Monitoring Intrusions and Security Breaches in Highly Distributed Cloud Environments

Aryan Taheri Monfared
Department of Computer Science, Aalto University
ataherim@cc.hut.fi

DRAFT v1.0

Abstract

Cloud computing is a new computing model. According to International Data Corporation (IDC) report [18], security is ranked first among challenges of the cloud model. In a perfect security solution, monitoring mechanisms play an important role. In the new model, security monitoring has not been discussed yet. this paper identified a few steps for studying security monitoring mechanisms in the cloud computing model. First, existing security monitoring mechanisms should be reviewed. These mechanisms are either part of commercial solutions or proposed by open communities. Second, top threats to cloud computing should be analyzed. In this step, we will go through new challenges in the new computing model. Third, current security monitoring mechanisms would be evaluated against new challenges which are caused by the new model. Here, we can find possible weaknesses in existing monitoring mechanisms and propose applicable approaches to mitigate them.

Keywords: Cloud Computing, Security Monitoring, Threats, Security breaches

1 Introduction

According to a definition which is proposed by National Institute of Standards and Technology (NIST) [25], 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 cloud provider. Cloud customer will have higher availability by means of this new model [25]. "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."[29]. Nevertheless, cloud computing will have great influences on business.

In the movement towards decreased IT hardware assets, one of the most significant obstacles is security challenges. Companies have doubts about different aspects of security in the new model. A lack of clear definition of perimeters, system dependability, data confidentiality and integrity are some of those security challenges which slow down the shift forward .

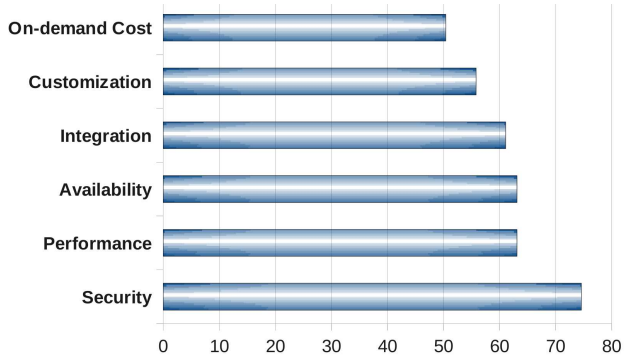

Figure 1: Challenges in Cloud Model based on a report from IDC that have more than 50% responding "significant" or "very significant" [23]

Additionally, it has been shown that hackers are becoming more and more interested in the cloud model. A survey conducted at the 2010 DEFCON [10] by Fortify Software, amongst 100 of the IT professionals. It 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.[11]

With regard to the importance of security in a cloud environment, there is a growing need to define and utilize proper monitoring mechanisms, as shown in Figure 1. 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 2). 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 3). We try to find out what is new in these security challenges. One possible approach here is to extract corresponding threat sources for each threats. 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" [34].

The last step is the evaluation of security monitoring mechanisms against new challenges in the model (Section 4). In this way, we try to find those issues which are not completely covered using available mechanisms. Finally, we could propose new mechanisms which fulfill the new requirements.

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

2 Security Monitoring Mechanisms

Due to an increase in the number of organized crime and insider threats, proactive security monitoring is crucial nowadays [7]. Moreover, in order to design an effective security monitoring system variety of challenges should be taken into account. As an example, we can mention some of them here: shortcoming in threat ecosystem, handling large number of incidents, cooperation among interested parties and their privacy concerns, product limitations, etc.

This section will start by reviewing our method for discussing monitoring mechanisms. Then, we will study security monitoring approaches from two different categories, commercial and open communities solutions. As a matter of fact, it should be noted that no single solution or mechanism exists for monitoring all kinds of threats. Different environments and threats impose variety of requirements. Each of these requirements are addressed by a group of monitoring techniques.

Conventionally cloud providers are not willing to disclose their security mechanisms. They justify these behaviors in different ways. First of all, by disclosing security functions, their competitors may utilize same mechanisms and reduce benefits of the origin company. Moreover, many companies still believe in security through obscurity. With regard to these types of problems, 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 those part of monitoring mechanisms which help us to cover new security challenges in the cloud model.

2.1 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. Then we tried to communicate with security teams for each them, to understand more about their monitoring mechanisms. This communication was the most unsuccessful part, because they were not willing to give out information more than what is available publicly. In some cases, like RackSpace, they have open-source projects or open community which may help more in analysis of their solutions. We will continue by going through some of those providers.

2.1.1 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. These components are 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)[1]. 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 find a vulnerability in any Amazon Web Services (AWS) products.[2]

- **Penetration Testing Procedure**
  As penetration testing is hardly distinguishable from security violations, Amazon has established a policy for customers to request permission to conduct penetration testing [2]. Establishing this policy helps AWS security monitoring service to face less 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 these testings to find out more about the threats 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." [2] Cloud customers monitor new vulnerabilities and change of policies using this service. As an example, we can refer to *Amazon Payments Signature Validation* a case on 22nd of September 2010. In this incident, a vulnerability has been identified in the sample code for application-side signature validation[3].

- **Catbird™ Vulnerability Monitoring**
  Vulnerability monitoring is a part of 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, Performance-enhancing implementation.

2.1.2 Google

Security monitoring in Google has three main targets, internal network, employee actions on Google systems and outside knowledge of vulnerabilities.[19]

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, security team checks security bulletins for incidents which may affect Google's ser-

vices [19]. On the top they have a correlation system that coordinates the monitoring process among variety of technologies. As a matter of fact, Google did not disclose any technical information about their monitoring mechanisms or even security functions. But if we refer to internal security breach on July 2010[5], we may see that those mechanisms are not working well enough to monitor such an incident. In July 2010, one of Google Site Reliability Engineers (SRE) had been dismissed because of breaking internal privacy policies by accessing users' account.

2.1.3 RackSpace

RackSpace started an open-source project called OpenStack [28] They included 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 2.2.2.

2.1.4 Microsoft Azure

Microsoft has a security frame to share security knowledge. 10 different categories are introduced in that frame comprising:[24] 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[24].

2.2 Open Communities

To study monitoring mechanisms proposed by open communities, we will first review the importance and influence of open-source solutions. Afterward, some of those communities and their solutions will be analyzed.

2.2.1 Importance of open source solutions

Open-source solutions and open communities are crucial in the cloud computing model. They address many security challenges in this 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. These open source platforms have public interfaces which are compatible with interfaces in other cloud environments. As an example for compatible interfaces we can refer to Eucalyptus APIs which are compatible with Amazon EC2 APIs. This compatibility provides the flexibility for cloud customers; So they can 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. Threat study can 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 constrains.

However, open source implementations of cloud software are not the only influence of open communities. Many open projects do not focus on software development for the cloud model but they work on other aspects of the new model including: *Common interfaces and namespaces* that are used for standardization of communications in the cloud model (e.g. CloudAudit open project on automating the Audit, Assertion, Assessment, and Assurance); another aspect is to *Promote a common level of understanding and knowledge* about different properties of the cloud computing (e.g. CloudSecurityAlliance research about the top threats to a cloud environment.).

At the end, to emphasize the urge to openness, we repeat a quote by Christofer Hoff [32], "The security industry is not in the business of solving security problems that don't have a profit/margin attached to it". The fact is that the cloud model is not mature yet and companies will not focus on an specific area until enough benefits exist for them. On the other hand, open communities develop different perspectives of the cloud model without looking for large financial benefit. This will help to explore new model in depth and introduce new ideas that may not be interested for industry unless specific challenges arise.

2.2.2 Standards and open source solutions

In the following section we have two parts, first part is about communities which develop open standards and second part is about some of those open source platforms which can be used in a cloud environment.

- CloudAudit/A6
  CloudAudit 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 [22].

- Cloud Security Alliance (CSA)
  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[9]. In the following we will mention some of those groups which are effective in designing proper monitoring mechanisms.

  1. Group 1: Architecture and Framework
  2. Group 2: GRC, Audit, Physical, BCM, DR
  3. Group 5: Identity and Access Mgt, Encryption & Key Mgt
  4. Group 6: Data Center Operations and Incident Response
  5. Group 8: Virtualization and Technology Compartmentalization

- Distributed Management Task Force (DMTF)
  DMTF's Open Cloud Standards Incubator try to design interoperable cloud management among service

providers, customers as well as developers. It will help to avoid lock-in challenge. They have two standards, Interoperable Cloud[13] and Architecture for Managing Clouds[12].

- Open Cloud Computing Interface Working Group (OCCI-WG)
  The OCCI-WG works on provisioning, monitoring and definition of cloud infrastructure services. Their solution will mostly fulfill three requirements: interoperability, portability and integration in Infrastructure as a Service (IaaS) model. This solution also focuses on the lock-in problem in the cloud.

- OASIS Identity in the Cloud (IDCloud) TC [26]
  They develop standards for identity deployment, provisioning and management. They also provide use cases which are useful for risk and threat analysis.

We will continue by introducing some of those open source platforms. Eucalyptus [15] , OpenNebula [27] and OpenStack [28] are three main open source platforms in the cloud computing. Each of them provide variety of features and functionality, but their main focus is how to convert an existing pool of hardware resources to IaaS provider. All of them have a common feature. The feature is that they are all compatible with Amazon EC2 interfaces.

Platforms are not the only type of software which are developed in open source projects. As an example, Zenoss [36] in an open source monitoring software which is compatible with the new concepts in the cloud computing model.

3 Security Challenges

This section initially discuss the importance of studying threats to the cloud computing. Then top threats, which are identified by CSA[9] will be reviewed. While reviewing these top threats we will study the abuse threat in more details. This will facilitate building a framework for further in-depth analysis of other threats. In-depth analysis of threats is useful in characterizing the specifications of monitoring mechanisms. These mechanisms will be evaluated in the next section. In the last part, we try to understand what the new challenges are in the new computing model.

3.1 Threat Specifications

Our two main interests in finding threats to cloud are:

- "Providing a needed context to assist organizations in making educated risk management decisions regarding their cloud adoption strategies."[8]

- Utilizing effective monitoring mechanisms and introducing new ones to fulfill requirements in the cloud environment.

Threat model in the cloud has some novelties.[6] 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 combinations of them. Parties in this trust chain will need mutual auditability. Stakeholders demand for mutual auditability, in order to have assurance, to some degree, 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.

It is noteworthy to keep in mind these novelties while analyzing threats in the new model.

According to [8], 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

Abuse and Nefarious Use of Cloud Computing, as a top threat to the cloud computing, is the one we will study here. 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[6]. In fact, these relations have crucial effect in mitigating this threat.

As an illustration, cloud customers may abuse services which they are paying for; hosting a phishing website is an example of it. In this case, both the cloud provider and end users faced 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 utilize 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 in the same direction. 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) [35] exit node.[1]
- Botnet activity
  - Command and control hosting
  - Bot hosting

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

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

In this section we discussed threat specifications briefly. lets move on by distinguishing new security challenges in the cloud computing model.

3.2 New Security Challenges

In this part we will study those new challenges in the cloud computing which have influence on monitoring techniques. For an exhaustive list of vulnerabilities and risks to cloud computing, check European Network and Information Security Agency (ENISA) report on cloud computing risk assessment. [4]

1. Cloud customers, which provide a service for end users, should assure their clients that their data is safe. Consequently, cloud customers must know about the cloud providers staffs who have enough privileges to access cloud customers' data. Security monitoring mechanisms in the new model should provide functionality which help cloud customers to trust cloud providers staffs without revealing too much information about 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. Contrary, in the cloud model, storage and computing facilities are distributed over number of regions. Now imagine a country that has restricting 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 which are from different regions. As an illustration, one can refer to the conceptual conflicts between USA Patriot Act [17] and PIPEDA (Personal Information Protection and Electronic Documents Act) [30] in Canada or the Data Privacy Protection Directive [14] in the EU. For a specific system, corresponding security monitoring approach must identify these conflicts and let the customer to 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[4] (Fate-sharing [6]). 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 corelation system existed on the underlying layer, the cloud provider could differentiate instances that had activities suspicious to spamming among 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.[16]

5. Data lock-in [6]. 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 interface 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 became more challenging in the cloud computing [33]. 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 [6]. 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 [6]. Complete analysis of this challenge and corresponding countermeasures can be founded here [31].

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

New concepts behind the cloud computing impose constrains on monitoring mechanisms. Part of these constrains 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 root for some incompatibilities. As an example, scaling up/down[20] 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[6]. Real life example is Amazon EC2 whitelisting procedure for email sender instances.

As shown in Figure 2, a cloud environment consists of different layers. Traditionally, each layer has its own monitoring mechanisms. These mechanisms are not aware of other layers, nor are deployed and administrated by same groups. Moreover, mechanisms in each layer are focused on monitoring the corresponding layer [21]. So, there is no interoperability at all.

Consequently, we propose a cross-layer monitoring solution, which try to mitigate some of weaknesses in the current mechanisms. We introduced main properties of our solution in Table 1. These properties are extracted from our previous study on new security challenges in Section 3.2. Each property deals with set of new challenges. In the table we use challenge number from Section 3.2 to show the relation.

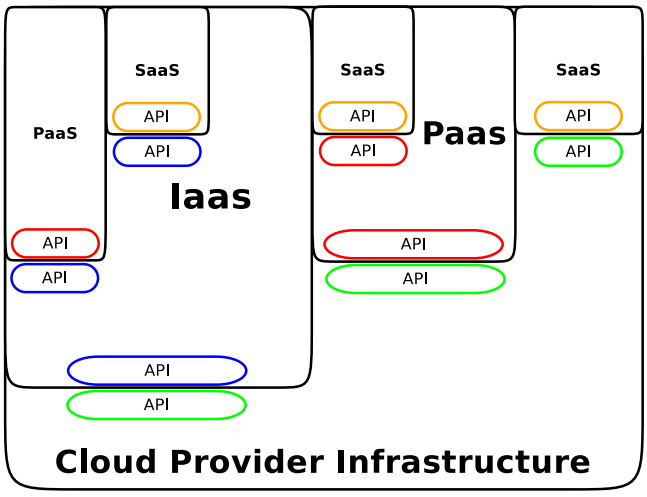

Figure 2: Cross-Layer Security Monitoring

Utilizing cross-layer monitoring mechanisms will have several advantages including:

- Avoid duplication of same tasks in each layer, as a result more resources will be saved.
- Monitoring will be more accurate because of the cooperation between different layers and utilizing richer information sources than traditional mechanisms.
- It is also possible to have enough redundancy to prevent monitoring mechanisms from becoming single point of failures.
- 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, specially 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 even more critical problems. One of these critical problems is conflicting laws that introduces compliance challenges, such as US Patriot Act and EU Data and Privacy Protection.

  Trust issue has been a concern in all kind of cooperation; mutual auditability [6] may help to improve mutual trustworthiness which can lead to relax the issue.

- Inter-layer Communication

  Another issue in cross-layer approach is that layers do not know about each other semantics and there is no way to share that context, even if they are willing to do so. Lack of standard communication interfaces is a reason for the problem. Defining APIs in each layer is a step forward, in order to build a cross-layer solution. APIs can also help in mutual auditability which relax the trust challenges.

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 requirement 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 1: Properties of cross-layer security monitoring approach and corresponding challenges that each property deal with.

Specifications of these APIs is out of the scope for this paper, but it would be an important topic for further research in this area.

5 Conclusion

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

Furthermore, 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. Using open source platforms everyone, including open communities and third parties that are interested in security solutions, can develop their mechanisms.

Additionally, while reviewing variety of security mechanisms, it was clear that the security model is not mature yet and monitoring mechanisms need extensive development. Again, open communities play a crucial role here. Some of them 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 security monitoring solution which has cross-layer architecture. This architecture helps in dealing with several new challenges in the recent computing model. In addition, our approach avoid duplication of same tasks in each layer and improve accuracy in existing monitoring mechanisms.

6 Acknowledgments

I am thankful to my tutor, Juha Saaskilahti, whose encouragement, guidance and support from the initial to the final steps enabled me to develop the idea and write this paper.

References

[1] Amazon cloudwatch developer guide. `http://aws.amazon.com/cloudwatch/`, May 2009. Amazon WebServices.

[2] Aws security center. `http://aws.amazon.com/security/`, October 2010.

[3] Aws security bulletin: Amazon payments signature validation. `http://aws.amazon.com/security/security-bulletins/amazon-payments-signature-validation/`, September 2010.

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

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

[6] Y. Chen, V. Paxson, and R. H. Katz. What is new about cloud computing security? Technical Report UCB/EECS-2010-5, EECS Department, University of California, Berkeley, Jan 2010.

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

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

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

[10] Def con is one of the oldest continuous running hacker conventions around, and also one of the largest. http://www.defcon.org, Nov 2010.

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

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

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

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

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

[16] In the united state district court for the northern district of texas dallas division, April 2009. Liquid Motors, Inc. v. Allyn Lynd and United States.

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

[18] F. Gens. It cloud services user survey, pt.2: Top benefits & challenges. Technical report, International Data Corporation - IDC, 2009.

[19] Google's Security Team. Security whitepaper: Google apps messaging and collaboration products. Google's Security Team.

[20] 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.

[21] C. Hoff. What's the problem with cloud security? there's too much of it. http://www.rationalsurvivability.com/blog/?p=2693, October 2010.

[22] C. Hoff, S. Johnston, G. Reese, and B. Sapiro. Cloudaudit 1.0 - automated audit, assertion, assessment, and assurance api (a6). Internet-Draft draft-hoff-cloudaudit-00, Internet Engineering Task Force, 2010. Experimental.

[23] International Data Corporation. From silicon to cloud: Building up to cloud computing. Technical report, International Data Corporation - IDC, 2009.

[24] P. E. J.D. Meier. Azure security notes. Exploring Microsoft Azure and the Cloud Security Space.

[25] P. Mell and T. Grance. The nist definition of cloud computing. Technical report, National Institute of Standards and Technology, Information Technology Laboratory, July 2009.

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

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

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

[29] C. Pettey and H. Stevens. Gartner highlights key predictions for it organizations and users in 2010 and beyond, January 2010.

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

[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 E. Al-Shaer, S. Jha, and A. D. Keromytis, editors, *ACM Conference on Computer and Communications Security*, pages 199–212. ACM, 2009.

[32] Christofer hoff. http://www.rationalsurvivability.com/, Nov 2010.

[33] 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.

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

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

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