

# Trustworthy Clouds Underpinning the Future Internet

Rüdiger Glott<sup>1</sup>, Elmar Husmann<sup>2</sup>, Ahmad-Reza Sadeghi<sup>3</sup>, and Matthias Schunter<sup>2</sup>

<sup>1</sup> Maastricht University, The Netherlands

`glott.ruediger@gmail.com`

<sup>2</sup> IBM Research – Zürich, Rüschlikon, Switzerland

`huselmar@de.ibm.com, mts@zurich.ibm.com`

<sup>3</sup> TU Darmstadt, Germany

`ahmad.sadeghi@trust.rub.de`

**Abstract.** Cloud computing is a new service delivery paradigm that aims to provide standardized services with self-service, pay-per-use, and seemingly unlimited scalability. This paradigm can be implemented on multiple service levels (infrastructures, run-time platform, or actual Software as a Service). They are expected to be an important component in the future Internet.

This article introduces upcoming security challenges for cloud services such as multi-tenancy, transparency and establishing trust into correct operation, and security interoperability. For each of these challenges, we introduce existing concepts to mitigate these risks and survey related research in these areas.

## 1 Cloud Computing and the Future Internet

Cloud computing is expected to become a backbone technology of the Future Internet that provides Internet-scale and service-oriented access to virtualized computing, data storage and network resources as well as higher level services. In contrast to the current cloud market that is mainly characterized by isolated providers, cloud computing in the Future Internet is expected to be characterized by a seamless cloud capacity federation of independent providers - similar to the network peering and IP transit purchasing of ISPs in today's Internet. For an end-user this means that via interacting with one cloud provider, resources and services provided by multiple similar providers are seamlessly accessed. Cloud computing goes beyond technological infrastructure that derives from the convergence of computer server power, storage and network bandwidth. It is a new business and distribution model for computing that establishes a new relationship between the end user and the data center, which "... gives the user 'programmatic control' over a part of the data center" [1, pp. 8-9].

For this cloud-of-clouds vision<sup>4</sup> this article will investigate the related challenges for trust and security architectures and mechanisms.

---

<sup>4</sup> For which the Internet pioneer Vint Cerf has recently suggested the term "Intercloud"

FIA projects like RESERVOIR or VISION are conducting research on core technological foundations of the cloud-of-clouds such as federation technologies, interoperability standards or placement policies for virtual images or data across providers. Many of these developments can be expected to be transferred into the Future Internet Core Platform project that will launch in 2011. This goes along with increased collaboration on open cloud standards under developments by groups such as the DMTF Open Clouds Standards Incubator, the SNIA Cloud Storage Technical Working Group or the OGF Open Clouds Computing Interface Working Group.

Trust and security are often regarded as an afterthought in this context, but they may ultimately present major inhibitors for the cloud-of-clouds vision. An important property of this emerging infrastructure will be the need to respect global legal requirements. Today, since the current legal systems are not prepared for the challenges that result from the complexity and pervasiveness of cloud computing, data protection and privacy issues as well as liability and compliance problems may hinder to tap the full potential of cloud computing [22,8,26]. By clouds becoming regulation-aware, in the sense that it will ensure that data mobility is limited to ensure compliance with a wide range of different national legislation including privacy legislation such as the EU Data Protection Directive 95/46/EC.

As of today, cloud computing is facing significant acceptance hurdles when it comes to hosting important business applications or critical infrastructures such as those of the usage domains addressed by FIA. This article will illustrate the reasons for this, and discuss the complex trust and security requirements. Furthermore, we survey existing components to overcome these security and privacy risks. We will explain the state-of-the-art in addressing these requirements and give an overview of related ongoing international, and particularly EU research activities as well as derive future directions of technology development.

## 2 Trust and Security Limitations of Global Cloud Infrastructures

### 2.1 Cloud Security Offerings Today

According to the analyst enterprise Forrester Research and their study “Security and the Cloud” [17] the cloud security market is expected to grow to 1.5 billion \$ by 2015 and to approach 5 % of overall IT security spending. Whereas today identity management and encryption solutions represent the largest share of this market, particular growth can be expected in three directions:

1. securing commercial clouds to meet the requirements of specific market segments
2. bespoke highly secure private clouds
3. a new range of providers offering cloud security services to add external security to public clouds

An example for the first category is the Google gov.app cloud launched in September 2009 that offers a completely segregated cloud targeted exclusively at US government customers. Similarly, IBM has launched a FISMA compliant Federal Community Cloud in 2010.

Other cloud providers also adapt basic service security to the needs of specific markets and communities. Following its software-plus-services strategy announced in 2007, Microsoft has developed in the past years several SaaS cloud services such as the Business Productivity Online Suite (BPOS). While all of them may be delivered from a multi-tenant public cloud for the entry level user, Microsoft offers dedicated private cloud hosting and supports third-party or customer-site hosting. This allows tailor made solutions to specific security concerns - in particular in view of the needs of larger customers. In the same way, the base security of Microsoft public cloud services is adapted to the targeted market. Whereas Microsoft uses, e.g., for the Office Live Workspace - in analogy to what Google does with Gmail - unencrypted data transfer between the cloud and the user, cloud services for more sensitive markets (such as Microsoft Health Vault) use SSL encryption by default.

On the other hand commodity public cloud services such as the Amazon EC2 are still growing even though they offer only limited base security and largely transfer responsibility for security to the customer. Therefore in parallel to the differentiated security offerings via bespoke private or community clouds, there is also a growing complementary service market to enable enhanced security for public clouds. Here a prime target is the small to mid-size enterprise market. Examples for supplementary services are threat surveillance (e.g., AlertLogic), access- and identity management (e.g., Novell, IBM), virtual private networking (e.g., Amazon Virtual Private Cloud), encryption (e.g., Amazon managed encryption services) and web traffic filtering services (e.g., Zscaler, ScanSafe).

## 2.2 Today's Datacenters as the Benchmark for the Cloud

Using technology always constitutes a certain risk. If the IT of any given business failed, the consequences for most of today's enterprises would be severe. Even if multiple lines of defense are used (e.g., firewalls, intrusion defense, and protection of each host), all systems usually contain errors that can be found and exploited. While off-line systems are harder to attack, exchanging media such as USB sticks allows transfer into systems that are not connected to the Internet [5].

Cloudsourcing [15] follows more or less the same economic rationale as traditional IT-outsourcing but provides more benefits, inter alia with regard to upgrades and patches, quick procurement services, avoidance of vendor lock-ins, and legacy modernization [18]. Many cloudsourcers offer bundles of consulting services, application development, migration, and management [14]. A problem that remains with this new stage of IT-outsourcing strategies is that the client still has to find trustworthy service providers. However, this problem has been solved in earlier forms of IT outsourcing, therefore it is not very likely that the emergence of new business opportunities and business models will fail on this

point. Rather than that, cloud computing might be significantly hindered by the legal problems that remain to be solved.

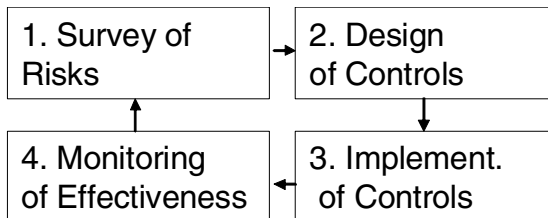
For the security objectives when adopting clouds for hosting critical systems we believe that today's datacenters are the benchmark for new cloud deployments. Overall, the benefits need to outweigh the potential disadvantages and risks. While the cost and flexibility benefits of using clouds are easy to quantify, potential disadvantages and risks are harder to qualitatively assess or even quantitatively measure. An important aspect for this equation is the perceived level of uncertainty: For instance, a low but contractually guaranteed availability (such as 98% availability) will allow enterprises to pick workloads that do not require higher guarantees. Today, uncertainty about the actual availability does not allow enterprises to make such risk-management decisions and thus will only allow hosting of uncritical workloads on the cloud.

For security this argument leads to two requirements for cloud adoption by enterprises: The first is that with respect to security and trust, new solutions such as the cloud or cloud-of-clouds will be compared and benchmarked against existing solutions such as enterprise or outsourced datacenters. The second is that in order to allow migration of critical workloads to the cloud, cloud providers must enable enterprises to integrate cloud infrastructures into their overall risk management. We will use these requirements in our subsequent arguments.

### 3 New Security and Privacy Risks and Emerging Security Controls

Cloud computing being a novel technology introduces new security risks [7] that need to be mitigated. As a consequence, cautious monitoring and management of security risks [13] is essential (see Figure 1 for a sketch following [12]).

We now survey selected security and privacy risks where importance has been increased by the cloud and identify potential security controls for mitigating those risks.



**Fig. 1.** Simplified Process for Managing Security Risks [12])

### 3.1 Isolation Breach between Multiple Customers

Cloud environments aim at efficiencies of scale by increased sharing resources between multiple customers. As a consequence, data leakage and service disruptions gain importance and may propagate through such shared resources. An important requirement is that data cannot leak between customers and that malfunction or misbehavior by one customer must not lead to violations of the service-level agreement of other customers.

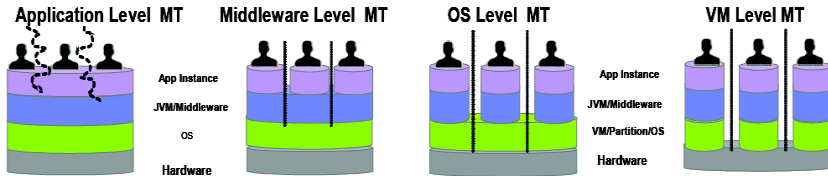


Fig. 2. Multi-tenancy at Multiple Levels [25].

Traditional enterprise outsourcing ensures the so-called “multi-tenant isolation” through dedicated infrastructure for each individual customer and data wiping before re-use. Sharing of resources and multi-tenant isolation can be implemented on different levels of abstraction (see Figure 2). Coarse-grained mechanisms such as shared datacenters, hosts, and networks are well-understood and technologies such as virtual machines, vLANs, or SANs provide isolation. Sharing resources such as operating systems, middleware, or actual software requires a case-by-case design of isolation mechanisms. In particular the last example of Software-as-a-Service requires that each data instance is assigned to a customer and that these instances cannot be accessed by other customers. Note that in practice, these mechanisms are often mixed: While an enterprise customer may own a virtual machine (Machine-level isolation), this machine may use a database server (Middleware isolation) and provide services to multiple individual departments (Application isolation).

In order to mitigate this risk in a cloud computing environment, multi-tenant isolation ensures customer isolation. A principle to structure isolation management is One way to implement such isolation is labeling and flow control:

*Labeling:* By default all resources are assigned to a customer and labeled with a corresponding label.

*Flow control:* Shared resources must moderate potential data flow and ensure that no unauthorized data flow occurs between customers. To limit flow control, mechanisms such as access control that ensures that machines and applications of one customer cannot access data or resources from other customers can be used.

Actual systems then need to implement this principle for all shared resources [4] (see, e.g., [2,3] for network isolation). An important challenge in practice is to identify and moderate all undesired information flows [19].

### 3.2 Insider Attacks by Cloud Administrators

A second important security risk is the accidental or malicious misbehavior of insiders that increased due to global operations and a focus on low cost. Examples may include a network administrator impacting database operations or administrators stealing and disclosing data. This risk is hard to mitigate since security controls need to strike a balance between the power needed to administrate and the security of the administrated systems.

A practical approach to minimize this risk is to adhere to a least-privilege approach for designing cloud management systems. This means that cloud management systems should provide a fine-grained role hierarchy with clearly defined separation of duty constraints. The goal is to ensure that each administrator only holds minimized privileges to perform the job at hand. While today, operators often have god-like privileges, by implementing a least privilege approach, the following objectives can be met:

- Infrastructure administrators can modify their infrastructure (network, disks, and machines) but can no longer access the stored or transported data.
- Security administrators can design and define policies but cannot play any other roles.
- Customer employees can access their respective data and systems (or parts thereof) but cannot access infrastructure or data owned by different customers.

This so-called privileged identity management system is starting to be implemented today and should be mandated for cloud deployments. In today's outsourced datacenters where management tasks are often off-shored, it ensures that the negative impact of remote administrators is limited and that their actions are closely monitored. Such privileged identity management systems usually follow an approach using the following steps:

1. Initially, roles are defined that define the maximum privileges obtained by individual administrators holding these roles. For instance, a database administrator may only obtain administrative privileges over the tables owned by its employer.
2. For a given task at hand, an administrator "checks out" the required privileges while documenting the task. For instance., a database administrator asks for privileges to modify a given database schema.
3. The administrator performs the desired task.
4. The administrator returns the privileges.

Due to the corresponding logging, the security auditors can later determine which employee has held what privileges at any given point in time. Furthermore, for each privilege, the system documents for what task these privileges were requested.

In the long run, these practical approaches may be complemented with stronger protection by, e.g., trusted computing [21] or computations on outsourced data [20].

### 3.3 Failures of the Cloud Management Systems

Due to the highly automated nature of the cloud management systems and the high complexity of the managed systems, software quality plays an important role in avoiding disruptions and service outages: Clouds gain efficiency by industrializing the production of IT services through complete end-to-end automation. This means that once errors occur in such complex and automated systems, manual intervention for detecting and fixing faults may lead to even more errors. It is furthermore likely that due to the global scale, errors will be replicated globally and thus can only be fixed through automation.

Another source of failure stems from the fact that large-scale computing clouds are often built using low-cost commodity hardware that fails (relatively) often. This leads to frequent failures of machines that may also include a subset of the management infrastructure.

The consequence of these facts is that automated fault tolerance, problem-determination, and (self-)repair mechanisms will be commonly needed in the cloud environment or recover from software and hardware failures.

For building such resilient systems, important tools are data replication, atomic updates of replicated management data, and integrity checking of all data received (see, e.g., [24]). In the longer run, usage of multiple clouds may further improve resiliency (e.g., as pursued by the TClouds project [www.tclouds-project.eu](http://www.tclouds-project.eu) or proposed in [11]).

### 3.4 Lack of Transparency and Guarantees

While the proposed mechanisms to mitigate the identified risks are important, security incidents are largely invisible to a customer: Data corruption may not be detected for a long time. Data leakage by skilled insiders is unlikely to be detected. Furthermore, the operational state and potential problems are usually not communicated to the customer except after an outage has occurred.

An important requirement in a cloud setting is to move away from today's "black-box" approach to cloud computing where customers cannot obtain insight on or evidence of correct cloud operations. A related challenge is how to best foster trust of customers into correct operation of the cloud infrastructure. While partial solutions exist as outlined below, there exists no well-accepted best practice.

The existing approaches range from superficial to academic. The prevailing approach is the so-called best effort approach where operators promise "to do their best" but do not give any guarantees. This is common for free services today. An improvement to this approach is third-party audits. This approach is common to today's outsourcing: (Cloud) service centers are validated by an independent organization to satisfy well-defined standards such as ISO27001 or SAS70. Customers can then be sure that the organization followed these standards at the time of certification. This approach is common best practice today but still only ensures compliance at a point of time and due to its spot-check approach may miss areas of non-compliance that by accident were not checked.

In the mid-term, it is important that cloud provider provide automated interfaces for observation and incident handling [10]. This will allow customers to automatically identify incidents and to analyze and react to such incidents.

In the long run, the ideal transparency mechanisms would *guarantee* that processes are implemented such that the agreed upon procedures are followed, the functional and non-functional requirements are met, and no data is corrupted or leaked. In practice, these problems are largely unsolved. Cryptographers have designed schemes such as homomorphic encryption [9] that allow verifiable computation on encrypted data. However, the proposed schemes are too inefficient and do not meet the complete range of privacy requirements [23]. A more practical solution is to use Trusted Computing to verify correct policy enforcement [6]. Trusted computing instantiation as proposed by the Trusted Computing Group (TCG) uses secure hardware to allow a stakeholder to perform attestation, i.e., to obtain proof of the executables and configuration that were loaded at boot-time . However, run-time attestation solution still remains an open and challenging problem.

### 3.5 What about Privacy Risks?

To enable trusted cloud computing, privacy protection is an essential requirement [26]. In simple terms, data privacy aims at protecting personally identifiable data (PID). In Europe, Article 8 of the European Convention on Human Rights (ECHR) provides a right to respect for ones “private and family life, his home and his correspondence”. The European Court of Human Rights states in several decisions that this article also safeguards the protection of an individual’s PID. Furthermore, the European Data Protection Directive (Directive 95/46/EC) substantiates this right in order to establish a comprehensive data protection system throughout Europe. This directive takes into account the OECD privacy principles [16] which mandate several principles such as, e.g., limited collection of data, the authorization to collect data either by law or by informed consent of the individual whose data are processed (“data subject”), the right to correction and deletion as well as the necessity of reasonable security safeguards for the collected data.

Since cloud computing often means outsourcing data processing, the user as well as the data subject might face risks of data loss, corruption or wiretapping due to the transfer to an external cloud provider. Related to these de-facto obstructions in regard to the legal requirements, there are three particular challenges that need to be addressed by all cloud solutions: Transparency, technical and organizational security safeguards and contractual commitments (e.g., Service Level Agreements, Binding Corporate Rules).

According to European law, the user who processes PID in the cloud or elsewhere remains responsible for the compliance with the aforementioned principles of data privacy. Outsourcing data processing does not absolve the user from his responsibilities and liabilities concerning the data. This means that the user must be able to control and comprehend what happens to the data in the cloud and which security measures are deployed. Therefore, the utmost transparency



regarding the processes within the cloud is required to enable the user to carry out his legal obligations. This might be technically realized by, e.g., installing informative event and access logs which enable the user to retrace in detail what happens to his data, where they are stored and who accesses them. Also, the cloud service provider could prove to have an appropriate level of security measurements by undergoing acknowledged auditing and certification processes on a regular basis. Legally, the compliance of the cloud service providers with the European law may be ensured by a commitment to Binding Corporate Rules (BCR). Another method is the implementation of Service Level Agreements (SLAs) into the contracts, which guarantee the adherence to the spelled out privacy requirements. These SLAs could, for example, stipulate an enforcement of privacy via contractual penalties in case of the breach of the agreement.

This applies all the more in cases of cross-border cloud computing with various subcontracting cloud service providers. Subcontracts are already commonly practiced in the cloud computing field. Cloud services commonly rely on each other, since their structures may be consecutively based upon each other. Hence, a computing cloud may use the services of a storage cloud. Unlike local data centers residing in a single country, such cloud infrastructures often extend over multiple legislation and countries. Therefore, the question of applicable law and safeguarding the user's responsibilities regarding data privacy in cross-border cloud scenarios is a matter of consequences for the use of these cloud services. So to avoid unwanted disclosure of data, sufficient protection mechanisms need to be established. These may also extend to the level of technical solutions, such as encryption, data minimization or enforcement of processing according to predefined policies.

## 4 Open Research Challenges

Today's technology for outsourcing and large-scale systems management laid the foundation for cloud computing. Nevertheless, due to its global scale and the need for full automation, there are still open research challenges that need to be resolved in order to enable hosting of enterprise-class and critical systems on a cloud.

*Customer Isolation and Information Flow.* For customer isolation, specific challenges are how to reliably manage isolation across various abstraction layers. A single notion of customers needs to be implemented across different systems. Furthermore, data generated by systems need to be assigned to one or more customers to enable access to critical data such as logs and monitoring data. A particularly hard challenge will be to reduce the amount of covert and side channels. Today, such channels are often frozen in hardware and thus cannot easily be reduced.

*Insider Attacks.* The second area of research are practical and cost-efficient schemes to mitigate the risk of insider fraud. The goal is to minimize the set of trusted employees for each customer through implementing a rigorous least privilege approach as well as corresponding controls to validate employee behavior. Furthermore, a practical scheme needs to support overseas management to reduce cost while still enabling compliance with privacy and other regulations.

*Security Integration and Transparency.* The third challenge is to allow customers to continue operating a secure environment. This means that security infrastructure and systems within the cloud such as intrusion detection, event handling and logging, virus scans, and access control need to be integrated into an overall security landscape for each individual customers. Depending on the type of systems, this can be achieved by providing more transparency (e.g., visibility of log-files) but may also require security technology within the cloud. One example is intrusion detection: In order to allow customers to 'see' intrusions on the network within the cloud and correlate these intrusions with patterns in the corporate network, the cloud provider either needs to allow the customer to run intrusion detection systems within the cloud (which would raise privacy issues) or else provide generic intrusion detection capabilities that each customer can configure.

*Multi-Compliance Clouds.* The fourth challenge is how to build clouds that are able to comply with multiple regulations at the same time. One example is the health care sector: A health care cloud would need to satisfy various national or regional privacy and health care regulations. Since manual implementation for each customer will not be cost efficient, an automated way to enforce different (hopefully non-conflicting) regulations would be needed.

One particular challenges in this are is to make regulations and the cloud compatible. Today, regulations often mandate that data needs to be processed in a particular country. This does not align well with today's cloud architectures and will result in higher cost. An alternative could be to define required protections and then leave it to the cloud provider to find a certifiable way to provide sufficient protection.

*Federation and Secure Composition* The final area of research that we see is cloud federation and secure composition: In order to further reduce the dependency on an individual cloud, services will be obtained from and load balanced over multiple clouds. If this is done properly, services will no longer depend on the availability of any individual cloud.

From a security perspective, this will raise new challenges. Customers need to provide a consistent security state over multiple clouds and provide means to securely fail-over across multiple clouds. Similarly, services will be composed from underlying services from other clouds. Without an accepted way to compose services securely, such compositions would require validation of each individual service based on fixed sub-services.

## 5 Outlook — The Path Ahead

Cloud computing is not new – it constitutes a new outsourcing delivery model that aims to be closer to the vision of true utility computing. As such, it can rely on security and privacy mechanisms that were developed for service-oriented architectures and outsourcing. Unlike outsourcing, clouds are deployed on a global scale where many customers share one cloud and multiple clouds are networked and layered on top of each other. We surveyed security risks that gain importance in this setting and surveyed potential solutions.

Today, demand for cloud security has increased but the offered security is still limited. We expect this to change and clouds with stronger security guarantees will appear in the market. Initially, they will focus on security mechanisms like isolation, confidentiality through encryption, and data integrity through authentication. However, we expect that they will then move on to the harder problems such as providing verifiable transparency, to integrate with security management systems of the customers, and to limit the risks imposed by misbehaving cloud providers and their employees.

**Acknowledgments.** We thank Ninja Marnau and Eva Schlehahn from the Independent Centre for Privacy Protection Schleswig-Holstein for substantial and very helpful input to our chapter on privacy risks. We thank the reviewer for helpful comments that enabled us to improve this chapter.

This research has been partially supported by the TClouds project <http://www.tclouds-project.eu> funded by the European Union’s Seventh Framework Programme (FP7/2007-2013) under grant agreement number ICT-257243.

**Open Access.** This article is distributed under the terms of the Creative Commons Attribution Noncommercial License which permits any noncommercial use, distribution, and reproduction in any medium, provided the original author(s) and source are credited.

## References

1. Babcock, C.: Management Strategies for the Cloud Revolution. McGraw-Hill, New York (2010)
2. Basak, D., Toshniwal, R., Maskalik, S., Sequeira, A.: Virtualizing networking and security in the cloud. *SIGOPS Oper. Syst. Rev.* 44, 86–94 (2010), doi:10.1145/1899928.1899939
3. Brassil, J.: Physical layer network isolation in multi-tenant clouds. In: Proceedings of the 2010 IEEE 30th International Conference on Distributed Computing Systems Workshops, Washington, DC, USA. ICDCSW ’10, pp. 77–81. IEEE Computer Society Press, Los Alamitos (2010), doi:10.1109/ICDCSW.2010.39
4. Cabuk, S., Dalton, C.I., Eriksson, K., Kuhlmann, D., Ramasamy, H.V., Ramunno, G., Sadeghi, A.-R., Schunter, M., Stübke, C.: Towards automated security policy enforcement in multi-tenant virtual data centers. *J. Comput. Secur.* 18, 89–121 (2010)

5. Chien, E.: W32.Stuxnet dossier. retrieved 2010-13-03, (Sep 2010), From <http://www.symantec.com/connect/blogs/w32stuxnet-dossier>
6. Chow, R., Golle, P., Jakobsson, M., Shi, E., Staddon, J., Masuoka, R., Molina, J.: Controlling data in the cloud: outsourcing computation without outsourcing control. In: ACM Workshop on Cloud Computing Security (CCSW'09), pp. 85–90. ACM Press, New York (2009)
7. Cloud Security Alliance (CSA): Top threats to cloud computing, version 1.0. (March 2010), <http://www.cloudsecurityalliance.org/topthreats/csathreats.v1.0.pdf>
8. Computer and Communication Industry Association (CCIA): Cloud computing (2009), [http://www.ccianet.org/CCIA/files/ccLibraryFiles/Filename/00000000151/Cloud\\_Computing.pdf](http://www.ccianet.org/CCIA/files/ccLibraryFiles/Filename/00000000151/Cloud_Computing.pdf)
9. Gentry, C.: Fully homomorphic encryption using ideal lattices. In: Proceedings of the 41st annual ACM symposium on Theory of computing, Bethesda, MD, USA. STOC '09, pp. 169–178. ACM Press, New York (2009), doi:10.1145/1536414.1536440
10. Grobauer, B., Schreck, T.: Towards incident handling in the cloud: challenges and approaches. In: Proceedings of the 2010 ACM workshop on Cloud computing security workshop, Chicago, Illinois, USA. CCSW '10, pp. 77–86. ACM Press, New York (2010), doi:10.1145/1866835.1866850
11. Guerraoui, R., Yabandeh, M.: Independent faults in the cloud. In: Proceedings of the 4th International Workshop on Large Scale Distributed Systems and Middleware, Zürich, Switzerland. LADIS '10, pp. 12–17. ACM Press, New York (2010), doi:10.1145/1859184.1859188
12. International Organization for Standardization (ISO): ISO27001: Information security management system (ISMS) standard (Oct 2005), <http://www.27000.org/iso-27001.htm>
13. Kaliski, Jr., B.S., Pauley, W.: Toward risk assessment as a service in cloud environments. In: Proceedings of the 2nd USENIX conference on Hot topics in cloud computing. pp. 13–13. HotCloud'10, USENIX Association, Berkeley, CA, USA (2010), <http://portal.acm.org/citation.cfm?id=1863103.1863116>
14. Marko, K.: Cloudsourcing - the cloud sparks a new generation of consultants & service brokers (2010), <http://www.processor.com/editorial/article.asp?article=articles%2Fp3203%2F39p03%2F39p03.asp>
15. Oclassen, G.: Why not cloudsourcing for enterprise app user adoption/ training? (2009), <http://velocitymg.com/explorations/why-not-cloudsourcing-for-enterprise-app-user-adoptiontraining/>
16. Organization for Economic Co-Operation and Development (OECD): Guidelines on the protection of privacy and transborder flows of personal data. From [http://www.oecd.org/document/18/0,2340,en\\_2649\\_34255\\_1815186\\_1\\_1\\_1\\_1,00.html](http://www.oecd.org/document/18/0,2340,en_2649_34255_1815186_1_1_1_1,00.html) (last modified January 5 1999), the OECD Privacy Principles
17. Penn, J.: Security and the cloud : Looking at the opportunity beyond the obstacle. Forrester Research (October 2010)
18. Rajan, S.S.: Cloudsourcing vs outsourcing (2010), <http://cloudcomputing.sys-con.com/node/1611752>
19. Ristenpart, T., Tromer, E., Shacham, H., Savage, S.: Hey, you, get off of my cloud: exploring information leakage in third-party compute clouds. In: Proceedings of the 16th ACM conference on Computer and communications security, Chicago, Illinois, USA. CCS '09, pp. 199–212. ACM Press, New York (2009), doi:10.1145/1653662.1653687

20. Sadeghi, A.-R., Schneider, T., Winandy, M.: Token-Based Cloud Computing Secure Outsourcing of Data and Arbitrary Computations with Lower Latency. In: Acquisti, A., Smith, S., Sadeghi, A.-R. (eds.) Proceedings of the 3rd international conference on Trust and trustworthy computing, Berlin, Germany, June 21-23, 2010. LNCS, vol. 6101, pp. 417–429. Springer, Heidelberg (2010)
21. Santos, N., Gummadi, K.P., Rodrigues, R.: Towards trusted cloud computing. In: Proceedings of the 2009 conference on Hot topics in cloud computing. pp. 3–3. HotCloud'09, USENIX Association, Berkeley, CA, USA (2009), <http://portal.acm.org/citation.cfm?id=1855533.1855536>
22. Sotto, L.J., Treacy, B.C., McLellan, M.L.: Privacy and data security risks in cloud computing. *Electronic Commerce & Law Report* 15, 186 (2010)
23. Van Dijk, M., Juels, A.: On the Impossibility of Cryptography Alone for Privacy-Preserving Cloud Computing. *IACR ePrint* 305 (2010)
24. Vukolić, M.: The byzantine empire in the intercloud. *SIGACT News* 41, 105–111 (2010), doi:10.1145/1855118.1855137
25. Waidner, M.: Cloud computing and security. Lecture Univ. Stuttgart (November 2009)
26. Weichert, T.: Cloud Computing und Datenschutz (2009), <http://www.datenschutzzentrum.de/cloud-computing/>