SLA-Based Cloud Security Monitoring: Challenges, Barriers, Models and Methods

Dana Petcu

West University of Timişoara, Romania
petcu@info.uvt.ro
http://web.info.uvt.ro/~petcu/

Abstract. Despite the tremendous efforts in cloud computing to overcome its main adoption barriers, like security concerns or quality of service guarantees, there is currently no commercial product or research prototype of a SLA-based cloud security monitoring system. This paper investigates the main challenges and barriers in designing a SLA-based cloud security monitoring system and the models and methods that can be used in its development.

Keywords: cloud computing, monitoring, service level, security.

1 Introduction

A monitoring process aims to observe and track applications and resources at run-time. In particular, cloud monitoring is a very important task for both cloud service provider (CSP in this paper) and consumer (CSC) as it involves dynamically tracking the Quality of Service (QoS) parameters related to virtualized resources (e.g., VM, storage, network, appliances), the physical resources they share, the applications running, and data hosted on them. Moreover, cloud monitoring is the basis of control operations and corrective actions for running systems on clouds [2]. Therefore, cloud monitoring is a key tool for managing software and hardware resources and providing continuous information on these resources as well as for consumer's applications hosted on the cloud. However, the monitoring is used in various other contexts, like performance, SLA management, security, billing and troubleshooting [1].

Service provisioning in the cloud relies on Service Level Agreements (SLAs) representing a contract signed between CSC and CSP which includes the requirements of the service specified as QoS and penalties in case of violations. Flexible and reliable management of resources and SLA agreements are of paramount importance to both CSP and CSC. On the one hand, CSP have to prevent SLA violations to avoid penalties, and, on the other hand, they have to ensure high resource utilization to prevent costly maintenance of unused resources. The continuous monitoring of the cloud and of its SLAs (e.g. in terms of availability, delay) supplies both CSP and CSC with such information as the workload generated by the CSC and the performance and QoS by the CSP, also allowing to implement mechanisms to prevent or recover violations.

L. Lopes et al. (Eds.): Euro-Par 2014 Workshops, Part I, LNCS 8805, pp. 359–370, 2014.

Cloud monitoring tools can assist a CSP or CSC in: (1) keeping their resources and applications operating at peak efficiency; (2) detecting variations in resource and application performance; (3) tracking the leave and join operations of cloud resources due to failures and other dynamic configuration changes; (4) accounting the SLA violations of given QoS parameters. Therefore the monitoring process is the key element that has to be studied further and enhanced to upgrade the QoS level. Cloud monitoring and SLAs are correlated in the sense that one has an impact on the other [1,2]: (a) enhancing monitoring functionalities can help to meet SLAs; (b) SLA has to be met by the CSP in order to reach the required reliability level required by consumers; (c) monitoring may allow CSP to formulate more realistic and dynamic SLAs and better pricing models by exploiting the knowledge of user-perceived performance.

Security monitoring is of high importance in a cloud environment. An extensive monitoring capability is essential if the operational security of a CSP platform has to be assessed [11]. To sustain information security in operation, it is necessary to plan the handling of attacks and security incidents in advance, and the service behaviour should be monitored. If regulated in the SLA – e.g., when there is a high availability requirement for the cloud services –, the CSC should also be able to contact the CSP' security incident handling and troubleshooting team. For administration to be auditable, all administrative activities should be logged. In this way, the CSP can provide their customers with evidence of when and which changes have been made to the service, and by whom. To identify attacks, log files (showing system statuses, failed authentication attempts, etc.) and other data sources related to security – e.g., analyses by system monitoring tools (like intrusion detection system or integrity checker) – should be used and correlated. Where a CSC has a requirement for protecting the confidentiality of his information (e.g., for data leakage protection), special tools need be deployed to control the data flow. These should detect or even intervene, if confidential data is sent via insecure routes or falls into the wrong hands.

An analysis of the available Cloud monitoring systems, SLA management systems, and Cloud security systems shows that no SLA-based cloud security monitoring system is currently available. We have reported this fact in the recent paper [20]. Moreover, that paper includes a review of various systems or tools for monitoring or SLA management or security in clouds (not to be repeated in this paper). More recently, we introduced in [19] a taxonomy that is necessary for the design of a SLA-based cloud security monitor. In this paper we discuss the main challenges that are faced in the design of such a system (Section 2) and the models and methods that can be followed or extended in its development (Section 3). This preliminary study is meant to support the development in the next year of the monitoring system of the SPECS project [22].

2 Challenges and Barriers

The main challenges and barriers related to the design of a SLA-based cloud security monitoring system are stated in what follows.

2.1 Security Related Challenges and Barriers

The ability to monitor what goes on in the cloud has become the most critical part of information security in the cloud. However, security monitoring lags behind other security features made available by CSP, and is typically less developed than operational performance monitoring.

A first barrier is the fact that security SLAs are not in place. A security SLA is an SLA that specifies the security obligations associated with a service. In contrast to traditional SLAs, a security SLA includes a set of security requirements [3]. According to [26], CSP contracts will not provide detailed and substantive security SLAs before 2016. The absence of security aspects in SLAs, combined with the lack of methods for making objective comparisons between different service offerings, makes it virtually impossible for CSP to offer trustworthy services to CSC when third party providers are involved [3]. Security SLAs can not only increase the trust in CSP, but also facilitate objective comparisons between different CSP on the basis of their security features. Such an approach will also form a basis for composing services from different CSPs, based on a set of pre-defined security requirements.

A second barrier is related to privacy. Privacy laws are restricting today CSP from instant monitoring, as considered an intrusion into the customer processes and data. Which data are allowed to be collected need to be well defined, and specific frameworks or SLAs are not available.

A high challenge is related to the data security monitoring. Guarantees and penalty clauses in the SLA are the best ways to ensure that the data are protected. However, data security is the most difficult problem in information security right now and data security-related risks have been greatly magnified by cloud computing. The processing of big data on clouds is introducing a new dimension to the problem as the control of large data sets is time consuming and instant reaction of the monitoring system is difficult to be achieved. The continuous monitoring of the data is coming with a potential penalty on the performance of the data processing.

2.2 SLA Related Challenges and Barriers

The fact that nowadays monitoring infrastructures lack appropriate solutions for SLA monitoring [9] is currently the main barrier.

A first challenge is the mapping between low-level metrics and application-based SLA parameters. Application level monitoring is a difficult task, as the infrastructure and platform layer metrics need to be mapped to the required metrics at the application to support SLA management. The performance of the application is described as a high-level SLA parameter, as, for example, the availability. But, applications run on physical or virtual resources, which are characterized with low-level metrics such as CPU, memory, uptime, downtime, etc. So, there is a gap between the low-level resource metrics and the high-level SLA parameters and a mapping between them is not obvious. Another related topic is how to determine appropriate monitoring intervals at the application

level, keeping the balance between the early detection of possible SLA violations and the intrusiveness of the monitoring tools on the whole system. Through monitoring of the cloud infrastructure resources, the CSP gains information about the usage of the resources and the current resource availability status. The rate of acquisition of this information is an important factor, impacting the overall performance of the system and the profit of the CSP. On the one hand, monitoring at a high rate delivers fast updates about the resource status to the CSP but it can cause high overhead, which possibly degrades the performance of the system. On the other hand, monitoring at a low rate causes the miss of information such as failing to detect SLA violations, which leads to SLA penalties for the CSP. To address this issue, techniques to determine the optimal measurement intervals to efficiently monitor to detect SLA violations are required [9]. Moreover, there is still lack of adequate monitoring infrastructures able to predict possible SLA violations: most of the available monitoring systems rely either on Grid or service-oriented infrastructures, which are not directly compatible with clouds, due to the differences in resource usage models.

A second challenge is related to the need of layer agnosticism. Application components (streaming servers, web servers, indexing servers, compute services, storage services, and network) can be distributed across cloud layers (e.g. PaaS and IaaS). Therefore it is critical to be able to monitor SLA parameters to multiple cloud layers. Hence, the challenge here is to develop monitoring tools that can capture and react to the parameters associated with different layers. Monitoring tools are originally oriented to perform monitoring tasks over services only in one of the layers. Moreover, most of current commercial tools are designed to keep track of the performance of resources provisioned at the IaaS layer [2].

A third challenge is related to the fact that the definition of the term security metric is still vague. Being quantifiable and measurable are essential metric attributes. However, the definition of a security that can be quantifiable and can be expressed in a service level is still a hurdle to be overcome [4].

2.3 Cloud Related Challenges and Barriers

A first barrier is related to the uncertainty associated with the cloud environments: due to the very high complexity of cloud systems, it not always possible to be sure that all events can be actually observed. For example, if we put a probe in an application that runs in the cloud to collect information on the rate at which it exchanges information with other applications running in the same cloud, we do not necessarily know if the measured rate is affected by the transfer rate of the network. The rate depends on where the two applications are running (on the same physical host or not) and this information is not always exposed by CSP. Similar issues arise for evaluating the performance of computation: the time required for a task completion can depend on the current hardware that is executing the instructions (can be a different hardware to the next deployment in the cloud, while the available information from CSP is only in terms of ranges of CPU model, not the concrete values) and on the workload due to other

virtualized environments running on the same physical server (which are not exposed to the CSC by the CSP) [1].

A second barrier is related to the fact that virtualization makes monitoring harder than in other environments. Most of existing monitoring tools (including security ones) have not yet grown to understand virtual and cloud environments. Notions like hypervisor security or cloud stack introspection are essentially not dealt with. Moreover, it is challenging (if not impossible) for a CSP to de-multiplex security monitoring data from shared environments.

A high challenge is the cloud agnosticism. Many public CSPs enable their CSCs to monitor their applications using monitoring tools. Often these tools are tightly integrated in their cloud and do not allow to monitor cloud services of other providers. For example, Amazon's CloudWatch enables consumers to manage and monitor their applications, but it is not possible to extend it to monitor an application component that may reside on other CSP infrastructure [2]. Engineering provider-agnostic monitoring tools is challenging, primarily due to fact that there is no common unified application programming interface for calling runtime statistics of cloud services. Agnostic monitoring tools are also required if one wants to realize a hybrid cloud architecture involving services from private and public clouds.

Only if the cloud agnosticism is achieved, the monitoring of large scale distributed virtual environments on Clouds can be enabled. Obtaining a comprehensive cross-domain monitoring solution represents a task that has not yet been properly addressed. Among different cloud monitoring infrastructures there is a high heterogeneity of systems, tools, and exchanged information. Moreover, a recent research [1] on cross-domain data leakage and its prevention pointed that the ability to monitor services performance is considered as a security risk.

3 Models and Methods

In this section we discuss the main models and methods that are the basic building blocks for a potential SLA-based cloud security monitoring system.

3.1 Cloud Security Models

Multi-layer Model for Cloud Security. According to [6], cloud security is a multi-layered approach. Clouds can be modeled in seven layers: facility, network, hardware, operating system, middleware, application, and the user. In more details, security monitoring is handled, according to [18,25], as follows.

At facility layer, security is mainly handled at physical level, involving the implementation of access control through authentication systems (e.g. using the access control model based on UCON [8]), alarm systems and sensors, and so on. The main objective is to prevent malicious intrusion and data manipulation, ensuring the integrity of facilities and components.

At hardware level, security metrics are in line with those adopted in the premises. The CSP is responsible for monitoring the hardware, and can use

specfic software to monitor the connection topology, memory use, bus speeds, processor loads, disk storage, temperature, voltage, and so on. The CSP measure such quantities to effectively load-balance its resources.

At network level, mechanisms such as firewalls, intrusion detection systems, intrusion prevention systems can be adopted. The network defense devices are collecting information about security events on the network. The CSP can log this information; these logs are used in auditing the network's security.

The security of virtual infrastructure resources can be associated with operating systems. In this case, the metrics should be extracted from monitoring operating system events and system calls between VMs and hardware. The purpose is mainly to prevent copy and data violations. The host operating system monitors and arranges all system calls between the VMs and the hardware, so it can access any data passing to or from the VM.

At middleware layer, the metrics are related to monitoring of virtualization and safety systems in heterogeneous cloud architectures. The middleware monitor ensure the secure communication between various system components as it mediates between the applications and the OS. Assurance concerns fall in three categories: software architecture flaws, e.g. as result from human misconfiguration of resources or policies; coding vulnerabilities, e.g. due to common software defects; security services, including monitoring, access control, data validation.

At application level the number of security vulnerabilities is a relevant metric, since it is necessary to monitor behavior to detect possible violations. Other components to be monitored are mostly digital certificates, private keys, etc.

If the cloud just provides services for distributing public information, such as a web page, the user's consumption has little security impact. However, if the users are members of the CSC organization, they are integral to the security policy. Access patterns can be monitored for malicious behavior. In addition, the CSC might need to make an addendum proscribing access to sensitive data.

Cloud Security Control Domains. These were defined recently in the Cloud Control Matrix [6]. The list of domains includes: application and interface security, interoperability and portability, identity and access management, governance and risk management, legal and standards compliance, data security and information lifecycle management, datacenter security, change control and configuration management, infrastructure and virtualization security, e-discovery and cloud forensics, encryption and key management, supply chain management, transparency and accountability, mobile security, threat and vulnerability management, business continuity management and operational resilience, human resources security.

3.2 Metrics and Security Parameters

Cloud Metrics. A conceptual metrics model, Cloud Service Measure and Metric (CSMM) (not focused on security metrics), was presented in [17]. The intent of the model is to capture the necessary information needed to describe and interpret metrics focused on cloud services. The concept model entities are:

(a) scenario: the user side of a metric (application, SLA definition); (b) measure definition: data and meta-data constitutive of a measure definition; (c) metric: data, meta-data and rules constitutive of a metric definition; (d) measurement: run-time data or dynamically generated data, resulting from applying a metric.

Service Measurement Index. It is a set of business-relevant key performance indicators that provide a standardized method for measuring and comparing a business service regardless of whether that service is internally provided or sourced from an outside company [24]. It is designed to become a standard method to help organizations measure cloud-based business services based on their specific business and technology requirements. However, it is not focused on security metrics. The category of 'Security and Privacy' includes attributes that indicate the effectiveness of a service provider's controls on access to services, service data, and the physical facilities from which services are provided: access control and privilege management; data geographic/political; data integrity; data privacy and data loss; physical and environmental security; proactive threat and vulnerability management mechanisms; retention/disposition.

Security Metrics. We can use the definitions from [23] for security indicators, measures and metrics.

A security indicator is any observable characteristic that correlates (or is assumed to correlate) with a desired security property. The set of feasible indicator values is assumed to form (at least) a nominal scale. For many proposed indicators, the required correlation with security has not been formally established, but is only postulated based on informal reasoning. An example of an indicator is the rate of compliance with a given catalogue of security criteria or security best practices (i.e., the relative number of requirements met).

A security measure assigns to each measured object a security indicator value from an ordinal scale according to a well-defined measurement protocol. In many cases, the measured values are numbers, but measures may also assign non-numeric designators such as low, medium, high.

A security metric is a security measure with an associated set of rules for the interpretation of the measured data values.

Cloud Security Properties. The CUMULUS project has established recently the principles for the construction of a generic attribute-based security property vocabulary [7], where each property has a unique identifier. A top-down approach was used to build a vocabulary starting with control domain borrowed from an industry cloud security control framework [6]. For each property in the vocabulary, three core elements are defined: a unique identifier, a definition, and a set of attributes, with a further distinction between performance and parametric attributes. Performance attributes are attributes of the property for which the CSP provide guarantees, such as the percentage of uptime or the level of confidentiality. Parametric attributes are attributes that contribute to the definition of the property itself, such as the length of a measurement period which allows to distinguish several flavors of the same property, such as weekly or hourly uptime.

The attributes included in security properties only describe the parameters that are strictly needed to describe a security property unambiguously.

Security Parameters for Monitoring. According to [10], the security parameters for a security monitoring framework can be classified in the following categories: incident response, data life-cycle management, change management, log management and forensics, service availability, service elasticity and load tolerance, technical compliance and vulnerability management, and data isolation. These parameters need to be considered according to the use-case: e.g. IaaS, PaaS and SaaS have different monitoring requirements and/or division of responsibilities.

3.3 Monitors

Monitoring Types. Two basic types of cloud monitoring can be considered, according [15]: CSC-oriented monitoring or CSP-side monitoring (either virtual system monitoring or physical system monitoring).

The approach undertaken in CSC-oriented monitoring is depending on the Cloud service delivery model. In SaaS model, service costs, usage of resources, status of the application and access history are monitored. In PaaS model, the impact of resource usage on costs and the usage of resources (development tools, network traffic and hosting space) are monitored. In IaaS model, the cost per instance, the consumed time, and the VM status are monitored.

CSP-side monitoring is done either on physical systems or on virtual systems. In the first case the evolution and the performance are monitored. In the second case the approach is depending again on the delivery model. In SaaS model, the resources sharing among applications and application usage patterns are tracked. In PaaS model, simultaneous connections and used hosting space are observed. In IaaS model, the status of internal resources and of each VM is monitored.

In particular, the security monitoring is currently done: on-premises, on monitored IaaS or via SaaS/other third party. In the first case, usually a Security Information and Event Management (SIEM) is able to make use of specific software-as-a-service APIs as well to collect logs from public cloud services. In the second case, the SIEM system is loaded directly into an IaaS. The advantages are that the tools are familiar and there is no high bandwidth requirement. However, high storage costs in the cloud can occur. Unfortunately, there is a lack of a unified view on on-premises and on-IaaS monitoring. In the third case, specific data from the cloud service are obtained (if available) and handed to a managed security service provider (e.g., Splunk Storm).

Monitoring the behavior of VMs is a critical requirement for CSP and CSC. There are two monitoring mechanisms on virtualized platforms [27]: (a) take a complete VM as the monitoring granularity, so that they cannot capture the malicious behaviors within individual VMs, or (b) focus on specific monitoring functions that cannot be used for heterogeneous VMs concurrently running on a single cloud node.

For monitoring software assets, two types of approaches have been proposed to provide an assurance of the behaviors of software elements [16]: static or

dynamic. Static approaches – e.g., code inspection and automated analysis, formal methods, testing and so on – are based on checking the security of the software before it is actually executed by the users. The static verification activities must be carried out in simulated environments. Dynamic approaches – e.g., monitoring, surveillance and other form of runtime analyses – are based on the observation of the actual behavior of the software and are carried out in the environment where the software is actually used.

High and Low Level Monitoring. According to [1], the monitoring can be of high-level or low-level. High-level monitoring is related to information on the status of the virtual platform. This information is collected at the middleware, application and user layers by CSP or CSC through platforms and services operated by themselves or by third parties. In the case of SaaS, high-level monitoring information is generally of more interest for the CSC than for the CSP (being closely related to the QoS experienced by the former). Low-level monitoring is related to information collected by the CSP and usually not exposed to the CSC, and it is more concerned with the status of the physical infrastructure of the whole cloud (e.g. servers and storage areas).

Low-level monitoring tests can be divided into two main categories: computation-based or network-based. Computation-based tests are related to monitoring activities aimed at gaining knowledge about and at inferring the status of real or virtualized platforms running cloud applications. The tests can be related, for example, to the following metrics: CPU speed or utilization, CPU time per execution, memory page exchanges per execution, throughput/delay of message passing or of disk/memory, server throughput, response time, access time, VM acquisition/release/startup time, up-time. Network-based tests are related to the monitoring of network-layer metrics; the monitored data are, for example: traffic volume, available bandwidth, throughput, round-trip time, packet/data loss, capacity.

Security monitoring falls mostly in the category of high-level monitoring. For low-level monitoring, specific utilities for collecting information about security refer to the followings: to the hardware layer, workload, voltage, temperature, memory, CPU; to the operating system and middleware layers, software vulnerabilities and bugs; to the facility layer, authentication data; to the network layer, firewall, intrusion detection systems, intrusion prevention systems.

Monitor Architecture, Models and Properties. According to [2], there are two types of architectures: centralized and decentralized. In the first case the PaaS and IaaS resources send status update queries to the centralized monitoring server; the monitoring techniques continuously pull the information from the components via periodic probing messages. Decentralized cloud monitoring tools have recently gained momentum. A monitoring tool is considered as decentralized if none of the components in the system is more important than others; in case one of the components fails, it does not influence the operations of any other component in the system. Following [21], other design criteria for the monitor architecture, are the followings: event notification (asynchronous or synchronous),

network transport (like UDP or TCP), historical data (with or without), measurement update strategy (like periodic, event or no update), communication model (pull or push), distributed architecture (like publish-subscribe, service-client, server-agent or client-server), QoS support (with or without), notification strategy (on change or event or periodic), metadata (out-band or in-band), exchange format (proprietary, XDR-XML, XDR, plain text or CDR), filtering (time-based, content-based or no filtering), discovery (with or without, only sensors, registration, or cluster level), communication cardinality (1:N or N:M), transport protocol (standard or proprietary).

Moreover, the models of monitoring frameworks are needed to assess their performance and verify results obtained from measurement. An analytic model of the behaviour of a monitoring framework that is usefull in the context of Cloud services is the one provided in [12].

According to [1,5], a monitoring system is required to have several properties: scalability, elasticity, adaptability, timeliness, autonomicity, comprehensiveness, extensibility, non-instrusiveness, accuracy. If the system is working with multiple clouds, a supplementary requirement is interoperability. If the system is dealing with security, than the following supplementary properties should be fulfilled, according to [13,14]: effectiveness, precision, transparency, non-subvertability, deployability, dynamic reaction, accountability and multi-tenancy.

Input Data for Security Monitoring. In terms of security requirements, the monitoring tests are quite complex. One of the reasons is the restricted access to the monitoring data. Here we mention shortly only the parameters categories. The data available are depending on the delivery model. In SaaS model, the available data are: if the CSP allows, application logs; if applicable, the access data like browser based or client-based monitoring data, proxy/gateway data. In PaaS model, the available data are: application logs; if the CSP allows, error or platform logs; if a proxy/gateway is used, the access data. In IaaS model, the available data are: logs of databases, applications or operating systems; local host traffic for network monitoring; antimalware or other agents logs for host/endpoint activity; if the CSP allows, change and hypervisor logs; if a proxy/gateway is used, access data.

4 Conclusions

The lack of a SLA-based cloud security monitoring system in the current market is reflecting the complexity of its design and implementation. This paper intended to reveal the main challenges and barriers (like the definition of security SLAs or big data monitoring), encountered in an initiative that intends to build a such system. Moreover, it has point towards the building blocks that make possible the development at this moment in time, following the recent definition of the cloud security parameters. The development of the prototype is an on-going work in the SPECS project (www.specs-project.eu).

Acknowledgment. This research is partially supported by the Romanian grant PN-II-ID-PCE-2011-3-0260 (AMICAS), as preliminary study for the grant FP7-ICT-2013-10-610795 (SPECS).

References

1. Aceto, G., Botta, A., De Donato, W., Pescapè, A.: Survey cloud monitoring: A survey. Computer Networks 57(9), 2093–2115 (2013), http://dx.doi.org/10.1016/j.comnet.2013.04.001
2. Alhamazani, K., Ranjan, R., Mitra, K., Rabhi, F.A., Khan, S.U., Guabtni, A., Bhatnagar, V.: An overview of the commercial cloud monitoring tools: Research dimensions, design issues, and state-of-the-art. CoRR abs/1312.6170 (2013), http://arxiv.org/abs/1312.6170
3. Bernsmed, K., Jaatun, M.G., Meland, P.H., Undheim, A.: Security slas for federated cloud services. In: 2011 Sixth International Conference on Availability, Reliability and Security (ARES), pp. 202–209 (August 2011), http://dx.doi.org/10.1109/ARES.2011.34
4. de Chaves, S.A., Westphall, C.B., Lamin, F.R.: Sla perspective in security management for cloud computing. In: 2010 Sixth International Conference on Networking and Services (ICNS), pp. 212–217 (March 2010), http://dx.doi.org/10.1109/ICNS.2010.36
5. Clayman, S., Galis, A., Chapman, C., Toffetti, G., Rodero-Merino, L., Vaquero, L.M., Nagin, K., Rochwerger, B.: Monitoring service clouds in the future internet. In: Towards the Future Internet, pp. 115–126. IOS Press (March 2010), http://dx.doi.org/10.3233/978-1-60750-539-6-115
6. Cloud Security Alliance: Cloud controls matrix. Tech. Rep. Version 3, CSA (September 2013), https://cloudsecurityalliance.org/download/cloud-controls-matrix-v3/
7. CUMULUS Consortium: Security-aware sla specification language and cloud security dependency model. Tech. Rep. Deliverable D2.1, CUMULUS (September 2013), http://cumulus-project.eu/index.php/public-deliverables
8. Danwei, C., Xiuli, H., Xunyi, R.: Access control of cloud service based on ucon. In: Jaatun, M.G., Zhao, G., Rong, C. (eds.) Cloud Computing. LNCS, vol. 5931, pp. 559–564. Springer, Heidelberg (2009), http://dx.doi.org/10.1007/978-3-642-10665-1_52
9. Emeakaroha, V.C.: Managing Cloud Service Provisioning and SLA Enforcement via Holistic Monitoring Techniques. Ph.D. thesis, Vienna University of Technology (2012), http://www.infosys.tuwien.ac.at/staff/vincent/pub/Emeakaroha_thesis.pdf
10. European Union Agency for Network and Information Security: Procure secure: A guide to monitoring of security service levels in cloud contracts. Tech. rep., ENISA (April 2012), http://www.enisa.europa.eu/activities/Resilience-and-CIIP/cloud-computing/procure-secure-a-guide-to-monitoring-of-security-service-levels-in-cloud-contracts
11. Federal Office for Information Security: Security recommendations for cloud computing providers. Tech. rep., BSI (June 2011), https://www.bsi.bund.de/SharedDocs/Downloads/EN/BSI/Publications/Minimum_information/SecurityRecommendationsCloudComputingProviders.html
12. Lahmadi, A., Andrey, L., Festor, O.: Design and validation of an analytical model to evaluate monitoring frameworks limits. In: Eighth International Conference on Networks, ICN 2009, pp. 397–402 (March 2009)

13. Laniepce, S., Lacoste, M., Kassi-Lahlou, M., Bignon, F., Lazri, K., Wailly, A.: Engineering intrusion prevention services for iaas clouds: The way of the hypervisor. In: 2013 IEEE 7th International Symposium on Service Oriented System Engineering (SOSE), pp. 25–36 (March 2013), http://dx.doi.org/10.1109/SOSE.2013.27
14. Manavi, S., Mohammadalian, S., Udzir, N.I., Abdullah, A.: Secure model for virtualization layer in cloud infrastructure. International Journal of Cyber-Security and Digital Forensics 1(1), 32–40 (2012)
15. Montes, J., Sánchez, A., Memishi, B., Pérez, M.S., Antoniu, G.: Gmone: A complete approach to cloud monitoring. Future Generation Computing Systems 29(8), 2026–2040 (2013), http://dx.doi.org/10.1016/j.future.2013.02.011
16. Muñoz, A., Gonzalez, J., Maña, A.: A performance-oriented monitoring system for security properties in cloud computing applications. The Computer Journal 55(8), 979–994 (2012), http://dx.doi.org/10.1093/comjnl/bxs042
17. NIST Cloud Computing Standards Roadmap Working Group: Nist cloud computing reference architecture cloud service metrics description. Tech. rep., NIST (September 2013), http://www.nist.gov/itl/cloud/
18. Palhares, N., Lima, S.R., Carvalho, P.: A multidimensional model for monitoring cloud services. In: Rocha, Á., Correia, A.M., Wilson, T., Stroetmann, K.A. (eds.) Advances in Information Systems and Technologies. AISC, vol. 206, pp. 931–938. Springer, Heidelberg (2013), http://dx.doi.org/10.1007/978-3-642-36981-087
19. Petcu, D.: A taxonomy for sla-based monitoring of cloud security. In: 2014 IEEE 38th Annual Computer Software and Applications Conference (COMPSAC) (in print July, 2014)
20. Petcu, D., Crăciun, C.: Towards a security sla-based cloud monitoring service. In: 2014 4th International Conference on Cloud Computing and Services Science (CLOSER), pp. 598–603 (April 2014), http://dx.doi.org/10.5220/0004957305980603
21. Povedano-Molina, J., Lopez-Vega, J.M., Lopez-Soler, J.M., Corradi, A., Foschini, L.: Dargos: A highly adaptable and scalable monitoring architecture for multi-tenant clouds. Future Generation Computer Systems 29(8), 2041–2056 (2013), http://dx.doi.org/10.1016/j.future.2013.04.022
22. Rak, M., Suri, N., Luna, J., Petcu, D., Casola, V., Villano, U.: Security as a service using an sla-based approach via specs. In: 2013 IEEE 5th International Conference on Cloud Computing Technology and Science (CloudCom), vol. 2, pp. 1–6 (December 2013), http://dx.doi.org/10.1109/CloudCom.2013.165
23. Rudolph, M., Schwarz, R.: A critical survey of security indicator approaches. In: 2012 Seventh International Conference on Availability, Reliability and Security (ARES), pp. 291–300 (August 2012), http://dx.doi.org/10.1109/ARES.2012.10
24. Siegel, J., Perdue, J.: Cloud services measures for global use: The service measurement index (smi). In: Annual SRII Global Conference, pp. 411–415 (2012)
25. Spring, J.: Monitoring cloud computing by layer, part 1. IEEE Security and Privacy 9(2), 66–68 (2011), http://dx.doi.org/10.1109/MSP.2011.33
26. Wagner, R., Heiser, J., Perkins, E., Nicolett, M., Kavanagh, K.M., Chuvakin, A., Young, G.: Predicts 2013: Cloud and services security. Tech. Rep. G00245775, Gartner (Nov 2012), https://www.gartner.com/doc/2254916/predicts--cloud-services-security
27. Zou, D., Zhang, W., Qiang, W., Xiang, G., Yang, L.T., Jin, H., Hu, K.: Design and implementation of a trusted monitoring framework for cloud platforms. Future Generation Computer Systems 29(8), 2092–2102 (2013), http://dx.doi.org/10.1016/j.future.2012.12.020