Olga Wenge*, Ulrich Lampe, Christoph Rensing and Ralf Steinmetz

Security Information and Event Monitoring as a Service: a Survey on Current Concerns and Solutions

Abstract: Today's cloud environments are very heterogeneous. Current security approaches of intrusion detection, prevention, and response in physical environments are sophisticated. However, the growth of virtualization and multi-tenant technologies is creating new targets for intrusion and raises many questions about the implementation of the same protection in cloud environments. As an answer to the clouds' heterogeneity, the heterogeneity of cloud security solutions is presented, which causes market confusion and brings more complexity in the selection process of sound security solutions. As not every enterprise has in-house tools, competences and expertise to secure cloud environments on its own, Security as a Service (SecaaS) solutions are becoming more popular, promising cost-savings and proper real-time threats detection and prevention. In our paper, we outline the current research areas in SecaaS, especially Security Information and Event Management (SIEM). Furthermore, we discuss requirements and concerns related to implementation of SIEM as a service and identify challenges for further research.

Keywords: cloud computing security; security as a service; security assessments; security event management; intrusion detection

***Olga Wenge:** E-Mail: olga.wenge@KOM.tu-darmstadt.de
Ulrich Lampe: E-Mail: ulrich.lampe@KOM.tu-darmstadt.de
Christoph Rensing: E-Mail: christoph.rensing@KOM.tu-darmstadt.de
Ralf Steinmetz: E-Mail: ralf.steinmetz@KOM.tu-darmstadt.de

I Introduction

Cloud computing, as a new significant and innovative shift in information technology, provokes further expansive innovations in the areas supporting its development and establishment in the market. One of these areas is the security area [1]. Due to the main characteristics of cloud computing (mainly, scalability and usage of shared resources), the security approach should be centralized to protect providers and users properly and detect security breaches in time [2].

The idea of the worldwide security implementation as an *outsourced commodity* can also lead to the standardization of cloud computing security frameworks and bridge the gaps caused by the current *cloud heterogeneity* and missing security agreements between cloud providers [3]. *Security as a Service (SecaaS)* is a new outsourcing model for security management that supervises, controls and manages security of cloud users and cloud providers from the cloud [4]. However, organizations will not be able to shift or outsource *the whole responsibility* for a data breaches onto their SecaaS provider, so they need to be proactive about keeping an eye out for potential problems and to be compliant with their security programs.

Virtualization and cloud computing break the current security solutions and, to some degree, add new security black holes to in-house security monitoring framework [5]. Transparency has become an important feature in cloud services and in SecaaS especially. Consumers wish to understand how security works. This understanding can be achieved through access to event and log data, processed by monitoring devices. But large providers, such as Amazon or Google, are not willing to provide any insider information or share their log data with consumers [4]. Security Information and Event Management (SIEM) as a service, as a component of SecaaS solutions, deals with such consumers' requirements and helps to bring more transparency into the opaque cloud world by outsourcing *event and log management*.

The remainder of the paper is organized as follows. In Section 2, we discuss the current SecaaS solutions in the market. Section 3 presents SIEM as a service for cloud environments. Furthermore, we outline the current SIEM requirements and concerns. In Section 4, we give an overview of related work. Finally, Section 5 concludes our paper and describes our future work.

II Security as a Service

Security as a Service (SecaaS) as a new outsourcing model for security management is currently very widely discussed in the cloud community, especially in the context of

establishing of *fair and orderly cloud markets*. SecaaS can be implemented as a security interface or a mediator between cloud market actors (consumers, providers, and brokers) to provide, guarantee, control and manage security from the cloud. Besides the opportunity to save time and money, this outsourced service usually offers greater security expertise and technology than within the consumers' own enterprises and performs constant update and modification of security tools to enhance the prevention and detection of *zero-day attacks*. The usage of configurable web interfaces enables in-house security experts to control external actions in their security environments and brings more transparency [6]. On the other side, the concerns around SecaaS have the right to exist, as security environments cannot be controlled in the in-house manner. Insufficient background checks of the personnel, incompliance with local and international laws and regulations, as well as non-secure web interfaces and communication channels and latency in the incident response are seen as further security concerns in the usage of SecaaS.

The results of the survey in [3] pointed out the following ten SecaaS categories that are of most interest and relevance among experienced security professionals and big industrial companies:

- Identity and Access Management (IAM)
- Data Loss Prevention (DLP)
- Web Security
- Email Security
- Security Assessments
- Intrusion Management
- Encryption
- Business Continuity and Disaster Recovery
- Network Security
- Security Information and Event Management (SIEM)

Identity and Access Management (IAM) is a preventive and protective security measure, which provides control over identities and assures authorized access. Besides the prevention of an unauthorized access and unauthorized privilege rights, IAM is a must-have to protect against identity theft, insider threat, fraud and non-repudiation. The configuration and implementation of IAM is provided in accordance with the enterprise security model, e.g., Bell-LaPadula, Biba, role-based or other access-based approaches [8].

Data Loss Prevention (DLP) mechanisms take care of the reputational and sovereignty issues, assuring and controlling that only approved and allowed information and data in the correct format can be transmitted and accessed. Implementation of information classification labeling (e.g., internal, confidential, secret), data filtering (e.g., data with credit card numbers, addresses, disease codes) are widely used examples of DLP [9, 10].

Web Security measures offer protection and detection of malware, spyware, virus and phishing attacks by web activities and can be also combined with further incident reactions, e.g., denial of access to a web site, blocking of downloads, blacklisting of web sites. These security measures are compulsory in cloud computing as in any internet-based technology and often implemented together with DLP and email security mechanisms, firewalls, and network perimeters security controls [11].

Email Security solutions are usually seen as a part of DLP (in case of outbound emailing) and as a part of Web Security (in case of inbound emailing) mechanisms and protect users from phishing, attachments with malicious content, spam, and data leakage. In combination with digital signatures and encryption mechanisms, email security solutions protect against non-repudiation and assure confidentiality and data integrity [3, 11].

Security Assessments are very *time-consuming* security measures. They are usually provided by intern or extern auditors or third parties in form of risk assessments and penetration tests to assess security policies, security configurations and security controls of cloud providers and users and to match them against multiple industrial standards (e.g., ISO [12], NIST [13]), local and international compliance regulations and laws (e.g., HIPPA, PIPEDA, EU Directive [14, 15]), cloud certificates, and in-house security measures. The identified security gaps must be further valued to decide how to deal with – *accept, mitigate, outsource, or stop* the activity.

Intrusion Management as a service provides identification of malicious actions using event patterns. The pre-defined patterns are used to recognize and prevent intrusions in real-time. Intrusion management is usually implemented together with event and incident management solutions to identify anomalies and response with automatic or manual remediation actions [16, 17].

Encryption measures protect users and users' data against reputational risk, disclosure of stolen information, forgery, man-in-the-middle attack and other information interceptions. As a rule, encryption systems include cryptographic algorithms for en- and de-coding of information, hashing functions, digital signature and certificate procedures, and key exchange methods. The last ones are the most critical,

as the unauthorized disclosure of keys can ease the data decryption for attackers [3, 11].

Business Continuity and Disaster Recovery (BC&DR) measures are responsible for an operational resiliency and continuity in case of any breaches of technical, man-made or natural origin. BC&DR measures must be properly planned accordingly to risk calculations or a business impact analysis. Currently, the best practices of BC&DR solutions are hot, warm or cold sites, data center mirroring and cloud collaborations [14, 15].

Network Security measures together with web security measures are the most wanted ones, as the most part of all attacks in cloud computing is aimed at network connectivity via Internet. Network security solutions in the cloud should be centralized, i.e., network activity monitoring of each resource should be aggregated to detect and protect the users and providers in time. Otherwise, due to a scalable and multi-tenant character of cloud computing, network attacks can be easily overlooked if malicious actions are treated separately. Firewalls, intrusion detection and protection solutions (IDPS), security gateways, de-militarized zones (DMZs) in combination with security monitoring and log management are currently mostly secure sets of network security measures [4, 5, 7].

Security Information and Event Management (SIEM) solutions handle logs and event information. Logs and events are sent from monitored systems to further analysis to SIEM systems, where they undergo correlation, aggregation, filtering, and matching steps to be efficiently used for real-time incident recognition and response and be prepared for alert messages and reporting. SIEM solutions are nowadays the most moot security solutions in cloud computing and that is why they are very challenging [4].

In the next section we discuss SIEM as a service in cloud computing and outline its requirements and concerns about implementation in cloud environments.

III Security Information and Event Management as a Service

Strict regulatory requirements and laws, especially after the last financial crises, with respect to security monitoring of information systems were launched and introduced as compulsory, to demand more responsibility from senior management and improve transparency in information security processes. As a consequence of these requirements, a lot of money is and will be spent by enterprises to develop, adopt, implement and maintain comprehensive solutions for security monitoring of information systems. Security information and event monitoring (SIEM) tools and techniques are significant components of them [18]. The adoption of cloud computing opens, of course, new challenges and requirements to SIEM, as such features as scalability, highly-distribution, elasticity and multi-tenancy of resources, were not considered in the "traditional", non-cloud SIEM solutions. That is why, SIEM solutions are currently moot and arguable in cloud computing. But, SIEM solutions are *compulsory* and must be implemented according to numerous requirements we discussed before. So, the sound adoption and re-architecture of SIEM for the cloud must take place.

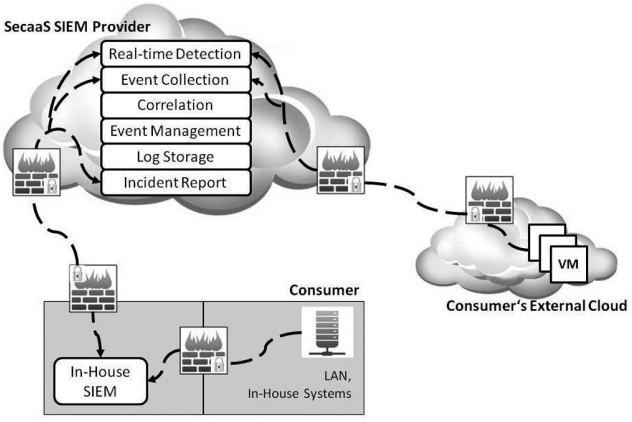

Fig. 1: SIEM as a Service.

The main function of SIEM is the treatment of log and event information to detect incidents and anomalies in information systems (Fig. 1). SIEM aggregates data from very many resources – firewalls, management systems, video systems, physical and virtual security systems, if required in an enterprise security policy. Usually, these resources and systems are not centralized and that causes a certain amount of risk to overlook the complete picture of security environments, especially in the clouds. The aggregated information is then put into a single data stream, normalized or translated into an acceptable format (if required), filtered, and de-duplicated. This, prepared for further analysis, event stream is correlated against a set of human defined rules and programmed correlation algorithms to provide real-time reporting and alerting on security incidents in the system. The correlation rules may vary from consumer to consumer and be very trivial or very complex and cover multitude of conditions and constrains.

A Correlation rules

Correlation rules are responsible for detection of *not allowed actions* (i.e., security threats) and misbehavior in a monitored system. These rules must have following attributes: *purpose* (definition of security threat this rule can identify), *action* (system's to-dos if the rule is triggered), *event or event pattern correlation* (description of events and their values, which are necessary to identify threats), *logic* (a correct sequence of events and event patterns), and *response* (a kind of reporting). Current "best practice" SIEM solutions use the following four types of correlation rules [18–21]:

1) Audit-based rules: These rules are the simplest rules. They compare single events to the value of pre-defined security configuration with the following logic:

```
if Event A then Alert B, or
if Event X does not exist then Alert Y.
```

2) Signature-based rules: These rules use pattern matching logic to identify threats e.g.:

```
if Events (A and B or (not C)) then Alert D.
```

3) Heuristic-based or anomaly-based rules: These rules aggregate event patterns, anomaly identification, suspicious behavior signs, assess them according to a pre-defined risk matrix, add risk calculations and compare the results with a pre-defined permitted threshold. If the calculated value exceeds this threshold, an alert will be triggered, e.g.:

```
compare Patterns A and B and ... X with Pattern Y ->
if threshold (similarity count) exceeds N then Alert Z.
```

Such rules are used to detect so-called *"zero-day" attacks*, which are new (only "zero-day" old) and unknown to a SIEM system and can be identified only by so-called "suspicious" events and system behavior.

4) Bayesian inference-based rules: This relatively new type is based on the Bayesian inference logic. This logic can predict possible occurrence of events, based on the hypothetical and comparative analysis of historical event data. Bayesian inference-based rules, in comparison to heuristic-based rules, can also predict whether any anomaly in an event pattern is potentially nefarious or not, what certainly helps to detect zero-day attacks.

B Requirements to SIEM as a Service

As many other security solutions, SIEM solutions should be adopted for cloud environments. We identified the following requirements in the current research literature [3–5, 14–16, 18, 19, 23, 26–29]:

1) *Real-time or close to real-time identification and detection of threats* in an optimal way combined with an incident response or ticketing system.

2) *Comprehensive coverage and cross-boundary intelligence*. SIEM solutions should provide exhaustive and optimally covered view of system events to be efficient.

3) *High flexibility and customization*. SIEM solutions should be easily adapted to consumers' in-house security policies and configurations. Enterprises, which use SIEM as a service, may have very different security policies due to their industrial peculiarities (e.g., banking, healthcare, chemistry).

4) *Adoption of correlation rules*. Due to scalability, a bigger dataflow is expected in the clouds and SIEM solutions should be able to handle it. A proper and real-time adoption of correlation rules, especially for heuristic-based or behavior-based rules, is necessary to identify zero-day attacks.

5) *Reduction of "false positive" alerts*. Again, due to scalability, a dataflow should be properly filtered and de-duplicated, to ensure providing of only relevant events.

6) *Compliance with regulatory and industrial requirements*. SIEM solutions should be designed and implemented with respect to current security and risk requirements (e.g., NIST, Basel Accords) and industrial peculiarities (e.g., SOx, PCI for financial industry).

7) *Automation*. Consumers usually wish as much automation as possible to save time and money.

8) *Subsequent forensic examination*. SIEM events in the cloud must be stored to be used as evidence to trace the identified questionable behavior or security incidents.

9) *Flexible log storage and log retention*. As different consumer can have different storage and retention policies, this requirement is necessary to be compliant with regulators and to act ad hoc to possible consumers' policy changes.

10) *Visibility and transparency*. SIEM solutions should be designed the way they are able to gain a centralized visibility for consumers, e.g., via consumer web interfaces or self-service portals. These allow consumers to control or glimpse into how their systems are monitored and managed.

11) *Cost savings*. SIEM solutions should be cheaper than in-house solutions and, of course, in pay as you go manner.

12) *Encryption of communication channel*. Log data must be transmitted and stored in manner that prevents tampering.
13) *Clear roles and responsibilities*. SIEM solutions can be fully managed or partially managed by providers; clear responsibilities between a consumer and a provider must be documented in e.g., SLAs (service-level agreements), contracts or SOWs (statements of work).
14) *User-friendly performance and reporting via graphical interfaces*. Consumers should be always aware about changes in their systems, which should be promptly reported.
15) *Sharing of information* to improve the identification of threats and maximize the visibility of attacks.

C Concerns about SIEM as a Service

Due to the peculiarity of cloud and Internet services the following concerns are still building hurdles in implementing of SIEM as a Service [3, 4, 14, 15, 22, 23, 26, 28–30]:
1) *Loss of connectivity*. SIEM as a service is fully depending on Internet connectivity and, in case of Internet failover, some alternate routes must be considered in a business continuity and disaster recovery plan.
2) *Deperimeterization*. The boundaries of cloud architecture components (e.g., virtual firewalls) within enterprise can be shifted and stay without control.
3) *Business continuity and disaster recovery solution for SIEM*. Optional SIEM providers should be considered for ad hoc data transfer in case of disaster. That is why interoperability between SIEM providers must be established.
4) *Key exchange between providers and consumers of SIEM*. By the usage of encryption and decryption the overhead on computation and additional storage is required and must be considered.
5) *Assurance of Quality of Services (QoS)*. Such assuarance is usually guranteed via SLAs and contracts.
6) *Legal and ethical considerations*. Sometimes consumers may not outsource part of log and event data, the decision of outsourcing must be conform to internal security policy and external requirements, e.g., governmental or industrial ones.
7) *Lack of standardized log format*. Standardization of log and event format is very important if a consumer wishes to change his/her SIEM provider and be independent in his/her choice. Such standardization is also profitable for SIEM providers, as they do not need to translate consumers' log formats into their own, what saves time and money.
8) *Delay in response time and reaction*. It is a very critical concern. The improvement of response time sometimes can be achieved by considering the localization of SIEM provider and faster connectivity and network throughput.
9) *Scaling for high volumes*. Current SIEM solutions can not deal with scaling up of log amounts that can open additional security holes in consumers' systems.
10) *Proper segregation of consumers' data by multitenancy*. Usage of additional virtual firefalls and physical seggregation should be in place by SIEM providers.
11) *Cloud providers' non-transparency or unwillingness to share log information with SIEM providers*. This is the most arguable issue. To solve it, contracts and legal agreements should be discussed and signed before any data transfer.

IV Related Work

In this section, we present current research challenges and solutions related to SIEM and SecaaS.

Aguirre and Alonso propose a *collaborative SIEM solution* that centralizes and aggregates information from different domains [31], which possess their own SIEM instances, building a kind of *federation*. The authors tested their approach with OSSIM, an open source SIEM, and identified improved rapidness in threat detection and system response, due to the expanded common knowledge base among federation partners and security expertise. However, information flow was not encrypted.

Băsescu et al. propose in [32] a *generic security framework* for detection of malicious behavior and a large array of DoS attacks, based on the usage of *expressive policy description language* for efficient communication between data management systems. The approach was evaluated with BlobSeer, a data management system for cloud storage, and video surveillance log and event data. The results identified drastically lowered performance and delay (from 10% to 70%) by scaling-up of data amount. Further tests with concurrent data streams and optimization of false negative – to – false positive relation are planned.

Hoßbach et al. present a *reactive cloud monitoring approach* with complex event processing (CEP) [33]. The authors argue CEP to be *the best fitting model* for cloud event management and present a CEP-based holistic close to real-time monitoring solution. Furthermore, the authors tested their solution with cloud databases and examined improvement in data stream correlation and system adoption to new correlation rules. However, such features as scalability and collaborative action framework are not yet tested.

Suneetha and Krishnamoorthi in [34] analyze *web logs* as a basis for identification of users' behavior and propose *web-log patterns* and discuss preliminary results of data

mining with web-log patterns. The authors plan to extend their research with examination of pattern frequency and clustering.

van der Aalst introduces in [35] *Casual nets* as a solution for process configuration and event data mining. The author advocates the merging of processes to a single configurable process, as an optimization in dealing with deadlocks and system anomalies in *multi-tenant environments*.

Yassin et al. propose *Cloud-based Intrusion Detection Service (CBIDS)* [36]. This solution acts as an intrusion prevention system and an antivirus tool as a service in cloud environments. The authors believe the solution is able to sniff and detect malicious packets in cloud networks. The technical implementations and evaluation are ongoing.

Modi et al. summarize in their survey [37] 17 existing Intrusion Detection Systems and Intrusion Prevention Systems for cloud environments. The identified solutions are still far from the integration in the clouds and must be combined with SIEM or additional security measures and correlation rules to identify internal attacks or to be prepared for *zero-day attacks*. The authors also pointed out the necessity of the *centralized view* in monitoring and extension of existing solutions with capability to analyze data stream by *scaling up and down*.

Lee at al. [38] propose *multi-level IDS* in combination with log management approach for identification of anomaly behavior in cloud environments. The approach is based on the *quantification of risk levels* and assigning risk points in proportion to risk anomaly behavior. The approach is fully quantitative and does not yet consider qualitative risk methods, which are also significant in any corporate security risk program.

Arshad, Townend, and Xu in [39] propose an automatic intrusion diagnosis approach for cloud environments. The described approach uses *machine learning technologies* facilitated by SLAs and presents *an ad hoc approach* for adoption of correlation rules.

Lassila analyzes in [40] an offering of a *Mobile Security as a Service (MSaaS)* in the cloud market and points out cost-efficiency, novelty, platform independence and real-time reaction as the main business drivers for MSaaS solutions for monitoring and detection of wireless security threats for mobile end-devices.

Savola and Ahola in [41] introduce a *security metric-based approach* for remote security monitoring of cloud services. Their security metrics assure the correctness of implemented security measures and in combination with "security sensor" devices and IPS/IDS provide real-time security monitoring.

Doelitzscher et al. [42] present a prototype of *Security Audit as a Service (SAaaS)* solution. This solution is based on distributed autonomous audit agents that check cloud environments and report detected deviations. However, the prototype is not yet validated in scalable environments.

V Conclusion and Future Work

Implementation and usage of SIEM as a service is in its *embryonic phase*. Due to still existing concerns and peculiarities in its implementation in clouds environments, SIEM as a service stays a great challenge in the current cloud security research.

In our work, we discussed identified requirements and concerns with SIEM. Furthermore, we gave an overview of related work in this research area. Finally, we identified *scalability*, *ad hoc adoption* and *centralization* as three main challenges that should be addressed by cloud research community to provide efficient and secure design and implementation of SIEM solutions in the cloud.

In our future work, we aim at the analysis of *current event correlation techniques* in combination with *complex event processing (CEP)* to examine new patterns for detection of zero-day attacks. Furthermore, we intend to consider SIEM system changes and correlation rules adoption with respect to scalable cloud environments.

Acknowledgment

This work is supported in part by E-Finance Lab e. V., Frankfurt am Main, Germany (http://www.efinancelab.com).

References

1 Gartner Research: Hype cycle for cloud computing, 2011.
2 L. Vaquero, L. Rodero-Merino, and D. Morán, "Locking the sky: a survey on IaaS cloud security," Journal Computing, vol. 91, issue 1, pp. 93–118, 2011.
3 CSA, https://cloudsecurityalliance.org/research/security-guidance.
4 V. Getov, "Security as a service in smart clouds – opportunities and concerns," IEEE 36th Annual Conference on Computer Software and Applications, pp. 373–379, 2012.
5 A.U. Khan, M. Oriol, M. Kiran, Ming Jiang, and K. Djemame, "Security risks and their management in cloud computing," IEEE 4th International Conference on Cloud Computing Technology and Science, pp. 121–128, 2012.

6 A. Abuhussein, H. Bedi, and S. Shiva, "Evaluating security and privacy in cloud computing services: a stakeholder's perspective," International Conferece For Internet Technology And Secured Transactions, pp. 388–395, 2012.
7 M. Ates, S. Ravet, A. Ahmat, and J. Fayolle, "An identity-centric internet: identity in the cloud, identity as a service and other delights," International Conference on Availability, Reliability and Security, pp. 555–560, 2011.
8 M. Kretzschmar and M. Golling, "Security management spectrum in future multi-provider inter-cloud environments – method to highlight necessary further development," 5th International Academic Alliance Workshop on Systems and Virtualization Management, pp. 1–8, 2011.
9 E. Gomes, Q.B. Vo, and R. Kowalczyk, "Pure exchange markets for resource sharing in federated clouds," Concurrency and Computation: Practice and Experience, vol. 24, issue 9, pp. 977–991, 2012.
10 J. Guitart and J. Torres, "Characterizing cloud federation for enhancing providers' profit," IEEE 3rd International Conference on Cloud Computing, pp. 123–130, 2010.
11 OASIS-Security-Services, https://www.oasis-open.org.
12 ISO, http://www.iso.org/iso/catalogue_detail?csnumber=42103.
13 NIST report, http://csrc.nist.gov/publications/nistpubs/800–145/SP800–145.pdf.
14 ENISA, http://www.enisa.europa.eu/activities/.
15 ISACA Information Security Governance Guidance for Boards of Directors and Executive Management, 2006, http://www.isaca.org/.
16 T. Uttam Kumar and H, Wache, "Cloud broker: bringing intelligence into the cloud," IEEE 3rd International Conference on Cloud Computing, pp. 544 – 545, 2010.
17 D. Bernstein and D. Vij, "Intercloud security considerations," IEEE International Conference on Cloud Computing Technology and Services, pp. 537 – 544, 2012.
18 H.A. Kholidy and F. Baiardi, "CIDS: a framework for intrusion detection in cloud systems," 9th International Conference on Information Technology: New Generations, pp. 379–385, 2012.
19 M. Gegick and L. Williams, "Matching attack patterns to security vulnerabilities in softwareintensive system designs," Workshop on Software engineering for secure systems, pp. 1–7, 2005.
20 M. Almgren and U. Lindqvist, "Application-integrated data collection for security monitoring," 4th International Symposium, pp. 23–36, 2001.
21 C. Sinclair, L. Pierce, and S. Matzner, S, "An application of machine learning to network intrusion detection," 15th Annual Computer Security Applications Conferenc, pp. 371–377, 1999.
22 R. von Ammon, T. Ertlmaier, O. Etzion, A. Kofman, and T. Paulus, "Integrating complex events for collaborating and dynamically changing business processes," International conference on Service-oriented computing, pp. 370–384, 2009.
23 W.M. Halton and S. Rahman, "The top ten cloud-security practices in next-generation networking," International Journal of Communication Networks and Distributed Systems, vol. 8, issue 1/2, pp. 70–84, 2012.
24 S.T. Zargar, H. Takabi, and J.B.D. Joshi, "DCDIDP: a distributed, collaborative, and datadriven intrusion detection and prevention framework for cloud computing environments," 7th International Conference on Collaborative Computing: Networking, Applications and Worksharing, pp. 332–341, 2011.
25 A. Paschke, and A. Kozlenkov, "Rule-based event processing and reaction rules," International Symposium, RuleML, pp. 53–66, 2009.
26 T.-F. Fortis, V.I. Munteanu, and V. Negru, "Towards an ontology for cloud services," 6th International Conference on Complex, Intelligent and Software Intensive Systems, pp. 787–792, 2012.
27 U. Lampe, O. Wenge, A. Müller, and R. Schaarschmidt, "On the relevance of security risks for cloud adoption in the financial industry," in press, 19th mericas Conference on Information Systems, 2013.
28 S. Ristov, M. Gusev, and M. Kostoska, "Cloud computing security in business information systems," International Journal of Network Security & Its Applications, vol. 4, no. 2, pp. 75–93, 2012.
29 S.N. Dhae, B. Meshram, R. Rawat, S. Padawe, M. Paingaokar, and A. Misra, "Intrusion detection system in cloud computing environment," International Conference & Workshop on Emerging Trends in Technology, pp. 235–239, 2011.
30 S. Bleikertz, M. Schunter, C. Probst, D. Pendarakis, and K. Eriksson, "Security audits of multi-tier virtual infrastructures in public infrastructure clouds," ACM workshop on Cloud computing security, pp. 93–102, 2010.
31 I. Aguirre and S. Alonso, "Improving the automation of security information management: a collaborative approach," Security & Privacy, vol. 10 , issue 1, pp. 55–59, 2012.
32 C. Băsescu, A. Carpen-Amarie, C. Leordeanu, A. Costan, and G. Antoniu, "Managing data access on clouds: a generic framework for enforcing security policies," IEEE International Conference on Advanced Information Networking and Applications, pp. 459 – 466, 2011.
33 B. Hoßbach, B. Freisleben, and B. Seeger, "Reaktives cloud monitoring mit complex event processing," Datenbank-Spektrum, vol. 12, issue 1, pp 33–42, 2012.
34 K.R. Suneetha and R. Krishnamoorthi, "Identifying user behavior by analyzing web server access log file," International Journal of Computer Science and Network Security, vol. 9, no. 4, pp. 327–332, 2009.
35 W.M.P. van der Aalst, "Business process configuration in the cloud: how to support and analyze multi-tenant processes?" 9th IEEE European Conference on Web Services, pp. 3–10, 2011.
36 W. Yassin, N.I. Udzir, Z. Muda, A. Abdullah, and M.T. Abdullah, "A cloud-based intrusion detection service framework," International Conference on Cyber Security, Cyber Warfare and Digital Forensic, pp. 213–218, 2012.
37 C. Modia, D. Patela, B. Borisaniyaa, H. Patelb, A. Patelc, and M. Rajarajanc, "A survey of intrusion detection techniques in cloud," Journal of Network and Computer Applications, vol. 36, issue 1, pp. 42–57, 2013.
38 Jun-Ho Lee, Min-Woo Park, Jung-Ho Eom, and Tai-Myoung Chung, "Multi-level intrusion detection system and log management in cloud computing," 13th International Conference on Advanced Communication Technology, pp. 552–555, 2011.
39 J. Arshad, P. Townend, and J. Xu, "An automatic intrusion diagnosis approach for clouds," International Journal of Automation and Computing, vol. 8, issue 3, pp. 286–296, 2011.
40 A. Lassila, "Offering mobile security as a service," 40th Annual Hawaii International Conference on System Sciences, pp. 58, 2007.

41 R.M. Savola and J. Ahola, "Towards remote security monitoring in cloud services utilizing security metrics," 6th International Conference on Application of Information and Communication Technologies, pp. 1–7, 2012.
42 F. Doelitzscher, C. Fischer, D. Moskal, C. Reich, M. Knahl, and N. Clarke, "Validating cloud infrastructure changes by cloud audits," IEEE 8th World Congress on Services, pp. 377–384, 2012.

Olga Wenge: Technische Universität Darmstadt – Multimedia Communications Lab – KOM, Rundeturmstr. 10, Darmstadt 64283, Germany

Ulrich Lampe: Technische Universität Darmstadt – Multimedia Communications Lab – KOM, Rundeturmstr. 10, Darmstadt 64283, Germany

Christoph Rensing: Technische Universität Darmstadt – Multimedia Communications Lab – KOM, Rundeturmstr. 10, Darmstadt 64283, Germany

Ralf Steinmetz: Technische Universität Darmstadt – Multimedia Communications Lab – KOM, Rundeturmstr. 10, Darmstadt 64283, Germany