Privacy aspects of Cloud Computing

Katja Vießmann
Institut für Telematik
Master-Seminar Cloud Computing
Universität zu Lübeck

***Abstract*—** Cloud computing seems like a new promising technology with a lot of advantages – yet being still in the early stages of development a lot of issues remain unsolved. It is important to address these adequately, so that the vision of Cloud computing as a new IT procurement model will not be compromised. One of these issues is the proper handling of privacy protection. Like recent studies show, a lot of German business companies are still hesitating to use Cloud computing solutions - with giving away sensitive data remaining the biggest obstacle. Whereas the concerns may be partly justified, it is also vitally important to open up to these new technologies to keep pace with world-wide IT evolution. The German government has recognized this problem and has initiated the project *Trusted Cloud* with the object making cloud computing more attractive for midsize companies. This paper discusses a few examples of *Trusted Cloud* and the concept *OmniCloud* by the Fraunhofer Institute. Both projects react to current problems of data protection in Cloud computing, aiming to future-proof the ICT location Germany.

1 Introduction

Public-Cloud computing (in the following addressed to as: Cloud computing) offers a new technology with a lot of possibilities: resources such as memory, processing power and applications can be provided, managed and charged dynamically over the internet. [1] Thus, enterprises can concentrate on their core business and don´t need to care (much) about IT administration anymore. They order what they actually need on demand. Through virtualization the complexity of the technical aspects of Cloud Computing is hidden to the users. [2] While this is appreciated for a smoothly handling of the software, also a lot of other details of data processing remain "cloudy".

A lot of end users, especially companies, are worried about a general lack of control of their data in the Cloud [11]. In this situation it is counter-productive, that there is a lack of established technological standards for Cloud computing. The heterogeneous landscape of used technologies and the unwillingness of Cloud storage providers to reveal details of used security mechanism increases distrust of potential clients. However, to use the advantages of Cloud Computing and do this kind of delegation, the trust of the costumers in Cloud Computing providers is the most important thing. Therefore a lot of companies either don´t use Cloud services at all or only put their less sensitive data into the Cloud.

As a recent survey [15] with IT professionals shows, 86% of the survey responders choose to keep their sensitive data on their organizations´s network. The present paper intends to analyze the current situation of data protection in existing Cloud services. The central question is if it is possible to store data in Clouds in a safe way. And how Cloud Computing customers can achieve enough certainty to trust Cloud Computing providers with their data. Section 2 discusses current situation about practiced security mechanisms and what a company should pay attention to when it is choosing a Cloud service provider. Section 3 presents some aspects which are mandatory for data protection in the cloud. In Section 4 and 5 a few examples by the Trusted Cloud initiative and the product OmniCloud by the Fraunhofer SIT as approaches for better data protection are presented.

2 current ways of privacy protection

As the Fraunhofer Institute study "On the Security of Cloud Storage Services" finds, there were a lot of security leakages at the examined Cloud services providers by that time (03/2012). [4] They analyzed seven Cloud service providers, finding that none of them met all mandatory security requirements which they specified. For instance, CrashPlan, TeamDrive and Wuala deny the usage of SSL/TLS, instead of using this established alternative, they use self-made, unpublished protocols for transportation. The study also revealed, that information, that should only be accessible by a secret URL – is presented by search engines. Furthermore, Mozy accepts weak passwords and doesn´t even show to users the strength of passwords. Mozy also encrypts files, but it does not decrypt file names. Dropbox and Wuala also did not verify the email-adress during the registration process. Meanwhile Dropbox has introduced two-factor authentication after an

attack exploiting this leakage. In general, a lot of legal aspects and problems when processing (personal) data in the cloud have not been solved yet. Some leakages, as Dropbox shows, are fixed step by step, but media scandals like these are not helping to raise the reputation of Cloud service providers. Cloud service providers e.g. Wuala [18] are advertising that they are being 'secure', but what that actually means is not quite clear and becomes only a phrase by redundant use.

2.1 Encryption variants used in cloud computing

Cloud storage services offer different kinds of encryption: some use no encryption at all (CloudMe, Ubuntu One), others use a provider´s key to encrypt data (e.g. Dropbox) and then there are the ones which offer the possibility to use built-in client sided software to encrypt data (CrashPlan, Mozy, Computerbild-Cloud, TeamDrive, Wuala). [4], [5] If a Cloud service uses server-side encryption the customer has to trust the Cloud server provider not to abuse his possibility to access the data. Furthermore the customer has to trust the Cloud service provider to use adequate encryption methods. Cloud service providers seldom reveal details about their used technologies and the security practices – so they stay quite obscure. But as the success of Dropbox shows, users do not hesitate to use such a service. From the provider´s perspective this is an appreciated situation, as there is a trade-off between security and costs: company keys reduce the amount of storage capacity needed by the provider. [4]

If a cloud costumer does not trust the server-sided encryption or the client-sided encryption, it is recommended to use own encryption software and store these encrypted files. For example TrueCrypt or GnuPrivacyGuard can perform local encryption. Unfortunately not every provider does support those self-encryption methods. Additionally, container-based encryption is prone to cause higher network traffic, and additional conflicts may occur when synchronizing data stored on different computers. As those encryption methods were not designed for Cloud computing, key management remains a problem left to the Cloud client.

2.2 Service Level Agreement (SLA)

The SLA is a contract between Cloud service providers and Cloud customers that contains an agreement about responsibilities, guaranties, availability, priorities and also about security measures [2]. Some enterprises like Amazon [13] have fixed SLAs, whereas Zimory-Cloud-Marktplatz [12] allows an individual adjustment of the safety requirements in the SLAs. It is important for Cloud customers to inspect the SLAs carefully before deciding for a Cloud service provider. The SLA may also reveal some facts not visible at first glance e.g. if the Cloud service provider is working with subcontractors which may have different regulations then the primary Cloud provider.

2.3 Certificates

It is recommended to use third-party-auditing to guarantee the realization of the security goals documented in the SLAs. [3] For gaining the trust of the customers most of the prominent Cloud service providers have their resource centers certified. In USA the SAS70 (Statement on Auditing Standard No. 70) is common. The SAS70-report has no validity period, so it makes sense to check the date of issue – serious providers will renew the audit annually [4]. There is a standard based on SAS70 in Germany: DW PS 951 issued by the German “Institut der deutschen Wirtschaftsprüfer”. The SAS70 audit is designed for each service provider individually – so it is necessary to request a copy of the report, to evaluate if it meets all of the security requirements needed by the client. In the EU the international standard ISO/IEC 27001 and 27002 issued by the ISO (the International Organization for Standardization) and IEC (the International Electrotechnical Commission) is widely used [2]. This kind of certificate is valid for three years.

This is not a specific Cloud Computing certification but a general standard how a IT-security-management-system is built and maintained. [1]Therefore there was the need for a specific cloud auditing service. Since early 2011, “EuroCloud” also certificates SaaS-products. EuroCloud Germany eco announced at the fair CeBIT 2011 that their test criteria have been developed in coordination with the German BSI. The “Security Recommendations for Cloud Computing Providers" [20] issued by the German BSI have been integrated into the test criteria. [4] For a “Seal of approval” it is possible to gain up to five stars, when four stars are gained the following security aspects have to be fulfilled [14]:

- providing of VPN access
- encryption on data level
- restrictions for administrator access
- authentication and authorization can be managed by the Cloud service customer

In order to get five stars the cloud service provider needs to perform a penetration test and hand the results in to the EuroCloud-commission. Since specialized Cloud Auditing is still in its early stages of development and other auditing forms are not specially suited for Cloud Computing, this certificates still need to prove themselves in practice [19].

2.4 The threat of non-transparency to data privacy

It is common knowledge of network security experts that often the biggest problem is often on layer 8 – the user. This also applies to Cloud computing technologies: users pick poor passwords or don´t mind about taking care about security precautionary. They only start thinking about privacy issues when their privacy is already harmed. In the paper “User Awareness and Policy Compliance of Data Privacy in Cloud Computing” [6] Uwe Röhm and Audrey Mei Yi Quah discuss the results of an online survey among Cloud computing users. It reveals, that almost 50% of the surveyed end-users did not

know that they were already using one or more Cloud computing services today. On the other hand, more than 90% of the participants complain that "companies need to inform customers if they store and process personal customer information in the cloud." As the technology is still new for many end-users, they often use it naively like conservative software solutions – for example, it is often unclear to users, which flavor of sharing they use [4]. Are they sharing files with others subscribers of the same service, with a closed group of non-subscribers (e.g. with a secret URL) or are they sharing files with the public? As many users seem not to know, what the difference is between file publication and file sharing with a closed group it is essential for Cloud computing providers to describe transparently which kind of sharing mode is used. Otherwise data that is only meant for a closed group can be revealed by accident to the public.

The survey of the study mentioned above also indicates, that a majority of the participants are unaware of server locations of Cloud services. Yet they also report that it is not important to have knowledge or control over server locations. This finding shows the unawareness of the importance of the knowledge about implications of transborder data flow.

3 Approaches towards secure cloud computing

By this time German Cloud service providers are still underrepresented in a market dominated by American companies [1]. While German companies are well aware of the pressure of competition of other countries, they seem to struggle with trusting Cloud solutions. At the same time Cloud service providers work on solutions superior in data privacy and safety, that is meant to be a unique selling proposition of the brand 'Made in Germany'. The German Government is aware of the urgent need of development in this area and has started different projects to help realize these visions.

3.1 Server Locations

Most of the big cloud service providers like Amazon or Dropbox [11] are based in the USA. This concludes that they are under American Law e.g. The Patriot Act. This allows the American Government access to the data stored at the cloud service provider without the owner of the data being informed. As the recent NSA spying scandal shows, the American Government does not hesitate at all to exercise their rights. This is a fact, that one should keep in mind before subscribing to an American Cloud provider. It is also possible for non-American Cloud providers to have servers situated in the USA – and this might not be obvious at a first glance. Ideally, a cloud storage provider should make his server locations public [4]. Even better, the Cloud storage provider would offer different storage locations from which the user can choose – so he has more control over his data. For companies working with individual-related data, it is a must to overview server location to avoid violating existing German data privacy laws.

3.2 identity and access management

The BSI recommends [20], that every IT system and service used in Cloud computing is only accessible by authentication and identification of the user. Safety-critical applications should use a two-factor authentication as for example practiced in Online Banking. Especially for employees of the Cloud service provider who have administration rights strong authentication means like a hardware token should be used. This is especially important for mobile maintenance of the system. Another possibility is the access over VPN, which already uses two-factor authentication.

After the logging-in process there should exist an authorization, after BSI a role-based authorization is the means of choice. To every role only these rights should be assigned which are urgently required for the corresponding task (Least Privilege Model). These roles should be examined frequently and updated if required. All administration procedures should be documented. Critically administration procedures should only be done under the four eyes principle.

3.3 key management

If server-sided encryption is used, the Cloud service provider should create a cryptographic concept [20]. This concept should be published to the Cloud client, this way he is informed which tasks the Cloud service provider succeeds and which he eventually has to take care of himself. The BSI recommends to take care of integrating e.g. the following Best Practice elements into the key management. A cryptographic key should be used for only one single purpose and it should be stored encrypted itself. Keys should be distributed integer, authentic and confidentially, which also means that admins have no access to them. It is important to label a created key with a life cycle and renew it regularly. When a key is changed it is important to destroy the old key completely. To access key management functions there should be a separate authentication necessary. Finally, it is important to train the employees at the Cloud service provider responsible for key management in cryptographic knowledge.

4 Trusted cloud

One approach to make Cloud computing more attractive for companies is the German BMWi initiative "Trusted Cloud" [7], by addressing privacy and standardization concerns. The total investments for this project are at 100 Million Euro, 50% financed by economical project partners and 50% by the German Bund. The program is designing Cloud solutions especially for midsize companies. There are 14 projects, with 26 companies of different sectors and 26 science departments working on this program which started in 10/2010. A major topic is the approach of legal aspects to create a legal foundation for Cloud services in Germany ("Arbeitsgruppe Rechtsrahmen des Cloud Computing"). In the following, a few

examples of Trusted Cloud projects concerning data privacy are presented: MimoSecco, Sealed Cloud and SkIDentity.

4.1 MimoSecco: Middleware for Mobile and Secure Cloud Computing

It is essentially important to secure data during transport and storage through encryption to guarantee confidentiality. But on the other hand, data elements need to be decrypted while authorized users operate on them. MimoSecco´s goal is to achieve both efficiency and confidentiality while working with encrypted files. It distributes necessary data on different independent Cloud service providers: a data server (1st level Cloud provider), the index servers (2nd level cloud providers) and a database adapter. In this model, the 1st level Cloud provider is the one which has a contract with the cloud user and is treated as partly trustworthy. The 2nd level Cloud providers are with unknown trustworthiness and the databank adapter is trustworthy. [11] The database adapter encrypts and indicates the data, the data server then keeps the data in encrypted form (so it is not able to access it) and the indices are kept in partly encrypted form on two different index servers.

If a Cloud user wants to access a file, he raises a request to the databank adapter [17]. The databank adapter requires the needed indices from the index server, then he fetches the data from the data server and hands it to the user after decrypting it. The data adapter uses token-based encryption, the token only reveals the key for decryption after a valid certificate of the user and the SaaS application is presented. The Cloud user also uses a token to get access to the Cloud data. Both Cloud user and databank adapter use CodeMeter® of WI-BU-SYSTEMS AG using AES128 and which additionally requires a password. This technology intents to minimize the risk of insider attacks of cloud service providers by taking them the possibility to access data. It acknowledges the risk of statistic analysis e.g. of keyword search in a database and distributes index data on different cloud servers.

The project is still running till March 2014 – there is no product on the market available at this moment implementing these functionalities. Yet the project partners CAS Software AG, WIBU SYSTEMS AG und "Karlsruher Institut für Technologie" (KIT) are developing such a software solution right now. There might be slight changes in the current architecture left to meet all requirements of actual data protection regulations.

4.2 Sealed Cloud

Sealed Cloud is another concept to avoid insider attacks of potentially untrustworthy Cloud service providers [7]. Furthermore it intends to avert any unauthorized access. As data files pass a lot of different stops, the whole way has to be secured: physical systems, operating systems, middleware and applications. The Cloud data is transported over SSL with 2048 Bit key length. After arriving in the Cloud, the files get encrypted with AES256 and saved in the Cloud database. The specialty of Sealed Cloud is, the not a general key, but a single key for every file is used. This key is created from log-in credentials and non-permanent features of the user and not known to the Cloud service provider. After creating the key, these user related data is deleted. When the session is finished, also the individually created key is deleted from the system.

While data is processed on the application server, it is in an unencrypted state. If a maintenance engineer has to work on the application server the data is first saved in the encrypted database and deleted in the application server. This clean-up procedure is realized in the following way:

First an authorized "Trust Center" has to send a work order with a valid access token to the Bluetooth device of an employee [16]. This token opens the lock on a physical box around the server computer, the so called rack. This maintenance engineer requests access to the particular server over its Bluetooth interface. All current sessions on the applications server are closed, the deleting process is started and the machine is rebooting. Only after completely transporting all application data out of reach, the access for the maintenance engineer is granted. Additionally there is a mechanism which takes care that no manipulations are possible while the maintenance of the system. A Trusted Platform Module (TPM) only allows the system to boot if there have been no manipulations since the last use of the certified software, operating system or the hardware components. Hence, the TPM serves as the root of a Chain of Trust. There is also a monitoring while the system is active – if there is a difference of the of the normal performance the particular components are switched off. In case of authorized access to the rack, the system also immediately stops all operations and shuts down, whereby the unencrypted data in the volatile memory is deleted. An external auditing company e.g. TÜV IT is monitoring the whole process to ensure it works the way it is supposed to be. The operating system used is not accepting any incoming commands – it only sends outgoing status reports, but there is no traffic possible the other way around. Sealed Cloud not only averts unauthorized access to the payload, but also the meta data like connection data. The project is still on till September 2014.

4.2.1 Web Privacy Service idgard based on Sealed Cloud

The Sealed Cloud infrastructure is implemented in the Web Privacy Service IDGARD from Uniscon (universal identity control GmbH) [8]. It is possible to integrate IDGARD with an add-on to common web browsers. It is designed for the secure exchange of data between business partners. It can be used as a Cloud storage system, with data transmitted to and stored at the Cloud server as described above. If a user wants to share data, he is able to give another user access to a so-called "Private Box" via a hyperlink. Over the hyperlink there is also a one-time-access possible, after this the Private Box is

sealed again. The user has to initiate a new share then, to enable a renewed access to his Private Box. There is also an email option using those Privacy Boxes, with the possibility of sending attachments over IDGARD.

A trial use shows that there is no way of distribution of the hyperlinks to the Private Boxes integrated in IDGARD. It is only possible to send them over email, the costumer has to rely on the confidentiality of the email transfer. There is no way of monitoring which persons have access to the Private Box over the hyperlink. It is only possible to examine the number of previous accesses and to limit accesses quickly in case suspicion of unauthorized access. However, there is no means of version control, so the Private Box owner has no transparency, what change has exactly happened to the data and when it took place.

IDGARD contains also a proxy option for browsing, which masks IP address and HTTP header, allowing the users pseudonymous visits of websites. Further, Sealed Cloud can securely host user names and passwords safely, to provide for convenient and secure online authentication. Uniscon claims to have no knowledge about connection and user data of its own, because it is stored encrypted. Uniscon only provides the SSL connection between Cloud user and Sealed Cloud. The data is saved with a transportation key on the Cloud server. However, with this key it is not possible to open the data. Yet the keys to the data is kept at a notary who has to pass further requested data of law enforcement agencies. This concept is called "Sealed Freeze" and it is patent pending by Uniscon.

4.3 SkIDentity

A considerable added value of Cloud computing applications is, that they create a considerable increase of flexibility [7]. Employees are able to access data or IT services from bureaus all over the world, at home and while traveling. With the enlarged possibilities of access, also increases the risk of unauthorized access – so authentication is an important topic to be addressed. While also the "Bundesamt für Sicherheit in der Informationstechnik" (BSI) recommends strong authentication mechanisms, a lot of Cloud services still only use username and password for logging in [9]. SkIDentity is a tool aiming at secure authentication. The core of its infrastructure is an eID-Broker who redirects a user two different existing authentication services. The selection criterion dependent on the requirements of the Cloud service provider. SkIDentity is using electronical identity cards (e.g. eGK, eID) for authentication. Therefore it is necessary, that the applied clients support eCard-API-Frameworks (BSI-TR-03112). "Open eCard App" as well as "AusweisApp" of the German "Bund" are deployed. The eID-Broker is supposed to support two different modes of operation in the longer term: the "Dispatcher mode", where it just functions as dispatcher which chooses the appropriate authentication service. The more complex mode of operation is the "Claims Transformer Mode". In this mode the eID-Broker merges authentication results and attributes from different authentication services into a format that the cloud service is able to process. The credentials created by the eID-Broker can be only for temporary use or they can be used for a longer period. The temporary variant is called "Session Credential," it can be an assertion like SAML or OpenID-Assertion which has a short time to live and is presented directly to the Cloud service provider. The long-term variant is called Attribute Based Credential (cf. Idemix, U-Prove, BBC08) and can be used autonomously by the Cloud service user for later sessions. These tokens only reveal as much information to the Cloud service providers as needed [10].

The SkIDentity project works on a common interface for existing interfaces e.g. BSI-TR-03130, STORK-API, in that different eID and authentication services can be integrated later and used together. While the current situation is that there exist a lot of strongly varying authentication services, it is the vision of SkIDentity to create a standardized infrastructure for authentication means. Therefore the relevant international standards are identified and integrated in one reference architecture together with new developed authentication services. The project is running till March 2015 [7].

5 OMNICLOUD

After revealing essential flaws in existing Cloud service solutions (as discussed above), the Fraunhofer Institute for Secure Information Technology (SIT) elaborated a Cloud solution of its own, that should solve existing problems. "OmniCloud" is a concept for Cloud computing which avoids unwanted dataflow from the Cloud [22]. The idea of OmniCloud is to connect arbitrary backup and application software to Cloud storage services. It is not necessary to install OmniCloud on a terminal device, it represents itself more like a network drive or a FTP-server to the user. OmniCloud supports various standard communication protocols used by different operating systems.

OmniCloud first encrypts data locally in the company network before transmitting it to the Cloud Server. The keys for encryption are generated in a pseudo random way by a Key Management Component. Every file is encrypted with a separate key by the Encryption Component. The needed keys are generated in the company network and are not known to the Cloud service provider. OmniCloud uses a secure key manager, which stores the key for encryption and decryption in a local database. Those keys are stored separately from the meta data e.g. file names, location which are also stored in this database. For the storage of the keys the Key Management Component is used, which encrypts the keys with an ID as meta information. This ID has to presented for decryption by the Key Management Component together with the

corresponding key. The Decryption Component then decrypts the file using this key. The Key Management Component supports various standard ciphering methods and it is also possible to encrypt different files with different ciphering methods. Thus, companies are able to change ciphering methods every now and then and it is possible to use the new ciphering methods successively, instead of having to decrypt and encrypt again all files at one time.

Not only the file contents are encrypted but also the file names and the structure of the file directory is disguised. The files are renamed by random generated file names and file extensions are removed. The file directory structure is completely changed by OmniCloud – so no internal or external attacker at the Cloud storage provider is able to draw conclusions from the file names and structure about the file content. For the distribution on the different Cloud storage providers there can be chosen from different storage strategies. It is possible, for instance, to store the same data at several different places -locally and at Cloud Storage providers- to increase redundancy ("mirroring"). Another variant is building a big Cloud memory consisting of different small Cloud memories. OmniCloud supervises the filling levels of each Cloud memory and decides then where to store new data.

OmniCloud is based on a trust model strictly separating into local company network and the Cloud provider. The Cloud provider only processes data which was encrypted independently from the Cloud applications. OmniCloud functions as an Enterprise-gateway in form of network appliance or a server. If a customer wants to access the OmniCloud gateway mobile, he has to connect over a VPN connection. To access the OmniCloud network there is an authentication necessary, credentials are distributed to entitled users. Admins have credentials themselves with whom they are able to start the key management component which is secured additionally. If someone loses his credentials, those are locked and new credentials for the concerned persons are generated. The OmniCloud user authenticates at the Input Module of the OmniCloud service e.g. the FTP-server, the input module then connects to a core component of the OmniCloud-Gateway, the Identity Management Component which is responsible for authorization. The Identity Management Component is able to map Input Module identities to OmniCloud identities. To simplify this process, the Identity Management Component can be connected via an IDM-adapter to the central identity management component of the company. The Identity Management Component sends its calculated information back to the Input Module. The Input Module then sends a request to another OmniCloud core component: the Access Control Component. OmniCloud uses role-based access control – for every single OmniCloud service it is possible to determine which user is allowed to do which operation on which single file. It is possible to create access rules of different granularity for every OmniCloud service and also to realize complex access rules using dynamic context constraints. The Access Control component sends the result of the access rules decision back to the Input Module. Access rules are defined by ORKA-Policy-Language (OPL).

The anchor principle of OmniCloud is the strict separation of identity, access and key management [23]. This is especially important for dynamically changing teams like they are typical today. If e.g. key-management and identity management are combined, the revocation of an role linked to access privileges is connected to the necessity of a whole re-encryption of concerning files. If an employee uses his privileges at the OmniCloud system, his credentials are revoked and he is no longer able to access files. This does not concern any other employee, as it would be the case with a shared password for instance. With the concept of OmniCloud employee absences or changes in responsibilities are flexible to handle. The product OmniCloud will be released in spring 2014.

6 CONCLUSION

In [11], the authors claim, that "in order to enable companies in Germany the secure usage of Cloud/Inter-Cloud-Computing technologies while maintaining economical advantages a holistic IT-security-architecture is needed, which is ideally already at the time of design an integral component of the overall concept ("Security by Design")". Unfortunately, often security means are traded secondary, yet it is quite difficult to impossible to implement them afterwards.

Being a new technology, at first Cloud service providers came up with own solutions, how to address security concerns properly from their point of view. Companies were confronted with various offerings, which were rather confusing and not inspiring confidence. Projects like SkIDentity aim on creating uniformly protocols and interfaces, which provide the basis for Cloud computing standards. If there exist some approved standards it is more likely, that Cloud computing services are trusted more and by this are able to become accepted broadly.

It is a good concept to distribute (meta-)data between different locations as used at MimoSecco or OmniCloud. As a consequence, the risk of external attacks is decreased, because not all data is concentrated at one location. It also decreases the risk of internal attacks, because not all privileges are concentrated at one Cloud provider, but spread to different ones. As the study by CapGemini [21] evaluated, there will be no growth in usage of Public-Cloud services as long as specific security concerns remain unsolved. So it is inevitable to research useful solutions for a secure usage of Cloud computing. While some security leakages still have to be fixed, as observed by IDGARD, the projects by BMWi and Fraunhofer SIT have the potential of setting new standards concerning Cloud services protecting data privacy.

References

[1] “Aktionsprogramm Cloud Computing – Eine Allianz aus Wirtschaft, Wissenschaft und Politik” - Publikation des Bundesministeriums für Wirtschaft und Technologie, 10/2010

[2] “Cloud Computing – Web-basierte dynamische IT-Services”, C.Baun, M.Kunze, S. Tai, Springer-Verlag Berlin Heidelberg 2010, 2011

[3] “An Efficient and Secure Dynamic Auditing Protocol for Data Storage in Cloud Computing”, Kan Yang with Xiaohua Jia, IEEE 6

[4] “SIT technical reports – on the security of cloud storage services”, Fraunhofer Institute for Secure Information Technology, 03/2012 8

[5] c´t 16/2013, S. 122 “Schlüsselkasten – Daten bei Dropbox, Skydrive&Co verschlüsselt speichern”, Jörg Wirtgen 9

[6] “User Awareness and Policy Compliance of Data Privacy in Cloud Computing”, Uwe Röhm, Audrey Mei Yi Quah AWC 2013 10

[7] „Trusted Cloud – Innovatives, sicheres und rechtskonformes Cloud Computing“, BMWi, 10/2012

[8] “Sealed Cloud – A Novel Approach to Safeguard against Insider Attacks”, Hubert A. Jäger, Arnold Monitzer, Ralf O. G. Rieken, and Edmund Ernst
Uniscon, universal identity control GmbH, Agnes Pockels-Bogen 1, 80992 Munich, Germany

[9] “Vertrauenswürdige Identitiäten für die Cloud”, Dr. Detlef Hühnlein, Johannes Schmölz (Fraunhofer Gesellschaft), Beitrag und Vortrag im Rahmen des „Smartcard Workshop 2012“, 2012

[10] „Eine Referenzarchitektur für die Authentisierung und elektronische Signatur im Gesundheitswesen“, Detlef Hühnlein, Johannes Schmölz, Tobias Wich, Benedikt Biallowons, Moritz Horsch, Tina Hühnlein, Beitrag und Vortrag zu GI-GMDS-Jahrestagung 2012, GI-LNI, Braunschweig

[11] “Inter-Clouds: Einsatzmöglichkeiten und Anforderungen an die IT-Sicherheit”, Gabi Dreo Rodosek, Mario Golling, Wolfgang Hommel, Alexander Reinhold, 2012

[12] Zimory Public Cloud Marktplatz: www.zimory.de

[13] Amazon Web Services: aws.amazon.com

[14] "Das Gütesiegel für die Cloud: EuroCloudStarAudit SaaS", EuroCloud Deutschland_eco e.V.: http://www.saas-audit.de/files/2011/01/EuroCloud-Star-Audit-SaaS-PK-.pdf
(accessed on: 15.10.2013)

[15] Lieberman Software's "2012 Cloud Security Survey", conducted at the 2012 Cloud Security Alliance Congress: http://www.liebsoft.com/cloud_security_survey/
(accessed on: 13.10.2013)

[16] "Sealed Cloud – Compliance durch versiegelte Cloud": http://trusted-cloud.de/de/1639.php
(accessed on: 22.12.2013)

[17] “Wer liest alle meine Daten in der Wolke? Wie Vertraulichkeit von Daten beim Cloud Computing möglich ist”, Gunther Schiefer in Online-Themenspecial Cloud Computing 2012: http://www.sigs.de/publications/os/2012/Cloud/schiefer_OS_Cloud_12.pdf
(accesssed on: 21.12.2013)

[18] “Wuala - Der sichere Cloud-Speicher - Backup. Sync. Teilen. Zugreifen.”: http://www.wuala.com/de/

[19] “DER WEG ZUR ENTERPRISE-CLOUD”, Prof. Dr. Andreas Heberle, Prof. Dr. Rainer Neumann, Fakultät für Informatik und Wirtschaftsinformatik Hochschule Karlsruhe – Technik und Wirtschaft in “Anwendungen und Konzepte der Wirtschaftsinformatik” 01/2013

[20] “Sicherheitsempfehlungen für Cloud Computing Anbieter (Mindestsicherheitsanforderungen in der Informationssicherheit)”, BSI 2011

[21] Capgemini. Studie IT-Trends 2012. Business-IT-Alignment sichert die Zukunft: http://www.de.capgemini.com/insights/publikationen/it-trends-2012/
(accessed on: 26.12.2013)

[22] “Whitepaper OmniCloud –Sichere und flexible Nutzung von Cloud-Speicherdiensten”, Thomas Kunz, Ruben Wolf, SIT 2013

[23] “Sichere Nutzung von Cloud-Speicherdiensten - Wie die Trennung von Identity-, Access- und Key-Management für mehr Sicherheit und Flexibilität sorgt”, Lukas Kalabis, Thomas Kunz, Ruben Wolf in Datenschutz und Datensicherheit - DuD August 2013, Volume 37, Issue 8