, but it helps avoiding unavailability by the deployment of intelligent software that might explore alternative paths finding the best cost-benefit solution	
Quality of service	Approaches towards SLA policy refinement for Quality of Service (QoS) management (based on routing) in Software-Defined Networking are feasible [24]	SDN architecture requires itself bandwidth for control-data traffic, and granting QoS in this link is a novel concern within the cloud infrastructure
Security Misconfiguration	In SDN, most intelligence is kept in software and not in specific switch configurations	With the responsibility to develop software, misconfiguration may cause bugs and process breaks
Multi-tenancy	Due to the centralized controlling and virtualization based on any packet characteristic, SDN improves multi-tenancy management, turning it easier and flexible. There is no more dependence in VLAN tags to differentiate traffic flows, for instance	SDN main control-data protocol is OpenFlow, which requires a flow table in data plane switches. Flow rules poorly designed or incorrectly set priorities is an additional concern to multi-tenancy in clouds

Table I
HOW SDN CHARACTERISTICS SOLVES OR WORSENS THE MAIN CLOUD SECURITY ISSUES

categorizations, such as [25]. Paper [26] mentions VM-level attacks, abuse and malicious use of cloud computing (due to easy registration and incomplete identification of users), loss of governance (SLAs with gaps in security parameters), lock-in (when a user is unable to migrate from one service provider to another), isolation failure, data loss or leakage, management interface compromise, compliance risk, malicious insiders, insecure interfaces and APIs, and account or service hijacking.

Although it comes from a non-exhaustive survey of papers discussing the subject, we noticed that network related issues are not the majority regarding cloud security. In [4] as well as in [25], network related issues represent 14% of stated total. In [26], network related issues are not shown explicitly under a network class, but from our analysis, 18% are related to networking, being the other issues, in general, related to access policies, computing infrastructure, and data. Figure 2 depicts the distribution of cloud security issues perceived from the overall sum of all issues stated in the referenced literature.

In the next sections this discussion aims at identifying situations in which SDN contributes to solving cloud networking related issues and also the situations in which SDN represents an additional concern.

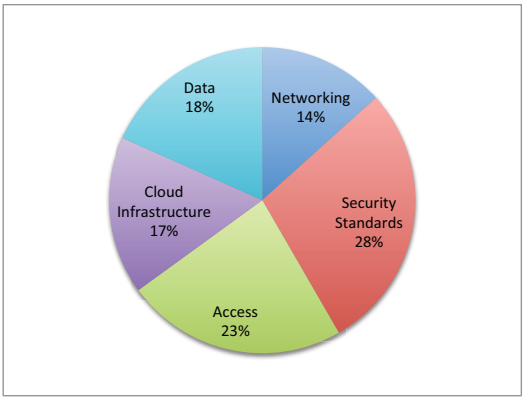

Figure 2. Cloud Issues Distribution

IV. SDN CONTRIBUTIONS FOR SECURE CLOUDS

Some broadly perceived advantages of using SDN for cloud computing networking come from the possibility to implement IDS, IPS, firewall [23], load balancers [27] and much more

network functions as software modules in the SDN controller. In so doing, emerging threats can be addressed quickly by the programming of additional software modules, or else, developing software with autonomic techniques that provide automatic and adaptive routing with multi-path, congestion control, or any necessary function [28].

In Table I, the first cloud network and infrastructure issue, regards the possible lack of proper installations of network firewalls, which could facilitate for hackers to access the cloud interface on behalf of legitimate users [25]. In [23], the authors propose a firewall application that runs over an OpenFlow-based SDN controller. OpenFlow is an open and widespread protocol used as interface between SDN control and data planes. This paper shows that most firewall functionalities may be implemented through software, without the aid of a dedicated hardware.

The third and fourth listed item refer to the possibility of hackers to hijack collective resources (hardware/applications) causing unavailability. Exploring Internet protocol vulnerabilities, such as SIP (Session Initiation Protocol), hackers could cause Denial of Service, for example. Considering the dependence of cloud application and services to be externally accessible, such problem might affect trust. In response to such class of issues, in [29], the authors present a Distributed DoS (DDoS) detection method based on traffic flow analysis enabled by SDN. Retrieving network statistics at regular intervals, such method uses Self Organizing Maps to identify anomalous flows. Other approach, CloudWatcher [30], provides monitoring services for large and dynamic cloud networks. This approach suggests using SDN global topology overview to detour flows to specific network security devices.

Considering that unproperly operating QoS procedures may produce loss of trust or even security flaws, it should be taken into account. Among SDN related publications, QoS has been a frequent term. In [24], the authors propose a SDN based approach capable of identifying the requirements and resources that need to be configured in accordance with SLA requirements. Using a different strategy, PolicyCop [31] provides an interface for specifying QoS SLAs and then uses SDN control plane APIs to enforce them in the network devices. PolicyCop also monitors the network and readjusts network parameters to address SLAs. Another proposal, QoS-aware Network Operating System (QNOX) [32] has extended a regular control plane system called NOX to turn it compatible with QoS requirements.

In non-SDN networs, each device implements so many protocols that many of them are not really employed. In addition to that, large networks may be composed by equipment from heterogeneous vendors, each one with its own intricate proprietary console commands. Setting device parameters one-by-one is certainly an error prone strategy and might compromise security configurations. SDN forwarding devices based purely in the OpenFlow protocol [33] are comparatively very simple. Few security configurations are required in the device itself; some of them needing at most the defining of control plane IP addresses and communications policy.

The cloud business model several preconizes users sharing computing, storage and networking resources. As an effort to orchestrate resource access, a multi-tenancy strategy is employed. However, such capability may lead to information leakage from one tenant to another [34]. There are two moments adequate for dealing with such issue, i.e., prevention or auditing. In [35] an improved architecture of the networking service for cloud platforms integrates SDN, Network Virtualization, and traditional methods, which are adapted for gathering evidence and auditing activities on a per-tenant basis. Meanwhile, in [36], the authors explore new challenges of multi-tenancy data center and propose a solution based on OpenFlow to meet secure resource sharing requirements.

V. Additional Concerns Introduced by SDN

Moving from traditional networks to SDN in Cloud computing environments has also unintended consequences. Before SDN, the network equipment was self contained and any change in one device?s function affected just this device. Consequently, any system upgrade should be done in all devices thus slowing the introduction of novel services. Within SDN, the network intelligence is centered in the control plane and allows the development of novel functions by way of software modules in the controller, regardless of modifications in the data plane pertaining to equipment modules. While such flexibility allows faster upgrades and innovation, it also introduces new concerns related to the proper SDN implementation and to the new approach for creating and deploying novel network services.

In a broad survey on SDN security issues [5], the authors propose a categorization of the issues associated with the SDN framework, which are: Unauthorized Access, Data Leakage, Data Modification, Malicious Applications, Denial of Service, and Configuration Issues. Each of these issues is associated with the layer/interface affected. Data Leakage, for example, affects just Data Layer.

While composing Table I, we considered Network security configurations as an item that needs attention (Impediments column) according to two aspects, the first one related to the challenge of addressing cloud use policies in the control plane through the development of software. The other aspect is related to the control and data plane security configurations and refers only to the proper functioning of the SDN architecture. Indeed, mistakes or negligence in security configurations of control-data or application-control communications may cause unauthorized controller access, fraudulent rule insertion, controller hijacking, and flow rule modification that lead to modifying flowing packets.

The employment of software modules instead of protocol interactions may be an advantage in most cases, but software is also prone to errors and vulnerabilities. Software related issues, such as bugs, runtime exceptions, low performance, and lack of functional and architectural validation, are increasingly becoming an additional concern to SDN controllers if compared with traditional network protocols.

The operation of the SDN architecture itself requires good link connection for control-data or application-control communications. Granting QoS in this link is a novel concern within cloud infrastructures. Additionally, hackers or intruders could compromise such communications and then proceed with attacks such as fraudulent rule insertion, flow rule discovery, and forwarding rule discovery. In [37], the authors analyze resiliency of the connection between control and forwarding planes in SDN. They propose algorithms to improve this resiliency by maximizing the possibility of fast failover, achieved through resilience-aware controller placement and control-traffic routing in the network.

Security policies in SDN are defined almost with the setting of software parameters. Security misconfiguration might lead to bugs and service breaks. So, ensuring the availability of resources and avoiding control plane software breaks also become additional concerns. Moreover, misconfiguration of software parameters might impact the whole network due to the centralized controlling defined by SDN.

Instead of using VLAN tags, OpenFlow implements virtualization by means of a traffic differentiation approach that considers any packet header field. The main concern in this case is with the flow rules sent from the control-plane to the data-plane switches. Poorly designed flow rules or incorrectly set priorities are additional concerns to multi-tenancy in clouds.

VI. Conclusion

Cloud computing has generated significant interest in both academia and industry especially because of its elastic and on-demand resources. However, without appropriate trust, security and privacy solutions designed for clouds, such successful computing paradigm is prone to failure. We point out in this paper several issues related to cloud models. Analyzing such issues, and referring existing literature, we found that a relatively small part of them is related to networking, the remaining concerning data, access, infrastructure, and security standards. Recently with the emergence of Software-Defined Networking concept, cloud environments have gone through modifications as traditional data centers adopted SDN as a network solution. In view of such new reality, in this paper, from the point of view of trust, security and privacy, we analyze whether SDN is an advantage or an additional concern to cloud computing development. Using SDN as their communications solution, cloud environments are taking advantages such as policy centralized control and easy configuration management, as with SDN it is possible to write policies that react according to network state changes, or to define appropriate virtual machine deployment strategies [38]. We identified several security solutions, such as PolicyCop, QNOX, IDS, IPS and anti-DDoS proposals, that might be useful to mitigate cloud networking concerns.

From another perspective, we also discussed additional concerns introduced by the use of SDN. Much of them are related to the SDN architecture itself, which defines the decoupling of application, control and data planes. Inherent to each plane, there are issues described in the literature regarding unauthorized access, data leakage, data modification, malicious applications, denial of service, and misconfiguration.

As a general conclusion, SDN seems to be much more an advantage than a problem to cloud computing network, all things considered. With the fast evolving demands, the traditional network paradigm is increasingly hindering innovations. With the use of SDN, cloud computing might benefit not just from the networking point of view, given that with the elaboration of integrated solutions, computing and storage strategies will also be improved.

A. Insights for Future Contributions

After analyzing the literature, we found that cloud computing security issues are much more related to other resources than to network, as illustrated in Figure 2. Most of them (28%) fit into the Security Standards category, which deals with regulatory authorities and governing bodies that define cloud security policies. This category includes service level agreements, auditing and other agreements among users, service providers and other stakeholders.

Secondly, we found the issues comprising the Access category, with 23% of citations. This category is more related to cloud users and includes identification, authentication and authorization issues. Neglecting this category might allow account and service hijacking, malicious insiders, and privileged user access, among other treats.

Future works should investigate the use of SDN as an integrated solution to tackle security issues outside the networking context. This integration might be feasible due to the nature of the control plane, which runs programmable software. A collaborative strategy could be developed combining access, data and organizational policies in order to achieve higher levels of confidence in cloud computing services, regardless of them been provided according to a public, private or hybrid model.

VII. Acknowledgments

The authors wish to thank the Brazilian Ministry of Planning, Budget and Management for its support to this work, as well as the Foundation for Research Support of the DF (FAPDF) and Brazilian Innovation Agency FINEP (Grant RENASIC/PROTO 01.12.0555.00).

References

[1] NIST, "Final Version of Cloud Computing Definition Published." 2014, available online: http://csrc.nist.gov/publications/nistpubs/800-145/SP800-145.pdf. Last access in: Julho 2014.

[2] J. Rubio-Loyola, A. Galis, A. Astorga, J. Serrat, L. Lefevre, A. Fischer, A. Paler, and H. Meer, "Scalable service deployment on software-defined networks," *Communications Magazine, IEEE*, vol. 49, no. 12, pp. 84 – 93, december 2011.

[3] F. Hu, Q. Hao, and K. Bao, "A survey on software defined networking (sdn) and openflow: From concept to implementation," vol. PP, no. 99, 2014, pp. 1–1.

[4] I. M. Khalil, A. Khreishah, and M. Azeem, "Cloud computing security: A survey," *Computers*, vol. 3, no. 1, pp. 1–35, 2014. [Online]. Available: http://www.mdpi.com/2073-431X/3/1/1

[5] S. Scott-Hayward, G. O'Callaghan, and S. Sezer, "Sdn security: A survey," in *Future Networks and Services (SDN4FNS), 2013 IEEE SDN for*, Nov 2013, pp. 1–7.

[6] R. Skowyra, S. Bahargam, and A. Bestavros, "Software-defined ids for securing embedded mobile devices," in *High Performance Extreme Computing Conference (HPEC), 2013 IEEE*, Sept 2013, pp. 1–7.

[7] S. Dotcenko, A. Vladyko, and I. Letenko, "A fuzzy logic-based information security management for software-defined networks," in *Advanced Communication Technology (ICACT), 2014 16th International Conference on*, Feb 2014, pp. 167–171.

[8] M. Deraman, J. Desa, and Z. Othman, "Multilayer packet tagging for network behaviour analysis," in *Information Technology (ITSim), 2010 International Symposium in*, vol. 2, June 2010, pp. 909–913.

[9] M. Bouet, J. Leguay, and V. Conan, "Cost-based placement of virtualized deep packet inspection functions in sdn," in *Military Communications Conference, MILCOM 2013 - 2013 IEEE*, Nov 2013, pp. 992–997.

[10] A. Zaalouk, R. Khondoker, R. Marx, and K. Bayarou, "Orchsec: An orchestrator-based architecture for enhancing network-security using network monitoring and sdn control functions," in *Network Operations and Management Symposium (NOMS), 2014 IEEE*, May 2014, pp. 1–9.

[11] B.-S. Lee, R. Kanagavelu, and K. Aung, "An efficient flow cache algorithm with improved fairness in software-defined data center networks," in *Cloud Networking (CloudNet), 2013 IEEE 2nd International Conference on*, Nov 2013, pp. 18–24.

[12] S. Pearson, "Privacy, Security and Trust in Cloud Computing," in *Privacy and Security for Cloud Computing*, ser. Computer Communications and Networks, S. Pearson and G. Yee, Eds. Springer London, 2013, pp. 3–42. [Online]. Available: http://dx.doi.org/10.1007/978-1-4471-4189-1_1

[13] Cloud Industry Forum, " Cloud UK: Adoption and Trends 2011." 2011.

[14] N. Robinson, L. Valeri, J. Cave, T. Starkey, H. Graux, S. Creese, and P. Hopkins, "The cloud: understanding the security, privacy and trust challenges." 2010.

[15] B. Heller, R. Sherwood, and N. McKeown, "The controller placement problem," *SIGCOMM Comput. Commun. Rev.*, vol. 42, no. 4, pp. 473–478, Sep. 2012. [Online]. Available: http://doi.acm.org/10.1145/2377677.2377767

[16] S. Schmid and J. Suomela, "Exploiting locality in distributed sdn control," in *Proceedings of the Second ACM SIGCOMM Workshop on Hot Topics in Software Defined Networking*, ser. HotSDN '13. New York, NY, USA: ACM, 2013, pp. 121–126. [Online]. Available: http://doi.acm.org/10.1145/2491185.2491198

[17] D. Levin, A. Wundsam, B. Heller, N. Handigol, and A. Feldmann, "Logically centralized?: State distribution trade-offs in software defined networks," in *Proceedings of the First Workshop on Hot Topics in Software Defined Networks*, ser. HotSDN '12. New York, NY, USA: ACM, 2012, pp. 1–6. [Online]. Available: http://doi.acm.org/10.1145/2342441.2342443

[18] C.-C. Tu, P.-W. Wang, and T.-c. Chiueh, "In-band control for an ethernet-based software-defined network," in *Proceedings of International Conference on Systems and Storage*, ser. SYSTOR 2014. New York, NY, USA: ACM, 2014, pp. 1:1–1:11. [Online]. Available: http://doi.acm.org/10.1145/2611354.2611359

[19] W. Paim de Jesus, J. Araujo Wickboldt, and L. Zambenedetti Granville, "Provinet – an open platform for programmable virtual network management," in *Computer Software and Applications Conference (COMPSAC), 2013 IEEE 37th Annual*, July 2013, pp. 329–338.

[20] J. Zhang, Z. Fang, G. Qu, and S. Zheng, "A new class of data center network structures," in *Global Communications Conference (GLOBECOM), 2013 IEEE*, Dec 2013, pp. 2852–2858.

[21] M. Al-Fares, A. Loukissas, and A. Vahdat, "A scalable, commodity data center network architecture," in *Proceedings of the ACM SIGCOMM 2008 Conference on Data Communication*, ser. SIGCOMM '08. New York, NY, USA: ACM, 2008, pp. 63–74. [Online]. Available: http://doi.acm.org/10.1145/1402958.1402967

[22] C. Guo, H. Wu, K. Tan, L. Shi, Y. Zhang, and S. Lu, "Dcell: A scalable and fault-tolerant network structure for data centers," in *Proceedings of the ACM SIGCOMM 2008 Conference on Data Communication*, ser. SIGCOMM '08. New York, NY, USA: ACM, 2008, pp. 75–86. [Online]. Available: http://doi.acm.org/10.1145/1402958.1402968

[23] M. Suh, S. H. Park, B. Lee, and S. Yang, "Building firewall over the software-defined network controller," in *Advanced Communication Technology (ICACT), 2014 16th International Conference on*, Feb 2014, pp. 744–748.

[24] C. Cleder Machado, L. Zambenedetti Granville, A. Schaeffer-Filho, and J. Araujo Wickboldt, "Towards sla policy refinement for qos management in software-defined networking," in *Advanced Information Networking and Applications (AINA), 2014 IEEE 28th International Conference on*, May 2014, pp. 397–404.

[25] N. Gonzalez, C. Miers, F. Redigolo, T. Carvalho, M. Simplicio, G. de Sousa, and M. Pourzandi, "A quantitative analysis of current security concerns and solutions for cloud computing," in *Cloud Computing Technology and Science (CloudCom), 2011 IEEE Third International Conference on*, Nov 2011, pp. 231–238.

[26] A. Tripathi and A. Mishra, "Cloud computing security considerations," in *Signal Processing, Communications and Computing (ICSPCC), 2011 IEEE International Conference on*, Sept 2011, pp. 1–5.

[27] S. Namal, I. Ahmad, A. Gurtov, and M. Ylianttila, "Sdn based inter-technology load balancing leveraged by flow admission control," in *Future Networks and Services (SDN4FNS), 2013 IEEE SDN for*, Nov 2013, pp. 1–5.

[28] J. Rubio-Loyola, A. Astorga, J. Serrat, W. Chai, L. Mamatas, A. Galis, S. Clayman, A. Cheniour, L. Lefevre, O. Mornard, A. Fischer, A. Paler, and H. De Meer, "Platforms and software systems for an autonomic internet," in *Global Telecommunications Conference (GLOBECOM 2010), 2010 IEEE*, Dec 2010, pp. 1–6.

[29] R. Braga, E. Mota, and A. Passito, "Lightweight ddos flooding attack detection using nox/openflow," in *Local Computer Networks (LCN), 2010 IEEE 35th Conference on*, Oct 2010, pp. 408–415.

[30] S. Shin and G. Gu, "Cloudwatcher: Network security monitoring using openflow in dynamic cloud networks (or: How to provide security monitoring as a service in clouds?)," in *Network Protocols (ICNP), 2012 20th IEEE International Conference on*, Oct 2012, pp. 1–6.

[31] M. Bari, S. Chowdhury, R. Ahmed, and R. Boutaba, "Policycop: An autonomic qos policy enforcement framework for software defined networks," in *Future Networks and Services (SDN4FNS), 2013 IEEE SDN for*, Nov 2013, pp. 1–7.

[32] K. Jeong, J. Kim, and Y.-T. Kim, "Qos-aware network operating system for software defined networking with generalized openflows," in *Network Operations and Management Symposium (NOMS), 2012 IEEE*, April 2012, pp. 1167–1174.

[33] N. McKeown, T. Anderson, H. Balakrishnan, G. Parulkar, L. Peterson, J. Rexford, S. Shenker, and J. Turner, "Openflow: Enabling innovation in campus networks," *SIGCOMM Comput. Commun. Rev.*, vol. 38, no. 2, pp. 69–74, Mar. 2008. [Online]. Available: http://doi.acm.org/10.1145/1355734.1355746

[34] A. Behl, "Emerging security challenges in cloud computing: An insight to cloud security challenges and their mitigation," in *Information and Communication Technologies (WICT), 2011 World Congress on*, Dec 2011, pp. 217–222.

[35] A. TaheriMonfared and C. Rong, "Multi-tenant network monitoring based on software defined networking," in *On the Move to Meaningful Internet Systems: OTM 2013 Conferences*, ser. Lecture Notes in Computer Science, R. Meersman, H. Panetto, T. Dillon, J. Eder, Z. Bellahsene, N. Ritter, P. De Leenheer, and D. Dou, Eds. Springer Berlin Heidelberg, 2013, vol. 8185, pp. 327–341. [Online]. Available: http://dx.doi.org/10.1007/978-3-642-41030-7_24

[36] L. Sun, K. Suzuki, C. Yasunobu, Y. Hatano, and H. Shimonishi, "A network management solution based on openflow towards new challenges of multitenant data center," in *Information and Telecommunication Technologies (APSITT), 2012 9th Asia-Pacific Symposium on*, Nov 2012, pp. 1–6.

[37] N. Beheshti and Y. Zhang, "Fast failover for control traffic in software-defined networks," in *Global Communications Conference (GLOBECOM), 2012 IEEE*, Dec 2012, pp. 2665–2670.

[38] J. A. Wickboldt, R. P. Esteves, M. B. de Carvalho, and L. Z. Granville, "Resource management in iaas cloud platforms made flexible through programmability," *Computer Networks*, vol. 68, no. 0, pp. 54 – 70, 2014, communications and Networking in the Cloud.