Journal of Cloud Computing
a SpringerOpen Journal

RESEARCH Open Access

Towards full network virtualization in horizontal IaaS federation: security issues

Anant V Nimkar* and Soumya K Ghosh

Abstract

Horizontal IaaS federation exploits datacenter for federation of IaaS provider by supplying virtual nodes (e.g. virtual machines, virtual switches, and virtual routers) and virtual links. Today's datacenters for cloud computing do not supply full network virtualization in terms of user-level network management and user-agreed network topology. The datacenters lack the basic security services required for the collocation of tenants' virtual networks. The network virtualization research projects from academia and industry support full network virtualization but lack the basic security services required for the collocation of tenants' virtual networks. This paper investigates the security issues in four areas namely, (a) monolithic IaaS cloud, (b) network virtualization research projects, (c) datacenter network virtualization and (d) virtual resources to incorporate full network virtualization environment in horizontal IaaS federation. Further, it presents the security related qualitative comparisons of datacenters, network virtualization research projects and virtual resources to incorporate full network virtualization in horizontal IaaS federation.

Keywords: Cloud computing; Security; Horizontal federation; IaaS

Introduction

The development of cloud computing as conjectured by Celesti et al. [1] is divided into three stages: i) monolithic cloud, ii) vertical federation, and iii) horizontal federation. In the first stage, the full-fledged cloud services are provided by the cloud provider. All the services are proprietary and hence all the granular services (e.g. a storage service, computing service etc.) needs to be taken from a single cloud provider. In the vertical federation, most of the cloud providers leverage cloud services from another provider. Currently, the second stage is in transition. The future stage will be the horizontal IaaS federation where cloud providers federate to borrow virtual resources (e.g. virtual machines, virtual nodes and virtual links) from another cloud provider to gain economics of scale. The cloud federation may be economically profitable, since the datacenter utilization is only 5% to 20% of its peak time [2]. This under-utilization can be used by another cloud provider in the federation. The cloud federation also solves the problem of service provider lock-in, unavailability of the particular service provider, heterogeneous environment unavailability etc. [3].

*Correspondence: anantn@sit.iitkgp.ernet.in
School of Information Technology, IIT Kharagpur, Kharagpur, India

The monolithic IaaS cloud has three limitations namely (a) maximum number of VLANs are limited to 4K because of 12 bits *VLAN ID* in 802.1Q Ethernet Header [4], (b) no user-agreed network topology at granular level configured and (c) the router gives connectivity between clouds (i.e. a single *route table* is used to manage all networks of a user), or cloud and the Internet. We will use the term *minimal network virtualization* for the three aforementioned limitations in the monolithic IaaS cloud. The IBM's TVDc is an example of vertical federation which supports minimal network virtualization [5,6]. In contrast to the minimal network virtualization, the *full network virtualization* is an environment in which the connectivity of virtual machines is provided using instances of physical network components (e.g. router and switch). It also will facilitate transparent network management of virtual network at a granular level (i.e. virtual switch, virtual router etc.).

Informally, the horizontal IaaS federation provides a federated IaaS cloud service of virtual servers using full network virtualization out of the datacenter. The transparent network virtualization in horizontal IaaS federation facilitates the network isolation, flexibility in network management, user-level network policy control [7] along

with the advantages of cloud federation mentioned earlier. The full network virtualization in horizontal IaaS federation also provides separation of duties (infrastructure provider and service provider etc.), inter-operability between network owners, and portability. Few topology-aware scientific and commercial applications which can be deployed in horizontal IaaS federation are explored in [8] and [9].

There are two major challenges in the development of horizontal IaaS federation. First, the datacenters and virtual resources lack *full network virtualization* required for the horizontal IaaS federation. The second obstacle in the development is the lack of security provision required for the collocation of tenants' virtual networks on the datacenter. The obstacles demand analysis of the existing network virtualization technologies in different domains for security provision.

In this paper, we have investigated potential areas of network virtualization environment (NVE): a) generic network virtualization, b) the datacenter network virtualization, c) network virtualization in monolithic cloud and d) network virtualization in virtual resources. We use the term *generic network virtualization* to denote the research projects for testing future generation networks from academia and industry. First, we give a qualitative comparison of monolithic cloud designs, datacenters, network virtualization projects and virtual resources related to security issues. We also give limitations of aforesaid areas to incorporate full network virtualization and security services required for horizontal IaaS federation. Finally, an insight in research directions on security issues is given for the development of horizontal IaaS federation.

The rest of this paper is organized as follows. We first formally re-define *horizontal IaaS federation* for the inclusion of full server and network virtualization in Section 'Horizontal IaaS federation'. A hypothetical example of horizontal IaaS federation is also given in Section 'Horizontal IaaS federation' to illustrate the reasons for the investigation of network virtualization security. Section 'Horizontal IaaS federation security issues' explores the domains for security of horizontal IaaS federation and also gives a list of security requirements for horizontal IaaS federation. Section 'Monolithic IaaS NVE security' presents NVE security issues of monolithic cloud and vertical federation. Section 'Datacenter NVE security' and 'Generic NVE security' give security issues of datacenter and generic NVE respectively. The security issues of virtual resources related to NVE are presented in Section 'Virtual resources security'. Finally, a discussion on research directions for security in horizontal IaaS federation and concluding remarks are presented in Section 'Research directions' and Section 'Conclusions' respectively.

Horizontal IaaS federation

In horizontal IaaS federation, the service provider gives service to another cloud called *home cloud*, and the service borrower takes service from another cloud called *foreign cloud*. The *home cloud* borrows virtual resources from the *foreign cloud* either because of virtualization infrastructure saturation in *home cloud*, or the economics of scale in cloud federation [10]. The three-phase cross federation [1,10] and mobile-agent based cloud federation [3] are examples of the horizontal IaaS federation in which a *home cloud* rents virtual machines from *foreign clouds* without considering full network virtualization.

The horizontal IaaS federation should provide full network virtualization to its clients to gain advantages mentioned earlier. The existing work on horizontal IaaS federation [1,3,10] incorporates full server virtualization and minimal network virtualization while the application of network virtualization in various domains [11,12] concentrates on one of the two virtualizations. So, we first investigate the roles in the full server and network virtualization; and then formally re-define it for the inclusion of full server and network virtualization.

The network virtualization supports existence of multiple virtual network infrastructures on the top of physical network infrastructure. The NVE has two roles: *service provider (SeP)* and *infrastructure provider (InP)*. The InP owns physical infrastructure and SeP borrows/owns virtual infrastructure. Figure 1 shows an example of network virtualization environment. The network topology in plain line rectangle shows the physical infrastructure of InP. The network topologies in single-dot-dash and double-dot-dash line rectangles shows the virtual resources of SePs. The virtual nodes are installed on the physical resources. e.g. the virtual nodes, K1 and K2 are installed on the physical node K. The virtual link may be mapped to any path reachable between two nodes by some virtual network placement algorithm.

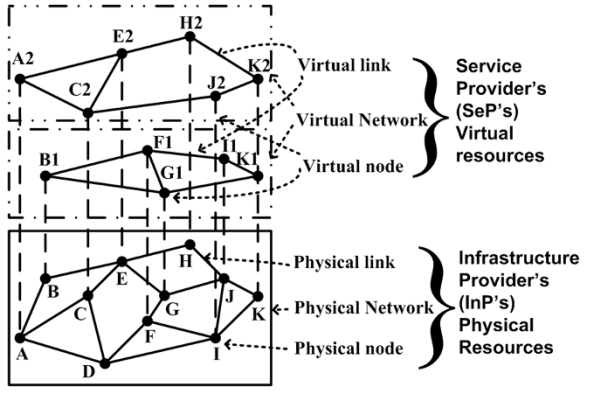

Figure 1 Network virtualization. The figure gives definition of network virtualization.

The current *horizontal IaaS federation* ecosystem has three key components: Cloud coordinators, Brokers, and an Exchange [13]. The cloud coordinators handle the datacenters for exporting market-based cloud services. A cloud coordinator can be cloud provider or consumer in the federation. A Cloud Broker is a mediator between cloud providers and cloud consumers for the federation. A cloud exchange performs match making services for the cloud users.

The *horizontal IaaS federation* with full server and network virtualization must consider at least two roles (viz. network service provider and infrastructure provider) from network virtualization and three roles (viz. a cloud provider, cloud consumer and a broker) from the current *horizontal IaaS federation* ecosystem. So the *horizontal IaaS federation ecosystem* must have four roles namely service provider (SeP), infrastructure provider (InP), broker (Br) and user to incorporate full network virtualization. The horizontal IaaS federation can be formally defined as:

Definition: *horizontal IaaS federation* The federated cloud service of virtual infrastructures of a set of virtual nodes (e.g. virtual switches, virtual routers), virtual links and virtual machines from a set of InPs (a virtual network infrastructure provider) and SePs (a IaaS cloud service provider) with transparent full server and network virtualization.

We will use the term *federation* to mean horizontal IaaS federation for the sake of brevity from now onward in the paper. We illustrate this definition with the following example. The hypothetical example presented in Figure 2 is inspired by the theoretical development of *federation* in *InterCloud* [13] and *open-flow* based network virtualization for cloud [14]. The IaaS cloud provider can be InP, or InP as well as SeP in the *federation* as shown in Figure 2. The figure shows a federation of three IaaS cloud providers ({InP-1, SeP-1}, {InP-2} and {SeP-3, InP-3}) and three users (User-1, User-2 and User-3). The plain-line rectangles are InP providers. The bottom topologies of plain-line rectangles are physical infrastructure of the InPs. The home cloud {InP-1, SeP-1} has a cloud user, User-1. The home cloud {InP-3, SeP-3} has two cloud users, User-2 and User-3. The home cloud {InP-1, SeP-1} provides a virtual network {VN-A,VN-F} by borrowing a virtual network {VN-F} from foreign cloud {InP-3} to User-1. The home cloud {InP-3,SeP-3} provides virtual networks {VN-C,VN-D,VN-G} and {VN-B,VN-E} by borrowing the virtual networks {VN-C,VN-D} and {VN-B} to User-3 and User-2 respectively. The virtual machines are not shown in Figure 2 as the present work is concerned about virtual network infrastructure.

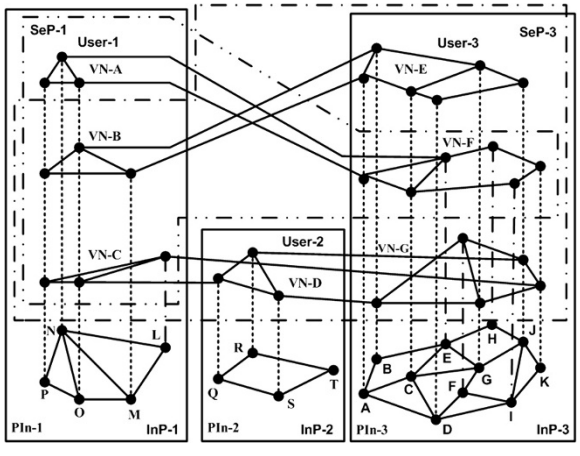

Figure 2 Horizontal IaaS federation. The figure shows an example of horizontal IaaS federation and boundary of security control.

The virtual nodes and links are created by their respective InPs on receiving request from SePs. The virtual resources are managed by the users of SePs. The double-dot-dash and single-dot-dash line polygons show the boundary of SeP-1 and SeP-2 control respectively. The management of virtual resources is done by their respective users. In a nutshell, the various functions like virtual resource management, control and configuration are cooperatively performed by the three roles of the federation, so it is necessary to consider various security issues for proper functioning of the *federation*.

Horizontal IaaS federation security issues

To incorporate full network virtualization in *federation* ecosystem, the security issues of all constituents in the ecosystem must be investigated. The two components, *Brokers* and *an Exchange* out of three components of federation system are very similar to any brokered architecture [13] where the service/resources are leased using some kind of negotiation between service consumer and provider through the *Brokers* and *an Exchange*. So, the investigation of these two components are omitted.

Vaquero et al. [15] surveyed monolithic IaaS security issues related to virtual machines but it did not address the security issues related to network virtualization. In [7,11], the authors investigated *generic network virtualization* without security concerns. Bari et al. [12] reported the survey of datacenter network virtualization without security issues. In a nutshell, none of the existing work have concentrated on the security issues in network virtualization environment. We mainly focus on NVE security issues in monolithic IaaS cloud (Section 'Monolithic IaaS NVE security'), datacenter network (Section 'Datacenter NVE security'), generic network virtualization (Section 'Generic NVE security') and virtual resources (Section 'Virtual resources security') to incorporate full network virtualization in the federation.

A detailed discussion on the security requirements of *federation* ecosystem is beyond the scope of current investigation. A few security requirements of the federation are already explored in the constituents of federation ecosystem in the literature: (a) cloud security requirements [16], (b) network virtualization security requirements [17], (c) *cloud security alliance V3.0* [18], and (d) web security survey [19]. So we use following security requirements which are derived and extended from the literature [16-19].

- **R1** - Layered network architecture in which physical resources are controlled by InPs and virtual resources are transparently controlled by SePs.
- **R2** - Provide transparent view of virtual network infrastructure with a clear SLA (service level agreement) between SePs, InPs and cloud users.
- **R3** - Autonomous local identity management for physical resources used by InP.
- **R4** - Cooperative global identity management for virtual resources used by SeP and cloud users.
- **R5** - A brokered architecture between Br, InPs, SePs and cloud users for the collaboration of local and global identity management.
- **R6** - An access control mechanism to create, destroy virtual resources out of physical resources after the negotiation between InPs, SePs and cloud users.
- **R7** - An access control mechanism to manage and use virtual resources as per SLA between InPs, SePs and cloud users.
- **R8** - Intra-InP routing protocol with source authentication, operational confidentiality for cloud users within a InP.
- **R9** - Inter-InP routing protocol with source authentication, operational confidentiality and least information disclosure among InPs.
- **R10** - Tight collaboration among SePs and InPs in terms of fault handling, configuration, accounting, performance monitoring, trust negotiation and QoS.

Monolithic IaaS NVE security

As monolithic IaaS clouds are proprietary and a few technical documents are publicly available, so only two designs have been selected for the investigation of NVE security. Amazon *Elastic Cloud 2* (EC2) [20-22] and *GoGrid* [23] are the representatives of the most popular and a randomly selected IaaS cloud provider respectively.

The first representative, EC2 provides minimal network virtualization using either a software or hardware gateway to facilitate the communication between VPCs or virtual machines. A software gateway uses *route tables* as *software virtual router* while hardware gateway uses hardware router. Cisco integrated service routers and Juniper J-series are examples of software virtual routers. RTX 3000 is an example of hardware router. The EC2 uses *security groups* to provide the basic security services among the users. A *security group* acts as a virtual firewall to control the traffic allowed that is allowed into a group of virtual machines instances.

The second representative, GoGrid offers limited network service using a private switch to each private cloud. GoGrid also makes use of hardware firewall to protect the servers of private clouds. Xu et al. [24] proposed secured *wide area network* virtualization for virtual private cloud using tunnelling.

Datacenter NVE security

Cloud computing exploits datacenter for the provision of large data storage and network services with highly redundant data network and backup power supplies. We have thoroughly gone through the literature to find the limitation of NVE and its security services in the datacenters. The main aim of NVE provided in current datacenter is high utilization of its resources and not for any kind of network virtualization provision to its user. Md Faizaul Bari et al. [12] reported the survey of datacenter network virtualization without any security features. The first four datacenters (i.e., CloudNAS, Diverter, VICTOR and SEC2) provide security services in terms of *security components* and *security implementations* as shown in Table 1. The security implementation can be tunnelling, anti-spoofing, policy enforcement and visibility filters. The security components can be FE (Fowarding Element), CC (Central Controller), DPI or IDS. The CloudNAS supports full network virtualization but optional confidentiality and authentication using tunnelling.

The Diverter provisions network virtualization on the top of customized layer-3 network addressing. Each host has triplet ⟨f:s:h⟩ address where f is farm of hosts, s is subnet identifier and h is a particular host. The layer-3 triplet addresses are transparent to the tenants. Each host also runs VNET as distributed router in OS kernel-space. The VNET implements anti-spoofing and visibility filters to provide security services to tenants. The anti-spoofing filter prevents a VM impersonation by another VM. The visibility filter contains all network visibility rules to enforce separation between virtual machines. The tenants can use optional tunnelling for confidentiality.

The SEC2 and VICTOR have some common features. The network infrastructure of SEC2 as well as VICTOR is organized in two levels: a core domain and edge domains. An edge domain consists of physical hosts and switches. The core domain is made of a set of customized layer 2 switch called as Forwarding Element (FE) and Central Controller (CC). Central Controller (CC) controls the operation of FEs. FE performs two functions namely, (a) address lookup and mapping and (b) policy enforcement. The security service of SEC2 is made available through tunnelling or FEs. FEs can implement firewalls, NAT and

Table 1 Datacenter network virtualization security

Datacenter	Features	Security components	Network virtualization	Security implementation
CloudNAS [25]	Network Specification and embedding	Middlebox (Deep Packet Insepction - DPI or IDS)	Full NVE	Optional tunnelling
Diverter [26]	Multi-tenant virtual networks	VNET	Layer-3 distributed virtual routing	Anti-spoofing and visibility filters
VICTOR [27]	Dynamic VM migration	FE and CC	Set of distributed FEs	Policy enforcement
SEC2 [4]	Multi-tenancy network isolation	FE and CC	Set of distributed FEs	Policy enforcement, VPLS and MPLS
Gatekeeper [28]	Bandwidth performance isolation	-	Set of vNIC	-
NetShare [29]	Bandwidth guarantees and high utilization	-	Topology-driven	-
NetLord [30]	Flexible network abstraction	-	L2 and L3 encapsulation	-
Oktopus [31]	Virtual network abstractions provision	-	Assumption - physical mapping to virtual and oversubscribed cluster	-
PortLand [32]	VM migration, automatic switch configuration	- -	L2 switching using hierarchical Pseudo MAC	-
SPAIN [33]	Multipath forwarding	-	Datacenter topology-driven	-
VL2 [34]	Performance isolation	-	AA(Application) and LA(Local) addressing	-

middleboxes. The remaining seven datacenters proposals have different aims but do not provide any security features as summarized in Table 1.

Generic NVE security

The existence of virtual network on the top of physical network may appear at any layers of OSI reference model. Consequently, there are mainly four types of network virtualization: (a) virtual local area network (VLAN), (b) virtual private network (VPN), (c) active and programmable network, and (d) overlay networks [11]. Some of the surveyed network virtualization projects using aforementioned types are not useful for the investigation of security issues. So we used three filtering criteria for the survey. The first, VLAN and VPN inherently provides security features to network virtualization environment using segmentation, isolation, tunnelling, IPSec and VLAN. Second, the main aim of some network virtualization projects (e.g. AKARI, CABO, 4WARD, Triology, and Clean-slate) is the design of next generation network. They are long-term projects; and are evolving and extending from another network virtualization projects like GENI and VINI. Third, the research in old network virtualization projects namely Genesis (is from Active and programmable network type) has been stopped. So the network virtualization projects for security investigation after applying the three filtering criteria are GENI, PlanetLab, UCLP, VINI and X-bone.

As per the security requirements of full network virtualization in *federation* given in Section 'Horizontal IaaS federation', we surveyed the network virtualization projects by classifying them under five categories: (a) identity management for resources, (b) authentication and trust management, (c) resource access control, (d) routing security issues; and (e) other security issues.

Identity management for resources

The digital identities for virtual resources in network virtualization environment give a provision of dynamic connectivity between virtual resources. An identity management for resources in network virtualization provides mechanisms for managing and gaining access to the resource's identity and information across organizational boundaries to SePs and InPs. Yuan et al. [35] classified the identity management models in three categories — isolated, centralized and federated — by considering various attributes. We will consider only four attributes — *the number of InPs*, *the number of SeP*, *user control over identity*, and *identities' storage* — as per the requirements, **R4** and **R5**. Table 2 shows the comparison of

Table 2 Identity management for resources: comparison

Project	No. of InPs	No. of SePs	User control	Identity storage
GENI [36]	Many	One	Yes	Decentralized
PlanetLab [37]	Many	One	Yes	Centralized
UCLP [38]	Many	Many	No	Decentralized
X-bone [39]	One	One	No	Centralized
NouVeau [40]	Many	Many	-	Decentralized

GENI, PlanetLab, UCLP, X-Bone and NouVeau using four attributes mentioned earlier. The roles from the projects are mapped to InP, SeP and cloud user so that it is easier to compare the projects.

The GENI have InPs (called as *Aggregates*) and SePs (called as research organizations). The users of research organization (i.e., SeP users) are called principal. The principal may be a researcher, principal investigator (which is an administrator) and slice admin. The virtual network instance is called slice and consists of objects. The GENI defines identifiers called GENI Global Identifiers (GGID) for all principal and objects in the system. The GENI uses X.509 certificate to represent GGID for authentication. In federated GENI system, an identity of an object in SeP is a union of identities stored across multiple InPs. The database of identity name-space is stored at the research organization's site and allows control by the principal.

The PlanetLab has three main roles: an owner, a user and PLC (PlanetLab Consortium). The owner (i.e., InP) supply physical nodes to create VMs. A service is installed on PlanetLab by a researcher (i.e., SeP). The PLC is a centralized entity and has mainly two functions: (a) manages physical resource and (b) maintains trust among owners and researchers. A slice is a collection of VMs. Each slice is uniquely identified by the hierarchical name where each level has the responsibility to manage and control the resources at that level. The PLC acts as slice authority and maintains state of all slices in the system.

The UCLP is the most promising project for *federation* in which the identities of virtual resources (e.g. LightPath, End2End object) is managed by *UCLP Admins* (SePs) and the identities of physical resources are managed by *network owners* (InPs). The UCLP end users cannot control UCLP virtual resources. The UCLP uses decentralized JavaSpace storage for the identities at InPs' sites. The overlay manager (SeP as well as InP) in X-bone manages the identity of virtual nodes at central repository. The X-bone user cannot control the identity of the virtual resources. The *NouVeau* is an identity management for a abstract network virtualization model and is similar to UCLP. It is based on three main principles: separation of identity and location, local autonomy, and global identifier space. It also requires special entities called controller and adapters for the managements of identities in SePs and InPs.

Authentication and trust management

A typical identity management has any of the three types of trust relationship between the service provider (SP) and identity provider (IdP) - pairwise, brokered and community trust models [41,42]. In network virtualization, SeP or InP may play a role as IdP and SP. The identity management may have any of the three trust relationships between SePs and/or InPs in network virtualization depending on the number of InPs and SePs. The PlanetLab, UCLP and X-bone uses PKI infrastructure (i.e., community trust) for authentication and trust management between SePs and InPs.

GENI uses a brokered trust model in which four entities namely clearinghouse, aggregates, research organization and researcher form a bilateral automatic trust negotiation [43-45] between them. The GENI is a decentralized system in which most of the times, a requester may not be from the same security domain (InP) for the authorization of resources. So, it uses attribute-based access control (ABAC) in which a request may be granted based on the characteristic of the requester's attributes. The negotiator contacts access mediator (i.e., GENI clearinghouse) to start bilateral negotiation (i.e., *automatic trust negotiation*). The negotiation is a sequence of credential exchange starting from non-sensitive credentials between negotiators. After successful negotiation, the request is granted to access the resource.

Resource access control

The authorization decision of an entity in a closed and open system about the resources is treated differently. So we divide the access control mechanism in two parts: local access control for a closed system and a global access control for the open system. The local access control performs the local authorization decision about the physical resources. The global access control performs the authorization decision of distributed virtual resources. We will compare three projects from academics and industry to know the status of resource access control in the network virtualization environment. Table 3 shows the access control mechanism used by the different projects.

The network *slices* of GENI are created out of physical network of *aggregates*. The aggregates are strangers to each other, so the GENI uses ABAC in which automatic trust negotiation is performed by exchanging

Table 3 Resource access control for network virtualization projects

Project	Physical resources	Virtual resources
GENI [36]	-	ABAC [43]
UCLP [38,46]	Switch management	MAC & DAC
X-bone [39]	ACL	ACL

sensitive credentials. ABAC authorizes the access to virtual resources using attribute *acknowledgement* (ACK) policies and *trust-target graph* (TTG) protocol. The ACK policy and TTG protocol perform attribute disclosure and resource access decisions respectively using directed graph.

The UCLP satisfies some requirements of **R6** and **R7** for physical and virtual network resources. The resource access control for UCLP physical resources is either implemented in the UCLP system, or an intermediate system between the UCLP and switch management. The UCLP system may use *mandatory access control* (MAC) or *discretionary access control* (DAC) for UCLP virtual resources. The UCLP supports three approaches for access control of UCLP virtual resources. The three approaches are traditional DAC, generic authorization-based distributed DAC and attributed-based distributed DAC. The first method performs all the evaluation of access and enforcement of policy in a centralized manner. The second method stores authorization information in different domains and performs the authorization process in multiple domains. The third method uses certificate-based system for authorization. The traditional DAC cannot make authorization of users in other domains. The second method is difficult to realize while the third approach is the easiest to implement.

X-bone system uses very simple access control mechanism for the authorization using ACL (access control list). It maintains the list of permission on the virtual resources for each user in the system. X-bone first checks the ACL for applicable entry to decide whether the requested operation is authorized based on subject and object identities.

Routing security issues

The user's virtual infrastructure of the SeP may be installed on an InP or a set of InPs in the *federation*. Similarly, the InP also collocates virtual networks from different SePs. The nature of the routing protocol used within InP and among InPs are totally different as per the security requirements, **R8** and **R9**. The routing protocol within InP for a set of SePs must provide *hop integrity*, *origin authentication* and *path validation*. The first three parameters are necessary for users' collocation of virtual networks in a InP. The fourth parameter provides least information disclosure and operational confidentiality of the virtual network installed on multiple InPs. The *hop integrity* of a routing protocol refers to the confidentiality between peers. The *origin authentication* is the authentication of a router. The *path validation* refers to the validity and authenticity of a received topological path. The *number of tenants* affects information leakage on the same physical network infrastructure. The routing protocol among InPs must provide control over the *information disclosure* and *routing basis*. The *routing basis* shows the significance of name-space and/or identity used in the routing protocol. Table 4 shows the comparison of routing protocols for all the parameters mentioned above. We have mainly focussed our investigation on the protocols which gives some security features and upcoming virtual network routing.

The three variants of BGP namely S-BGP, IRV, and So-BGP provide security services in terms of - *PKI*, *address attestation* (a statement of delegation of identity), a special SECURITY message, or *IRV–Identity Request Server* with no provision for *information disclosure*. The minimum disclosure routing (MDR), routing on flat label (ROFL) and secure virtual trust routing (SVTR) are the upcoming routing protocols for virtual network in the field of *federation*. The MDR gives the minimum disclosure and operational confidentiality through the extension of Secure Multi-party Computation (SMC). The SMC reveals secret information among multiple parties using their individual secrets. The nodes of ROFL routing guarantees origin authentication and path validation using self-certification and access control mechanism respectively. SVTR is the only protocol that gives provision for multi-tenant collocation using *hop integrity*.

Basic security services

The network virtualization projects have components to perform the specific functions related to either management or security services. Any data traffic — plain or protocol related — transferred in the projects may provide basic security services like authentication, confidentiality etc. Table 5 shows the data traffic among the component(s) and/or resource(s) of the projects. We will use the convention - "Authentication | Confidentiality | Protocol" for brevity to describe the basic security services. The values for the convention are: A for Authentication, S for Confidentiality, $\sim$ for negation, * for all available protocols for data transmission. The communication between the components of GENI, PlanetLab and UCLP is secured and authenticated while X-bone does not use authenticated communication. All projects do not provide secured communication between the resources while GENI provides authenticated data transfer between them. X-bone does not provide authenticated communication between resources and components while all other projects provide authenticated communication. All projects provide secured data transfer either optional or compulsory.

Virtual resources security

The virtual resources for network virtualization in monolithic cloud are fully or partially implemented as software. We specifically focussed on virtual resources namely virtual routers, virtual switches and virtual links. Sections 'Virtual routers', 'Virtual switches', 'Virtual links' and 'Virtual resource migration' gives the detailed survey

Table 4 Routing security issues for horizontal IaaS federation

Routing protocol	Hop integrity	Origin authentication	Path validation	Information disclosure	Routing basis	No. of tenants
MDR [47]	IPSec	-	-	YES (SMC)	Location & identity	Single
ROFL [48]	-	Self certification	ACM	-	Flat-label	Single
SVTR [49]	Secured	-	-	NO (Privacy of attributes)	Flow-level	Multiple
S-BGP [50]	PKI	Address attestation	Address attestation	-	Location & identity	Single
IRV [51]	Secure transport	Source attestation	IRV server	-	Location & identity	Single
So-BGP [52]	SECURITY message	SECURITY message	SECURITY message	-	Location & identity	Single

of virtual resources in monolithic IaaS cloud and generic network virtualization.

Virtual routers

The virtualization of software routers called *virtual software routers* exploits processing power out of physical router or commodity hardware using NICs or NetFPGA. Juniper's *intelligent logical router* on the top of M-Series and T-Series routers are examples of virtual software routers [53]. The *intelligent logical router* supports customized policy control, protocol assignment, configuration but no on-the-fly configuration and administration. It also does not support source authentication. Most of *virtual software routers* from monolithic cloud including Amazon EC2 use *route tables*. The *route table* maintains network filtering policy and are managed by VPC network administrator. The EC2 also uses *security groups* which offer secured virtual network isolation among cloud users.

The router has two modules: *control plane* and *data plane*. The control plane performs the function of routing and maintains routing table. The data plane performs the function of packet forwarding. All the router architectures using the combination of data and control plane proposed by Pisa et al. concentrates on performance in terms of delay [54]. The VROOM [55,56] router architecture also concentrates on the performance in terms of delay using control plane virtualization. Table 6 classifies the literature in two areas. First six literatures give the proposal of the router. The remaining gives the performance evaluation of *virtual software routers*. It is found that all *virtual software routers* provide physical or logical isolation to improve the performance but no specific security services. Some software routers on commodity hardware are implemented with general-purpose workstations [57-62]. The proposals for router design aim at low-cost and moderate-performance solutions and have no security provision.

Virtual switches

The virtual switches can be broadly divided into *hypervisor-based* or *hardware-based* depending on the location of the implementation of virtual switches. The hypervisor-based virtual switches are typically written entirely in software. The hardware-based virtual switch is partly implemented on special hardware like NIC, NetFPGA etc. The basis of hypervisor-based virtual switch is Open vSwitch [71]. Open vSwitch resides within the management domain of hypervisor (e.g. Domain-0 in Xen) and provides connectivity between virtual machines and physical interfaces. Open vSwitch uses VLANs and GRE tunnels for secured virtual network and virtual path respectively. It also supports basic ACL.

Hardware-based virtual switch eliminates some limitations (like CPU or memory usage) of software-based virtual switch. Two hardware-based virtual switch implementations are *Virtual Ethernet Port Aggregator* (VEPA) [72] and VNTag [73]. The Virtual Ethernet Port Aggregator (VEPA) is a standardization led by HP Extreme, IBM, Brocade and Juniper etc. The VEPA allows traffic of VM to exit and re-enter the same port to enable switching among VMs. The VEPA has *MACSec* scheme to provision a secure connection between VEPA and bridges.

Tseng et al. [74] proposed the integration of open-source hypervisor with software-based virtual switch and aims at secure network environment among VMs.

Table 5 Basic security services of network virtualization projects

Project	Resource-Component	Component-Component	Resource-Resources
GENI [36]	A | ∼S | SSL	A | S | SSL	A | ∼S | *
PlanetLab [37]	A | S | SSL	A | S | SSL	∼A | ∼S | *
UCLP [38]	A | S | (SSL/JINI)	A | S | (SSL & JINI)	∼A | ∼S | *
X-bone [39]	∼A | (S/∼S) | (UDP/UDP-S/TCP/TCP-SSL)	∼A | S | (UDP-S/TCP-SSL)	∼A | ∼S | *

* indicates all available protocols for data transmission.

Table 6 Commodity and physical virtual routers' control plane properties

Hardware type	Virtualization type	Control plane (Routing table)	Performance	Isolation	Migration	Flexibility
Commodity-Intel IXP2400 [58]	Pattern tables	L3VR and L3/4VR	×	√	-	√
Commodity-Click [63]	Trie braiding	Shared trie	√	-	-	-
Commodity-FPGA [64]	Hybrid DS	TCAM/SRAM	-	√	-	-
Commodity [65]	PEARL	NetFPGA & TCAM	√	√	-	√
Commodity-NetFPGA [56]	VROOM	Software & hardware	√	√	√	√
Simulation [66]	-	Trie braiding	-	-	×	×
Commodity [67]	Container-based	Guest OS	Evaluation(OpenVZ,LinuxNamespace) (OpenVZ,LinuxNamespace)	-	-	-
Commodity [68]	Hypervisor-based	Guest OS	Evaluation(SR,VSR)	-	-	-
Commodity [69]	Hypervisor-based	Guest OS	Evaluation(1,2,4 flows)	-	-	-
Commodity [70]	Container-based	Application	√	×	×	×
	Hypervisor-based	Guest OS	√	×	×	×
	Hypervisor-NIC mapping	Guest OS	√	√	×	×
	Hypervisor-Host OS	Guest OS	×	√	√	√

× indicates the property doesn't exist for the router.
√ indicates the property exist for the router.

Luo et al. [75] proposed hardware-based virtual switch using special NIC to provide network connectivity among VMs in the datacenter.

Virtual links

The virtual links can be created using either *signalling protocol* or *encapsulation*. The virtual link setup protocol (VLSP) is an example of signalling protocol to create the virtual links. The encapsulation-based virtual link creation in the literature are *Virtual Tunnel (VTun)*, *Layer Two Tunnelling Protocol - V3 (L2TPV3)*, *Generic Routing Encapsulation (GRE)* and *IP in IP Tunnelling (IIP)*.

Roland Bless et al. [76] proposed VLSP to create authenticated and secured virtual link using NSIS authorization [77] and secured signalling [78] protocols. It also provides QoS as per user's requirement for link creation. The L2TPV3 [79] encapsulation protocol creates tunnel between nodes at layer 2. It does not inherently provide authentication and encryption but IPSec can be used for security provision. The VTun is a virtual link implementation over various kinds of tunnels (e.g. Ethernet, serial tunnel, pipe tunnel) and; provides security services like authentication, compression and encryption etc. [80]. The GRE [81] encapsulation protocol is used to create a virtual link between two nodes using an additional header in the packet called *delivery header* without any security features. The IIP [82] link creation protocol has a packet format consisting of the outer header, security header, original header and IP payload. The security header adds optional security services using IPSec.

Virtual resource migration

As network virtualization is new emerging field, there is few literature on some important field like the migration of virtual router and link etc. Chen et al. uses VROOM [56] router architecture to provide energy-saving IP-WDM network architecture [83] by the process of virtual router migration. All the router architecture proposals and their migration methods using the combination of data and control plane proposed by Pisa et al. concentrates on performance in terms of delay [54]. The full virtual network migration including virtual machines is proposed by Keller et al [84]. All the literature concentrate on virtual resource migration without any security concerns. The virtual link migration suggested by Pisa et al does not provide any security services.

Research directions

All domains surveyed in the paper lacks network virtualization and/or its security provision. Most of network virtualization projects are meant for scientific purpose where the performance is major concern so the focus of the projects are collocation of SePs' networks on InPs' physical network without any security concerns. Similarly, datacenters do not exploit full network virtualization and facilitates minimum security services in terms of VLAN or VPN technology. The virtual resources lack very basic level of security services. As a result of aforementioned shortcomings, we will discuss NVE security issues for *federation* and give few research directions. The research directions are classified as: (a) router architecture (b)

datacenter NVE security, (c) resource identity management, (d) resource access control and (e) intra-InP and inter-InP routing.

Router architecture

All the router architectures using the combination of data and control plane concentrates on performance in terms of delay. The control plane as well as data plane virtualization allows best-effort memory utilization but may promote confidentiality threat due to the collocation of multiple SePs' virtual routers on the same physical router. The *software virtual routers* on commodity as well as physical router lacks source authentication, remote configuration using SeP's access control as shown in Table 6. The source authentication, remote configuration and access control mechanism are basic requirements (**R6**-**R10**) to perform inter-InP and intra-InP routing by the *software virtual routers*. By adding the above functionality, we pose few research questions like: What will be the impact on router performance in terms of packet-delay? What is the maximum number of tenants' virtual software routers that can coexist on a physical router without degrading the performance? How the router virtualization handles intra-InP and inter-InP routing by considering the collocation of tenants' virtual networks? How the virtual router migration be handle by this architecture?

Datacenter NVE security

The most promising datacenter network virtualization architecture for the *federation* is SEC2 [4] which supports basic security services like source authentication, transparent network management etc., but does not support full network virtualization (requirements **R1** and **R2**). The network isolation among customers of CloudNAS can be compromised if hypervisors, switches, or middleboxes are compromised [4]. The customized devices like FEs or CCs may expose MAC address of host and VM [30]. No datacenter supports federation of virtual resources (requirement **R10**), full NVE (requirements **R1**-**R2**) and resource access control (requirements **R6** and **R7**). All datacenter network virtualization projects support minimum security services using VLAN, L2/L3 addressing or special routing devices (e.g. FE, CC etc.) as shown in Table 1. The datacenter also do not permit *transparent network management* (requirement **R2**), user-level policy control and resource access control (requirements **R6** and **R7**) required for the *federation*.

Resource identity management

Table 2 shows that there is no identity management which provides the feature of multiple InPs and SePs (requirement **R5**), user's control over identities (requirement **R4**) and decentralized storage. We used the generic term *user control* to mean various operations on virtual resources e.g., creation of virtual link, configuration of virtual resource etc. The UCLP project shows some potential towards the design of an identity management for *federation* but lacks users' control over identities (requirement **R4**). The *federation* requires federated identity management, so a trust between InPs and/or SePs must be established to gain the control over the requested resources automatically on-the-fly. So, the *federation* needs the identity management with automated trust negotiation (requirement **R10**). We must also address the following research question related to resource identity management: How to map heterogeneous address space of resources in datacenters to local and global identity namespace?

Resource access control

The trivial resource access control for horizontal IaaS federation requires user-controlled access control mechanism (requirement **R7**) at virtual infrastructure and *mandatory access control* (requirement **R6**) at physical infrastructure. The GENI does not provide any kind of resource access control over the physical resources while virtual resources are managed in terms of *Trust-Target Graph* protocol of ABAC (requirement **R7**). The UCLP provisions MAC or DAC at virtual infrastructure level but it does not fulfil the requirement at physical level. X-bone uses ACL, a simplest access control management of resources. Some research questions related to resource access control are: Where should be the placement of resource access controls in physical resources? If the location of access control is in *control plane* of physical resource; and distributed among InPs and SePs, how would they interact? What would be *bandwidth-delay product* performance of physical as well as virtual network infrastructures after deploying resource access controls?

Intra-InP and Inter-InP routing

Keller et al. [85] and Fukushima et al. [47] open up theoretical research directions for intra-InP and inter-InP routing respectively. The inter-InP routing should not disclose routing information to InPs other than intended InPs (i.e *minimum disclosure*) and also provide operational confidentiality in routing process. MDR offers both *minimum disclosure* and operational confidentiality among InPs but does not provide other properties mentioned in Table 4. The intra-InP and inter-InP routing should possess the security requirements, **R6** and **R7** with the consideration of tenants' virtual network collocation. We pose the following research questions for routing process in the *federation* by including aforementioned security requirements: How the router maintains *routing table* using intra-InP and inter-InP routing? How the information (i.e., packets) of different virtual networks of cloud users are separated? How the router will forward the

packets of different virtual networks without exposing or compromising?

Conclusions

With the motivation of adding full network virtualization in horizontal IaaS federation, we investigated network virtualization security in four areas: monolithic IaaS cloud, generic network virtualization, datacenter network virtualization and virtual resources. We presented the qualitative comparisons of *generic network virtualization projects*, datacenters, routing protocols and virtual resources from aforementioned areas. Our qualitative comparisons show the following important insights related to network virtualization and security issues in horizontal IaaS federation. The monolithic IaaS clouds do not support full network virtualization but give minimal network virtualization to offer the connectivity of virtual networks or virtual machines. The simple security services are offered in terms of VLAN, VPN or tunnelling for the collocation of multiple tenants in monolithic IaaS clouds. The datacenters lack both full network virtualization and basic security services for the horizontal IaaS federation. The network virtualization projects offer full network virtualization but partial security provisions in terms of one or more services of identity management, resource access control and trust management. The router architectures mostly focus on the performance of virtual software routers and do not add any security features for the collocation of tenants networks. The virtual switches cannot have more than 4K VLANs. This paper shows that the virtual links can be created using either signalling protocol or encapsulation. The encapsulation-based virtual link has an extra overhead of encapsulation on the top of L2/L3 protocols but give *hop integrity* security service. The signalling-based virtual link offers various security services like *origin authentication*, *hop integrity* and *path validation*. The research challenges mentioned in Section 'Research directions' are crucial to the success of horizontal IaaS federation in cloud computing.

Competing interests

The authors declare that they have no competing interests.

Authors' contributions

All the listed authors made substantive intellectual contributions to the research work and manuscript. AVN formally defined the network virtualization for horizontal IaaS federation. He and SKG investigated the domains presented in the manuscript. SKG was responsible for the overall technical approach and edited the paper. Both authors read and approved the final manuscript.

Received: 20 February 2013 Accepted: 15 November 2013
Published: 21 November 2013

References

1. Celesti A, Tusa F, Villari M, Puliafito A (2010) How to enhance cloud architectures to enable cross-federation. In: Cloud Computing (CLOUD), 2010 IEEE 3rd international conference on. IEEE, Miami, pp 337–345
2. Armbrust M, Fox A, Griffith R, Joseph AD, Katz R, Konwinski A, Lee G, Patterson D, Rabkin A, Stoica I, Zaharia M (2010) A view of cloud computing. Commun ACM 53(4): 50–58. http://doi.acm.org/10.1145/1721654.1721672
3. Zhang Z, Zhang X (2009) Realization of open cloud computing federation based on mobile agent. In: Intelligent computing and intelligent systems, 2009. ICIS 2009. IEEE international conference on, Volume 3. IEEE, Shanghai, pp 642–646
4. Hao F, Lakshman TV, Mukherjee S, Song H (2010) Secure cloud computing with a virtualized network infrastructure. In: Proceedings of the 2nd USENIX conference on Hot topics in cloud computing, HotCloud'10. USENIX Association, Berkeley, pp 16–16. http://dl.acm.org/citation.cfm?id=1863103.1863119
5. Berger S, Cáceres R, Goldman K, Pendarakis D, Perez R, Rao JR, Rom E, Sailer R, Schildhauer W, Srinivasan D, Tal S, Valdez E (2009) Security for the cloud infrastructure: trusted virtual data center implementation. IBM J Res Dev 53(4): 560–571. http://dl.acm.org/citation.cfm?id=1850659.1850665
6. Berger S, Cáceres R, Pendarakis D, Sailer R, Valdez E, Perez R, Schildhauer W, Srinivasan D (2008) TVDc: managing security in the trusted virtual datacenter. SIGOPS Oper Syst Rev 42: 40–47. http://doi.acm.org/10.1145/1341312.1341321
7. Chowdhury N, Boutaba R (2009) Network virtualization: state of the art and research challenges. Commun Mag IEEE 47(7): 20–26
8. Fan P, Chen Z, Wang J, Zheng Z, Lyu M (2012) Topology-aware deployment of scientific applications in cloud computing. In: Cloud Computing (CLOUD), 2012 IEEE 5th international conference on. IEEE, Honolulu, pp 319–326
9. Chae Y, Merugu S, Zegura E, Bhattacharjee S (2000) Exposing the network: support for topology-sensitive applications. In: Open Architectures and Network Programming, 2000. Proceedings. OPENARCH 2000. 2000 IEEE Third Conference on. IEEE, Tel, Aviv, pp 65–74
10. Celesti A, Tusa F, Villari M, Puliafito A (2010) Three-phase cross-cloud federation model: the cloud SSO authentication. In: Advances in Future Internet (AFIN), 2010 second international conference on. IEEE, Venice, pp 94–101
11. Chowdhury NMK, Boutaba R (2010) A survey of network virtualization. Comput Netw 54(5): 862–876. http://dx.doi.org/10.1016/j.comnet.2009.10.017
12. Bari M, Boutaba R, Esteves R, Granville L, Podlesny M, Rabbani M, Zhang Q, Zhani M (2012) Data center network virtualization: a survey. Commun Surv Tutorials, IEEE PP(99): 1–20
13. Buyya R, Ranjan R, Calheiros RN (2010) InterCloud: utility-oriented federation of cloud computing environments for scaling of application services. In: Proceedings of the 10th international conference on algorithms and architectures for parallel processing - Volume Part I, ICA3PP'10. Springer-Verlag, Berlin, Heidelberg, pp 13–31. http://dx.doi.org/10.1007/978-3-642-13119-6_2
14. Matias J, Jacob E, Sanchez D, Demchenko Y (2011) An OpenFlow based network virtualization framework for the cloud. In: Cloud Computing Technology and Science (CloudCom), 2011 IEEE Third International Conference on. IEEE, Athens, pp 672–678
15. Vaquero LM, Rodero-Merino L, Morán D (2011) Locking the sky: a survey on IaaS cloud security. Computing 91: 93–118. http://dx.doi.org/10.1007/s00607-010-0140-x
16. Iankoulova I, Daneva M (2012) Cloud computing security requirements: A systematic review. In: Research Challenges in Information Science (RCIS), 2012 sixth international conference on, pp 1–7
17. Natarajan S, Wolf T (2012) Security issues in network virtualization for the future Internet. In: Computing, Networking and Communications (ICNC), 2012 international conference on, pp 537–543
18. Security Guidance for Critical Areas of Focus in Cloud Computing V3.0, Cloud Security Alliance. Tech. rep. 2011. https://cloudsecurityalliance.org/guidance/csaguide.v3.0.pdf
19. Rubin A, Geer JDE (1998) A survey of Web security. Computer 31(9): 34–41
20. Onisick J (2012) Access Layer Network Virtualization: VN-Tag and VEPA. http://wikibon.org/wiki/v/Edge_Virtual_Bridging
21. Amazon Virtual Private Cloud Network - Administrator Guide. Tech. rep. 2012. http://awsdocs.s3.amazonaws.com/VPC/latest/vpc-nag.pdf
22. Amazon Virtual Private Cloud - User Guide. Tech. rep. 2012. http://awsdocs.s3.amazonaws.com/VPC/latest/vpc-ug.pdf
23. GoGrid - Getting Started Guide L-20121018. Tech. rep. 2012. http://storage.pardot.com/3442/103057/WP_Getting_Started_L_20121018.pdf

24. Xu Z, Di S, Zhang W, Cheng L, Wang CL (2011) WAVNet: Wide-area network virtualization technique for virtual private cloud. In: Parallel Processing (ICPP), 2011 international conference on, pp 285–294
25. Benson T, Akella A, Shaikh A, Sahu S (2011) CloudNaaS: a cloud networking platform for enterprise applications. In: Proceedings of the 2nd ACM symposium on cloud computing, SOCC '11. ACM, New York, pp 8:1–8:13. http://doi.acm.org/10.1145/2038916.2038924
26. Edwards A, Fischer A, Lain A (2009) Diverter: a new approach to networking within virtualized infrastructures. In: Proceedings of the 1st ACM workshop on Research on enterprise networking, WREN '09. ACM, New York, pp 103–110. http://doi.acm.org/10.1145/1592681.1592698
27. Hao F, Lakshman TV, Mukherjee S, Song H (2010) Enhancing dynamic cloud-based services using network virtualization. SIGCOMM Comput Commun Rev 40: 67–74. http://doi.acm.org/10.1145/1672308.1672322
28. Rodrigues H, Santos JR, Turner Y, Soares P, Guedes D (2011) Gatekeeper: supporting bandwidth guarantees for multi-tenant datacenter networks. In: Proceedings of the 3rd conference on I/O virtualization, WIOV'11. USENIX Association, Berkeley, pp 6–6. http://dl.acm.org/citation.cfm?id=2001555.2001561
29. Lam T, Vahdat A, Radhakrishnan S, Varghese G (2010) NetShare: Virtualizing Data Center Networks across Services. Tech. rep., Microsoft Research Lab. http://research.microsoft.com/apps/video/dl.aspx?id=132892
30. Mudigonda J, Yalagandula P, Mogul J, Stiekes B, Pouffary Y (2011) NetLord: a scalable multi-tenant network architecture for virtualized datacenters. SIGCOMM Comput Commun Rev 41(4): 62–73. http://doi.acm.org/10.1145/2043164.2018444
31. Ballani H, Costa P, Karagiannis T, Rowstron A (2011) Towards predictable datacenter networks. SIGCOMM Comput Commun Rev 41(4): 242–253. http://doi.acm.org/10.1145/2043164.2018465
32. Niranjan Mysore R, Pamboris A, Farrington N, Huang N, Miri P, Radhakrishnan S, Subramanya V, Vahdat A (2009) PortLand: a scalable fault-tolerant layer 2 data center network fabric. SIGCOMM Comput Commun Rev 39(4): 39–50. http://doi.acm.org/10.1145/1594977.1592575
33. Mudigonda J, Yalagandula P, Al-Fares M, Mogul JC (2010) SPAIN: COTS data-center Ethernet for multipathing over arbitrary topologies. In: Proceedings of the 7th USENIX conference on Networked systems design and implementation, NSDI'10. USENIX Association, Berkeley, pp 18–18. http://dl.acm.org/citation.cfm?id=1855711.1855729
34. Greenberg A, Hamilton JR, Jain N, Kandula S, Kim C, Lahiri P, Maltz DA, Patel P, Sengupta S (2009) VL2: a scalable and flexible data center network. SIGCOMM Comput Commun Rev 39(4): 51–62. http://doi.acm.org/10.1145/1594977.1592576
35. Cao Y, Yang L (2010) A survey of identity management technology. In: Information Theory and Information Security (ICITIS), 2010 IEEE international conference on. IEEE, Beijing, pp 287–293
36. GENI Security Architecture, Global Environment for Network Innovations. Tech. rep. http://groups.geni.net/geni/attachment/wiki/GENISecurity/GENI-SEC-ARCH-0.4.pdf
37. Peterson L, Roscoe T, Muir S, Klingaman A (2006) PlanetLab architecture: an overview. Tech. rep., PlanetLab Consortium
38. Hulsebosch B, Groote R, Snijders M (2009) Secure user-controlled lightpath provisioning with user-controlled identity management. In: Proceedings of the 3rd international conference on autonomous infrastructure, management and security: scalability of networks and services, AIMS '09. Springer-Verlag, Berlin, Heidelberg, pp 1–14. http://dx.doi.org/10.1007/978-3-642-02627-0_1
39. Clem J, MacAlpine T, Badgett B (2003) X-Bone: Automated System for Deployment and Managament of Network Overlays Security Assessment Report. Tech. rep., Information Design Assurance Red Team, Sandia National Laboratories, P. O. Box 5800, Albuquerque, NM 87185-0784, 2003. http://www.isi.edu/xbone/pubs/xbone_security_assessment.pdf
40. Chowdhury N, Zaheer FE, Boutaba R (2009) iMark: An identity management framework for network virtualization environment. In: Integrated Network Management, 2009. IM '09. IFIP/IEEE International Symposium on. IEEE, Long Island, pp 335–342
41. Bhargav-Spantzel A, Squicciarini A, Bertino E (2007) Trust negotiation in identity management. Secur Privacy, IEEE 5(2): 55–63
42. Zhang P, Durresi A, Barolli L (2011) Survey of trust management on various networks. In: Complex, Intelligent and Software Intensive Systems (CISIS), 2011 international conference on. IEEE Computer Society, Seoul, pp 219–226
43. Winsborough W, Jacobs J (2003) Automated trust negotiation technology with attribute-based access control. In: DARPA Information Survivability Conference and Exposition, 2003. Proceedings, Volume 2. IEEE Computer Society, Los Alamitos, pp 60–62
44. Li N, Winsborough W (2002) Towards practical automated trust negotiation. In: Proceedings of the 3rd international workshop on policies for distributed systems and networks (POLICY'02), POLICY '02. IEEE Computer Society, Washington, p 92. http://dl.acm.org/citation.cfm?id=863632.883493
45. Winsborough WH, Li N (2002) Protecting sensitive attributes in automated trust negotiation. In: Proceedings of the 2002 ACM workshop on Privacy in the Electronic Society, WPES '02. ACM, NY, pp 41–51. http://doi.acm.org/10.1145/644527.644532
46. Chen J (2004) UCLP Security. Tech. rep., School of Information Technology and Engineering University of Ottawa. www.uclp.ca/files/uclp1.x/Report-UCLP-Security.pdf
47. Fukushima M, Hasegawa T, Hasegawa T, Nakao A (2011) Minimum disclosure routing for network virtualization. In: Computer communications workshops (INFOCOM WKSHPS), 2011 IEEE Conference on. IEEE, Shanghai, pp 858–863
48. Caesar M, Condie T, Kannan J, Lakshminarayanan K, Stoica I (2006) ROFL: routing on flat labels. SIGCOMM Comput Commun Rev 36(4): 363–374. http://doi.acm.org/10.1145/1151659.1159955
49. Huang D, Ata S, Medhi D (2010) Establishing secure virtual trust routing and provisioning domains for future internet. In: Global telecommunications conference (GLOBECOM 2010), 2010 IEEE. IEEE, Miami, pp 1–6
50. Kent S, Lynn C, Seo K (2000) Secure Border Gateway Protocol (S-BGP). Selected Areas Commun, IEEE J 18(4): 582–592
51. Goodell G, Aiello W, Griffin T, Ioannidis J, McDaniel P, Rubin A (2003) Working around BGP: an incremental approach to improving security and accuracy of interdomain routing. In: In Proc. NDSS. Internet Society, San Diego
52. Ng J (2002) Extensions to BGP to Support Secure Origin BGP (soBGP). Tech. rep., IETF. http://tools.ietf.org/pdf/draft-ng-sobgp-bgp-extensions-00.txt
53. Kolon M (2004) Intelligent Logical Router Service. Tech. rep., Juniper Networks. http://netscreen.com/solutions/literature/white_papers/200097.pdf
54. Pisa P, Fernandes N, Carvalho H, Moreira M, Campista M, Costa L, Duarte O (2010) OpenFlow and Xen-Based Virtual Network Migration. In: Pont A, Pujolle G, Raghavan S (eds) Communications: wireless in developing countries and networks of the future, Volume 327 of IFIP advances in information and communication technology. Springer, Berlin, Heidelberg, pp 170–181. http://dx.doi.org/10.1007/978-3-642-15476-8_17
55. Layer 3 Virtual Switching - Integrated Virtual Routing with Multi-Layer Switching. Tech. rep., Extreme Networks, Inc 2006. http://www.extremenetworks.com/libraries/whitepapers/WPL3Virtual_1185.pdf
56. Wang Y, Keller E, Biskeborn B, van der Merwe J, Rexford J (2008) Virtual routers on the move: live router migration as a network-management primitive. SIGCOMM Comput Commun Rev 38(4): 231–242. http://doi.acm.org/10.1145/1402946.1402985
57. Rus A, Barabas M, Boanea G, Dobrota V (2010) Implementation of QoS-Aware virtual routers. In: Electronics and Telecommunications (ISETC), 2010 9th International Symposium on, pp 161–164
58. Comer D, Martynov M (2006) Building experimental virtual routers with network processors. In: Testbeds and Research Infrastructures for the Development of Networks and Communities, 2006. TRIDENTCOM 2006. 2nd International Conference on. IEEE, Barcelona, pp 9–230
59. Bianco A, Birke R, Bolognesi D, Finochietto J, Galante G, Mellia M, Prashant M, Neri F (2005) Click vs. Linux: two efficient open-source IP network stacks for software routers. In: High performance switching and routing, 2005. HPSR. 2005 workshop on. IEEE, Hong Kong, pp 18–23
60. Dobrescu M, Egi N, Argyraki K, Chun BG, Fall K, Iannaccone G, Knies A, Manesh M, Ratnasamy S (2009) RouteBricks: exploiting parallelism to scale software routers. In: Proceedings of the ACM SIGOPS 22nd symposium on Operating systems principles, SOSP '09. ACM, New York, pp 15–28
61. Karlin S, Peterson L (2001) VERA: an extensible router architecture. In: Open architectures and network programming proceedings, 2001 IEEE, pp 3–14

62. Spalink T, Karlin S, Peterson L, Gottlieb Y (2011) Building a robust software-based router using network processors. SIGOPS Oper Syst Rev 35(5): 216–229. http://doi.acm.org/10.1145/502059.502056
63. Fu J, Rexford J (2008) Efficient IP-address lookup with a shared forwarding table for multiple virtual routers. In: Proceedings of the 2008 ACM CoNEXT Conference, CoNEXT '08. ACM, New York, pp 21:1–21:12. http://doi.acm.org/10.1145/1544012.1544033
64. Erdem O, Le H, Prasanna V, Bazlamacci C (2011) Hybrid data structure for IP lookup in virtual routers using FPGAs. In: Application-Specific Systems, Architectures and Processors (ASAP), 2011 IEEE international conference on. IEEE, Santa Monica, pp 95–102
65. Xie G, He P, Guan H, Li Z, Xie Y, Luo L, Zhang J, Wang Y, Salamatian K (2011) PEARL: a programmable virtual router platform. Commun Mag, IEEE 49(7): 71–77
66. Song H, Kodialam M, Hao F, Lakshman T (2010) Building scalable virtual routers with trie braiding. In: INFOCOM, 2010 proceedings IEEE. IEEE, San Diego, pp 1–9
67. Rathore M, Hidell M, Sjodin P (2010) Performance evaluation of open virtual routers. In: GLOBECOM workshops (GC Wkshps), 2010 IEEE. IEEE, Miami, pp 288–293
68. Rojas-Cessa R, Salehin K, Egoh K (2011) Experimental performance evaluation of a virtual software router. In: Local Metropolitan Area Networks (LANMAN), 2011 18th IEEE Workshop on. IEEE, Chapel Hill, pp 1–2
69. Rojas-Cessa R, Salehin K, Egoh K (2012) Evaluation of switching performance of a virtual software router. In: Sarnoff symposium (SARNOFF), 2012 35th IEEE. IEEE, Newark, pp 1–5
70. Bourguiba M, Haddadou K, Pujolle G (2010) Evaluating the forwarding plane performance of the commodity hardware virtual routers. In: Communications and Networking (ComNet), 2010 second international conference on. IEEE, Tozeur, pp 1–8
71. Pfaff B, Koponen T, Amidon K, Casado M, Pettit J, Shenker S (2009) Extending networking into the virtualization layer. In: 8th ACM Workshop on Hot Topics in Networks (HotNets-VIII). ACM SIGCOMM, NY
72. Congdon P (2008) Virtual Ethernet Port Aggregator Standards Body Discussion. http://www.ieee802.org/1/files/public/docs2008/new-congdon-vepa-1108-v01.pdf
73. Pelissier J (2008) VNTag 101. http://www.ieee802.org/1/files/public/docs2009/new-pelissier-vntag-seminar-0508.pdf
74. Tseng HM, Lee HL, Hu JW, Liu TL, Chang JG, Huang WC (2011) Network virtualization with cloud virtual switch. In: Parallel and Distributed Systems (ICPADS), 2011 IEEE 17th international conference on. IEEE, Tainan, pp 998–1003
75. Luo Y (2010) Network I/O virtualization for cloud computing. IT Prof 12(5): 36–41
76. Bless R, Rohricht M, Werle C (2011) Authenticated setup of virtual links with quality-of-service guarantees. In: Computer Communications and Networks (ICCCN), 2011 proceedings of 20th international conference on. IEEE, Maui, pp 1–8
77. Manner J, Tschofenig H, Bless R, Stiemerling M (2001) Authorization for NSIS Signaling Layer Protocols. RFC5981. Internet Engineering Task Force. https://tools.ietf.org/html/rfc5981
78. Bless R, Röhricht M (2009) Secure signaling in next generation networks with NSIS. In: Proceedings of the 2009 IEEE international conference on Communications, ICC'09. IEEE Press, Piscataway, pp 2156–2161. http://dl.acm.org/citation.cfm?id=1817271.1817673
79. Lau J, Townsley M, Goyret I (2005) Layer Two Tunneling Protocol - Version 3 (L2TPv3). RFC3931. Internet Engineering Task Force. http://www.ietf.org/rfc/rfc3931.txt
80. VTun - Virtual Tunnels over TCP/IP networks. Tech. rep. http://vtun.sourceforge.net/tun/
81. Farinacci D, Li T, Hanks S, Meyer D, Traina P (2000) Generic Routing Encapsulation (GRE). RFC2784. Internet Engineering Task Force. www.ietf.org/rfc/rfc2784.txt
82. Simpson W (1995) IP in IP Tunneling. RFC1853. Internet Engineering Task Force. http://www.ietf.org/rfc/rfc1853.txt
83. Chen X, Phillips C (2012) Virtual router migration and infrastructure sleeping for energy management of IP over WDM networks. In: Telecommunications and Multimedia (TEMU), 2012 International Conference on, pp 31–36
84. Keller E, Ghorbani S, Caesar M, Rexford J (2012) Live migration of an entire network (and its hosts). In: Proceedings of the 11th ACM Workshop on Hot Topics in Networks, HotNets-XI. ACM, New York, pp 109–114. http://doi.acm.org/10.1145/2390231.2390250
85. Keller E, Lee RB, Rexford J (2009) Accountability in hosted virtual networks. In: Proceedings of the 1st ACM workshop on Virtualized infrastructure systems and architectures, VISA '09. ACM, New York, pp 29–36. http://doi.acm.org/10.1145/1592648.1592654

doi:10.1186/2192-113X-2-19
Cite this article as: Nimkar and Ghosh: **Towards full network virtualization in horizontal IaaS federation: security issues.** *Journal of Cloud Computing: Advances, Systems and Applications* 2013 **2**:19.