Security and Compliance in Clouds[1]

Kristian Beckers[1] · Jan Jürjens[12]

[1] Project Group APEX, Fraunhofer ISST, Dortmund, Germany

[2] Software Engineering (LS 14), Fak. Informatics, TU Dortmund, Germany

kristian.beckers@isst.fraunhofer.de

http://jan.jurjens.de

Abstract

The use of cloud computing services is an attractive opportunity for companies to improve IT Services and to achieve almost unlimited scalability of the IT infrastructure, and all of this at a significantly reduced cost than this is possible with internal resources. However, the use of a cloud service requires a company to trust the vendor to deal with the company's secret data. In order to check the compliance demands for the required security level, the business processes of the cloud vendor have to be inspected thoroughly. This is a time consuming and expensive task which has to be repeated continuously. Furthermore, company data is increasingly subject to compliance checks for legal regulations that differ in each geographical location, for instance the Sarbanes-Oxley Act (SOX) or the HIPPAA Act in the health domain in the U.S., or Basel II, Solvency II in Europe. We report on ongoing research about an automated compliance analysis method specifically for the analysis of the business processes of a cloud service provider. Nowadays, customers of cloud services can only inquire the existence of single security features like a firewall. The review of the entire security concept on a process level is seldom possible.

1 Introduction

"Cloud computing is a model for enabling convenient, on-demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction." according to the US National Institute of Standards and Technology (NIST).

The economical attraction of cloud computing is the ability to purchase computer resources without any upfront commitment and to pay only for the used amount of resources. This ability offers a number of new possibilities in the business world. Thus, companies are not limited to activities that their current resource pool can accomplish anymore. Cloud computing offers them almost unlimited scalability of IT resources. Furthermore, Return on Investment (RoI) calculations can be done faster, due to the fact that cloud computing has in many cases no fixed cost [JaSc10].

[1] This work was supported through the Fraunhofer-Attract project "Architectures for Auditable Business Process Execution (APEX)"

The usage of cloud computing services is an attractive opportunity for companies to improve IT-Services, achieve almost unlimited scalability of the IT infrastructure and all of this at a significantly reduced cost than this is possible with internal resources. However, the usage of a cloud service requires a company to trust the vendor explicitly with companies' secrets. One way to ensure the trust is satisfied is to maintain a strong security supervision of the cloud service. In order to check the compliance demands for the required security level, the business processes of the cloud vendor, at least the ones regarding the security of the cloud service, have to be inspected thoroughly.

This is a time consuming task that can only be executed by experts in the field and thus an expensive task. Furthermore, this effort has to be repeated constantly in order to verify the security level is maintained. While single technical methods exist in a cloud, e.g. network security, holistic automatic compliance checks on the basis of business processes are rather limited [StRu09]. An automated compliance analysis method specifically for the analysis of the business processes of a cloud service provider is a solution to this problem. This will provide a verifiable trust relationship between cloud vendors and customers at a low cost. Nowadays, customers of cloud services can only inquire the existing of single security features like a firewall. The review of the entire security concept on a process level is seldom possible.

Furthermore, company data e.g. in the form of business processes are increasingly subject to compliance checks for legal regulations, for instance the Sarbanes-Oxley Act (SOX) or the Health and Human Services Health Insurance Probability and Accountability Act (HIPPAA) in the U.S[AFG+09][CSA10]. This in particular relevant to cloud computing since a number of cloud vendors are based in the U.S., making customers data from all over the world subject to these compliance checks. However, legal regulations for risk management are not solely relevant in the U.S., for instance in Europe the Basel II and Solvency II accords aim also towards this goal.

A tool-supported method specifically designed for the evaluation of business process against legal and security compliance requirements making use of current model-driven and generative techniques such as the Eclipse Modelling Frameworks to achieve these goals in a process that includes cost-effective adherence to compliance regulations can improve the current situation. Furthermore, these techniques provide workflow monitoring capabilities for dynamic compliance checks.

Cloud computing business will grow at an accelerated rate then conventional enterprises. "It used to take years to grow a business to several million customers – now it can happen in months." according to Berkeley Armbrust et. al. [AFG+09]. This requires security systems to scale with an increased frequency as well. Moreover, businesses providing a service in the cloud want to interact with numerous business partners that use different technologies for security. Solutions for Cloud Federation Management is required that enables e.g. the authorization of users between the different security technologies of the business partners.

2 Security Issues in Cloud Computing

"Cloud computing is a model for enabling convenient, on-demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction." [MeGr09]. A study from the IDC in 2009 points out that the security of cloud services presents a significant barrier for the acceptance of cloud computing systems in companies [IDC09]. The cause is a poor support of security techniques [StRu09], the

significant requirements on scalability and elasticity of cloud computing systems [MeGr09], for which specific security techniques are just in development.

The security issues in the cloud computing area have resulted in the founding of user alliances, for instance the Cloud Security Alliance (CSA), which supports companies with the security evaluation of cloud systems [CSA10]. Confidentiality in cloud computing systems is a significant problem. There are possibilities today to transfer data to and from the cloud encrypted, also data can be stored encrypted. However, the processing of encrypted data is still a problem of research. Thus, data in today's cloud systems have to be decrypted to be processed [MaKuL10]. Moreover, authentication of cloud users in numerous systems is solely based upon the verification of credit card data [MaKuL10]. This is the reason for a rising number of attacks from within the cloud [Esso09][Bar09][MeGr09][CASa10].

An unresolved legal issue is the storage of data in a foreign country. Which law is applied in this case? The law from the country the data originates or the law from the country where the data is actually stored? Can the government of the country where the data is stored access the data? Can the customer choose a law? [BIE09]. The availability of cloud systems is not without interruptions, e.g. Amazon's Cloud System had already multiple outages. In Juli 2008 the systems was down for 8 hours [MaKuL10]. Moreover, attacks on the availability of clouds are becoming more frequent, for instance Distributed Denial of Service (DDoS) attacks [Esso09][AFG+09]. Solutions for these problems are topics of ongoing research. Data integrity checks in cloud systems cannot be executed in most cases by cloud users. These have to rely on the services of the cloud vendors [MaKuL10][StRu09]. Further research investigates message-, configuration-, and software integrity of cloud computing systems [StRu09].

3 Privacy regulations on a global scale

Personal data of German companies cannot be stored in a so-called unsecure third country e.g. India or the USA, due to legal reasons. However, there are data protection contracts, for instance the safe harbor agreement for the USA, which enables cooperation with a company in an unsecure third country. However, until today no international agreement on the usage of cloud computing has been devised and each cloud computing endeavour has to be prepared and checked individually [Cav08][BIE09].

Business transactions in a cloud computing system demand a unique assignment of a transaction to a user. Electronic certificates can be used to proof these transactions. However, the verification of the certificates should be provided by an independent third party. Furthermore, there are conflicting goals of accountability and data privacy in a cloud in a cloud computing system [StRu09].

"However, these systems have to consider privacy constraints, which make the job even harder. Information in digital form facilitates the collection and sharing of large amounts of data. The simple approach only to "collect as little information from individuals as possible" [HaScC08] is not practical, due to identity-risk-analysis procedures. For instance, in order to establish that an identity in a financial transaction is not forged or stolen a significant amount of data has to be checked. In the case of fraud detection based upon unusual usage of a credit card e.g. purchases in countries where it was never used before, user profiles are necessary that require lots of data. Moreover, in order to categorize information into security levels in order to determine which data needs more or less protection, the data has to be present [HaScC08].

A number of guidelines for privacy are available, the most widely accepted [HaScC08] are the *Fair Information Practice principles (FIPs)*, which state that a persons informed consent is required for the data that is collected, collection should be limited for the task it is required for and erased as soon as this is not the case anymore. The collector of the data shall keep the data secure and shall be held accountable for any violation of these principles. In the European Union the *EU Data Protection Directive* doesn't permit processing personal data at all, except when a specific legal basis explicitly allows it or when the individuals concerned consented prior to the data processing [HaScC08]. The US has no central data protection law, but separate privacy laws for e.g. the *Gramm-Leach-Bliley Act* financial information, the *Health Insurance Portability and Accountability Act* for medical information, and the *Children's Online Privacy Protection Act* for data related to children [HaScC08].

In the computing world two further major informational privacy concerns are eavesdropping of data and the linking of an individual to a set of data. The eavesdropping issue can be addressed via encryption of data and the linking issue requires different pseudonyms for different contexts. Workflows over different domains should be "delinked", for instance in an online shop the shop itself needs to know the goods that are purchased, the delivery service requires only the shipping address and the payment service requires only the financial information. All of them should use a different pseudonym to prevent user profiling [HaScC08]. Identity management systems that support multilateral security and privacy requirements exist in most cases isolated. The SSONET architectures combine the existing parts [ClKö01]. The BBAE federated identity management protocol offers enhanced security and privacy, due to the absence of single points of control [PfWa03].

The research question how much information is required in what scenario is been addresses as so-called *contextual integrity* and how can this be automated [BDMN]. In addition, ongoing research proposes to "stick" policies by cryptographic means to data, to ensure the data is only used for the purpose the user gave an informed consent [MoPeB03]. Bertino et. al. identified also confidentiality of business relations among various Cloud Services Providers (CSP) as a requirement for cloud computing identity management [BPFS09].

4 Compliance in clouds

The service level of a cloud vendor is defined in so-called *Service Level Agreements (SLAs)*, which often cannot be negotiated. Instead a customer has to accept the SLAs presented by the vendor. Moreover, automatic audit tools to verify the presented SLAs are fulfilled are missing [MaKuL10].

Relevant security standards for cloud computing are the Statement on Auditing Standards (SAS) Number 70 Type II and the ISO certificate 27001. SAS 70 II confirms a cloud vendor from an external party that monitoring activities for IT technologies and processes are present and documented. The ISO certification demands a management concept for IT security, which e.g. evaluates security measures in Plan-Do-Check-Act cycles on a permanent bases [MaKuL10]. One result of an SAS 70 II certification is a security report, which is filed under the individual standards of the evaluated organisation. It is not a certificate with a predefined set of terms [StRu09]. A further type of compliance in the cloud area are so-called Trust Audit Frameworks, e.g. SysTrust or WebTrust. These frameworks focus on internal controls in a company based upon financial systems. These systems were developed for ecommerce applications [StRu09].

Cloud computing offers elasticity, services can be added or deleted on demand by a customer. Thus, any part of the cloud computing system has to support this scalability. In Fig.1 we present several areas of Governance, Risk and Compliance that has to be modified or even reinvented to achieve a viability for cloud computing. In Governances policies have to be written that accommodate the permanent change of a system. Today's policies are written for comparable stable systems and are tightly focused on them. This will not suffice for a cloud computing system, because of the elasticity.

Furthermore, a detailed classification of data is required. Data in a closed company network needs to be protected and the responsible personal in a company has full control of the infrastructure. In a cloud computing scenario data will be given to a cloud provider and the customer has to trust on the security capabilities of the vendor. Thus, for instance highly sensible data or processes that are vital for a company should not enter the cloud. Moreover, multiple customers or even cloud vendors might be involved in a business process that involves cloud usage. In these cases the trust of each partner has to be taken into account of security considerations.

Risk management requires a strategy that includes every possibility of security failures with a cloud computing integration. This becomes increasingly difficult due to the almost infinitive number of possible scenarios, because of the change of the companies structure when cloud computing is used in a part of it. In addition, possible impacts of cloud computing on the effectiveness and efficiency of business processes of a company has to be evaluated on a similar scale. Numerous new threats and vulnerabilities of cloud computing have to be analysed and the risk analysis itself for each cloud scenario has to be verified continuously.

Compliance also becomes more difficult, due to the fact that companies rely on cloud vendors for security policy enforcement, the adherence to regulations e.g. SOX or Solvency II. Furthermore, companies have to find ways to gain control of specific scenarios. For instance, in case highly classified data made it into the cloud by accident an emergency procedure should exist that erases the data completely from the clouds systems.

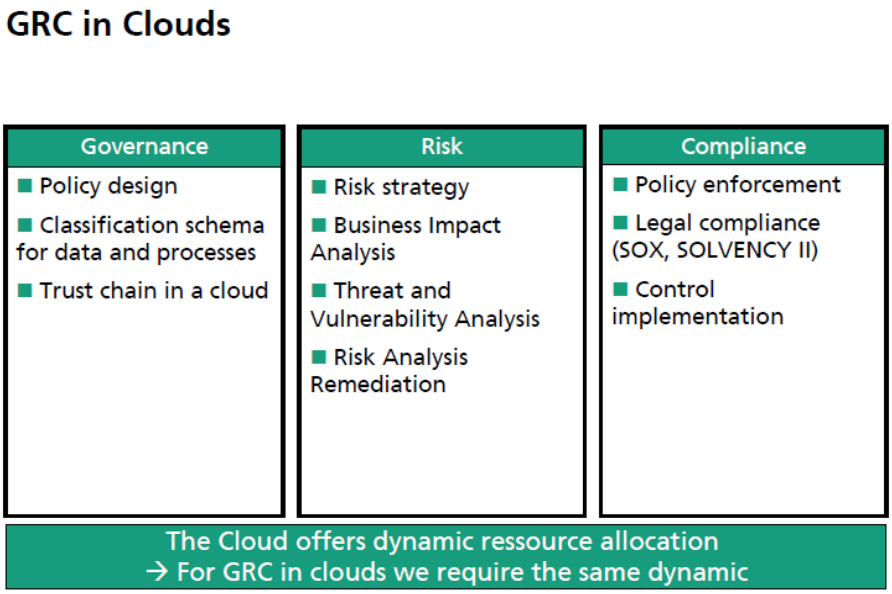

Fig. 1: Governance, Risk and Control (GRC) in cloud computing systems

In Fig. 2 we are presenting examples for GRC related standards that can help to evaluate a cloud computing scenario. However, there are almost no specific standards for cloud computing. On an economic level the integration of cloud and company has to result in effective and efficient business processes. This can be verified, for instance with the ISO 9001, the Gartner BPM Maturity Model, and the EDEN Maturity Model for Business Processes. Cobit and Coso offer models for documenting, analysing and creating internal control systems. Relevant security standards are the BSI Grundschutzhandbuch and the Common Criteria. A topic specifically relevant for cloud computing is transparency. In many cases customers of cloud computing offers have to trust the vendor that the GRC demands are met. However, several standards evaluate the capabilities of the cloud system, like ISO 27001, SAS 70 Type II, and Truste. Further agreements for instance safe harbor ensure that certain privacy demands are met.

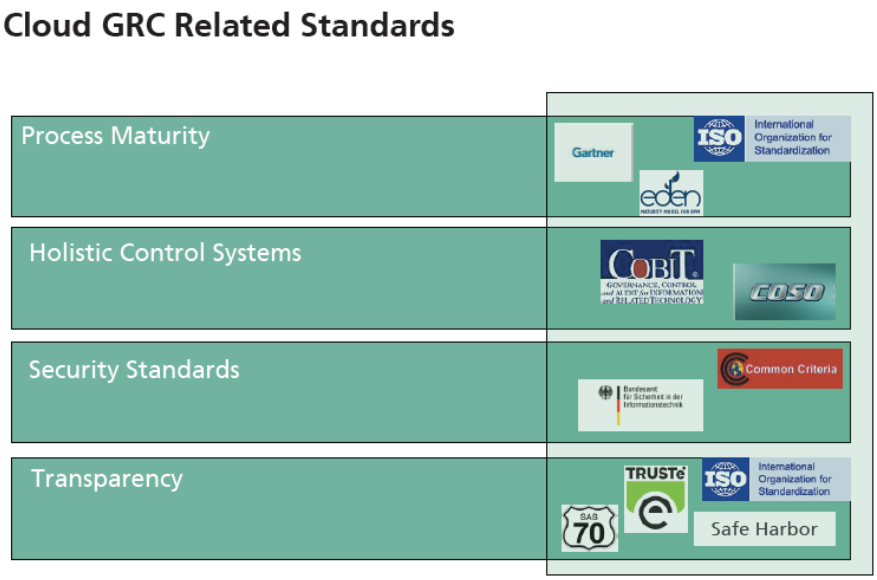

Fig 2: Cloud GRC related standards

5 Applying the APEX approach to Cloud Computing Systems

The Fraunhofer-Attract project Architectures for Auditable Business Process Execution (APEX) develops a software tool for the insurance domain that eases the effort of implementing the increasing number of compliance frameworks, laws and regulations in the insurance domain (in particular Solvency II) into their processes and into the IT landscape. Numerous requirements arise from these compliance regulations. This poses demands at the software that is developed for and used in the insurance domain in two ways: One the one hand, the Software must be developed in a way that allows the software vendors to make a convincing argument that it is sufficiently reliable to support the sophisticated requirements derived from the compliance regulations (such as security requirements), which today often is not the case. On the other hand, it creates a demand for special purpose software whose function it is to monitor and enforce compliance of the company's business processes while they are executed over the IT infrastructure. Developing these kinds of systems efficiently while meeting compliance demands with minimal cost overhead is a goal which reveals a severe gap in current software engineering methods and tools. Current approaches and technologies neither support

the seamless analysis and management of compliance risks and requirements during the software life-cycle nor their systematic enforcement in the context of service-oriented architectures.

We are currently investigating how to adapt the APEX approach for an application to cloud computing systems. In the following we present an approach for improving cloud security based upon the APEX work. Enterprise cloud software platforms also have to deal with inherent compliance problems. On the one hand, customers should be able to check if their security requirements are met with a specific cloud computing offer. On the other hand, customers require the ability to verify that the cloud offer satisfies legal compliance regulations. Compliance monitoring software is required as well in clouds, together with an approach to machine-interpretable and enforceable policies that map to the business level extend the pursued approach towards the achievement of compliance in the presence of dynamically created adaptive business processes and value chains in open service architectures. These challenges demand an extension of the APEX method to take the elasticity of cloud computing into account.

A compliance repository is designed in the APEX project to be functionality directly in line with customer demands and current development efforts. For the area of compliance management in legal and security requirements, there is no ready-to-use solution on the market today. State-of-the-art is to express these as additional requirements in Word or RE-tools with very poor semantics and traceability or assurance mechanisms. We are currently investigating how to adapt the APEX approach for an application to cloud computing systems. Even though the elasticity in the clouds demands a more frequent compliance checks, the rules, laws and regulations do change rarely. Moreover it will still take some time before regulations and laws appear in significant numbers,

We are currently investigating how to adapt the APEX approach for an application to cloud computing systems.

We aim to close the semantic gap between business processes and security/legal requirements. A repository maps these requirements to specific tasks within a business process in order to simplify the implementation and maintenance of compliance checks. The repository will provide an ontology that leads for instance from the security requirement confidentiality to the specific encryption functions in a business process. In addition, we provide methods and tools for model-driven development and adaptation of compliant service-oriented enterprise systems the eclipse modelling framework will be extended to support input from different business process modelling tools. Furthermore, proven model checking software will be integrated into the framework to execute the actual compliance checks.

Moreover, we enable compliance monitoring workflow engines to support compliance monitoring and reporting of the business process execution. Moreover, we aim to integrate all project results into a compliance-engineering framework for developers, business analysts and auditors.

A tool support offers the required scalability of security analysis in a cloud computing in a cost effective manor. Human security experts will no doubt still be required, however numerous analyses can be executed when e.g. the cloud system scales and provide information for security specialists. This approaches the cloud security and compliance problem on a holistic level from compliance regulations and business process to the technical level of soft- and hardware. This tool will present the technical realization of a semantic repository (to be linked to the processes and ontologies of a given company) that will allow reference to com-

pliance demands at different levels of abstraction as well as integration of compliance artefacts in a traceable fashion.

Furthermore a business process modelling language that spans all development stages and technical layers for enterprise cloud business applications. It integrates compliance-relevant artifacts and related security/legal properties as a requisite part of the language. It can be used to specify which data is needed, which process steps need to be executed, and which constraints have to be satisfied within a given business process. A set of model transformations from business process models to model checking tools for the automatic compliance checks derived from security policies and legal resolutions to enforce these policies at all layers of the application. These solutions include Role-based Access Control, separation of duty, rights delegation, network, and middleware layer protection, legal aspects of SOX, Basel II and Solvency II. This leads to a business process modelling framework specific for the cloud environment that is tightly integrated into the Eclipse tool platform. This allows the combination of existing Eclipse solutions for development, debugging, versioning, validation etc. with the modelling tool. Our framework will allow the differing stakeholders in the cloud usage process, who do not (and simply can not) possess all the required compliance, security and risk expertise, to verify quickly the requirements, as well as design, develop, test, deploy and audit the cloud software integration of the business software solutions that fully take compliance-driven aspects into account. The needs of the different stakeholders that will later adopt the Secure-Clouds approach are an important factor for its success. As basic roles interacting with the Secure-Clouds methods and tools we identified the following actors: The auditor is in charge of checking the system with regard to the fulfilment of compliance requirements. The auditor requires aggregated information on business level. He/she will use the compliance repository. The business analyst is an expert of the business domain with a focus on analysing security risks and compliance constraints at business level. He/she will use the Secure-Clouds compliance repository, as well as the Secure-Clouds modelling language. The deployer develops the services configurations in the runtime environment. The deployer works at the levels of the Technical Architecture and Code and Runtime Environment and uses Secure-Clouds techniques of model-driven software development. The test engineer is responsible for developing, executing and analysing system tests. In the process the test engineer focuses on security and compliance aspects and uses model-based techniques for test specification and execution. He/she uses the Secure-Clouds modelling language and model-driven development tools. Our research will provide assurance for the compliance of the currently almost exponentially increasing amount of cloud business operations is expected to become unmanageable. Our work ensures security and legal compliance by design and will allow its users to quickly assess, evaluate and trace the necessary requirements when integrating, deploying and maintaining cloud business operations.

Our research profits from previous work in the field of secure software engineering. There has been a significant amount of work towards Model-based Security Engineering: [Jur02,Jur05] presents a verification framework for UML models enriched with security properties through a UML profile called UMLsec. Supporting tools perform automated analysis on the UMLsec models for security and compliance properties [HöJü08]. Also relevant are approaches for Model-Driven Security for Role-Based Access Control such as [LoBaD02] or the SECTET-Framework presented in [HaAlB06].

There is virtually no work towards engineering enterprise cloud software platforms given a set of compliance regulations. Also relevant are standardization efforts such as the OMG's Regulatory Compliance Alliance. Furthermore the Cloud Security Alliance has done significant work in identifying security threats in enterprise cloud environments [CSA10]. We will

also investigate methods for assessing the effectiveness of security investments in the cloud computing context using ideas such as presented in [HGF+05].

6 Conclusion

Today the security and compliance of cloud computing systems is evaluated on different levels of granularity. For instance the BSI showed possible attacks on a detailed level [Esso09], while the Cloud Security Alliance focused on more general attacks [Cav08]. A detailed analysis of the topic is presented in [MaKuL10] and [StRu09], which both describe the possibility to increase security technique due to improved compliance. Documentation, monitoring and control of security measures are vital sales arguments for cloud computing offers. Moreover, a research initiative already exists for automated audits of cloud systems [CAA10]. Specific concepts for identity management and data privacy in cloud computing are topics of ongoing research [Cav08] [BPSF09].

Another fundamental approach to the security issues is the transparency of security. Customers have to accept clouds as a black box solution, which they have to trust. Security certification and automated audits are technical possibilities and increase the trust of customers. This is an important possibility for distinction in the cloud market.

Several cloud security approaches focus on possible attacks. However, there is virtually no work towards engineering enterprise cloud software platforms given a set of compliance regulations. Our research aims to fill this gap.

References

[AFG+09] Armbrust, M.; Fox, A.; Griffith, R.; Joseph, A.D.; Katz, R.H.; Konwinski, A.; Lee, G.; Patterson, D.A.; Rabkin, Ariel; Stoica, Ion; Zaharia, M.: Above the Clouds: A Berkeley View of Cloud Computing, technical report, UCB/EECS-2009-28, EECS Department University of California, Berkeley, 2009

[Bar09] Bartsch, M.: Cloud Security, TüV Informationstechnik GmbH, Unternehmensgruppe TÜV NORD, Präsentation, 2009

[BeBaS08] Beres, Y.; Baldwin, A.; Shiu, S.: Model-Based Assurance of Security Controls, technical report HPL-2008, HP Labs Bristol, 2008.

[BDMN] Barth, A.; Datta, A.; Mitchell, J. C.; Nissenbaum, H.: Privacy and Contextual Integrity: Framework and Applications SP '06: Proceedings of the 2006 IEEE Symposium on Security and Privacy, IEEE Computer Society, 2006, 184-198

[BPFS09] Bertino, E.; Paci, F.; Ferrini, R.; Shang, N.: Privacy-preserving Digital Identity Management for Cloud Computing. IEEE Data Eng. Bull., 2009, 32, 21-27

[BIE09] Bierekoven, C.; Rödl & Partner: Die Herausforderung für die Daten- und Rechtssicherheit, GI Workshop „Cloud-Computing“, 2009

[BPSF09] Bertino, E.; Paci, F.; Shang, N.; Ferrini, R.: Privacy-preserving Digital Identity Management for Cloud Computing, IEEE Data Eng, Bull, 32(1), 21--27, 2009

[CAA10] The Cloud Audit A6, http://www.cloudaudit.org/page3/page3.html, 2010

[CSA10] The Cloud Security Alliance: Security Guidance for Critical Areas of Focus in Cloud Computing, homepage,http://www.cloudsecurityalliance.org/, 2010

[CASa10] The Cloud Security Alliance: Top Threats to Cloud Computing, homepage,http://www.cloudsecurityalliance.org/, 2010

[Cav08] Cavoukian, A.: Privacy in the clouds, Identity Journal Limited, Springer, 2008

[ClKö01] Clauss, S.; Köhntopp, M.: Identity management and its support of multilateral security Comp. Netw., Elsevier North-Holland, Inc., 2001, 37, 205-219

[Esso09] Essoh, A.D.: IT-Grundschutz und Cloud Computing, SECMGT Workshop, BSI, 2009

[HaAlB06] Hafner, M., Alam, M. & Breu, R. (2006) Towards a MOF/QVT-based Domain Architecture for Model Driven Security. Proceedings of the 9th International Conference on Model Driven Engineering Languages and Systems (Models 2006). Geneva, Italy.

[HaScC08] Hansen, M.; Schwartz, A.; Cooper, A.: Privacy and Identity Management IEEE Security and Privacy, IEEE Educational Activities Department, 2008, 6, 38-45

[HGF+05] Houmb,S.H.; Georg, G.; France, R.; Bieman, J.; Jürjens, J.: Cost-Benefit Trade-Off Analysis using BBN for Aspect-Oriented Risk-Driven Development, ICECCS 2005, IEEE Computer Society, pp 195-204

[HöJü08] Höhn, S.; Jürjens, J.: Rubacon: automated support for model-based compliance engineering, 30th International Conference on Software Engineering (ICSE 2008), ACM 2008, pp. 875-878

[IDC09] IDC-Study: Cloud Computing in Deutschland ist noch nicht angekommen http://www.idc.com/germany/press/presse_cloudcomp.jsp, 2009

[JaSc10] Jaeger, T.; Schiffman, J.: Outlook: Cloudy with a Chance of Security Challenges and Improvements IEEE Security and Privacy, IEEE Computer Society, 2010, 8, 77-80

[Jur02] Jürjens, J.: Principles for Secure Systems Design, PhD thesis, 2002, Oxford University

[Jur05] Jürjens, J., Secure Systems Development with UML, Springer Academic Publishers, 2005.

[LoBaD02] Lodderstedt, T., Basin, D.; Doser, J.: SecureUML: A UML-Based Modeling Language for Model-Driven Security. IN JÉZÉQUEL, J.-M., HUSSMANN, H. & COOK, S. (Eds.) 5th International Conference on the Unified Modeling Language. Springer, 2002

[MaKuL10] Mather, T.; Kumaraswamy, S.; Latif, S.: Cloud Security and Privacy, O'Reilly, 2009

[MeGr09] Mell, P.: Grance, T.: Effectively and Securely Using the Cloud Computing Paradigm, NIST, Presentation, 2009

[MoPeB03] Mont, M. C.; Pearson, S.; Bramhall, P.: Towards Accountable Management of Identity and Privacy: Sticky Policies and Enforceable Tracing Services DEXA '03: Proceedings of the 14th International Workshop on Database and Expert Systems Applications, IEEE Computer Society, 2003, 377

[PfWa03] Pfitzmann, B. & Waidner, M.: Federated Identity-Management Protocols - Where User Authentication Protocols May Go-

In 11th Cambridge International Workshop on Security Protocols, Springer-Verlag, 2003, 153-174

[StRu09] Streitberger, W.; Ruppel, A.: Cloud Computing Sicherheit – Schutzziele.Taxonomie.Marktübersicht, Fraunhofer Institute for Secure Information Technology SIT, 2009

Index

Security, compliance. Cloud computing, Governance Risk and Control (GRC), automated security analysis