Privacy, Security and Trust in Cloud Computing The Perspective of the Telecommunication Industry

Leonardo A. Martucci*, Albin Zuccato†, Ben Smeets§‡, Sheikh M. Habib‖, Thomas Johansson‡, Nahid Shahmehri*

*University of Linköping, SE 581-83 Linköping, Sweden
†TeliaSonera, SE 106-63 Stockholm, Sweden
§Ericsson Research, SE 221-83 Lund, Sweden
‖Technische Universität Darmstadt, DE 642-93 Darmstadt, Germany
‡Lund University, SE 221-00 Lund, Sweden

***Abstract*—The telecommunication industry has been successful in turning the Internet into a mobile service and stimulating the creation of a new set of networked, remote services. Most of these services now run or are supported by cloud computing platforms. Embracing cloud computing solutions is fundamental for the telecommunication industry to remain competitive. However, there are many legal, regulatory, business, market-related and technical challenges that must be considered first. In this paper we list such challenges and define a set of privacy, security and trust requirements that must be taken into account before cloud computing solutions can be fully integrated and deployed by telecommunication providers.**

***Keywords*-cloud computing; security; privacy; trust.**

I. Introduction

The telecommunication industry has been successful in turning the Internet into a mobile service and stimulating the creation of a new set of networked, remote services. Most of these services are currently supported by or run in cloud computing platforms.

Cloud computing represents a threat to the status quo of the telecommunication industry and, at the same time, a unique opportunity to deliver new high value-added services. On the one hand, the threat is that cloud computing platforms may reduce telecommunication providers to delivering commodity "dumb" pipes [1] that just forward data from customers to cloud computing providers, which then offer services with high value-added. The income from services represents an important share of the total revenue of telecommunication providers and service provision is usually more profitable than packet forwarding. On the other hand, the telecommunication industry's unique position offers an opportunity for integration and development of new cloud-based services that take into consideration knowledge of the network status, the ability to redirect and prioritize data traffic, and knowledge about its customers. Such advantages have the potential to dramatically boost the revenues of telecommunication providers.

The impact of cloud computing solutions in the telecommunication industry is caused by the decoupling of applications, also known as service provisioning, from networking services, i.e. packet forwarding and routing. Consequently, the traditional bundling of services and networking equipment, such as routers and radio base stations, is now eroding. It is then foreseeable that revenues from networking equipment will decline. Revenues from telecommunication providers will also tend to decrease due to the commoditization of network access services. As a result the telecommunication industry is now being forced to integrate new services into the connectivity business, such as packet inspection and network management, to promote service interoperability and also to customize services for different business sectors and governments [1]. In addition, the telecommunication industry has started to integrate cloud computing solutions into its portfolio. For instance, Ericsson recently launched its own network-enabled cloud [2] and telecommunication providers, such as T-Systems and TeliaSonera, now offer cloud computing based solutions and products [3], [4].

At the same time, traditional Internet solution providers have been adapting their services to mobile users. The communication between such solution providers and users is controlled by the telecommunication industry. The increasing dependency on reliable IT infrastructures for delivering cloud services to mobile users places the telecommunication industry a unique position, as it controls and manages the communication media and, thus, is able to deliver reliable cloud services. Although the above development seems inevitable, there are still barriers to overcome. One of the most important barriers originates from security concerns raised when considering the adoption of cloud computing solutions [5].

These concerns stem from the nature of public cloud computing in which knowledge about where the computation takes place and by what means is largely unknown and/or hard to assess in a reliable way[1]. Business and market concepts, e.g., cloud computing marketplaces and cloud computing brokers, further complicate such a reliable assessment.

Moreover, cloud computing solutions for the telecommunication industry will likely be integrated with other cloud services. It is natural for telecommunication providers to also act as cloud providers and/or service brokers for other cloud providers. Furthermore, there are legal concerns that are

[1]These concerns do not exist in private cloud computing platforms, as they are dedicated platforms that are controlled by a single organization.

tightly coupled to security concerns. Legal concerns regarding cloud solutions can come from customer contracts and/or from national requirements on privacy and legal interception. Although the latter are well-known to the telecommunication industry it is necessary to find ways to carry them over into cloud solutions.

In this paper we argue that embracing cloud computing is fundamental for the telecommunication industry, and focus on the privacy, trust and security challenges and requirements that arise from such integration. In particular, the problem that we address in this paper is the following one: to deliver its own cloud solutions, the telecommunication industry has to address privacy, security and trust challenges. Which are the challenges and what are the resulting requirements?

This paper is organized as follows. In Section II we present the network architecture assumed in this paper, and in Section III we list the challenges faced by the telecommunication industry regarding: legal and regulatory, business and markets, and technical aspects. In Section IV we present the privacy, security and trust requirements for the telecommunication industry when providing cloud computing services. The concluding remarks are presented in Section V.

II. Background

The network architecture assumed in this paper is that of a *Long Term Evolution* (LTE or 4G) mobile network. In reality, mobile networks are more complex than that, as they also include legacy technologies, e.g., GSM, in the set of network services offered to end-users. LTE systems are a good example of a modern high speed telecommunication system. Limits in radio propagation force radio cells to shrink in size to be able to support data rates up to $1Gbps$. Thus, the number of base stations dramatically increases when compared to 3G and GSM systems. Consequently in areas where LTE services are to be offered, one has to build a dense network of base stations. Traditionally such base stations are deployed by a *Mobile Network Operator* (MNO). However, due to their high cost, LTE base stations, which are called *evolved NodeBs* or *eNBs* in the LTE nomenclature, are mostly co-owned and shared by the MNOs that use them, or may not even be owned by the MNOs, which might instead just rent shares of an eNB's capacity. Such arrangements are also commonplace in the deployment of 3G networks.

The trend for networking services to be deployed on infrastructures that belong to multiple owners is clear. Cloud computing is pushing the separation between infrastructure and services further by introducing new applications and tools to the telecommunication industry. In particular, cloud computing combined with network virtualization allows the creation of *virtual mobile networks* (VMNs). VMNs can be offered as a *platform as a service* (PaaS). MNOs can offer VMNs to large organizations, such as utility companies, and governmental agencies. VMNs can provide tailored network services in which their data communication is kept isolated from others' data communication channels and can be routed according to customizable or agreed-upon rules. Such cloud

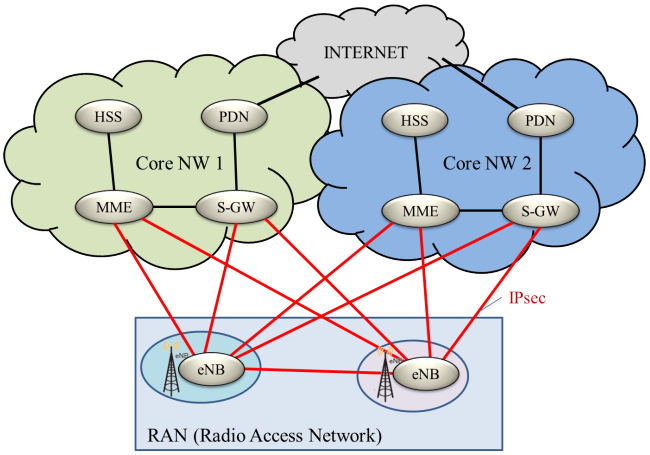

Fig. 1. An example of an LTE network with a physical Radio Access Network (RAN) and two Core networks (Core NW) Clouds that are connected to the Internet through their Packet Data Network (PDN) gateways. HSS, MME and S-GW are other components of a Core NW, which are described in the 3GPP LTE architecture [6].

infrastructure can also support services for organizations that operate networked machine-to-machine devices, e.g., for car fleet management or surveillance purposes. These services can be delivered under the *software as a service* (SaaS) model. Fig. 1 illustrates such a setup: the *Radio Access Network* (RAN) is used by two cloud-based *Core Networks* (Core NW), each containing a standard *Mobility Management Entity* (MME), a *Home Subscriber Service* (HSS), a *Serving Gateway* (S-GW), and a *Packet Data Network* (PDN) gateway.

III. Challenges

Without a doubt, cloud computing services offer a number of opportunities and benefits. There are already various reports describing the benefits and challenges for cloud computing services in general [7], [8]. In addition to those challenges, we identify a number of additional issues that are specific to the telecommunication industry in regard to: legal and regulatory, business and market, and technical aspects.

A. Legal & Regulatory Challenges

In this section we discuss the challenges to the telecommunication industry emerging from legislation and regulation, with an emphasis on the European case. In particular, we evaluate the legal and regulatory challenges arising from data protection legislation, data retention legislation, lawful interception and protection of the national infrastructure.

Data protection legislation implies a number of challenges for cloud services. Most significant is that the data controller (i.e. the telecommunication provider) is no longer the data processor. The EU legislation requires the data controller to know who processes which data and for what purpose. The cloud computing service providers must therefore be able to deliver this information and they and all their subcontractors (such as other cloud computing providers) must abide by data processing agreements that are compliant with national legal

demands. This becomes especially challenging when one of the data processing partners is outside the EU.

Another challenging area is data retention. Data retention means that the operator is obliged to provide traffic data to law enforcement agencies. Depending on the nature of the service, the traffic data may be owned by the cloud service provider. The telecommunication provider's challenge is to make sure that the cloud provider is capable of collecting and providing information whenever requested by the authorized parties.

Lawful Interception (LI) implies that law enforcement may request access to the communication channel and data. In the current model, the telecommunication systems are located where law enforcement has jurisdiction. When it comes to cloud services this is not necessarily true, as services may be produced in different jurisdictions, such as one or more different countries. The LI support obligation, however, still remains with the telecommunication provider. The challenge is then twofold. Firstly, the telecommunication provider must be able to deliver the data and must therefore contractually assure that the cloud service provider will make the data available upon request. Secondly, a challenge arises when the legal framework in two or more jurisdictions imply different rules concerning the preconditions under which data may be provided. In such a case, contractual solutions are not feasible and a legal pre-assessment is advisable.

Finally, telecommunication is, in many countries, considered to be part of the critical national infrastructure and, thus, a strategic asset. Therefore, in case of a crisis, telecommunication services are obliged to be fully producible inside the national borders. Such restrictions limit the applicability/range of some cloud computing services, such as VMNs, as the cloud provider must be able to offer its services from within national borders. This either implies that cloud services can be immediately moved within a country's borders or that a redundant infrastructure is locally available. This challenge also includes the protection of one country's telecommunication data and infrastructure against other nations that may have jurisdiction over cloud service providers. The *USA PATRIOT Act* [9], for instance, provides US law enforcement agencies with significant capabilities to demand access to cloud computing services hosted, controlled or maintained by American companies. Deutsche Telekom, a German telecommunication provider, has been using such argument to promote its cloud services [10].

B. Business & Market Challenges

The cost pressure on the telecommunication industry makes it necessary to deal with production costs. Cloud computing services promise cost reductions and new sources of revenue. Hence, the telecommunication industry's interest in cloud computing services. The main challenge is to realize the cost reduction without jeopardizing the core business. The following business and market challenges should therefore be taken into account.

Customers and customers' data are two of the most valuable non-tangible assets of a telecommunication provider [11].

When it comes to cloud computing services, telecommunication providers must share customers' data with cloud computing providers, as user related information is usually required for service provisioning. It is of vital interest to the telecommunication providers that they provide their customers with access to cloud computing services without actually losing the control over the customers' data and identity to the cloud computing provider. The telecommunication providers' challenge is to share only the minimum amount of customers' data with the cloud service providers in order to prevent them from taking control over the customers and their data.

Traditionally, the telecommunication industry has protected its customers' communication as this coincided with protecting its own network [6]. This has resulted in a trust relationship between telecommunication providers and customers, where the customers implicitly assume that their data are protected by their telecommunication providers. This trust relationship offers a unique business opportunity, where the telecommunication provider acts as an intermediary which stands for security and privacy. As a consequence, the telecommunication providers are faced with the challenge of assuring that no harm comes to their customers. Apart from the actual safeguards, it is also important to have unobtrusive trust enforcers that make protection evident to the customer.

When it comes to market opportunities, statements from Nordic data protection authorities, such as from the Danish[2] and the Swedish[3] authorities, and also media statements (see IDG.se[4]) clearly indicate that the usage of cloud services by government agencies is not without problems and could potentially infringe on current legislation. For the telecommunication industry the challenge is twofold. Firstly, it means that telecommunication services that include cloud services may not be sellable to agencies. A good understanding of how services are provided is therefore fundamental. Secondly, secure, trusted and privacy-friendly cloud services are needed so that governmental agencies are allowed to buy / hire them.

C. Technical Challenges

The mobile telecommunication infrastructure was originally constructed in the 1980's. In many countries, the infrastructure was originally owned by a single entity, usually government-owned monopolies. During the design of these networks it was therefore assumed that all network components could trust each other as they belonged to a single owner. Furthermore, communication channels would only be established inside the network under control of this single entity (roaming did not exist, and international calls were established from a few exit points).

The most noteworthy and lasting consequence is that both control and data traffic share a common signaling protocol (*Signaling System 7* or SS7 [12]) with virtually no security

[2]http://www.datatilsynet.dk/english/processing-of-sensitive-personal-data-in-a-cloud-solution/

[3]http://www.datainspektionen.se/press/nyhetsarkiv/2011/risker-med-otydliga-avtal-for-molntjanster/

[4]http://cloud.idg.se/2.16150/1.382336/pul-forsenar-myndighetsmoln

functionality. For instance, SS7 does not provide any authentication mechanism between the network components, such as radio base stations. Therefore, a single misbehaving or compromised radio base station is able to compromise the entire network. It is thus a major challenge to manage and control such an environment where all components need to trust each other. Another reason for concern is the control plane of the mobile networks whose reliable operation depends on certain security assumptions, such as having only trusted base stations. Control planes[5] were originally designed based on the assumption that the network infrastructure was controlled by of a group of relatively well-trusted operators. This is no longer true in LTE, which already has a more evolved security design that can handle compromised eNBs and the communication between eNBs and Core NWs is done using IPSEC tunnels. Nevertheless, 4G networks co-exist with legacy mobile networks, which are used as fall-back networks. Legacy networks also provide most of the mobile network coverage.

The advent of cloud computing raises the following questions regarding its impact on the telecommunication industry: to what extent should management and operation of control planes be transferred to cloud providers? How can this transfer be achieved? And what are the appropriate requirements for performing such a transfer? These concerns and questions are well-founded as illustrated by the insufficient security implementation in femtocells [13], which are short-ranged cellular base stations designed to be deployed at homes or offices. It strongly indicates that cloud computing solutions for the telecommunication industry will have to cope with security requirements in an heterogeneous telecommunication infrastructure, while also addressing the need to have all components of the infrastructure cooperating to provide requested services according to its service-level agreement (*SLA*).

Apart from network related challenges, the integration of value-added telecommunication services like SMS, voice messaging, short-numbers, number normalization, etc. and other general applications, e.g., administration applications and office tools, also presents multiple challenges. Interfaces and procedures for running such services are slightly different between telecommunication operators. One of the challenges for integrating cloud computing and telecommunications services is the development of standardized interfaces. Most such services are not expected to be re-developed for running in cloud platforms or deployment by telecommunication providers, but will instead be wrapped around software components to make them cross-compatible between different platforms.

Other technical challenges relate to business support systems, e.g., billing systems, customer relationship management systems and vendor support, and operation support systems integration, such as network monitoring and deployment. Contracting all of those services from a single cloud computing provider would mean that the telecommunication provider would be fully dependent on that single cloud provider, and could eventually run into problems when migrating some services to other cloud providers, as there are no available standards for interoperability between different cloud computing platforms. Interoperability is crucial for the commoditization of cloud computing services, and the standardization of interfaces is the related challenge. Furthermore, in the case of integration of multiple or cascading cloud computing platforms, or the advent of cloud computing marketplaces, the trust assessment of the network and of its services has the potential to turn into a complex and challenging problem [14].

The integration of cloud computing services implies that the business processes of the telecommunication industry have to be modified and adapted. The challenge, then, is to offer services that are not only price competitive, but which also provide quality of service and distinguishable features. In addition, the telecommunication industry has to increase the complexity of an already complex network. This results in a series of challenges for the network operator, as the tasks of planning and managing the network must now include a considerable number of additional components, each with a different SLA. Furthermore, business continuity planning and disaster recovery planning must also account for the threats and countermeasures associated with the added cloud computing platforms.

IV. Requirements

In this section we present the privacy, security and trust requirements related to the integration of the telecommunication industry and cloud computing services that proceed from the list of challenges presented in Section III. The requirements are presented as a set of action points and technical solutions that can be applied to address the identified challenges.[6]

A. Privacy Requirements

The concept of privacy is not universally defined, since it is a cultural construct and, hence, subjective. In this paper we refer to informational privacy[7], which is related to the person's right to determine when, how and to what extent information about him or her is communicated to others [17].

The privacy requirements related to cloud computing are closely related to the set of applicable legislation and regulations mentioned in Section III-A. In Europe, they include a series of European Commission directives [18], [19], [20]. Those directives regulate the processing of personal data, protection of privacy and data retention in the EU. In addition, a comprehensive reform of the data protection rules was recently proposed in [21], [22]. The reform includes a single set rules on data protection to be enforced throughout the EU, including users' right to access their own data, to transfer personal data from one service to another and the "right to

[5]Control planes are architectural elements in telecommunication devices that are responsible for packet forwarding, routing and discarding.

[6]Not all requirements are exclusive to telecommunication providers, and some can be generalized to other providers of cloud computing services.

[7]Informational privacy is one of the three basic aspects that construct the concept of privacy. The other two aspects are: territorial privacy and privacy of the person. More details on these aspects can be found in [15], [16].

be forgotten". The new directive and regulation will result, if approved, in a new set of privacy requirements that the telecommunication providers will need to comply with.

The principle of necessity of data collection and processing, which is one of the most essential privacy requirements, determines that the collection and processing of personal data should only be allowed if it is necessary for the tasks falling within the responsibility of the data processing agency. Hence, personal information should ideally not be collected or used for identification purposes when not absolutely necessary. The best strategy to enforce such a requirement is the avoidance or minimization of personal data [15], [16]. Thus, privacy is best protected if no personal identifiable information (PII) is stored or processed in the cloud computing platform or transferred to or from it. Hence, the telecommunication providers must consider the implementation of privacy enhancing technologies (PETs) for the anonymization or pseudonymization of data.

It is, nevertheless, expected that a significant share of data being transmitted, processed or stored on the cloud computing platform will have PII associated to it. Therefore, other PETs, such as those based on obfuscation [23] or on the concept of privacy by design [21], [24], in which privacy is integrated into all phases of the design and implementation of the cloud computing platform, are required to embed privacy protections into the system. The implementation of cloud marketplaces and their use by telecommunication providers must also take privacy aspects into consideration, as the EU legislation obliges the data controller to have knowledge about which entity processes which PII and the purpose of such processing. Hence, a telecommunication provider must necessarily have knowledge about all cloud computing providers that process PII of its customers.

B. Security Requirements

Cryptographic techniques are essential to provide information separation and data confidentiality in cloud computing platforms. At the same time, such techniques greatly reduce the ability to provide simple caching and filtering/screening services that increase efficiency and robustness against unwanted traffic. Cryptographic techniques, such as homomorphic encryption, may solve, in principle, some problems but it is still rather unexplored and untested in practice. Also regulatory requirements for LI must be carefully taken into consideration when deploying cryptographic techniques.

Cryptography separation is realized with strong compartmentalization techniques provided in secure operational systems, virtualization or hardware. Virtualization using hypervisors is a technique that is available in open-source solutions, such as Xen [25] and KVM (Kernel-based Virtual Machine) [26]. Moreover, access control mechanisms can also be used to protect information.

Despite the huge success of cloud computing as a computing model and as an economic platform, many enterprises still hesitate to join the cloud in full because of security concerns. Many major organizations only allow their employees to use cloud services for less sensitive data. Other organizations use private cloud computing platforms to overcome some of these problems. This hesitation comes from concerns about the security of cloud solutions as well as loss of control of data and computation [5]. Such a situation creates a clear advantage for the telecommunications industry, as it can be the enabler of the security services. For instance, the problem of cross-authenticating customers is a key problem in cloud computing platforms, and telecommunication providers are already able to provide strong and practical solutions to it. Thus, the telecommunication providers can potentially take a great share of the business role of cloud computing providers.

Security requirements in cloud computing platforms are a well documented subject [27]. Standard security concerns are, for example, vulnerabilities that appear in hypervisors or other virtualization technologies that are used by cloud computing vendors; network attacks on the user's connection to the cloud providers; weaknesses in the user authentication process; and availability issues, including *denial of services* (DoS) attacks.

Another key problem is the loss of control of data. From a security perspective, this has to do with confidentiality and data integrity issues. The cloud computing provider may take part of a customer's PII directly, or may use it indirectly (for example, the cloud computing provider may provide statistical analysis of the data for advertising purposes). This problem has accelerated the search for technical solutions to provide confidentiality and integrity in cloud computing. Cryptographic techniques can be applied, but have negative practical implications regarding computational performance, as discussed in [28].

In cloud storage, operations on the data are commonplace, such as searching for keywords. Decrypting an entire data set when searching for a single keyword is of course not an acceptable solution. *Searchable Encryption* algorithms offer the possibility of searching over encrypted data [29]. In cloud computing platforms, it might be possible to perform computation on encrypted data without decrypting it beforehand by using *homomorphic encryption* techniques. However, current techniques for homomorphic encryption may not be practical enough yet for deployment in cloud computing platforms.

Inter virtual machine attacks need to be evaluated when considering virtualization. Methods based on Chinese-wall techniques [30] mitigate the risks of such attacks. VM image protection is also an important aspect when considering secure procedures for migration and backup.

C. Trust Requirements

The cloud computing ecosystem consists of several entities, e.g., cloud providers, resellers, carriers and customers. This ecosystem is highly distributed and customers possess only a limited and abstract view of it. This situation is rather similar to what customers face with telecommunication networks in which base stations are co-owned by different telecommunication providers. Again, customers possess only a limited view of the telecommunication infrastructure. Introducing cloud computing technologies on top of telecommunication networks

pushes such abstraction even further, and with it the trust that customers invest in their telecommunication providers.

The abstract and distributed nature of cloud computing environments represents a considerable obstacle for the acceptance and market success of cloud based services. Recent surveys have demonstrated that cloud consumers are concerned about their outsourced data and the related services provided by cloud providers [31]. Such concerns can be mitigated by using preventive controls, e.g., encryption and authentication, as discussed in Section IV-B. These preventive controls would permit users to establish trust with cloud providers from a technical point of view, which is known as a "hard trust" mechanism [32]. "Hard trust" mechanisms make assumptions about an information system's security, dependability and reliability based on existence of different primitives, e.g., certificates, audits and secure hypervisors. However, "hard trust" mechanisms are not necessarily sufficient for cloud consumers to trust cloud providers. Trust involves aspects such as intrinsic human emotions and perceptions, interaction and exchange of experiences, and loyalty to a brand. Such aspects are fundamental when establishing trust with cloud providers. This kind of trust is known as "soft trust" [32]. "Soft trust" assumes that no "hard trust" mechanisms are perfect and errors exist no matter how rigid the design procedures are [31].

"Soft trust" mechanisms can be complemented with "hard trust" to support telecommunication providers in establishing trustworthy cloud computing environments. Moreover, trust mechanisms require knowledge of the architecture of the system and the trustworthiness of its subsystems and components when evaluating trustworthiness of cloud providers.

V. Conclusions

In this paper we have argued that embracing cloud computing solutions is fundamental for the telecommunication industry. However, we have shown that the process is not without challenges. We have the listed a set of privacy, security and trust requirements that must be taken into account before cloud computing solutions can be fully integrated and deployed by telecommunication providers.

References

[1] A. Joshipura, "The cloud: what operators stand to gain – or lose," *Ericsson Business Review*, vol. 12, 2010.

[2] "Ericsson's network-enabled cloud meets needs of the networked society," Ericsson AB Press Release, 26 Feb 2012.

[3] T-Systems. (2012, 15 Mar) Cloud computing. [Online]. Available: http://www.t-systems.com/tsip/en/152272/home/solutions/hot-solutions/cloud-computing/1-cloud-computing

[4] TeliaSonera. (2012, 15 Mar) Telia Molnet. [Online]. Available: http://www.telia.se/foretag/battreaffarer/kampanjer/molnet

[5] "European CIO cloud survey: Addressing security, risk and transition (Colt)," Loudhouse Marketing & Research, Mar 2011.

[6] 3GPP, "3GPP System Architecture Evolution (SAE), Security architecture," 3GPP, Release 11, 3GPP TS 33.104, 2009.

[7] D. Catteddu and G. Hogben, Eds., *Cloud Computing – Benefits, risks and recommendations for information security*. ENISA, Nov 2009.

[8] A. Reed, C. Rezek, and P. Simmonds, Eds., *Security guidance for critical areas of focus in cloud computing v3.0*. Cloud Security Alliance, 2011.

[9] "Uniting and strengthening america by providing appropriate tools required to intercept and obstruct terrorism (USA PATRIOT Act)," Public Law 107-56, US Government, 26 Oct 2001.

[10] Bloomberg. (2011, 13 Sep) Deutsche Telekom wants "German cloud" to shield data from US. [Online]. Available: http://www.bloomberg.com/news/2011-09-13/deutsche-telekom-wants-german-cloud-to-shield-data-from-u-s-.html

[11] N. Klapisz, Ed., *Valuation drivers in the telecommunication industry*. Ernst & Young, 2011.

[12] *Specifications of Signalling System No. 7*, International Telecommunication Union (ITU-T) Std. Q.700, Mar 1993.

[13] R. Borgaonkar, K. Redon, and J.-P. Seifert, "Security analysis of a femtocell device," in *Proc. of the* 4^{th} *ACM Int. Conf. on Security of Information and Networks (SIN)*. New York, NY, USA: ACM, 2011, pp. 95–102.

[14] S. M. Habib, S. Ries, and M. Muhlhauser, "Towards a trust management system for cloud computing," in *Int. Joint Conf. of IEEE TrustCom/IEEE ICESS/FCST*. IEEE Computer Society, 2011, pp. 933–939.

[15] S. Fischer-Hübner, *IT-Security and Privacy*, ser. Lecture Notes in Computer Science. Springer Berlin/Heidelberg, 2001, vol. 1958.

[16] L. A. Martucci, "Identity and anonymity in ad hoc networks," Ph.D. dissertation, Karlstad University, Jun 2009.

[17] A. F. Westin, *Privacy and Freedom*. New York, NY, USA: Atheneum, 1967.

[18] "Directive 2002/58/EC of the European Parliament and of theCouncil concerning the processing of personal data and the protectionof privacy in the electronic communications sector, Brussels," Official Journal L No.201, 31 Jul 2002.

[19] "Directive 95/46/EC of the European Parliament and of the Councilof 24 October 1995 on the protection of individuals with regardto the processing of personal data and on the free movement of such data," Official Journal L No.281, 23 Nov 1995.

[20] "Directive 2006/24/EC of the European Parliament and of theCouncil of 15 March 2006 on the retention of data generated or processed in connection with the provision of publicly available electroniccommunications services or of public communications networks and amendingdirective 2002/58/EC," Official Journal L No.105, 13 Apr 2006.

[21] "Proposal for a directive of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data," COD 2012/0010, 25 Jan 2012.

[22] "Proposal for a regulation of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data and on the free movement of such data (general data protection regulation)," COD 2012/0011, 25 Jan 2012.

[23] S. Pearson, Y. Shen, and M. Mowbray, "A privacy manager for cloud computing," in *Proc. of the* 1^{st} *Int. Conf. on Cloud Computing Technology and Science (CloudCom)*. Springer-Verlag, 2009, pp. 90–106.

[24] K. Zeng and A. Cavoukian, "Modelling cloud computing architecture without compromising privacy: A privacy by design approach," NEC Company, Ltd. and Information and Privacy Commissioner, Ontario, Canada, May 2010.

[25] P. Barham, B. Dragovic, K. Fraser, S. Hand, T. Harris, A. Ho, R. Neugebauer, I. Pratt, and A. Warfield, "Xen and the art of virtualization," in *Proc. of the* 19^{th} *ACM Symp. on Operating Systems Principles*. Bolton Landing, NY, USA: ACM, 2003.

[26] A. Kivity, Y. Kamay, D. Laor, U. Lublin, and A. Liguori, "KVM: the linux virtual machine monitor," in *Proc. of the 2007 Ottawa Linux Symposium (OLS'07)*, 2007, pp. 225–230.

[27] R. Chow, P. Golle, M. Jakobsson, E. Shi, J. Staddon, R. Masuoka, and J. Molina, "Controlling data in the cloud: outsourcing computation without outsourcing control," in *Proc. of the 2009 ACM workshop on Cloud computing security*, ser. CCSW'09, 2009, pp. 85–90.

[28] Y. Chen and R. Sion, "On securing untrusted clouds with cryptography," in *Proc. of the 2010 ACM Workshop on Privacy in the Electronic Society (WPES)*. ACM, 4 Oct 2010, pp. 109–114.

[29] S. Kamara and K. Lauter, "Cryptographic cloud storage," in *Financial Cryptography and Data Security*, ser. Lecture Notes in Computer Science. Springer Berlin/Heidelberg, 2010, vol. 6054, pp. 136–149.

[30] T. Tsai, Y. Chen, H. Huang, P. Huang, and K. Chou, "A practical chinese wall security model in cloud computing," in *APNOMS*, 2011.

[31] I. Uusitalo, K. Karppinen, A. Juhola, and R. Savola, "Trust and cloud services - an interview study," in *Proc. of the* 2^{nd} *IEEE Int. Conf. on Cloud Computing Technology and Science (CloudCom)*, 30 Nov–3 Dec 2010, pp. 712–720.

[32] V. Varadharajan, "A note on trust-enhanced security," *IEEE Security and Privacy*, vol. 7, pp. 57–59, 2009.