INTERNATIONAL JOURNAL OF COMPUTERS COMMUNICATIONS & CONTROL
ISSN 1841-9836, 11(3):348-357, June 2016.

Dynamic Secure Interconnection for Security Enhancement in Cloud Computing

L. He, F. Huang, J. Zhang, B. Liu, C. Chen, Z. Zhang, Y. Yang, W. Lu

Liwen He*, Feiyi Huang, Jie Zhang, Bin Liu,
Chunling Chen, Weifeng Lu
Nanjing University of Posts and Telecommunications
66 New Mofan Road (P. Code:210003), Nanjing, China
helw@njupt.edu.cn, feiyi.huang@gmail.com, zhangjie@njupt.edu.cn,
clchen@njupt.edu.cn, luwf@njupt.edu.cn
*Corresponding author: helw@njupt.edu.cn

Zonghua Zhang
Institut Mines-Télécom of France
Rue Guglielmo Marconi, 59650, Villeneuve-d'Ascq, France
zonghua.zhang@lifl.fr

Yang Yang
ShanghaiTech University, Chinese Academy of Sciences
Information Building No 1, 280 Linhong Road, 200335, Shanghai, China
yang.yang@shrcwc.org

Abstract: Cloud computing brings efficiency improvement on resource utilization and other benefits such as on-demand service provisioning, location independence and ubiquitous access, elastic resource pooling, pay as usage pricing mode, etc. However, it also introduces new security issues because the data management and ownership are separated, and the management is operated on a virtualized platform. In this paper, a novel dynamic secure interconnection (DSI) mechanism is proposed to isolate the cloud computing system into a couple of dynamic virtual trust zones with different security policies implemented for different customers so as to enhance security. Experimental results are presented to demonstrate the feasibility and effectiveness of the DSI mechanism.
Keywords: Cloud Computing, virtualization management, security, dynamic secure interconnection

1 Introduction

In recent years, cloud computing is drawing more and more attention with its capabilities of efficient resource utilization, virtual machine live migration and multi-tenancy operational mode. Virtualization is the fundamental technology for both public and private cloud, virtual machine is expected to be dynamically allocated according to the requirements of customers, to be seamlessly migrated from one physical machine to another, and to be managed appropriately to prevent illegal access. However, cloud computing brings unprecedented challenges on security issues. As long as customers upload their sensitive data into a cloud computing system, the cloud computing service provider (CSP) is responsible for managing the data. Customers will lose the control of the data, who is using them, and when it is deleted.

And in a cloud computing environment, virtualization cannot be protected by conventional network security solution, such as Ą˚security zoneĄą separation, firewall, VPN, intrusion detection/prevention system, anti-DDoS solution, deep packet inspection technology [1].

In this paper, we propose a security enhanced virtual machine management mechanism named dynamic secure interconnection (DSI) for cloud computing system. A Ą˚dynamic virtual trust

zonesĄą is established to enhance information and virtualization security. In section 2, backgrounds about the cloud computing and virtualization security issues are reviewed. Section 3 provides a typical cloud computing model and states the typical security problems and requirements, and Section 4 proposes the DSI mechanism and operational procedure in details. A testbed and some experimental results are presented in Section 5. The paper is concluded in Section 6.

2 Related Work

The security issues are the major concerns for enterprise to adopt cloud computing [2] [3] [4]. Seven cloud computing security risks are identified by Gartner [5], i.e. privileged use access, regulatory compliance, data location, data segregation, recovery, investigation support, long-term viability. The root cause of these security risks is data storage, management and computation are performed on a shared and virtualized environment.

Since VMs work over hypervisor, malicious VMs cannot gain access to other VMs or launch cross-VM attacks when security countermeasures are implemented on hypervisors. However, this security boundary can be broken and malicious VMs can get full access to the physical host so as to get access to other VMs located on the same host illegally [6] [7]. Virtualization security has been studied from many aspects. In [8], an out-of-VM monitoring mechanism is proposed by using a trust VM to monitor the statues of guest VMs which deliver services to customers. The solution assumes the trust VM can prevent a variety of security threats. However, there is a large performance overhead associated with this solution when traffic is switched between the guest VMs and the trust VM. In order to provide a trusted VM on untrusted computing OS, a secure virtualization architecture is proposed to provide a secure execution environment [9]. The architecture includes a secure run-time environment, secure network interface and a secure secondary storage. Apart from the secure architecture, trust platform module has be used to establish the root of trust for VMs [10]. In [11], a virtual layer management framework is presented to ensure that cloud providers properly isolate VMs that run in the same physical platform, a cloud computing system is divided into a number of domains on the virtualization layer. Corresponding protocols are also proposed to manage the domain creation, interaction and termination. The interaction among the domains is based on secure channels [12] to establish trustworthy self-management foundation.

Data protection is another critical issue. Service providers such as Foursquare which provides a location based service and Reddit which supplies social news voting services use Amazon EC2 (Elastic Cloud Computing platform). In 2011, the crash of Amazon EC2 service takes down the service of Foursquare, Reddit, Cydia, Discovr and Scvngr [13]. Also, application (software) service provider can only rely on the infrastructure service provider to ensure the business continuity under the umbrella of SLA (service level agreement). They can implement their own security policies to achieve data security, preventing data loss or leakage. In [14], Hwang and Li propose a data coloring and software watermarking technique to establish trust among cloud service providers. In particular, if data objects and software modules are shared over multiple data centres, the trust-overlay network can establish a reputation system to protect data security and integrity.

Cloud privacy is to ensure the personal or sensitive information only be accessed by intended and authorized person or applications. The privacy issue originates from the lack of user access control and information transparency. That is when adopting a cloud storage service, e.g. the Dropbox [15], the customers are difficult to implement mechanisms to protect their information from unauthorized access or misuses. Promising privacy preservation solutions include minimizing personal information stored in the cloud, maximizing use control, allowing user to

choose, specify and limit the data usage [16]. In addition, data encryption is always a popular way, despite the extra overhead and complexity resulting from encryption algorithms and key management issues. In [17], a data secure sharing mechanism is proposed to enforce data access control, strengthening data encryption and improving the key sharing process when cloud customers store their data in a public cloud platform. The solution can protect the cloud storage providers from unauthorized access, ensuring data confidentiality and privacy. In [18], a privacy-preserving public auditing supported secure cloud storage system is proposed, which enables that data privacy of cloud storage to be publicly audited by a third party auditor. In particular, the homomorphic liner authenticator and random masking techniques are utilized to guarantee that the third party auditor would not learn any knowledge about the data content stored on the cloud server during the auditing process.

3 Problem Description

A number of open source cloud computing platform is based on the policies configured such as user authentication, authorization and accounting, VM allocation, drifting and state management, host machine management, service provision management. In the model, the security issues become much more complicated. First, the conventional network security solutions become less effective since they are usually deployed at the edge of a physical network to control and protect the incoming or outgoing traffic of a LAN. Second, new virtualization security countermeasures should be implemented on the virtualized perimeters where the physical network perimeter does not exist. Third, in the multi-tenancy environment, customers who share the same local network should have logically or physically separated computing, storage and networking resources, especially when customers come from different enterprises. That means cloud service provider should allocate each customer and their resources within a same virtualized trust group, permitting the interconnection within the same group and control the communication among different groups. Finally, when customers are on travel, the VMs related to them will be drifted and migrated from one physical machine to another, the security policies that implemented by the customer and on related VMs are expected to move along with migration.

4 Dynamic Secure Interconnection Mechanism

In this section, a novel mechanism, DSI-VM management mechanism is proposed to enhance security in a cloud computing system. A new concept of Ą˚virtual trust zoneĄą is also introduced.

4.1 Definitions and Assumptions

Virtual Trust Zone: VMs are the basic operation unit to implement management and security policies. When customers login and get service from a cloud computing system, they are allocated with virtualized resources in terms of VMs according to their requirements. VMs that assigned to the same customer should be aggregated in a same group and implemented with the unified management and security policies. Thus, the VMs that stay in the same group have basic trust among each other, and this group is defined as a Ą˚virtual trust zoneĄą.

Virtual Bridge:VMs that operate over a physical machine share the same physical MAC and IP addresses when the physical machine have only one NIC card. Each VM has its own virtual MAC and virtual IP addresses. A virtual bridge is a function module implemented on the hypervisor. It forwards packets with virtual MAC and IP address to their destination. A virtual bridge can serve all VMs on a hypervisor as well as a single VM.

4.2 The DSI Components

The DSI components include a DSI server, several virtual bridges and DSI clients. The DSI server works at a centralized mode while virtual bridge and DSI clients works at a peer-to-peer mode.

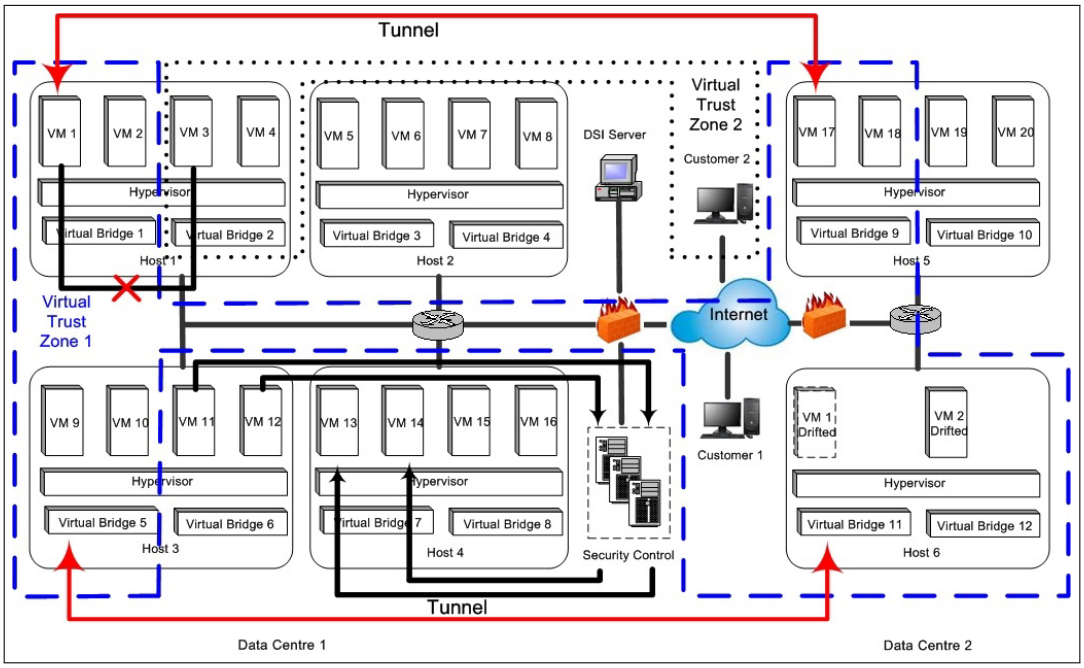

Figure 1: Overview of Dynamic Secure Interconnection Mechanism

DSI Server

The DSI server is the central controller for handling the management and security policies. When a VM is initialized, it is connected with the DSI server to register and start to operate in the system. When the VM state changes, e.g. suspend, restart, drift or phase out, it will inform DSI server to update the VM state. Thus, the DSI server maintains all VM properties and states, such as the virtual MAC (vMAC) and virtual IP (vIP) addresses of VMs, the VM owner, the corresponding virtual bridge, the real-time VM state, etc.

In addition, DSI server maintains the VM communication protocols, policies and activities. If VMs stay within a same local network, they can talk with each other using vMAC and vIP. If VMs stay in different local network, especially behind NAT devices, vIP based tunnels will be established to connect VMs. Meanwhile, appropriate traffic control policies will be implemented during the connection bootstrapping stage, such as encryption algorithms, key management protocol and traffic redirection.

DSI client and virtual bridge

The DSI clients are a large number of VMs. The properties of each DSI client includes vMAC and vIP addresses, VM state, VM owner, corresponding virtual bridge, host and its own virtual trust zone ID. Virtual bridges are in charge of performing and implementing the communication protocols and policies. The communication between two DSI clients is performed at a peer-to-peer mode. As shown in the Fig. 1, virtual bridge 1 and 5 can establish a direct connection between VM 1 and VM 9 based on virtual MAC addresses since they belong to the same local

network and can communicate with each other via vMAC and vIP. However, virtual bridge 1 and 9 have to establish VPN tunnels to transit through the NAT device based on the vIP to connect VM 1 and VM 17.

4.3 DSI Operation

The DSI operation refers to the interactions among DSI server, several DSI clients and virtual bridges. More specifically, the system administrator specifies the management policy on the DSI server, which then allocates the corresponding communication control policies to individual virtual bridges. Virtual bridges control the communication among DSI clients by relaying, blocking or rate-limiting packets to establish virtual trust zones.

Policy Configuration

The system management and security policies are configured on the DSI server according to the administrative requirements. That includes the DSI client initialization procedures, DSI client state change procedures, virtual bridge switching protocols and some other traffic management and security protection policies such as client registration, VM state management, access control, network isolation, transmission encryption, traffic redirection, etc.

Client Initialization and State Maintenance

A new user registration or additional resource request from existing users will incur the creation of VMs (DSI clients). This process is managed by the cloud computing platform based on policies such as load balancing, energy efficiency. After that, the newly generated VMs (DSI clients) will be registered on the DSI server, and provide the DSI server with information such as vMAC and vIP addresses, virtual bridge, VM owner and host machine name. Then the DSI server instructs the DSI clients and corresponding virtual bridges to perform bootstrapping process. That includes the notification of virtual trust zone ID, other clients within the same virtual trust zone, communication protocols and policies.

When the VMs (DSI clients) start to change their states, e.g. suspended, drifted or terminated, the DSI server will be notified with the change. The related communication protocols and policies will then be updated by the DSI server and reconfigured on each virtual bridge. For example, the VM 1 and VM 2 are suspended when their owners travel to other cities. The VMs are drifted and migrated into another data centre and will be allocated on virtual bridge 11 and 12 respectively, with their previous virtual MAC and IP addresses inherited. Previous and existing virtual bridges (virtual bridge 1, 11 and 12) will then report DSI server about the update and new tenant. DSI server will then update the related information in all virtual bridges to make sure the drifted VM 1 and drifted VM 2 can be connected seamlessly.

Virtual Bridge Communication Management

Virtual bridge is responsible for managing VM interconnection, traffic flow and virtual network topology. In Fig. 1, the VM 1 and VM 2 reside on the same virtual bridge 1 and serve the same customer. Thus, by allowing the interconnection between the VM 1 and VM 2, these two DSI clients are allocated into a same virtual trust zone. On the other hand, if VM 1 and VM 3 are serving customers from different enterprises, the interconnection between them will be blocked by virtual bridge 1 and 2. Thus, the VM 1 and VM 3 are regarded as staying in different virtual trust zone. Virtual bridges configure and maintain ACL (access control list) to authenticate vMAC addresses to start interconnection between DSI clients. Therefore, vMAC

based communication management is more suitable between VMs within the same local network where the virtual MAC addresses can be recognized.

If the two clients stay in different networks or behind NAT devices, the vIP address of a DSI client registered on the DSI server may be meaningless for another DSI client. The virtual IP addresses based tunnelling among VMs is performed by establishing peer-to-peer tunnels between virtual bridges, e.g. VM 1 and VM 17 in Fig. 1. The DSI server configures the virtual bridges to create tunnels with proper parameters such as the vIP address of the destination, the tunnelling protocols and encapsulation options. By doing that, access control and virtual network isolation can be further extended between VMs that stay in different local network.

4.4 Security

The dynamic security interconnection mechanism enhances cloud computing security by implementing access control mechanisms among VMs. In particular, virtual trust zones can be established by building the tunnels among virtual bridges.

Virtual Trust Zone Establishment

A virtual trust zone is a group of DSI clients (VMs) that interconnected by virtual bridges with some interconnection policies. A DSI client (e.g. VM 1) will be generated when a customer first login the system and request for computing and storage resources. When the customer requests for additional resources, a virtual trust zone is established to include the newly generated DSI client and the original one. The clients are trusted with each other and thus the interconnection between them is permitted. When the newly generated clients share the same physical host (e.g. VM 2) or local network (e.g. VM 9) with the original client, the virtual MAC address based access control mechanism and corresponding policies are implemented. If a new client resides in a remote data centre (e.g. VM 17), the IP tunnels based interconnection will be implemented. The IP tunnels based interconnection is also operational between VMs within a data centre (e.g. between VM 1 and VM 9). The virtual bridges will select the light-weighted vMAC based protocol in order to reduce the operation overhead and the management complexity of IP tunnelling protocol.

Encrypted Tunnel Establishment

When the customer travels from one city to another, the drifted DSI clients (e.g. VM 1 and VM 2) will migrate into a different network. The communication within a virtual trust zone, e.g. between the drifted VM 1 and VM 9, may go through an insecure public network. The encrypted tunnel will be established to protect the information exchange against various attacks such as eavesdropping. The DSI server may provide additional information to facilitate tunnel setup authentication, e.g. the certificate fingerprint [19]. In that case, DSI server presents an IKE/IPsec tunnel for NAT traversal, e.g. the UDP encapsulation of IPsec tunnelling [20].

Traffic Redirection

The virtual bridges can redirect the outgoing traffic of VMs to a dedicated traffic analysis and cleaning device before relaying them to their destination when the customers require them or when the system is under attacks. The dedicated device may be a secure VM or conventional security system such as anti-DDoS solution [1]. As an example in Fig. 1, the traffic from VM 11 and VM 12 are redirected to a traffic cleaning centre before it is forwarded to their destination, VM 13 and VM 14. The cost of this kind of security solution is performance degradation and operation overhead.

Security Policy Consistency

Since the network is separated into several virtual trust zones, security countermeasures can be implemented on a per-trust-zone basis. When the VMs in a virtual trust zone migrated from one host to another, e.g. VM 1 and 2, virtual bridge 1, 11 and 12 will then update DSI server about this information. And the DSI server will then reconfigure the tunnels among the virtual bridges accordingly. As a result, DSI server maintains the information about the dynamic trust zone no matter where the VMs migrate. The security policies can also be shifted along with the VM movement.

Comparison and Discussion

With the DSI mechanism, the traffic among VMs in the same trust zone is permitted while the traffic among VMs in different trust zones is controlled. Thus the trust zones are separated by simply managing the interconnection among VMs. This mechanism has several advantages.

- First, compared with the virtual layer management framework proposed in [11], our solution is relatively simple. In [11], several domains and complicated management mechanisms are introduced to manage the virtual layer. The DSI maintains virtual trust zones based only on the interconnection control mechanism.
- Second, DSI is very practical to make full use of all existing protocols, hypervisors and platforms to ensure the compatibility with most of existing cloud computing system.

5 Testbed and Experiment Results

A proof-of-concept testbed is constructed for demonstration of the DSI mechanism,and a simple Cloud computing platform named Ą˚VM Management platformĄą is implemented to perform the virtualized resource management, as shown in Fig.2.

Configurations. Libvirt toolkit and its virtualization APIs are utilized to construct the platform based on hypervisors of KVM, Xen Server or Virtual Box. Several VM management functionalities and policies are established written by C programs. VM initialization policies include VM instant created on host whose CPU/RAM is most idle; VM instant created on hosts already power on as far as possible; VM instant created on all hosts in average. Apart from that, VM management policies also include the VM suspend, migration, error control and disaster recovery policies. The VM management platform manages all VMs on host 2, 3 and 4.

Hardware settings. The testbed is composed of a Cisco Catalyst 2960PD-8TT-L switch and four PCs, host 1 is used for management, host 2, 3 and 4 are used for resource provision. Each PCs has a Intel CORE i5 four core 3.3GHz CPU, 4G RAM and 320G hard disk, and is able to accommodate 4 VMs. On host 1, 2, 3 and 4, hypervisor is installed on Linux Redhat Enterprise 5.6. In the experiment, three typical open source hypervisors of KVM, Xen Server and Virtual Box are selected to operate on the OS. The KVM and Virtual Box are type 2 hypervisors, while the Xen Server belongs to the type 1.

Virtual bridge functionality is implemented on host 2, 3, and 4. It is enabled based on the tun/tap device of Linux. Apart from switching, protocols of traffic filtering, traffic redirection, tunnel establishment are achieved by a set of C programs. The DSI server functionality is enabled by running a set of C program on the OS of host 1. The DSI functionalities include a management user interface (UI) and maintenance on DSI client information database.

In the experiment, the DSI mechanism operates normally on each of the three hypervisors, no matter whether it is type 1 or type 2. First, four VMs are configured on host 2, four on host

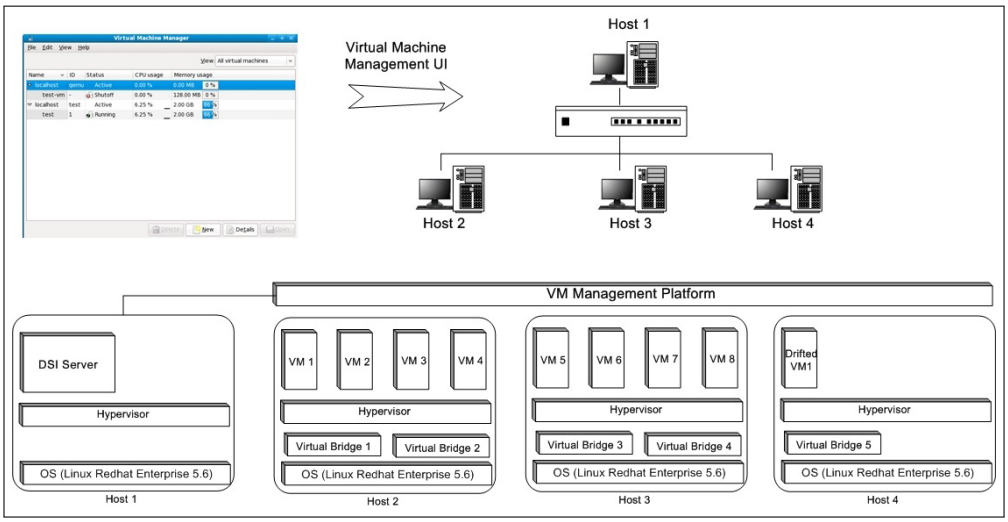

Figure 2: Testbed and Experiment

3 and IP addresses are assigned from 10.0.0.1 to 10.0.0.8. VM 1, 2, 5, 6 are configured in the same virtual trust zone and VM 3, 4, 7, 8 in the same zone. That can be achieved by permitting the interconnection between virtual bridge 1 and 3, and between virtual bridge 2 and 4. Ping command is used to check the interconnection control within and among virtual trust zones. The Ą°pingĄą between VM 1 and 5 is successful and between VM 1 to 3 is failed. In the second test case, VM 1 drifts from host 2 to 4, the virtual bridges on hosts inform the DSI server about this change, and DSI server updates the DSI client information database and informs related virtual bridge to update their interconnection configuration accordingly. In the test, the database is updated as expected. The Ą°pingĄą command from drifted VM 1 to VM 5 and 3 get the same result with the first test case. It is shown that the drifted VMs still stay within the same virtual trust zone and security policies keep the same after the migration.

6 Conclusion and Future Work

In this paper, dynamic secure interconnection (DSI) mechanism is proposed, analyzed and tested. By managing the VM interconnection and traffic direction of a cloud computing system, the virtualized network can be isolated into a couple of virtual trust zones. Direct connection within the same zone is established regardless the VM location while the traffic among different virtual trust zones will be carefully controlled. Coped with corresponding security service level agreement, security can be enhanced for customers to adopt cloud computing platform. Our proposed mechanism can protect sensitive data and information against various attacks such as eavesdropping to enhance cloud computing security.

As stated in section 4.4, traffic redirection is an important security feature of the DSI mechanism. It can release the working load of traffic scanning and monitoring on VMs and potentially facilitate the deployment of conventional security mechanisms such as anti-DDoS, virus, malware systems. However, this solution may consume extra amount of bandwidth when the traffic is redirected to a monitoring centre. More studies on this issue will be conducted in the future. In addition, the testbed with the VM management functionality is currently implemented only for concept proof, so a real-life cloud computing platform will be established by using open source tools such as Openstack or Eucalyptus to create more practical scenarios. Furthermore, our current experiments only selected some primary open source hypervisors to prove the compatibility

of the DSI mechanism, and the future experiments will involve more commercial hypervisors such as VMware or Hyper-V. DSI performance comparison on type 1 and type 2 hypervisors will also be studied.

Bibliography

[1] Xiaoming Lu, Weihua Cao, Xusheng Huang, Feiyi Huang, Liwen He, Wenhong Yang, Shaobin Wang, Xiaotong Zhang and Hongsong Chen (2010); A Real Implementation of DPI in 3G Network, *Proceedings of 2010 IEEE Global Telecommunications Conference (GLOBECOM 2010)*, 1-5.

[2] Cloud Computing Survey, IDC Enterprise Panel, [Online] Available: http://blogs.idc.com/ie/?p=210, Aug. 2008.

[3] S. Pearson and A. Benameur, Privacy (2010); Security and Trust Issues Arising from Cloud Computing, *Proceedings of 2010 IEEE Second International Conference on Cloud Computing Technology and Science (CloudCom)*, 693-702.

[4] S. Pearson (2009); Taking account of privacy when designing cloud computing services, *Proceedings of ICSE Workshop on Software Engineering Challenges of Cloud Computing, CLOUD '09*, 44-52.

[5] Jon Brodkin (2008); Gartner: Seven Cloud Computing Security Risks, July 2008, Available at http://www.infoworld.com/article/2652198/security/gartner–seven-cloud-computing-security-risks.html.

[6] K. Kortchinsky (2009); *CLOUDBURST: A VMware Guest to Host Escape Story*, BlackHat, USA, 2009.

[7] T. Ristenpart, E. Tromer, H. Shacham and S. Savage (2009); Hey, You, Get Off of My Cloud: Exploring Information Leakage in Third-party Compute Clouds, *CCS'09, ACM*, Chicago, Illiois, November 2009.

[8] B. Payne et al. (2008); Lares: An Architecture for Secure Active Monitoring Using Virtualization, *Proceedings of IEEE Symposium of Security and Privacy*, IEEE Press, 233-247.

[9] C. Li, A. Raghunathan and N. Jha (2011); A trusted virtual machine in an untrusted management environment, *IEEE Transactions on Services Computing* , 5(4): 472 - 483.

[10] M. Achemlal, S. Gharout and C. Gaber (2011); Trusted Platform Module as an Enabler for Security in Cloud Computing, *2011 Conference on Network and Information Systems Security (SAR-SSI)*, 1-6.

[11] Imad M. Abbadi, Muntaha Alawneh and Andrew Martin (2011); Secure Virtual Layer Management in Clouds, *Proceedings of IEEE 10th International Conference on Trust, Security and Privacy in Computing and Communications (TrustCom), 2011*, 99-110.

[12] Muntaha Alawneh and Imad M. Abbadi (2008); Preventing information Leakage between Collaborating Organizations, *Proceedings of the 10th International Conference on Electronic Commerce, ACM Press, August 2008*, 185-194.

[13] Amazon EC2 cloud outage downs Reddit, Quora, CNN News, [Online] Available: http://money.cnn.com/2011/04/21/technology/amazon _server_outage/index.htm

[14] Kai Hwang and Deyi Li (2010); Trusted Cloud Computing with Secure Resources and Data Coloring, *IEEE Internet Computing*, 14(5); 14-22.

[15] http://www.dropbox.com/.

[16] S. Pearson, (2009); Taking account of privacy when designing cloud computing services', *Proceedings of ICSE Workshop on Software Engineering Challenges of Cloud Computing, May 2009*, 44-52.

[17] Gansen Zhao, Chunming Rong, Jin Li, Feng Zhang and Yong Tang (2010); Trusted Data Sharing over Untrusted Cloud Storage Providers, *Proceedings of 2010 IEEE Second International Conference on Cloud Computing Technology and Science (CloudCom), 2010*, 97-103.

[18] C. Wang, S. Chow, Q. Wang, K. Ren and W. Lou (2011); Privacy-Preserving Public Auditing for Secure Cloud Storage, *IEEE Transactions on Computers*, 1-14.

[19] J. Lennox (2006); RFC 4572: Connection-Oriented Media Transport over the Transport Layer Security (TLS) Protocol in the Session Description Protocol (SDP), July 2006.

[20] A. Huttunen, B. Swander, V. Volpe, L. DiBurro and M. Stenberg (2005); RFC 3948 UDP Encapsulation of IPsec ESP Packets, January 2005.