Monitoring Intrusions and Security Breaches in Highly Distributed Cloud Environments

Aryan TaheriMonfared
Department of Telematics
Norwegian University of Science and Technology
taherimo@stud.ntnu.no

Martin Gilje Jaatun
SINTEF ICT
Trondheim, Norway
Martin.G.Jaatun@sintef.no

***Abstract*—Cloud computing is a new computing model, and security is ranked first among its challenges. This paper reviews existing security monitoring mechanisms compared with new challenges which are caused by this new model. We highlight possible weaknesses in existing monitoring mechanisms, and propose approaches to mitigate them.**

Keywords: Interoperable and Federated Cloud Security and Trust, Cloud Architecture, Experiences and Lessons

I. Introduction

According to the definition proposed by the National Institute of Standards and Technology (NIST) [1], Cloud computing is a model for on-demand network access to a shared pool of resources (e.g., networks, servers, storage, applications, and services) that can be rapidly provisioned and released. This process is done with minimal management effort or interaction with the cloud provider. A cloud customer will experience higher availability through this new model [1]. "By 2012, 20 percent of businesses will own no IT assets. Several interrelated trends are driving the movement toward decreased IT hardware assets, such as virtualization, cloud-enabled services, and employees running personal desktops and notebook systems on corporate networks"[2].

One of the most significant obstacles to cloud computing adoption is represented by security challenges. A lack of clear definition of perimeters, system dependability, data confidentiality and integrity are some of the security challenges which slow down the shift forward. Additionally, it has been shown that hackers are becoming more and more interested in the cloud model. A survey conducted among 100 IT professionals at the 2010 DEFCON conference [3] revealed that 96 percent claim that the cloud will provide more hacking opportunities for them. 89 of them said that they thought that cloud providers were not being proactive enough in their security, and 45 of them admitted to already have engaged in cloud hacking, while 12 of them said that they hack for financial gain.

There is thus a growing need to define and utilize proper monitoring mechanisms in cloud environments. We need threat monitoring mechanisms which not only perfectly assess the old model, but also cover different aspects of the new computing model.

The first step to approach this goal is a brief review of existing mechanisms and an analysis of their specifications (Section II). In this way we characterize different mechanisms, their use-cases, features and weaknesses.

The second step is to analyze security challenges which are identified in the cloud model because of the new concepts in it (Section III). We try to find out what is new in these security challenges. One possible approach here is to extract corresponding threat sources for each threat. A threat source is "the intent and method targeted at the intentional exploitation of a vulnerability or a situation and method that may accidentally trigger a vulnerability" [4].

The last step is the evaluation of security monitoring mechanisms against new challenges in the model (Section IV). In this way, we try to find those issues which are not completely covered using available mechanisms. Finally, we propose new mechanisms which fulfill the new requirements.

In the following section, we will discuss security monitoring mechanisms.

II. Security Monitoring Mechanisms

Due to an increase in the amount of organized crime and insider threats, proactive security monitoring is crucial nowadays [5]. Moreover, in order to design an effective security monitoring system, a variety of challenges should be taken into account, for example, previous knowledge of threats and their specifications in the new environment, handling a large number of incidents, cooperation among interested parties and their privacy concerns, product limitations, etc.

Conventionally, cloud providers are not willing to disclose details of their security mechanisms. They justify this behavior in different ways, but it seems that the main motivation is fear of competitors stealing their ideas. To counter this, we reviewed security monitoring mechanisms from not only commercial solutions, but also open communities which are doing research in this field. In this analysis, we focus more on monitoring mechanisms which help us to cover new security challenges in the cloud model.

A. Commercial Solutions

We studied security solutions in the cloud model which are proposed by Amazon, Google, RackSpace and Microsoft. In this study, we started by reviewing white-papers and documents for each of those commercial solutions. In some cases, like RackSpace, they have open-source projects or

open communities, which may help more in analysis of their solutions.

1) Amazon: In the following, we highlight products and functions in the Amazon cloud environment which may help us in designing a proper security monitoring solution.

- **CloudWatch**
  Amazon CloudWatch is a web service that provides monitoring for cloud components, covering resource utilization, operational issues (request count and request latency on Elastic Load Balancing (ELB)), and overall demand patterns. It is designed to provide comprehensive monitoring for Amazon Elastic Compute Cloud (EC2), Amazon ELB and Amazon Relational Database Service (RDS)[6]. CloudWatch can be used to retrieve statistical data. Later, these data can be utilized to demonstrate availability parameters, such as mean up-time and mean time between failure.
- **Vulnerability Reporting Process**
  This process is used when someone finds a vulnerability in any Amazon Web Services (AWS) products.[7]
- **Penetration Testing Procedure**
  As penetration testing is indistinguishable from security violations, Amazon has established a policy for customers to request permission to conduct penetration testing [7]. Establishing this policy helps AWS security monitoring service to reduce the number of false-positive alarms. Moreover, penetration testings that are conducted by variety of cloud customers, reveal useful information for understanding the ecosystem of security threats in the new model. Cloud providers should coordinate such testing to find out more about the threat ecosystem as well as possible security breaches in their own infrastructure.
- **Security Bulletins**
  "AWS tries to notify customers of security and privacy events using Security Bulletins." [7] Cloud customers monitor new vulnerabilities and change of policies using this service. As an example, we can refer to *Amazon Payments Signature Validation* where a vulnerability was identified in the sample code for application-side signature validation [8].
- **Catbird™ Vulnerability Monitoring**
  Vulnerability monitoring is a part of the Catbird vSecurity product that provides security solutions for a cloud environment. Catbird vulnerability management has the following functionality: Audit, Continuous Compliance, Incident Response, Hybrid Vulnerability and IDS/IPS.

2) Google: Security monitoring in Google has three main targets, internal network, employee actions on Google systems and outside knowledge of vulnerabilities [9].

At many points across their global network, internal traffic is inspected for suspicious behavior. They do this analysis using a combination of open-source and commercial tools. They also analyze system logs to identify unusual activity from their employees. In addition, a specific security team checks security bulletins for incidents which may affect Google's services [9]. On top they have a correlation system that coordinates the monitoring process among a variety of technologies. Google did not disclose any technical information about their monitoring mechanisms or even security functions, but if we refer to an internal security breach in July 2010 [10], we see that those mechanisms are not working well enough to monitor such an incident.

3) RackSpace: RackSpace started an open-source project called OpenStack [11], including the code for Cloud Files and Cloud Servers Technology. NASA also joined this project with its Nebula platform which will be merged to Cloud Servers Technology and would become the computing component of OpenStack. This project will be discussed more in Section II-B2.

4) Microsoft Azure: Microsoft has a security frame to share security knowledge. 10 different categories are introduced in that frame comprising [12]: Auditing and Logging, Authentication, Authorization, Communication, Configuration Management, Cryptography, Exception Management, Sensitive Data, Session Management, Validation.

Based on these categories and their definitions "Auditing and logging" is the category related to security monitoring. Auditing and Logging explains how security-related events are recorded, monitored, audited, exposed, compiled and partitioned across multiple cloud instances [12].

B. Open Communities

We will first review the importance and influence of open-source solutions, and then analyze some of those communities and their solutions in more detail.

1) Contribution of open source solutions: Open-source solutions and open communities address many security challenges in the cloud computing model. Open source platforms which are compatible with interfaces in commercial solutions (e.g. Amazon EC2 APIs), help customers to *avoid data lock-in*. Moreover, *building a hybrid cloud* becomes easier by means of open source platforms, which have public interfaces compatible with interfaces in other cloud environments. As an example of compatible interfaces we can refer to Eucalyptus APIs which are compatible with Amazon EC2 APIs. This compatibility provides flexibility for cloud customers, enabling them to export data or processes to another cloud, when it is needed.

Additionally, open-source platforms and open communities can lead to a *bigger ecosystem* which is useful in studying threats. A threat study has at least two phases, first analyzing the ecosystem for possible security breaches, and second, verifying proposed security solutions to make sure that they satisfy the constraints.

2) Standards and open source solutions: In the following section we introduce communities who develop open standards which can be used in a cloud environment.

- **CloudAudit/A6** is a set of interfaces and namespaces that allows cloud providers to automate Audit, Assertion, Assessment, and Assurance of their different service models for authorized users [14].

- The **Cloud Security Alliance (CSA)** is a non-profit organization that develops effective ways of bringing security into the cloud computing model. Moreover, using cloud computing services to secure other types of computing models. They have eight working groups that work on different aspects of the cloud security[15].
- The **Distributed Management Task Force (DMTF)** has an Open Cloud Standards Incubator for interoperable cloud management among service providers, customers and developers, with a goal to deal with the lock-in challenge. They have two standards, Interoperable Cloud [16] and Architecture for Managing Clouds [17].
- The **Open Cloud Computing Interface Working Group (OCCI-WG)** works on provisioning, monitoring and definition of cloud infrastructure services. Their solution will mostly fulfill three requirements: interoperability, portability and integration in an Infrastructure as a Service (IaaS) model. This solution also focuses on the lock-in problem in the cloud.
- The **OASIS Identity in the Cloud (IDCloud) TC** [18] develops standards for identity deployment, provisioning and management. They also provide use cases which are useful for risk and threat analysis.

Eucalyptus [19], OpenNebula [20], and OpenStack [11] are the three main open source platforms in cloud computing today. Each of them provide a variety of features and functionality, but their main focus is how to convert an existing pool of hardware resources into an IaaS provider. All of them have the common feature that they are compatible with Amazon EC2 interfaces.

Platforms are not the only type of software which are developed in open source projects. As an example, Zenoss [21] is an open source monitoring solution which is compatible with the new concepts in the cloud computing model.

III. Security Challenges

This section motivates the study of threats to cloud computing, and then reviews the top threats identified by CSA [15]. While reviewing these top threats we will study the abuse threat in more detail, facilitating building a framework for further in-depth analysis of other threats, which will be useful in characterizing the specifications of monitoring mechanisms. Finally, we try to understand what the new challenges are in the new computing model.

A. Threat Specifications

Our two main interests in finding threats to the cloud are:

- "Providing a needed context to assist organizations in making educated risk management decisions regarding their cloud adoption strategies." [22]
- Utilizing effective monitoring mechanisms and introducing new ones to fulfill requirements in the cloud environment.

The threat model in the cloud has some novelties [23]. First, in addition to data and software, activity patterns and business reputation should be protected. Moreover, a longer trust chain should be accepted. This is due to multiple service models (Software as a Service, Platform as a Service and Infrastructure as a Service) and possible combination of them. Parties in this trust chain will need mutual auditability in order to have some degree of assurance about the other parties. Another novelty is about availability issues in the cloud. We should always keep in mind that the same failure in the cloud computing will have more catastrophic effect than a failure in the traditional computing model.

According to [22], top threats could be identified as follows:

1) Abuse and Nefarious Use of Cloud Computing
2) Insecure Application Programming Interfaces
3) Malicious Insiders
4) Shared Technology Vulnerabilities
5) Data Loss/Leakage
6) Account, Service & Traffic Hijacking
7) Unknown Risk Profile

We will look a little closer into *Abuse and Nefarious Use of Cloud Computing* as a threat. Initially, abusive behavior should be clearly declared, for instance, it should be defined from whose perspective a behavior is called abusive or nefarious. In order to achieve that, we may identify three stakeholders in the cloud computing model: Cloud provider, cloud customer and end user. Relations between these stakeholders are complicated, and this is one of the novelties of the cloud computing threat model [23].

As an illustration, cloud customers may abuse services which they are paying for; hosting a phishing website is an example. In this case, both the cloud provider and end users face threats which are caused by this behavior. In addition, end users or clients of cloud customers can also misuse services which are provided for them. It will cause troubles for both the cloud provider and cloud customers: for instance, hosting illegal data on a storage service that utilizes IaaS as its infrastructure. Additionally, in both cases, communications between different stakeholders play a vital role in mitigating the threat. Moreover, it is clear that interests of stakeholders are not necessarily perfectly aligned. Therefore, conflicts may happen.

Different abuse cases can be itemized as follows:

- Anonymous Communication using cloud services for nefarious purposes.
- Running The Onion Routing (TOR) [24] exit node.[1]
- Botnet activity
  - Command and control hosting
  - Bot hosting
- Sending email spam or posting spam into forums
- Hosting harmful or illegal content:
  - Site advertised in spam
  - Host for unlicensed copyright-protected material
  - Phishing website
  - Malware host
- Attack source:

[1] It is a Terms of Service (TOS) violation with most cloud service providers.

  - Intrusion attempts
  - Exploit attacks (SQL injections, remote file inclusions, etc)
  - Credit card fraud
  - Port scanning
- Excessive web crawling
- Open proxy

B. New Security Challenges

We are most interested in those new challenges in the cloud computing which have influence on monitoring techniques. For an exhaustive list of vulnerabilities and risks to cloud computing, please refer to the European Network and Information Security Agency (ENISA) report on cloud computing risk assessment [25].

1) Cloud customers, who provide a service for end users, should assure their clients that their data is safe. Consequently, cloud customers must have some information about the cloud providers' staff with privileges to access the customers' data. Security monitoring mechanisms in the new model should provide functionality which help cloud customers to trust cloud providers' staff without revealing too much information about the personnel.
2) Data location and Conflicting laws. This is a new challenge, because in previous computing models the location of service providers' storage was clear. In the cloud model, however, storage and computing facilities are distributed over a number of regions. Now imagine a country that has restrictive laws which do not allow companies to store their data outside of the country borders. In this case, monitoring mechanisms should keep track of data location. Such mechanisms highly depend on cloud providers' cooperation and common interfaces among providers and customers.
   Moreover, cloud customers may need to ensure data privacy for their clients. On the other hand, cloud providers must obey their government regulations in disclosing data for lawful interception. This is one of the conflicting points between cloud customers and cloud providers when they are from different regions. As an illustration, one can refer to the conceptual conflicts between the USA Patriot Act [26] and PIPEDA (Personal Information Protection and Electronic Documents Act) [27] in Canada, or the Data Privacy Protection Directive [28] in the EU. For a specific system, a corresponding security monitoring approach must identify these conflicts and let the customer decide on using a particular cloud service or not. Additionally, end users of cloud customer services must be informed about these details by means of security mechanisms in each layer in the cloud model.
3) Reputation Isolation [25] (Fate-sharing [23]). Cloud stakeholders' activities and behaviors affect each others reputation. For instance, in Amazon EC2's IP addresses blacklisting incident, if a monitoring agent was attached to each VM instances and a correlation system existed on the underlying layer, the cloud provider could differentiate instances that perform activities suspected to be spamming from others.
4) Incident Handling. Incidents happen in different layers of the cloud model and each layer may be operated by different authorities. Handling an incident needs not only cooperation among all authorities, but also policies and procedures for mitigating the incident. These policies and procedures should be introduced in the security monitoring solution. Stakeholders and authorities will apply these guidelines to handle the incident in the best fashion and decrease the degradation of services. Defining policies and procedures is the challenging part; as an example, a cloud customer should have access to log files which contain any traces of the incident. However, privacy of other customers must be protected. Additionally, investigation of one cloud customer should not affect the performance of other customers. One real case is about the FBI raid on two data centers in Texas. In this investigation, they powered off the whole data center.[29]
5) Data lock-in [23]. In case of a major security breach in the cloud infrastructure, customers should be able to migrate to another cloud infrastructure smoothly. A complete monitoring solution should check the compatibility of cloud service interfaces with standard interfaces to make sure that the migration will happen as it supposed to be.
6) Data deletion. File deletion has been a concern in all distributed systems, but it has became more challenging in the cloud computing paradigm [30]. Monitoring mechanisms, which have been used to track data location, are also useful in the file deletion challenge. In other words, same marking and tracking mechanisms can be used for hierarchical multi-label data marking. Therefor, cloud providers can keep track of data among all backup files and distributed storage.
7) Mutual auditability [23]. Stakeholders need to be sure of each others trustworthiness. Collaborative monitoring mechanisms in each cloud layer is crucial for this purpose. These collaborative mechanisms should communicate through a common interface among layers.
8) Side channels and Covert channels [23]. Complete analysis of this challenge and corresponding countermeasures is provided by Ristenpart et al. [31].

IV. Evaluation of Mechanisms against Threats

Considering extracted threat specifications and new security challenges, we try to find weaknesses in existing mechanisms. By identifying weaknesses and their features, it becomes possible to find proper monitoring techniques in order to fulfill security monitoring requirements in the cloud computing model.

Commercial cloud services are closed environments. On the other hand, monitoring mechanisms should be changed in order to fulfill requirements in the new model. Lack of ecosys-

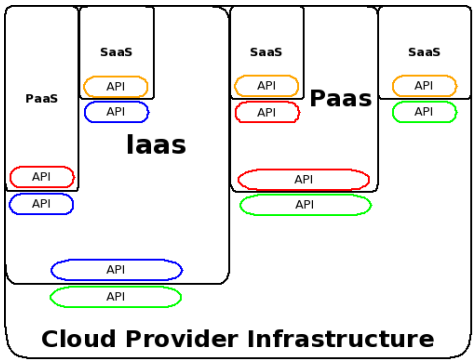

Fig. 1. Cross-Layer Security Monitoring

tems for monitoring solution providers is a major obstacle in the way to develop new solutions for new challenges.

New concepts behind the cloud computing concept impose constraints on monitoring mechanisms. Part of these constraints are not applicable to existing monitoring mechanisms. On-demand access and data perimeters are parts of new concepts.

Elasticity and on-demand access in the cloud model is a cause of some incompatibilities. As an example, scaling up/down[32] are not completely supported in current monitoring techniques. Moreover, definition or even existence of perimeters is not the same as before, therefor security solutions can not simply put guards at communication channels to control everything. This requires exhaustive research and development to add elasticity to solutions and control data at possible perimeters.

Another concern is about compliance of monitoring activities with legal issues (as explained in Section 2). Monitoring mechanisms should have flexibility so customers can choose from a set of compatible mechanisms regarding to their concerns and environmental constrains.

Security mechanisms are not mature enough to support reputation isolation; in order to cover this shortcoming, human interaction is required in some monitoring decisions. Human interaction in decision making is not scalable and can become a bottleneck[23]. A real life example is the Amazon EC2 whitelisting procedure for email sender instances.

As shown in Figure 1, a cloud environment consists of different layers, each of which traditionally has its own monitoring mechanisms. These mechanisms are not aware of other layers, nor are they administered by the same groups. Moreover, mechanisms in each layer are focused on monitoring the corresponding layer [33]. So, there is no interoperability at all.

Consequently, we propose a cross-layer monitoring solution, which tries to mitigate some of the weaknesses in the current mechanisms (see Table I). Each property deals with a set of new challenges. In the table we use challenge number from Section III-B to show the relation.

Utilizing cross-layer monitoring mechanisms will have several advantages. The first advantage is avoiding duplication of tasks in different layers. Second, monitoring will be more accurate because of the cooperation between different layers and use of richer information sources than traditional mechanisms. Third, redundancy can prevent monitoring mechanisms from becoming a single point of failure. Fourth, a cross-layer framework makes it easier for each layer to provide security services to layers above.

There are at least two main issues on the way for the cross-layer monitoring mechanism.

Trust and Compliance challenges: Companies are not willing to disclose information to others; because they can not trust one another, especially with information that can be used for security monitoring purposes. Moreover, if services in each layer are provided by companies from different countries, they may face critical problems such as conflicting laws that introduces compliance challenges, e.g., US Patriot Act and EU Data and Privacy Protection.

The trust issue has been a concern in all kind of cooperation; mutual auditability [23] may help to improve mutual trustworthiness which can lead to relax the issue.

Inter-layer Communication: Another issue in cross-layer approach is that lack of standard communication interfaces prevent layers from knowing about each other's semantics, and there is no way to share that context, even if they are willing to do so. Defining APIs in each layer is a step forward, and this can also help in mutual auditability which relaxes the trust challenges.

V. Conclusion and Further Work

It is not feasible to fit all existing monitoring mechanisms into the new model. Cloud computing has new challenges, and new techniques thus need to be developed for resolving these challenges. As an illustration, new mechanisms need to be implemented for the reputation isolation challenge in 3. On the other hand, existing mechanisms should also be adapted to new concepts such as elasticity, hence they would be still applicable in mitigating old challenges.

There are some obstacles in the way of developing new security mechanisms. First of all, solution providers need to have access to different components of a cloud environment so they can study them and also propose and develop proper solutions. Cloud providers work on their proprietary solutions but of course that is never enough. Open environments should be available so others can do the same. Open source platforms, like Eucalyptus, are the way to address that requirement.

Additionally, while reviewing available security mechanisms, it was clear that the security model is not mature yet, and monitoring mechanisms need extensive development. Open communities are working on standards for components in the model; these standards help us not only in securing the model, but also in clarifying the common understanding of security requirements.

Finally, we proposed a cross-layer security monitoring solution which helps in dealing with several new challenges in the cloud computing model. In addition, our approach avoids duplication of tasks in multiple layers, and improves accuracy in existing monitoring mechanisms.

Solution properties	Challenges
Components of cross-layer monitoring approach	
Common interfaces between each layer	all
Monitoring agent attached to each instance or delivered service	4, 3
Hierarchical multi-label data marking	2, 6
Layer specific monitoring coordinator which manage monitoring agents in the corresponding layer.	2, 4, 3, 8
Layer specific Log manager which provides proper log details for customers based on their requirements without putting other customers' privacy at risk.	4
Compatibility monitoring of deployed interfaces against standard APIs.	5
Document artifacts	
List of regulations that influence the specific cloud environment.	2
Policies and procedures approved by authorities and service providers for handling an incident in a predictable way, with least side effect on other customers.	4

TABLE I
PROPERTIES OF CROSS-LAYER SECURITY MONITORING APPROACH AND CORRESPONDING CHALLENGES THAT EACH PROPERTY DEAL WITH.

Our contribution could be expanded in the future by taking into account intrusion detection approaches in Grid Computing and enterprise-wide Security Information and Event Management systems.

ACKNOWLEDGMENTS

Thanks to Juha Saaskilahti, whose guidance and support enabled the development of this idea and the writing of this paper. We also thank the anonymous reviewers for constructive comments.

REFERENCES

[1] P. Mell and T. Grance, "The NIST Definition of Cloud Computing," National Institute of Standards and Technology, Information Technology Laboratory, Tech. Rep., January 2011. [Online]. Available: http://csrc.nist.gov/publications/drafts/800-145/Draft-SP-800-145_cloud-definition.pdf

[2] C. Pettey and H. Stevens, "Gartner Highlights Key Predictions for IT Organizations and Users in 2010 and Beyond," January 2010.

[3] "Hackers see opportunities in the cloud according to def con survey," August 2010.

[4] M. Swanson, J. Hash, and P. Bowen, "Guide for developing security plans for federal information systems," The Internet Engineering Task Force, SP, February 2006, http://csrc.nist.gov/publications/nistpubs/800-18-Rev1/sp800-18-Rev1-final.pdf.

[5] M. N. Chris Fry, *Security Monitoring: Proven Methods for Incident Detection on Enterprise Networks*, 1st ed. O'Reilly Media, February 2009.

[6] "Amazon CloudWatch Developer Guide," http://aws.amazon.com/cloudwatch/, May 2009, amazon WebServices.

[7] "AWS Security Center," http://aws.amazon.com/security/, October 2010.

[8] "AWS Security Bulletin: Amazon Payments Signature Validation," http://aws.amazon.com/security/security-bulletins/amazon-payments-signature-validation/, September 2010.

[9] Google's Security Team, "Security whitepaper: Google apps messaging and collaboration products," Google's Security Team.

[10] A. Chen, "Gcreep: Google engineer stalked teens, spied on chats," http://gawker.com/5637234/gcreep-google-engineer-/stalked-teens-spied-on-chats.

[11] "Openstack, open source software to build private and public clouds," http://www.openstack.org/, Nov 2010.

[12] J. Meier and P. Enfield, "Azure security notes," exploring Microsoft Azure and the Cloud Security Space.

[13] C. Hoff, "Incomplete thought: Why we need open source security solutions more than ever..." http://www.rationalsurvivability.com/blog/?p=2173, July 2010.

[14] C. Hoff, S. Johnston, G. Reese, and B. Sapiro, "Cloudaudit 1.0 - automated audit, assertion, assessment, and assurance api (a6)," Internet Engineering Task Force, Internet-Draft draft-hoff-cloudaudit-00, 2010, experimental. [Online]. Available: https://tools.ietf.org/html/draft-hoff-cloudaudit-00

[15] "Cloud security alliance," http://www.cloudsecurityalliance.org/, Nov 2010.

[16] "Interoperable clouds – a white paper from the open cloud standards incubator," Distributed Management Task Force, DMTF Informational DSP-IS0101, 2009.

[17] "Architecture for managing clouds – a white paper from the open cloud standards incubator," Distributed Management Task Force, DMTF Informational DSP-IS0102, 2010.

[18] "Oasis identity in the cloud (idcloud) tc," http://www.oasis-open.org/committees/tc_home.php?wg_abbrev=id-cloud, Nov 2010.

[19] "Eucalyptus," http://www.eucalyptus.com/, Nov 2010.

[20] "Opennebula, the open source toolkit for cloud computing," http://www.opennebula.org/, Nov 2010.

[21] "Zenoss," http://www.zenoss.com/, Nov 2010.

[22] Cloud Security Alliance, "Top threats to cloud computing," 2010.

[23] Y. Chen, V. Paxson, and R. H. Katz, "What is new about cloud computing security?" EECS Department, University of California, Berkeley, Tech. Rep. UCB/EECS-2010-5, Jan 2010. [Online]. Available: http://www.eecs.berkeley.edu/Pubs/TechRpts/2010/EECS-2010-5.html

[24] "The onion routing project," http://www.torproject.org/, Nov 2010.

[25] P. Balboni, K. Mccorry, and P. W. David Snead, "Cloud computing – benefits, risks and recommendations for information security," European Network and Information Security Agency, Tech. Rep., November 2009, http://www.enisa.europa.eu/act/rm/files/deliverables/cloud-computing-risk-assessment/.

[26] FinCEN, "Usa patriot act," http://www.fincen.gov/statutes_regs/patriot/index.html.

[27] "Personal information protection and electronic documents act," http://laws.justice.gc.ca/en/P-8.6/.

[28] "Data privacy protection directive," http://ec.europa.eu/justice/policies/privacy/index_en.htm.

[29] "In the United States district court for the northern district of Texas Dallas division," April 2009, Liquid Motors, Inc. v. Allyn Lynd and United States.

[30] B. Schneier, "The battle is on against facebook and co to regain control of our files," http://www.guardian.co.uk/technology/2009/sep/09/bruce-schneier-file-deletion, Nov 2010.

[31] T. Ristenpart, E. Tromer, H. Shacham, and S. Savage, "Hey, you, get off of my cloud: exploring information leakage in third-party compute clouds." in *ACM Conference on Computer and Communications Security*, E. Al-Shaer, S. Jha, and A. D. Keromytis, Eds. ACM, 2009, pp. 199–212. [Online]. Available: http://dblp.uni-trier.de/db/conf/ccs/ccs2009.html#RistenpartTSS09

[32] M. Govshteyn, "Top 5 reasons why traditional managed security services will fail in the cloud," http://securecloudreview.com/2010/08/top-5-reasons-why-traditional-/managed-security-services-will-fail/-in-the-cloud/, August 2010.

[33] C. Hoff, "What's The Problem With Cloud Security? There's Too Much Of It ," http://www.rationalsurvivability.com/blog/?p=2693, October 2010.