An Ontological Framework for a Cloud Forensic Environment

N.M. Karie[1,2], H.S. Venter[1]

[1]Department of Computer Science, University of Pretoria, Private Bag X20, Hatfield 0028, Pretoria, South Africa
[2]Department of Computer Science, Kabarak University, Private Bag - 20157, Kabarak, Kenya
E-mail: menza06@hotmail.com, hventer@cs.up.ac.za

Abstract

Cloud computing is an emerging field and is considered to be one of the most transformative technologies in the history of computing. This is so because it is radically changing the way how information technology services are created, delivered, accessed and managed. Cloud forensics, on the other hand, is utilising network forensics – a subset of digital forensic techniques – in a cloud environment. However, with the continued evolution from internet-based applications to cloud computing, the environments and components surrounding cloud forensics can easily become incomprehensible. In this paper, therefore, we present an ontological framework meant to provide a structure and depiction of the different cloud environments and components an investigator should be acquainted with, in the case of a cloud investigation process. In addition, we show the relationships and interactions between the different environments by capturing their content and boundaries. Furthermore, the purpose of this paper is meant to provide a common ontological framework for sharing coherent cloud computing concepts and also promote the understanding of the cloud environments and cloud components. Finally, the ontological framework presents an approach towards structuring and organizing the environments and components surrounding the cloud and constitutes the main contribution of this paper.

Keywords

Cloud forensics, cloud computing, cloud environments, cloud components, ontological framework

1. Introduction

With the emergence of cloud computing technologies, the need for cloud forensics has become inevitable. This is due to the notion of cloud computing opening a whole new world of possibilities for criminals to exploit. This also means that criminals can now use cloud computing environments to share information and to reinforce their hacking techniques (Garfinkel, 2011). As a result, the major potential security risks, such as malicious insiders, data loss/leakage and policy violations now invade the existing cloud environments.

Cloud forensics, as defined by Ruan et al (2011), is an emerging field that deals with the application of digital forensic techniques in cloud computing environments and forms a subset of network forensics. Technically, cloud forensics follows most of the main phases of network forensic processes. The only difference is that such phases are simply extended with techniques tailored for cloud computing environments within each phase. However, the continued widespread deployment of the Internet-based applications and network-enabled devices in an effort to support mechanisms for cloud computing, can potentially render the cloud environments and components incomprehensible.

In this paper we present an ontological framework in an attempt to provide a structure and depiction of the different cloud environments (cloud deployment models) and cloud components (cloud service models) that an investigator should be well-versed with in the case of an investigation processes involving the cloud. In addition, the proposed framework also shows the relationships and interactions between the different cloud environments and the cloud components. Furthermore, this paper provides a novel contribution and offers a simplified ontological framework that can, for example, help investigators comprehend the cloud environment and components with less effort.

As for the remaining part of this paper, section 2 presents previous and related work while section 3 briefly explains the cloud environments and components. The proposed ontological framework is presented in section 4 followed by a discussion in section 5. Finally, section 6 presents the conclusion and future work.

2. Related Work

There exist several frameworks in cloud computing proposed by other researchers, which have made valuable contributions towards the development of the ontological framework presented in this paper. In this section, therefore, a summary of some of the most prominent efforts in previous research work is provided.

To begin with, Hoefer and Karagiannis (2010) argues that several organisations want to explore the possibilities and benefits of cloud computing. However, with the amount of cloud computing services increasing quickly, the need for taxonomy frameworks rises. In their paper they describe the available cloud computing services and propose a tree-structured taxonomy based on their characteristics, in order to easily classify cloud computing services so that it is easier to compare them. However, in this paper, we focus on an ontological framework meant to provide a common framework to share coherent cloud computing concepts as well as to promote the understanding of cloud environments and essential cloud components. Such a framework will assist investigators, for example, in planning of investigation techniques to be employed in specific cloud environments in the case of an investigation process and thus enhancing the investigation of criminal cases involving the cloud.

Yan (2011) argues that cloud computing, as a service, provides a luring environment for criminals and increases the difficulties of digital forensics. He then presents a forensic framework that focuses on the security issues of cloud services in order to beat cybercrime. Yan’s framework, however, focuses on security issues of cloud services while we, in the current proposed ontological framework, focus on structuring and organising the different cloud environments and cloud components.

In their paper, Takahashi et al (2010) propose an ontological approach to cybersecurity in cloud computing. They built an ontology for cybersecurity operational information based on actual cybersecurity operations mainly focused on non-cloud computing. In order to discuss necessary cybersecurity information in cloud computing, they apply the ontology to cloud computing. Their work is centred on cybersecurity operations. However, the current framework is centred on, as mentioned earlier, cloud environments and cloud components.

Lamia et al (2009) also explains that the progress of research efforts in a novel technology is contingent on having a rigorous organisation of its knowledge domain and a comprehensive understanding of all the relevant components and their relationships of the technology. In their paper, they propose an ontology for cloud computing which demonstrates a dissection of the cloud into five main layers. However, there work does not elaborate on the cloud environments and cloud components in the way that is presented in this paper.

There also exist other related works on ontological frameworks, but neither those nor the cited references in this paper have presented an ontological framework for the cloud environments and cloud components in the way that is introduced in this paper. However, we acknowledge the fact that the previous proposed frameworks have offered useful insights toward the development of the ontological framework in this paper. In the section that follows we briefly explain the different cloud environments and components based on our review of the literature.

3. Cloud Environments and cloud Components

Cloud Computing is an emerging technology that uses the internet and remotely located servers to maintain data and applications. The ‘cloud’, therefore, can be viewed as a network of virtual machines geographically dispersed. Cloud computing technology is creating a revolution in computer architecture, software and tools development. Furthermore, it is changing the way organizations store, distribute and consume information. In this section of the paper, the authors explain the different cloud environments and cloud components that form the basis of the proposed ontological framework.

3.1. The Cloud Environments (Cloud Deployment Models)

3.1.1. Public Cloud Environment

A public cloud is one in which a service provider makes resources, such as applications, platforms and infrastructures available to the general public over the internet. Public clouds are owned and operated at datacentres belonging to the service providers and are shared by multiple customers (Subramanian, 2011a). This also means that, public clouds offer unlimited storage space and increased bandwidth via internet to any organisation across the globe. Such services on the public cloud may be offered free or on a pay-per-usage model. The degree of visibility and control of public clouds depends on the delivery mode. However, there is less visibility and control in public clouds compared to private clouds because the underlying infrastructure is owned by the service providers.

3.1.2. Private Cloud Environment

A private cloud can be viewed as the implementation of cloud computing services on resources dedicated to an organisation (i.e. the organisation owns the hardware and software), whether they exist on-premises or off-premises. A private cloud gives an organisation the advantage of greater control over the entire stack, from the bare metal up to the services accessible to users (Ubuntu, 2013).

3.1.3. Community Cloud Environment

A Community cloud is one that is tailored to the shared needs of a business community. Community clouds are operated specifically for a targeted group. Usually, such groups (communities) have similar cloud requirements and their ultimate goal is to work together to achieve their business objectives. According to Techopedia (2013), community clouds are often designed for businesses and organisations working on joint projects, applications, or research, which requires a central cloud computing facility for building, managing and executing such projects, regardless of the solution rented. The infrastructure in a community cloud is shared by several organizations with common concerns such as (security, compliance, jurisdiction, etc.), whether managed internally or by a third-party or hosted internally or externally. The cost is, however, shared by all the participating organizations.

3.1.4. Hybrid Cloud Environment

A hybrid cloud is a combination of both public and private clouds (Subramanian, 2011b). This means that a vendor who owns a private cloud can form a partnership with a public cloud provider, or a public cloud provider can form a partnership with a vendor that provides private cloud platforms. However, according to Mell and Grance (2011) of the National Institute of Standards and Technology (NIST), a hybrid cloud is a composition of two or more public, private, or community cloud infrastructures that remain unique entities but are bound together by either standardised or proprietary technology that enables data and application portability. Using the hybrid cloud architecture, organisations and individuals are able to obtain degrees of fault tolerance combined with locally immediate usability without dependency on internet connectivity. This is due to some of the resources in a hybrid cloud being managed in-house while others are provided externally. In the next sub-section the authors elaborate on the essential cloud components which also form part of the proposed ontological framework in this paper.

3.2. The Essential Cloud Components (Cloud Service Models)

Whichever the cloud environment deployed, cloud service providers will always offer their clients (individuals and organisations) with the following three categories of cloud service models: Infrastructure-as-a-Service (IaaS), Platform-as-a-Service

(PaaS) and Software-as-a-Service (SaaS). In the next sub-sections, these service models are further explained.

3.2.1. Infrastructure-as-a-Service (IaaS)

IaaS is a cloud computing service model that offers physical and virtual systems (cloud computing infrastructure), including an operating system, hypervisor, raw storage, and networks (Oracle Corporation, 2012). Servers represent the main computing resource in IaaS and are often virtual instances within a physical server. The service providers usually own the computing infrastructure and are responsible for housing, running and maintaining it. On the other hand, organisations pay on a per-use basis. IaaS helps organisations realize cost savings and efficiencies while modernising and expanding their information technology capabilities without spending capital resources on infrastructure (GAS, 2013).

3.2.2. Platform-as-a-Service (PaaS)

PaaS as explained in an expert group report by the European Commission (2010) provides computational resources (cloud computing platforms) via a platform upon which applications and services can be developed and hosted. PaaS typically makes use of dedicated APIs to control the behaviour of a server hosting engine which executes and replicates the execution according to user requests. Cloud computing platforms may include the operating system, the programming language execution environment, the database, and the web server. PaaS also allows clients to use the virtualised servers and associated services for running applications or developing and testing new applications.

3.2.3. Software-as-a-Service (SaaS)

SaaS sometimes referred to as Service or Application Clouds (European Commission, 2010) offers implementations of specific business functions and business processes that are provided with specific cloud capabilities. I.e. they provide cloud computing applications or services using a cloud infrastructure or platform, rather than providing cloud features themselves. Moreover, SaaS also provides internet-based access to different software, thus presenting new opportunities for software vendors to explore. In the next section, the proposed ontological framework is presented and explained.

4. The Proposed Ontological Framework

In this section of the paper the authors present the proposed ontological framework. Figure 1 shows the structure of the ontological framework. Note that, due to the small font size of Figure 1, Figures 2 to 4 contains enlarged extracts of the ontological framework as depicted in Figure 1.

The framework consists of five layers arranged from left to right and with the first layer depicting the main domain of focus (i.e. the cloud/cloud computing). This is followed by the cloud environments in the second layer and the essential cloud components in the third layer. Services and service providers are introduced in the fourth and fifth layer of the ontological framework as a way of representing individual, finer-grained details of the essential cloud components, also referred to as cloud service models.

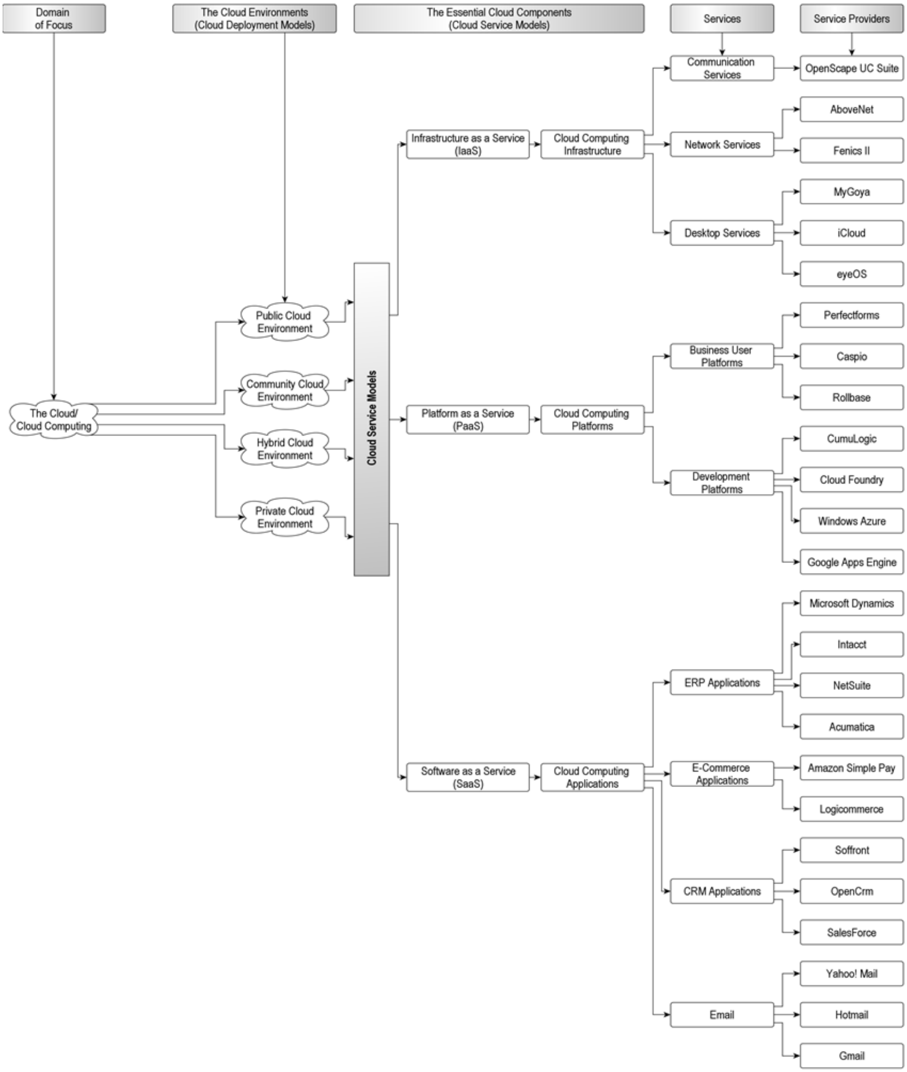

Figure 1: Conceptualisation of the cloud environments and essential components

Cloud service models enable software, platform and infrastructure to be delivered as services. The term service is used to reflect the fact that they are provided on demand and are paid for, on a usage basis (Czarnecki, 2011). In the authors' experience, organising the framework into the particular cloud environments, essential cloud components, services and service providers, was necessary to simplify the understanding of the framework as well as to present specific finer details of the framework. The services and service providers listed in the fourth and fifth layers (see Figure 1) were only selected as common examples to facilitate this study and should not be treated as an exhaustive list.

The major areas explored (with their details as shown in Figure I) include the cloud environments, the essential cloud components, services and the service providers. For the purpose of this study, the cloud environments (cloud deployment models) are divided into public cloud environment, private cloud environment, community cloud environment and hybrid cloud environment. The essential cloud components (cloud service models), on the other hand, are divided into Infrastructure-as-a-Service (IaaS), Platform-as-a-Service (PaaS) and Software-as-a-Service (SaaS). However, infer from Figure 1 that the IaaS, PaaS and SaaS are accessible through cloud computing infrastructure, cloud computing platforms and cloud computing applications respectively.

The cloud computing infrastructure (see Figure 2) is further divided into communication services, network services and desktop services forming the fourth layer of the ontological framework. The communication services show OpenScape UC Suite as one of the service providers. The network services have AboveNet™ and Fenics II as service providers. Finally, desktop services show MyGoya, iCloud and eyeOS as service providers. The service providers form the fifth layer of the framework as shown in Figure 1. However, note that, the contents of the fourth and fifth layer (services and service providers) in Figure1 were introduced in this framework to provide only selected examples for the purpose of this study. Therefore, such contents should not be treated as an exhaustive list.

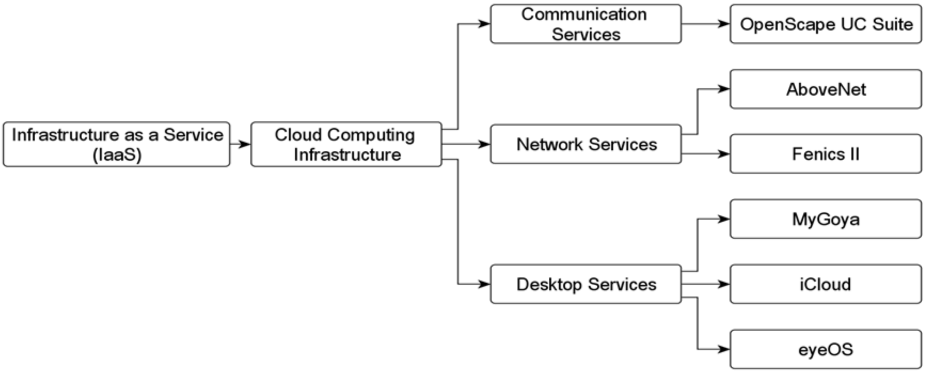

Figure 2: Infrastructure-as-a-Service

The cloud computing platforms as shown in Figure 3 are divided into two: business user platforms and development platforms. Business user platforms have PerfectForms, Caspio™ and Rollbase as service providers. The development platforms show CumuLogic, Cloud Foundry™, Windows Azure™, and Google™ Apps Engine as selected service providers. However as said earlier these are only common examples for the purpose of this study and should not be treated as an exhaustive list.

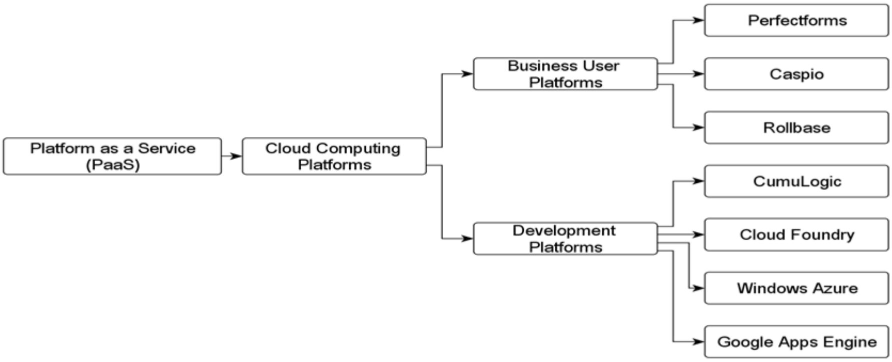

Figure 3: Platform-as-a-Service

The cloud computing applications shown in Figure 4 are divided into Enterprise Resource Planning (ERP) applications, E-commerce applications, Customer Relationship Management (CRM) applications and Email as selected examples. The ERP applications have Microsoft Dynamics™, Intacct®, NetSuite and Acumatica as service providers. E-commerce applications show Amazon Simple Pay and Logicommerce™ as examples of service providers. The CRM applications have Soffront®, OpenCrm and SalesForce® as service providers. Finally, Email has Yahoo!®, Hotmail® and Gmail™ as examples of the service providers. As said earlier, these were only selected as common examples for the purpose of this framework and, therefore, should not be treated as an exhaustive list.

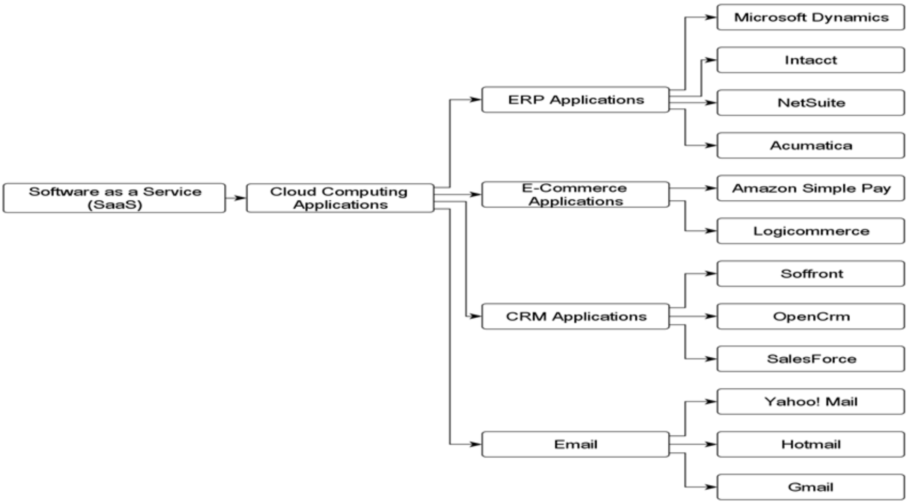

Figure 4: Software-as-a-Service

5. Discussion

The ontological framework presented in this paper is a new contribution and its scope is defined by the cloud environments, the essential cloud components, services and the service providers (see Figure 1). Such an ontological framework can be used, for example, as a common platform to share coherent cloud computing concepts and also promote the understanding of the cloud environments and cloud components. Moreover, the ontological framework can also serve, for example, as a basis for sharing common views of the structure and depiction of cloud computing information in a bid to enable the reuse of domain knowledge.

Furthermore, the framework in this paper can, for example, help investigators to explicitly describe investigation processes and procedures that focus on specific cloud environments in the case of cloud forensics. In addition, forensic tools developers can also use the ontological framework to fine-tune their tools so as to be able to cover as many potential security risks and policy violations experienced in the different cloud environments. This also implies that developers will find the ontological framework in this paper constructive, especially when considering new cloud forensic techniques for specific cloud environments.

In the case of cloud forensics, the proposed ontological framework can also assist in the design and development of high-tech acquisition tools incorporating, for example, hybrid cloud architectural designs with shareable features such as automated acquisition, reporting, visualisation and presentation of evidence in a manner that is acceptable in a court of law. Moreover, such high-tech tools will also enhance the investigation of criminal cases involving multiple cloud computing environments.

The proposed ontological framework can also be useful, for example, in cloud interoperability and exchanging of information between the different cloud environments. Moreover, it can be helpful in the design and development of standardised technology that also enables data and application portability in the different cloud environments. This is backed up by the fact that, the framework has explicitly described the distinctions of the various cloud environments, essential cloud components, services and service providers shown in Figure 1.

Finally, the ontological framework is, therefore, a new contribution towards advancing the field of cloud computing. To the best of the authors' knowledge, there exists no other work of this kind and, therefore, this is a novel contribution towards advancing the cloud computing and cloud forensic domain.

6. Conclusion and Future Work

The problem addressed in this paper was that of the incomprehensible cloud environments and components we are currently faced with. This incomprehensibility has been caused by the continued evolution from internet-based applications to cloud computing. In this paper we have proposed an ontological framework that provides a structure and a depiction of the different cloud environments and cloud components as a way to help individuals comprehend them with less effort. In addition, the cloud environments, the essential cloud components, services and service providers were also captured in the framework and explained. Therefore, the authors believe that by using this ontological framework a better understanding of the cloud environments and associated cloud components can be gained. However, more research needs to be conducted in order to identify new components and also to improve on the proposed ontological framework in this paper. Finally, the framework should spark further discussion on the development of new cloud computing ontological frameworks.

7. References

Czarnecki, C., (2011), “Cloud Service Models: Comparing SaaS PaaS and IaaS", *Perspectives on Cloud Computing & Training from Learning Tree International*. Available at: http://cloud-computing.learningtree.com/2011/11/09/cloud-service-models-comparing-saas-paas-and-iaas/ [Accessed February 13, 2013].

European Commission, (2010), Editors: Jeffery, K. and Neidecker-Lutz, B., “The future of cloud computing”, opportunities for European cloud computing beyond 2010. *Expert Group Report*

GAS, (2013), Infrastructure as a Service (IaaS). Available at: http://www.gsa.gov/portal/content/112063 [Accessed March 20, 2013].

Garfinkel, S.L., (2011), The Criminal Cloud, *MIT Technology Review*, Available at: http://www.technologyreview.com/news/425770/the-criminal-cloud/ [Accessed February 4, 2013].

Hoefer, C.N., Karagiannis, G., (2010), "Taxonomy of cloud computing services", *Proceedings of the GLOBECOM Workshops*, pp.1345-1350

Lamia, Y., Butrico, M., and Da Silva, D., (2008), "Toward a Unified Ontology of Cloud Computing", *Proceedings of the Grid Computing Environments Workshop*, pp.1-10

Mell, P. and Grance, T., (2011), "The NIST Definition of cloud computing", *Recommendations of the National Institute of Standards and Technology.*

Oracle Corporation, (2012), “Making Infrastructure-as-a-Service in the Enterprise a Reality”, *An Oracle White Paper.*

Ruan, K., Carthy, J., Kechadi, T. and Crosbie, M., (2011), “Cloud forensics”, *Proceedings of the 7th IFIP WG 11.9 International Conference on Digital Forensics 2011*, Orlando, FL, USA

Subramanian, K., (2011a), "Public Clouds", *A whitepaper sponsored by Trend Micro Inc.*

Subramanian, K., (2011b), "Hybrid Clouds", *A whitepaper sponsored by Trend Micro Inc.*

Takahashi, T., Kadobayashi, Y. and Fujiwara, H., (2010) "Ontological Approach toward Cybersecurity in Cloud Computing", *Proceedings of the 3rd international conference on Security of information and networks (SIN '10), ACM, New York, NY, USA*, pp 100-109

Techopedia, (2013), "Community Cloud”, Available at: http://www.techopedia.com/definition/26559/community-cloud [Accessed February 8, 2013]

Ubuntu, (2013), “Private cloud”, Available at: http://www.ubuntu.com/cloud/private-cloud [Accessed February 8, 2013].

Yan, C., (2011), "Cybercrime Forensic System in Cloud Computing", *Proceedings of the Image Analysis and Signal Processing (IASP) Conference*, pp.612-615