2012 IEEE Eighth World Congress on Services

Secure Private Cloud Architecture for Mobile Infrastructure as a Service

Susmita Horrow
Department of mathematics
IIT Roorkee, India
hsusmita4@gmail.com

Sanchika Gupta
Department of Electronics and Computer Engineering
IIT Roorkee, India
sanchigr8@gmail.com

Anjali Sardana
Department of Electronics and Computer Engineering
IIT Roorkee, India
anjlsfec@iitr.ernet.in

Ajith Abraham
Faculty of Electrical Engineering and Computer science
IT for Innovations - EU Center of Excellence
VSB-Technick Univerzita Ostrava
Ostrava – Poruba, Czech Republic
ajith.abraham@ieee.org

Abstract— **Cloud based systems have gained popularity over traditional systems owing to their advantages like cost effectiveness, pay per use, scalability and ease to upgrade. Market is dominated by various cloud vendors providing Infrastructure as a Service (IaaS). However threat to security in mobile IaaS based cloud environment prohibits the usage of services specially, in case of public cloud environment. In this paper we propose secure private cloud architecture for mobile infrastructure as a service. As a prototype service, we deploy a virtual research lab which provides infrastructure and computing resources dynamically in a secure way. The proposed secure private cloud architecture for the lab environment provides the cloud services along with mobility. Mobility gives the researcher the flexibility to access cloud services on their mobile devices anywhere and anytime. We analyse the proposed architecture using a prototype on OpenNebula platform and compare it with traditional computational infrastructure. Results show that our architecture is capable to support 84% more users.**

Keywords- ***Cloud Computing, Private Cloud, Security, Mobility***

I. INTRODUCTION

Cloud Computing has changed the way of managing computing resources. It has enabled to use the computing resources as public utility. The following discussion throws light on how cloud computing can enhance the environment of research lab. Assume the environment of a research lab in the present scenario. A researcher is constrained by the working hour of the lab, because he/ she need to be physically present in the lab to work in the computer systems of the lab. Hence there is a need of a system which can provide remote access to the systems present in the lab from any place outside the lab. Traditional approach tries to solve the above problem by providing remote desktop access to the systems or server present in the lab. Hence work can be done conveniently at any place. But this approach has certain limitations and this does not address the requirements of the researchers in the present scenario.

In present scenario, it is unlikely that a researcher will be confined to a single operating system platform. There are a number of computing platforms, software tools etc. which a researcher might want to access simultaneously. He/ she may need different combinations of operating system platforms and software tools depending on the requirement from time to time. So each time reinstalling and backing up data become a monotonous job. Along with actual research, a researcher's attention is deviated towards setting of computing environment. Hence there is a need of a system which can free a researcher from the worries of setting up computing environment. Even if a researcher relies on remote server for computational task, he/ she have to be constrained by the computing platform of the server.

Again the present computing environments are very rigid and do not scale well. If we closely study the usage of computing resources in traditional environment, we find that there is non-uniform pattern in the demand of computing resources at different point of time. At certain period of time such as heavy experimentation or analysis period, the number of active users is the highest. Hence the demand of computing resources increases and the traditional infrastructure becomes inadequate to meet those demands in effective manner. In rest of the time, the computing resources are not fully utilized. Hence if infrastructure is built keeping in mind the heavy demand period, then the computing resources are likely to be underutilized at certain period of time. So there is trade-off user satisfaction and resource utilization.

978-0-7695-4756-5/12 $26.00 © 2012 IEEE
DOI 10.1109/SERVICES.2012.25

IEEE computer society

Hence a system is required which can provide computing resources on demand which can be scaled up or down as per requirement and can be accessible to the user remotely. Such systems can be achieved by the deployment of cloud. Cloud operates on the principle of virtualization. Cloud virtualizes all the physical resources and provides customized infrastructure to the user in the form of a virtual machine. The access to the virtual machine can be provided to the user with the help of any remote desktop access technology. This approach can solve the problems sited above and can provide features as follows:

Mobility: Here by mobile infrastructure, we mean that infrastructure will reside in cloud and users can access them through mobile devices from any place they like.

Scalability: As cloud works on the principle of virtualization, it is very easy to provision new computing environment within no time. So user need not worry about the setting up the computing environment. Whenever there is a change of computing environment, customized infrastructure can be leased from cloud.

Flexibility: User not only can scale up the capabilities of the infrastructure, he/ she can have the flexibility of changing the computing platform.

However, moving to cloud involves the risk of security. The user does not have the same level of control as that of standalone system in case of cloud, because user data present in the cloud provider's system. In an educational institute, there are information related to research work, patents and other confidential issues. The confidentiality and privacy of data cannot be ensured completely. Again the service is provided through internet, the data in transit is vulnerable to various kinds of network level attacks like eavesdropping and session hijacking. Hence there is a need of a system which can provide cloud service to the organization or institute internally as which can be trusted for the confidentiality of data. This kind of systems can be realized by building private cloud. A private cloud is solely owned by a single organization and managed internally or a trustworthy third party. As the private cloud is meant for a single organization, the threat of compromise of data with outside world is mitigated. Enforcement and management of security policy become easier as these things have to deal with a single organization. Private cloud is cost effective as compared to the public cloud. As it is meant for a single organization, the requirements of the users are limited and properly specified. So building a private cloud can be more cost effective rather than using public cloud services.

The proposed system aims to provide infrastructure that is mobile in nature. In other words researchers do not have to be fixed with particular location to work. They may work wherever they like. Besides they need not be constrained with the working hour of lab, because they can work at any time.

The rest of the paper is organized as follows. Section II describes the proposed architecture followed by the discussion of design issues in Section III. Section IV gives the evaluation of the proposed system against the parameters, number of users serviced. Section V gives the overview of the related work. Finally Section VI concludes the paper.

II. ARCHITECTURE OF THE PROPOSED SYSTEM

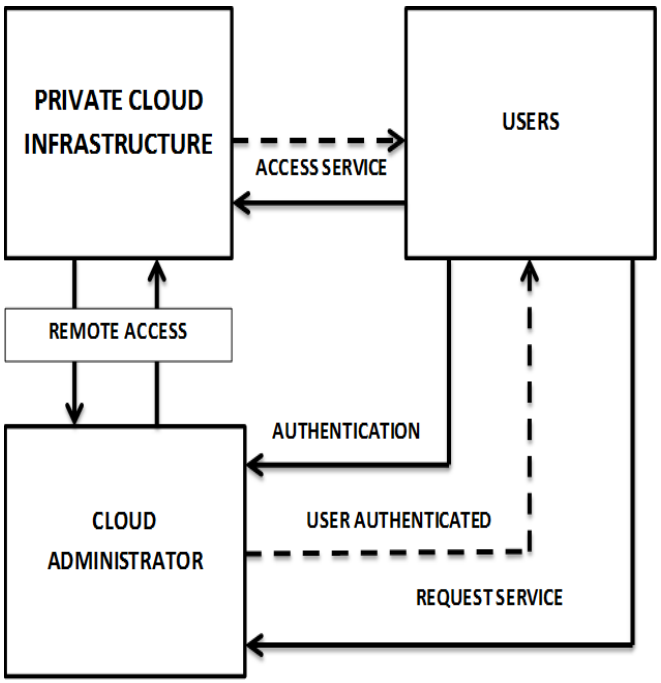

Fig. 1. High Level Architecture of the Proposed System

In this section, we discuss the basic components of the proposed architecture and interaction among these components.

Figure1 shows the high level architecture of the proposed system which consists of Users, Cloud Infrastructure and Cloud Administrator. Cloud Administrator refers to the person or group of people responsible for management of the infrastructure and for servicing user request. The user needs to authenticate

himself/herself to the Cloud Administrator. Cloud Infrastructure refers to a set of computers configured to provide cloud service to the user as per specification. Whenever any request for resources comes, cloud administrator provides a virtual machine of specified configuration through the cloud infrastructure. The virtual machine runs in one of the computers of the Cloud Infrastructure. Then the user can access the virtual machine either through the desktops or mobile devices.

Front end acts as an administrator and keeps the accounting information about the virtual machines and the users accessing the virtual machines. It keeps the required installation files which are made available to the cluster nodes through file sharing.

Clusters are the computers which host the virtual machines. So cluster node should have any of the virtualization technique enabled. The images of the operating systems required by the virtual machines are stored in the image repository.

The work flow of our system is explained in the following steps:

1. Authentication: The user has to authenticate himself/herself to the Cloud Administrator.
2. Request: Then the user gives the specification in the given format < Operating system, Memory, Hard Disk, Processor, Software >.
3. Once a client submits the specification, the Cloud Admin creates a template for virtual machine. Then a virtual network is created. Then Cloud Admin issues the create virtual machine command.
4. Thenfront end runs scheduling algorithm and selects a suitable cluster which can host a virtual machine of required configuration.
5. The requested operating system image is selected from the image repository and is copied to the cluster.
6. Then the hypervisor (Virtual Machine Monitor) present in the cluster is signalled to deploy the VM.
7. The VM comes to running state after setting up network bridging to provide a virtual NIC with a virtual MAC.

III. DESIGN ISSUES

A. *Networking*

There should be robust networking among the front end and the cluster nodes as well as among the virtual machines running in the cluster nodes. In order to communicate with virtual machines, a virtual network has to be created. A single virtual network is analogous to a physical switch containing DHCP server. Virtual machines attached to this physical switch are isolated from the network traffic on another physically separated switch. Creation of virtual network requires the following parameters <Name, Bridge, Type> where Name: Name of the Virtual Network, Bridge: Name of the physical bridge in the physical host where the VM should connect its network interface, Type: Ranged/Fixed.

In case of Ranged type, the user has to mention the network address along with the subnet mask. In case of fixed type, a set of IPs are needed to be specified which are called as leases.

When a new Virtual Machine is launched, its virtual network interface (defined in the NIC section of the VM template) is connected to the pre-existing bridge or physical device specified in the Virtual Network definition. The IP and MAC addresses are assigned to the virtual machine. The VM is assigned IP as per the specification provided in virtual network template. The MAC address assigned to the virtual machine is a transformation of the IP address. For example if a VM has got a MAC address: 00:03:c0:a8:00:01, then it corresponds to an IP address: 192.168.0.1 which is obtained by converting hex to int as follows: c0 = 192 a8 = 168.

In case of virtual networking, all the packets that arrive through the physical device are forwarded over all the virtual network interfaces of all the running VMs. If a VM has configured with an IP of the network same as the network of the recipient, then that VM will capture the packet, otherwise it will simply ignore the packet.

B. *Virtualization*

To host virtual machines, cluster nodes any one of the virtualization technology. KVM, Xen, VMWare and VBox are some of the eminent virtual technologies available. Among them, KVM and Xen require hardware virtualization technology enabled processors.

While implementing cloud, front end keeps track of the cluster nodes which will run the virtual machine. Hence while adding a cluster node as a potential node to run virtual machine, the specification of its virtualization technology must be given to the front end so that appropriate driver would be invoked to interact.

C. *Remote Access*

The front end needs to access the cluster nodes to deploy the virtual machine. So the cluster nodes should be remotely accessible. To do remote access to cluster nodes, secure shell technique has been employed. The front end should have complete access that is it should not be prompted for the password of the cluster nodes while connecting via SSH. In order to accomplish this task, a public key of front end is generated and it is copied over to the cluster node. That key is added to the list of known users in the cluster node. Hence when the front end user SSH into the cluster node, it will not be prompted to enter the password of the cluster.

D. *User Interface*

Interaction of the user with the system is a three-way process. First the user has to register to the system. Once an account is created, the user can login to the system and can use the services provided.

For security reasons and ease access of management, we have kept the provision for creating different user profiles.

Different user profiles have different level of credibility. The user profile is defined as a vector of three attributes such as User Name, User Type, User Specification. It is represented as follows:

$U_j[i] = \langle N, T, V \rangle$

Where $U_j[i]$ represents i^{th} attribute for the user j

User type specifies the level of credibility. There are three levels of credibility depending upon the level of security with level 1 having the highest security and level 3 having the lowest security.

User specification is defined as a vector of five parameters such as Operating system, Memory, Hard Disk, Processor, Software.

$V_j[i] = \langle O,M,H,P,S \rangle$

Where $V_j[i]$ represents i^{th} specification for the user j.

<O,M,H,P,S> represent operating system, memory, hardware, processor and software respectively. Among these five parameters the first four are mandatory to specify. The last parameter is optional.

E. *Security*

For any computing environment, security is a major concern. But certain dimensions of security are changed while moving to cloud. In this section we discuss the security issues that are going to be addressed.

In cloud environment, each user has its dedicated virtual machine to perform the computational operations. But all the information is present on the same physical infrastructure. There might be case when an attacker on the virtual machine can gain access to another victim VM. The attacker can monitor the victim's resource usage causing threats to the confidentiality, integrity and availability of the data of the victim that reside in cloud. This kind of attack is termed as VM Hopping. Thomas Ristenpart et al [10] have shown that it is possible to determine the IP address of the existing VM running on the cloud infrastructure. They have shown the approaches to determine the placement policy of VMs and then placing malicious VM to extract information of the victim VM. As cloud services are hosted over internet, it is prone to network based attacks like Denial of Service attack, eavesdropping. In this work we have taken care to mitigate such type of attacks.

In this design we have considered the following security issues.

1) *User Isolation:* User Isolation is achieved by network isolation through the VLAN configuration. As discussed earlier, there are different user profiles depending upon the credibility of the users. To provide user isolation, different Virtual LANs (VLANs) are created for different user profiles. Hence the virtual machines of certain profile will be configured to belong to appropriate VLAN. This facilitates the enforcement of security policies corresponding to different user profile. This can be done by VLAN tagging. In our design VLAN is enabled by configuring Open vSwitch. By this configuration, the host machine which runs virtual machine becomes capable of providing each virtual machine interface a VLAN tag. This approach will prevent virtual machines belonging to one user from sniffing the network connection of virtual machines belonging to other user.

2) *Packet Filtering*: To secure our infrastructure, we need to be careful about malicious activities of the user inside the virtual machine. To prevent the cloud user to misuse cloud resources for malicious activities, we have deployed a sensor in each node to monitor the network traffic of the virtual machines residing inside that node. We keep one virtual machine to analyze the network traffic. It checks the malicious behavior of the virtual machine according to the predefined rules. It periodically sends the report to the front end for appropriate action.

We have deployed a detector of TCP SYN flood attack in the virtual machine that is in charge of security. It basically keeps track of the incomplete TCP connections. It generates alert when this limit crosses some threshold value.

Figure 2 describes the secure private cloud architecture for Mobile Infrastructure. This figure shows the interconnections among the front end and clusters. To achieve user isolation, separate VLANs have been created for different user profile. The network traffic entering into the cloud infrastructure is checked by firewall. Again in order to save the cloud infrastructure from the attacks generated inside VMs, IDS is deployed at each host. In case of any malicious activities, the hypervisor is signalled to shut down the VM.

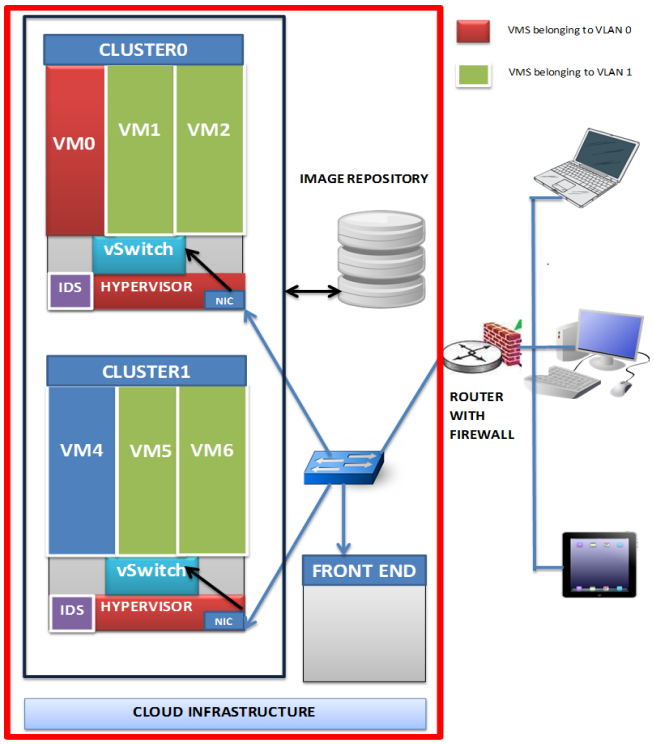

Fig. 2. Secure Private Cloud Architecture

IV. EVALUATION

For this work, a private cloud was deployed in a computing laboratory with 20 computers. One of the computers was made front end and other computers were treated as clusters. The aim was to build a secure private cloud to provide mobile IaaS with existing hardware. The private cloud is deployed using an open source cloud computing tool kit OpenNebula.

Table 1 gives the specification of the available computing resources.

TABLE 1

SPECIFICATIONS OF THE COMPUTER SYSTEM TAKEN

Operating System	Ubuntu 11.10
File Sharing	NFS
Hypervisor techniques used	Virtual Box
RAM	2 GB
Hard Disk	300 GB
Processor	Core2 Duo

The working hour of lab is from 8 am to 8 pm. The workload on the system of the lab is not constant throughout the day. Hence we have divided the time duration into four slots of three hours such as 8-11, 11-2, 2-5 and 5-8. The number of users accessing the system and the payload on the system are different during different time slots. In order to evaluate the system, we have considered two scenarios. In the first scenario, we consider the heavy workload and compare the two systems and in the second scenario, we consider the normal workload. We have evaluated the system against the parameter of number of users serviced.

A. Heavy workload

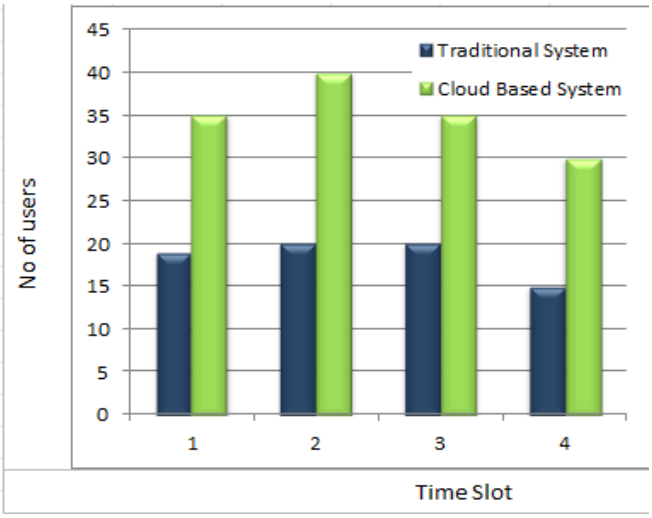

Fig 3. Graph showing comparison of traditional and cloud based system in terms of users serviced

Figure 3 compares the number of users our system can handle in different time slots. By experiments we found that our system can handle 89% more number of users. This increment owes to the proper resource utilization in our proposed system. During heavy workload, the maximum user, the traditional system can handle in a single slot is the number of computers it has. Even though all the computer systems are occupied, they are not fully utilized. Whereas a Cloud based system can serve twice number of users. This is because in this case instead of allocating a single dedicated system to the user, we allocate one virtual machine. In one system, at least two virtual machines can run.

B. Normal workload

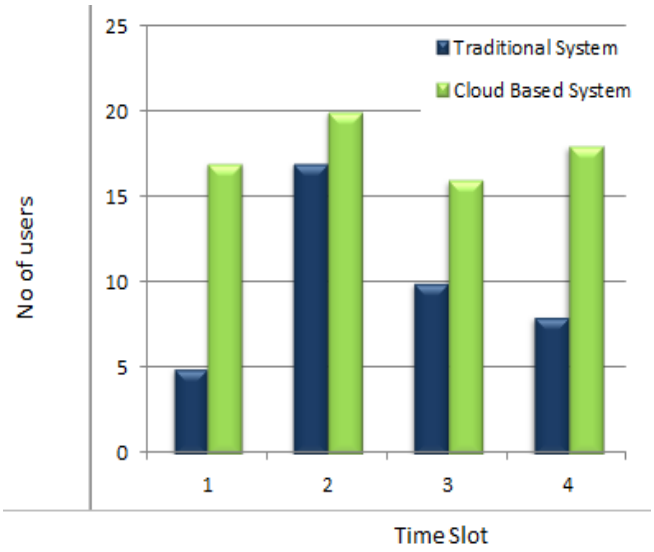

Fig 4. Graph showing comparison of traditional and cloud based system in terms users serviced in normal workload

Figure 4 shows showing comparison of traditional and cloud based system in terms users serviced in normal workload. Here we found that 78% more the number of users can be serviced in our proposed system. In traditional system, we see the variation in the number of users in different time slots. In case of cloud based system, there is uniform use of system irrespective of the time slot. The reason behind this is the mobility provided by our system that a user can have access to the cloud from anywhere inside the premise.

V. CONCLUSION

In this paper we have proposed and evaluated the secure private cloud architecture for mobile infrastructure as a service. We conducted exhaustive experiments against the parameter of number of users serviced. The results show that our system provides computing resources dynamically with very little overhead, fully utilizing the resources in hand. It can provide the easy access of cloud from any place which frees the user from being physically present in the lab to work. Further work is directed to deploy the prototype in

large scale and further increase cost effectiveness by reducing administrative overheads.

VI. RELATED WORK

North Carolina University of USA has done pioneer work in deploying private cloud for educational purpose. Though architecture is very much sophisticated and covers many aspects of computational demand like HPC. This kind of system requires building cloud from the scratch. Our proposed system focuses on building cloud infrastructure in order to enhance the availability of the infrastructure. Similar architecture has been proposed by Horrow et al [15]. But security features like data isolation are enhancement to that architecture. Besides network based IDS is implemented to secure the architecture for network attacks. So this architecture is capable of providing secure mobile infrastructure. However this approach requires certain administrative overheads like creating virtual network, preparing virtual machine templates and managing image repository.

ACKNOWLEDGMENT

We are grateful to all the persons involved in mailing lists, development and documentation of OpenNebula project.

REFERENCES

[1] A. T. Velte, T. J. Velte and R. Elsenpeter, *CloudComputing – A Practical Approach*, Wiley Publishing,Inc. 2011.

[2] B. Sosinsky, *Cloud Computing Bible*, McGraw-Hill Companies, 2010.

[3] (2011) The OpenNebula website [Online]. Available :http://www.opennebula.org/

[4] (2011) OpenNebula VirtualBox driver plugin (OneVBox). [Online]. Available: http:// github.com/hsanjuan/OneVBox /

[5] (2011) OpenNebula Workshop. [Online].Available: http://hpc.uamr.de/wissen/opennebula-workshop/OpenNebula workshop.

[6] R.S. Montero, "Building Clouds with OpenNebula 1.4," CESGA Santiago de Compostela, Spain, January 2010.

[7] R.S. Montero," Deployment of Private and Hybrid Clouds Using OpenNebula/ RESERVOIR", Open Grid Forum 28, March 15-18, 2010.

[8] M. A. Morsy, J. Grundy, and I. Miller, "An Analysis of The Cloud Computing Security Problem," in Proc. APSEC, 2010 Cloud Workshop.

[9] A.S. Ibrahim, J. Hamlyn-Harris, and J. Gurundy, "Emerging Security Challenges of Cloud Virtual Infrastructure," in Proc. APSEC, 2010 Cloud Workshop.

[10] T. Ristenpart, E. Tromer, H. Shacham, and S. Savage, "Hey, You, Get Off of My Cloud: Exploring Information Leakage in Third-Party Compute Clouds", Proc. 16th ACM Conf. Computer and Communication Security (CCS 09), ACM Press, 2009, pp. 119-212.doi: dx.doi.org/10.1145/1653662.1653687.

[11] W. Dawoud, I. Takouna, and C. Meinel," Infrastructure as a service security: Challenges and solutions," The 7th International Conference on Informatics and Systems (INFOS), pp.1-8, March. 2010.

[12] H. Tsai, M.Siebenhaar, A. Miede, Y. Huang, and R. Steinmetz, "Threat as a Service? Virtualization's Impact on Cloud Security", IT Professional,vol. 14, no. 1, pp.32-37.

[13] F. Sabahi, "Cloud Computing Security Threats and Responses", 3rd International Conference on Communication Software and Networks (ICCSN), IEEE,2011, pp.245-249.doi: dx.doi.org/10.1109/ICCSN.2011.6014715.

[14] M. Zhou, R. Zhang, W. Xie, W. Qian, and A. Zhou," Security and Privacy in Cloud Computing: A Survey," The 6th International Conference on Semantics, Knowledge and Grid (SKG), Nov. 2010,pp.1 05-111.doi: dx.doi.org/10.1109/SKG.2010.19.

[15] S. Horrow, S. Gupta, and A. Sardana, "Implementation of Private Cloud at IIT Roorkee: An Initial Experience", in International Workshop on Cloud Computing & Identity Management (CloudID 2012). in press.