Dynamic Certification of Cloud Services

Iryna Windhorst
Department "Service & Application Security"

Fraunhofer Research Institution AISEC
Garching near Munich, Germany
e-mail: iryna.windhorst@aisec.fraunhofer.de

Ali Sunyaev
Faculty of Management, Economics and Social Sciences
University of Cologne
Cologne, Germany
e-mail: sunyaev@wiso.uni-koeln.de

***Abstract*—Cloud computing introduces several characteristics that challenge the effectiveness of current certification approaches. Particularly, the on-demand, automated, location-independent, elastic, and multi-tenant nature of cloud computing systems is in contradiction with the static, manual, and human process-oriented evaluation and certification process designed for traditional IT systems. Cloud-specific certification processes can improve trust in the cloud computing paradigm, and can lead to the wide adoption of cloud services in enterprises by mastery of uncertainty, lack of transparency, and trust. Through third party evaluation cloud customers could receive more unbiased information about cloud-based services and security measures implemented as well as they could compare different cloud service providers much easier.**

Common certificates are a backward look at the fulfillment of technical and organizational measures at the time of issue and therefore represent a snapshot. This creates a gap between the common certification of one to three years and the high dynamics of the market for cloud services and providers. The proposed dynamic certification approach adopts the common certification process to the increased flexibility and dynamics of cloud computing environments through using of automation potential of security controls and continuous proof of the certification status. Dynamic certification is based on a new semi-automated certification process and the continuous monitoring of critical parameters of cloud services.

Keywords-Dynamic certification; cloud computing; compliance; audit; security automation; continuous monitoring

I. INTRODUCTION

Cloud Computing has been envisioned as the next generation of IT due to its advantages: on-demand self-service, ubiquitous network access, location independent resource pooling, rapid resource elasticity, and measured service (i.e., usage-based pricing) [14]. According to location independency, and rapid elasticity of cloud computing systems, as well as complexity resulting from the different cloud service (IaaS, PaaS, SaaS) and deployment models (Private, Public, Hybrid, Community), service evaluation and especially security evaluation becomes much more difficult. Furthermore, there is no overall evaluation standard for cloud computing, like the worldwide accepted ISO 27001 for security audit, and cloud customers using cloud services have still to fulfill different compliance regulations.

One major hindrance for the adoption of cloud services is the fact that customers have to trust their cloud service provider (CSP), if they want to use cloud services. The more information about the particular cloud service offering and its security is available, the easier it is to trust a provider [10]. An approach to receive more unbiased information about cloud-based services and the risks associated with their usage could be an evaluation by an independent third party. According to Gartner certification will become the norm for cloud offerings [10]. Users can therefore refer to the evaluation results and don't depend solely on information from the CSP. Additionally, they can also compare the results of evaluations of different cloud providers to gain a market overview and make better selection decision [17]. Such an approach would have also an economical benefit because one single certification or assessment can satisfy the needs of multiple customers and can reduce costs dramatically [10].

In this context the term certification describes the process whereby an organization, a product, or a process is tested and evaluated by an (accredited) party to determine whether or not it complies with a specific standard or a set of standards [6]. Certificates are approved means, not only in the IT industry[1], to give customers fast, simple, transparent, and comparable information on protective measures implemented, compliance with standards, and internal quality processes (e.g. ISO 27001 or EuroCloud Star Audit[2]).

The certification of cloud services by independent third parties can lead to the wide adoption of cloud services in enterprises by mastery of uncertainty, lack of transparency, and trust [20]. Therefore it can help to achieve economies of scale, increase efficiency of resource utilization, and save costs, as promised by cloud computing industry. The main challenge is the adoption of a common certification approach to the cloud specifics. This point is addressed with our *concept of dynamic certification*.

Section 2 discusses related work. In section 3 we explain the characteristics of cloud computing which are in contradiction with a common certification process. In section 4 we present our concept of dynamic certification. Section 5 gives a conclusion and the idea of future work.

II. RELATED WORK

Even if some approaches in the field of automated assessment do already exist, the research of cloud

[1] See many different TÜV certifications, e.g. certification according to European directives http://www.tuev-sued.de/industry_and_consumer_products/_services/legal_requirements/certification_of_directives

[2] EuroCloud, EuroCloud Star Audit, 2011, http://www.saas-audit.de

978-0-7695-5008-4/13 $26.00 © 2013 IEEE
DOI 10.1109/ARES.2013.55

certification and especially dynamic cloud certification is a new field and in its infancy.

Close to the idea of dynamic certification is the vision statement of the Cloud Security Alliance (CSA) with its Open Certification Framework (OCF) structured by three levels of trust from the STAR Self-Assessment to Continuous Monitoring based certification [18]. The majority of other research papers describe only some specific topics, either from technical perspective, e.g. security automation, or with focus on certification criteria. Some ideas of them are presented below.

Foster et al. propose a run-time certification and compliance mechanism combining static and dynamic model-checking techniques with event monitoring and violation detection, but without reference to cloud computing. They focus on SOA environment and do not consider multi-tenancy, location independency and on-demand provisioning [8]. Dhiyanesh and Thiyagarajan concentrate in their paper on third party auditability in cloud storage systems via simultaneous integrity check in order to ensure cloud data storage security. The authors focus only on the auditability of cloud storage by third party without reference to certification process [4]. Gul et al. analyze different cloud security auditing protocols for data integrity and privacy, data access management architecture, and auditing frameworks for cloud environments based on literature review, but do not propose a new approach aiming at cloud service offerings [9]. Chen and Yoon present a framework for secure cloud computing through IT auditing using checklist by following data flow and its lifecycle. However, they do not focus on certification at all [3]. Kaliski and Pauley go in a similar direction and recommend addressing the challenges coming with cloud computing, and enabling the evaluation of security risks in cloud environments, by introducing Risk Assessment as a Service. The authors present the vision of such assessment based on automated real-time measurement and analysis of risks, but they do not discuss challenges of such an approach or technical details of the proposed concept [11]. Kuo et al. propose and implement a dynamic risk assessment mechanism using SaaS web service. The proposed mechanism is designed for internal use in organizations in order to help security managers realize the security awareness and vulnerability assessment in end client devices [12]. Rannenberg describes criteria for certification and weaknesses of common security certification without focus on cloud computing [17]. Montesino and Fenz analyze in their paper, how many controls can be automated based on the standards ISO 27001 and NIST SP800-53, but without focus on certification or cloud computing [15]. The paper of Edwards et al. is also focused on automated approach to security. Even security automation is potentially beneficial in theory, they argue, that it is not a panacea for end-user security in practice and present limitations of such approach [5]. Accorsi and Lowis propose ComCert approach for automated compliance certification of cloud-based business processes, but they focus only on regulatory requirements and a process layer [1]. The main statement of Pinkett is that the automation obviously improves audit quality [16].

In this paper we are focusing on characteristics of cloud computing that are in contradiction with common certification process and propose a dynamic certification approach as an option to fill the gap between the evaluations of traditional IT systems and cloud environments.

III. WHY THE COMMON CERTIFICATION PROCESS DOES NOT FIT THE CLOUD

Cloud computing introduces several characteristics that challenge the effectiveness of current assessment and certification approaches [11]. Such characteristics that make cloud computing attractive and help to realize his economic potential, make it also hard to certificate [11]. Current manual audits for certifications, such ISO 27001, ISAE 3402 /SSAE 16 Type II (former SAS 70), and EuroCloud Star Audit, are in contradiction with increased flexibility and dynamics that cloud computing offers [1, 11]. Common evaluation and certification process is static, manual, and human process-oriented as well as designed for traditional IT systems [11]. Cloud computing systems are on-demand, automated, elastic, location-independent, and multi-tenant in their nature [14]. Additionally, one of the core design principles of cloud computing paradigm is to provide dynamic scalability for several applications [22]. In the following we discuss the changes from the cloud computing model and their impact on certification process.

A. On-demand Self-Service

In traditional IT environments people, for instance, install, configure, deploy, and maintain IT systems, manage security and privacy controls, supported by tools, but mostly manually. In cloud environments per definition the human interaction should be reduced to the minimum, almost everything should happen automated reducing costs and time. The humans should not have the full control about the cloud environment, the control mechanism should be automated and thereby increase effectiveness [11]. The less control and direct access to data and applications, the more complicated it is to evaluate cloud systems.

B. Dynamic allocation and location independency of cloud resources

Depending on the cloud service model (IaaS, PaaS, SaaS) used customers and providers have responsibility for different layers, like infrastructure, software stack or application. Nevertheless, they always share the responsibility and governance. In traditional IT environments only one party, either the company itself or hosting/outsourcing partner is responsible for the data center operation and therefore for the governance and compliance of the company and IT infrastructure. An audit takes place on the location of the responsible party, i.e. in the company itself or on the location of the hosting provider. Therefore the company or outsourcing partner is certified for instance to ISO 27001 or ISAE 3402/SSAE 16. The certification of cloud computing systems is complex, because the most of technologies and controls are housed outside the entity being evaluated [19].

Due to the shared governance and responsibility between cloud customer and CSP, today's certification approaches allow only a partial evaluation of cloud systems. The certification process gets more complex

when combining IaaS cloud services from one provider, for instance Amazon from the USA, and SaaS services from another CSP, e.g. located in Germany. If these providers are spread over the world a certification process has to deal with an even more intricate situation taking different laws into account. Location independence of the physical resources results in different local compliance regulations, because data cross different security domains and regulations. Even if cloud providers use their own resources, data processing and data storage are not necessarily in the same location in the cloud environment. Additionally, backup and data destruction can permanently change the location. The common certification process is not designed for the evaluation of a run-time environment and such a high dynamic with different compliance regulations due to crossing of borders.

C. *Multi-tenancy*

Multi-tenancy describes the use of the same infrastructure to application services from many organizations. Multi-tenant structure of clouds enables new opportunities to attack from inside the cloud, as some tenants could be malicious. The traditional evaluation approaches do not consider multi-tenancy and shared usage of physical resources, infrastructure and applications at all. Especially isolation mechanisms should be taken into account in the cloud certification process.

Another important point is that traditional audit tools (e.g. audit and monitoring software) are not yet integrated in cloud services [21]. The environment is new, and audit techniques, best practices, controls, and metrics for cloud based services are just starting to develop as described in chapter 2. Today available certification standards, like ISO 27001 or ISAE 3402, audit only the information handling processes of a provider, but not such important topics like Service Level Agreement (SLAs), contract with subcontractors, or migration across multiple providers etc.

Many cloud providers advertise with a certification. However, users often cannot evaluate the relevance of such certifications. A large amount of certifications with different scope, validity period, audit process, certification provider, and used certification framework actually confuse users instead of helping with the comparison of different cloud offers.

The high complexity by recombination of cloud services, use of multiple providers and different environments, automation, multi-tenancy, and geographical dispersal of part services make a dynamic certification indispensable. To achieve an ongoing compliance in the cloud environment it is important to adapt the common certification approach to the dynamics of clouds and realize the evaluation in run-time and near real time.

IV. Dynamic Certification of Cloud Services

A. *Our Concept of Dynamic Certification*

Traditional certificates as a result of extensive evaluation represent a backward look at the fulfillment of technical and organizational measures at the time of issue. Therefore, they demonstrate a snapshot. This creates a gap between the currently common certification with one to three years validity period and the high dynamics and rapid technological progress in cloud computing and the underlying technologies. Today's cloud certificates suggest a high level of security and quality of services evaluated, even though the conditions and requirements are no longer met, for instance, after the configuration changes in the cloud systems.

We believe that the concept of dynamic certification can help to fill this gap. The main idea of our approach is the continuous proof of certification status and the adapted certification process (see Fig. 1).

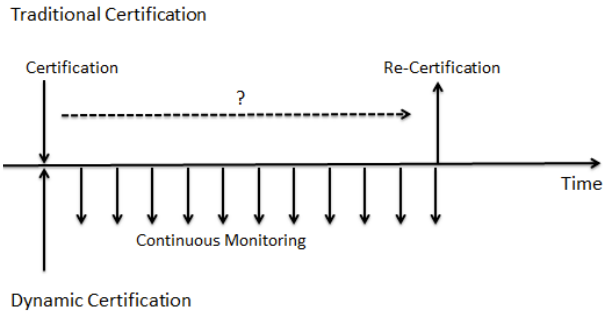

Figure 1. Gap between common certifications and proposed dynamic certification concept.

The dynamic certification is based on

- Standards such as CSA CCM, ISO 27001/27017, NIST SP800-53, EuroCloud Audit questionnaire,
- Continuous monitoring of critical parameters of cloud services and data center organization,
- Automation of the certification/ evaluation process, and
- Appropriate technical, organizational, legal, and economic conditions for the integration of the dynamic certification into the regular operations of cloud providers.

From our point of view monitoring and verification of results should be done continuously and automated, where it is possible, as a continuous monitoring service. Approximately 30% of security controls could be automated according to Montesino and Fenz [15]. We believe that the use of this automation potential can adapt the common certification process to the specifics of cloud computing. A dynamic certificate delivers a reliable proof that a provider of cloud services satisfies continuously (part-) automatically-evaluable technical, legal, and organizational requirements for quality, privacy, and security and therefore it is much more trustworthy than a common certificate.

B. *Actors and Roles in the Dynamic Certification*

There are several actors and roles typically involved in a cloud ecosystem and certification efforts from a business perspective. Their roles, responsibilities, and their relationships with other actors could vary a little bit. Based on analysis we identified six major participating actors in the context of dynamic certification. They are the Cloud Service Provider, Cloud Service Customer, Provider of Cloud Dynamic Certification, Cloud Auditor, Accreditation Body and Legislation. In the following we describe these actors with their roles and responsibilities.

Cloud Service Provider (CSP): A person, organization, or entity responsible for making a cloud service available to interested parties [13]. A CSP develops, operates and delivers the *Cloud Service* to the customer. Sometimes a CSP only delivers the *Subservice*, which is created and operated by Cloud Service Creator/ Developer [2] or he offers e.g. only Software as a Service (SaaS) based on Infrastructure as a Service (IaaS) of another cloud provider, who is called in this case Cloud Sub-Provider (e.g. Infrastructure or Platform Provider).

Cloud Service Customer: The service customer is the end user or enterprise that maintains a business relationship with a CSP. He actually buys the cloud service through different distribution channels, directly from the CSP or through a cloud market (platform provider) and uses the service [2, 13].

Provider of Cloud Dynamic Certification (Continuous Monitoring Service): The provider develops with the aid of Cloud Certifier, operates and delivers the Continuous Monitoring Service (CMaaS) to different customers.

Cloud Auditor or Cloud Certifier (Certification Body): A party qualified to conduct independent assessments or audits of cloud services, information system operations, performance and security of the cloud implementation, like security audit, privacy impact audit or performance audit. The Cloud Auditor provides a valuable inherent function for the government by conducting the independent performance and security monitoring of cloud services [13]. The Cloud Auditor could be a person, employed by Certification Body or freelancer accredited to conduct an audit of cloud services according to the *Cloud Service Certification Catalogue*, as well as an organization, an auditing firm. The both of them handle many different clients and certify different cloud services. The audit may involve interactions with the Cloud Service Customer and the Cloud Service Provider.

Accreditation Body, e.g. International Accreditation Forum (IAF) or National Accreditation Body, e.g. German accreditation body GmbH (DAkkS), develops Cloud Service Certification Catalogue and accredits the Certification Body's (Cloud Auditor's) compliance to Certification Catalogue.

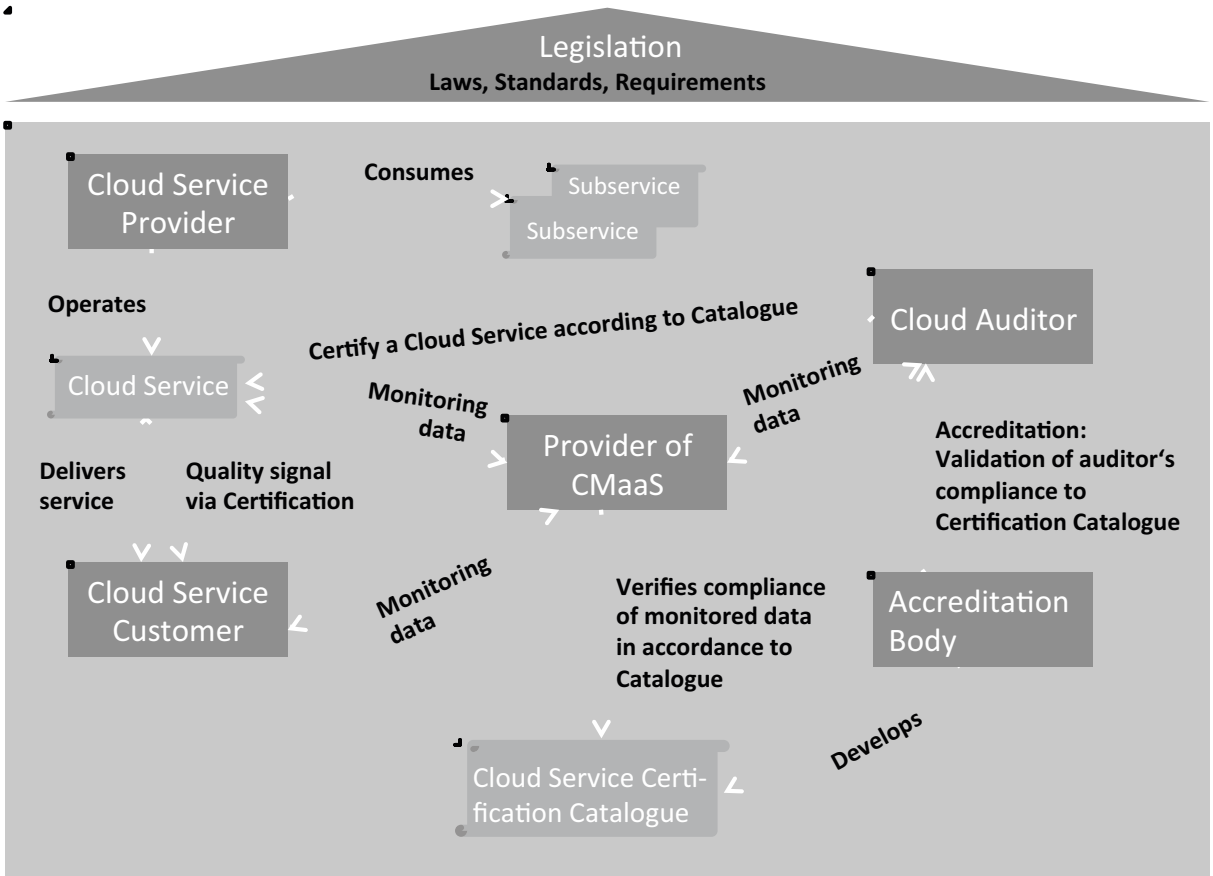

Figure 2. Identified Actors of Dynamic Certification

Legislation is understood in this paper as a general term covering laws enacted by parliaments, standards written by different standardization organisations, e.g. International Organization for Standardization (ISO) or Deutsches Institut für Normung e.V. (DIN; in English: German Institute for Standardization), as well as requirements or certification catalogues specified by some bodies or organizations.

The starting point is delivery of the service by a CSP to its customers. CSP provides a certificate as a quality message. This is a neutral (third party) certification based on the Cloud Service Certification Catalogue developed by

Accreditation Body. Cloud auditors could be different organizations or individuals. The Cloud Auditor should be accreditated, i.e. his qualification to conduct an audit according to the Cloud Service Certification Catalogue should be validated by an Accreditation Body. Accreditation as well as common certification itself are a largely formal act, and does not monitor the actual work. In our dynamic certification concept we have additionaly Provider of Continuous Monitoring Service, who monitors the cloud service continuously and communicates results to Cloud Auditor, Cloud Service Provider and Cloud Service Customer (see Fig. 2).

Out of all the roles described above there are also another actors in the cloud ecosystem, like cloud brocker, cloud administrator, cloud user or cloud carrier, because they are not very important in this certification use case.

V. Conclusion and Future Work

Certification of cloud services is a very important mechanism on the young cloud market to help cloud (potential) customers to make right and better founded decisions selecting an appropriate CSP or cloud service. Furthermore, the certification by a third party helps to receive unbiased information about risks associated with cloud service used and to increase transparency on the cloud market. All this can lead to increased trust in cloud services and their wide adoption in enterprises. That's why European Commission sees also a certification of cloud services and especially a framework for certification as the most important action for the EU to take [7].

The field of cloud certification research is only just emerging. Existing research focuses particularly on some aspects, like security automation or risk assessment service for clouds. Cloud certification offers are available in the practice, but in research area they have been studied only to a limited degree.

In this paper we demonstrated the differences between cloud computing and traditional IT environments, which have significant impact on certification process. Especially, on-demand Self-Service, automation, dynamic allocation, location independency of cloud resources and data (at rest, in motion and in use), shared governance, multi-tenancy, non-existence of adopted audit tools, standards, best practices and metrics for cloud-based services as well as complexity with recombination of cloud services from different CSPs are in contradiction with a common certification process.

To fill this gap we proposed the dynamic certification approach. Such a dynamic certification permits customers of cloud services to be constantly informed about the actual security and quality state as well as the compliance with the requirements of the certification, using continuous monitoring and (partially) automation of the certification process. Therefore, the dynamic certification can achieve a much more accurate statement of compliance with the various requirements and standards, like ISO 27001, HIPAA, FISMA, NIST, and German BSI IT-Grundschutz, than the common certification approaches. Further, the dynamic certification allows transfer of the trust-building process of certification in the dynamic and rapidly changing world of cloud services.

We have not implemented such a dynamic certification, but we offer it as an approach. For actual implementation, we suggest several research directions and challenges briefly below. During the certification process or the certificate's validity period, unexpected events like leaking of some major security incidents could happen or the certification standard could be updated. Research of organizational and technical impacts of such actions should be considered.

Additionally, the third party auditor (TPA) doing certification should be trustworthy and if the automated part of the audit is realized through privileged access of TPA to various internal monitoring tools and interfaces of cloud provider it should be secure enough and regularly checked for integrity, availability and confidentiality in order to resist malicious attacks and prevent from unauthorized access even from internal cloud tenants and cloud provider itself [22]. In this case the research on manipulation possibilities of the monitoring results by cloud provider and on possibilities of safeguarding that the results are reliable is needed.

For future work we plan to analyze different cloud controls and the possibilities how they can be automated. Amongst others we want to evaluate the usage ability and possibility of Secure Content Automation Protocol (SCAP) specified by the National Institute of Standards and Technology (NIST) and Cloud Trust Protocol (CTP) specified by Cloud Security Alliance (CSA) for this scenario. We plan to analyze the challenges and limitations of dynamic certification and their significance in terms of quality, privacy, and security for the selection and comparison of cloud services. Another question to explore is how far through dynamic certification the information asymmetry dominating between cloud (potential) customer and CSP could be minimized. Furthermore we wish to design and implement the concept of dynamic certification for the real use cases.

Acknowledgment

The information in this document was developed in the context of the Value4Cloud research project, funded by the German Federal Ministry for Economics and Technology (FKZ: 01MD11043A).

References

[1] R. Accorsi and L. Lowis, ComCert: Automated Certification of cloud-based Business Processes. ERCIM News(83), October 2010.

[2] M. Ahronovitz et al., Cloud Computing Use Cases White Paper. 2. July 2010.

[3] Z. Chen and J. Yoon, IT Auditing to assure a secure cloud computing. 2010 IEEE 6th World Congress on Services.

[4] B. Dhiyanesh and A. Thiyagarajan, A novel third party auditability and dynamic based security in cloud computing. International Journal of Advanced Research in Technology, 2011, Vol. 1(Issue 1), pp. 29-33.

[5] W. Edwards, E. S. Poole, and J. Stoll,. Security automation considered harmful? NSPW 2007.

[6] M. Eloff and S. von Solms, Information Security Management: A hierarchical framework for various approaches. Computers & Security(19), 2000, pp. 243-256.

[7] European Commission, Unleashing the Potential of Cloud Computing in Europe. 27.09.2012.

[8] H. Foster, G. Spanoudakis, and K. Mahbub, Formal certification and compliance for run-time service

environments. 2012 IEEE Ninth International Conference on Services Computing, 2012, pp. 17-24.

[9] I. Gul, A. Rehman, and M. Islam, Cloud computing security auditing. The 2nd International Conference on Next Generation Information Technology (ICNIT), 2011, pp. 143 – 148.

[10] J. Heiser and M. Nicolett, Assessing the security risks of cloud computing. ID Number: G00157782, 03.06.2008, pp. 1-6.

[11] B. Jr. Kaliski and W. Pauley, Toward Risk Assessment as a Service in Cloud Environments. Proceeding HotCloud'10 Proceedings of the 2nd USENIX conference on Hot topics in cloud computing, 2010.

[12] C.-T. Kuo, H.-M. Ruan, C.-L. Lei, and S.-J. Chen, A mechanism on risk analysis of information security with dynamic assessment. 2011 Third International Conference on Intelligent Networking and Collaborative Systems, 2011, pp. 643-646.

[13] F. Liu, J. Tong, J. Mao, R. Bohn, J. Messina, M. Badger, et al., NIST Cloud Computing Reference Architecture, Recommendations of the National Institute of Standards and Technology. NIST Special Publication 500-292. National Institute of Standards and Technology, September 2011.

[14] P. Mell and T. Grance, The NIST Definition of Cloud Computing, Recommendations of the National Institute of Standards and Technology. Special Publication 800-145, September 2011.

[15] R. Montesino and S. Fenz, Information security automation: how far can we go? 2011 Sixth International Conference on Availability, Reliability and Security, IEEE, 2011, pp. 280-285.

[16] F. Pinkett, Automating system security audits. Automation Systems Control Journal, 2004.

[17] K. Rannenberg, IT Security Certification and Criteria Progress, Problems and Perspectives. in Sihan Qing, Jan H.P.Eloff: Information Security for Global Information Infrastructures; Proceedings of the 16th Annual Working Conference on Information Security, 2000, pp. 1-10.

[18] J. Reavis and D. Catteddu, Open Certification Framework. Vision Statement. Cloud Security Alliance, August 2012.

[19] T. Singleton, IT-Audits of Cloud and SaaS. ISACA Journal(Volume 3), 2010.

[20] A. Sunyaev and S. Schneider, Cloud Services Certification. Communications of the ACM(56(2)), 2013, pp. 33-46.

[21] Wikibon, Audit and the cloud. Wikibon Blog, 26.02.2010.

[22] Y. Zhu, G.-J. Ahn, H. Hu, S. Yau, H. An, and S. Chen, Dynamic audit services for outsourced storages in clouds. IEEE transactions on services computing, 2011.