HAL
archives-ouvertes.fr

The Infrastructure Level of Cloud Computing as a Basis for Privacy and Security of Software Services

Ina Schiering, Jan Kretschmer

▶ To cite this version:

Ina Schiering, Jan Kretschmer. The Infrastructure Level of Cloud Computing as a Basis for Privacy and Security of Software Services. Jan Camenisch; Bruno Crispo; Simone Fischer-Hübner; Ronald Leenes; Giovanni Russello. 7th PrimeLife International Summer School (PRIMELIFE), Sep 2011, Trento, Italy. Springer, IFIP Advances in Information and Communication Technology, AICT-375, pp.88-101, 2012, Privacy and Identity Management for Life. <10.1007/978-3-642-31668-5_7>. <hal-01517597>

HAL Id: hal-01517597
https://hal.inria.fr/hal-01517597

Submitted on 3 May 2017

HAL is a multi-disciplinary open access archive for the deposit and dissemination of scientific research documents, whether they are published or not. The documents may come from teaching and research institutions in France or abroad, or from public or private research centers.

L'archive ouverte pluridisciplinaire **HAL**, est destinée au dépôt et à la diffusion de documents scientifiques de niveau recherche, publiés ou non, émanant des établissements d'enseignement et de recherche français ou étrangers, des laboratoires publics ou privés.

Distributed under a Creative Commons Attribution| 4.0 International License

The Infrastructure Level of Cloud Computing as a Basis for Privacy and Security of Software Services

Ina Schiering[1] and Jan Kretschmer[2]

[1] i.schiering@ostfalia.de
[2] j.kretschmer@ostfalia.de

Abstract. An important basis for cloud computing are public IaaS cloud services as offered e.g. by Amazon, Rackspace, VmWare. Since IaaS cloud services are often used as a flexible infrastructure for SaaS cloud services, it is important to investigate IaaS cloud services as a basis to realise regulatory requirements in cloud computing, e.g the European Data Protection Directive and the E-Privacy Directive. In this context a prototype of an IaaS cloud service is presented which serves as a basis for software services (e.g. SaaS services) compliant with these European Directive. This is achieved by a combination of organisational, and technical measures accompanied by auditing and monitoring.
Keywords: cloud computing, privacy, security, IT service management, auditing

1 Introduction

Cloud computing is an important trend towards standardisation and industrialisation of IT services. It is a further development of paradigms as virtualisation and utility computing as stated by Armbrust et al. [1] and offers flexible, scalable IT services with a usage based price model. In this paper the service model Infrastructure as a Service (IaaS) is investigated. See the National Institute of Standards and Technology (NIST) [2] for a definition of cloud computing. The focus of the IaaS cloud service investigated here is the provisioning of virtual resource sets as indicated by Lenk et al. [3](e.g. Amazon EC2, Eucalyptus. OpenStack, etc.). This service is investigated in the form of a public cloud service, i.e. the cloud service is supposed to be provided by an external cloud provider for the general public.

The characteristics of cloud computing, especially the usage based price model and the flexible deployment model of public cloud services have great advantages, especially for small and medium sized enterprises. They avoid investment in hardware, data centres and need less trained IT specialists compared to a traditional IT infrastructure which is built and operated in-house. In particular they profit from the scalability of the service. Despite the economic advantages there are a lot of obstacles concerning the use of public cloud services in the area of security, privacy, availability and legal compliance as indicated by

Jansen [4], Chow et. al. [5] and the cloud computing risk assessment provided by the ENISA [6].

In this paper we focus on privacy requirements in public cloud services. Because of the complexity and broad range of cloud services it is important to start at the bottom of the cloud stack in the sense of Lenk et al. [3] with IaaS virtual resource sets. The organisation that provides the cloud service is the *cloud provider*. Cloud services are used by *cloud users*. It is an interesting approach to realise SaaS (Software as a Service) cloud services but also other IT systems based on IaaS and PaaS (Platform as a Service) cloud services, see e.g. the Amazon case studies [7], since the flexibility, scalability and the usage-based price model fit well to the requirements of these services.

This paper describes a prototype of an IaaS cloud based on the open source cloud stack Eucalyptus [8], see Nurmi et. al. for an overview of the architecture [9]. There privacy requirements based on the Data Protection Directive 95/46/EC [10] and the E-Privacy Directive 2002/58/EC [11] are investigated. The aim of this IaaS cloud service is to be a basis for IT systems in general or SaaS cloud services in particular where personal data is processed. There the IaaS service should serve as a basis for the IT system resp. SaaS service to be compliant with the Data Protection Directive and if applicable to the E-Privacy Directive. Examples for IT systems are Mail- and Calendar Servers, SAP Systems, examples for SaaS cloud services are Dropbox, Gmail, social communities, enterprise content management.

The approach investigated here is focussed on the IT operation of the cloud provider and uses a combination of automated procedures to avoid access to data where possible, encryption, accompanied by operational processes and auditing. Since concepts where encrypted data is processed like homomorphic encryption (see Gentry [12]) are not feasible yet, it is important to review alternatives. In the following, the adversary model and the legal requirements on the European level are summarised. Afterwards, the prototype as a basis for the considerations are presented. Then it is discussed how the requirements concerning privacy on the legal level could be achieved and what risks are still present.

2 Adversary Model

What are the implications when the data processing of an IT system or a SaaS service is transferred from a data centre of the service provider or a dedicated outsourcing company to an IaaS cloud provider? In general it is unclear where the data is operated. Since the cloud provider can itself use e.g. for peak load resources of other providers the data might be transferred to a third party. When data is operated by a cloud provider there is the risk of unauthorised access by personnel of cloud providers. Hence the *personnel of the IaaS provider* is an adversary to be analysed. This adversary is characterised by access to the physical hardware and administrative access to the operating system level of the systems, the software managing the cloud and the network layer. See the section about the prototype for details concerning the cloud technology stack.

Furthermore the data is not processed on dedicated resources, but resources are shared with other customers of the cloud service. The cloud provider has to ensure the separation between the data and services of different customers (multi-tenancy). Hence the second type of adversary are *other cloud users*. Instead of accessing data over a local network when it is processed in a local data centre, the data is accessed over the internet which leads to risks concerning network security and access control to services and data. The third type of adversary is therefore a *person with internet access*. A risk which is always present in IT systems is the risk inside the organisation of the user of the IT system or the SaaS service. There personell data could be processed for other purposes without consent of the data subject or also unauthorized access to data can happen if roles and responsibilities are not properly managed. Hence the fourth type of adversary is the *personnel of the user of the IT system resp. SaaS service*.

Concerning these four types of adversaries the focus in this paper is to investigate measures concerning the personnel of the cloud provider as an adversary. There we focus on the IT operation of the IaaS cloud. The risks inside the organisation of the users of an application are always present when IT systems are used and are therefore not specific for a cloud service. Also the issues with adversaries with internet access focus more on network security than on cloud computing. The adversary other cloud users is interesting in SaaS cloud environments. There especially in SaaS services very often the data of different cloud users is integrated in a common database. Hence multi-tenancy is realised in the application via identity management and access control. In this environment the role of other cloud users is interesting to evaluate. In an IaaS environment the risk reduces mainly to software bugs in the virtualisation layer resp. the cloud layer, where standard software is used. Hence for IaaS services the most interesting adversaries are the personnel of the IaaS provider which is investigated in this paper.

3 Technical Requirements derived from the Regulatory Framework

The regulatory framework concerning the processing of personal data in the European Union consists of the Data Protection Directive 95/46/EC [10] and e.g. concerning web services and services addressing mobile phones often additionally the E-Privacy Directive 2002/58/EC [11].

In the Data Protection Directive the basic roles which are used are the data controller and the data processor. In a general cloud computing environment, it is an intricate task to differentiate these roles. See Leenes [13] for a thorough discussion of this issue. The *data controller* is characterised in Article 2 (d) as the party that "determines the purposes and means of processing of personal data" and the *data processor* processes "personal data on behalf of the controller".

In the scenario of an IaaS cloud which is used to built SaaS cloud services or general IT systems for processing of personal data the provider of the IT system resp. SaaS service could be a data controller e.g. in the case of services directly

addressing users. Otherwise the provider of the service could also be a processor in the case that the service provided is a B2B (business to business) service, where the user of that service is e.g. a company that processes personal data, e.g. names, addresses and bank accounts of customers. There could be even more complex scenarios with respect to the roles of data controller and data processor. But in all cases the provider of the IaaS cloud is the data processor that processes personal data on behalf of another party.

In the following the Data Protection Directive and the E-Privacy Directive are investigated. Technical requirements for IaaS cloud services as data processors in the scenario described above are extracted and explained.

3.1 Requirements derived from the Data Protection Directive

The processing of personal data is in this paper restricted to personal data that does not belong to the special categories of data stated in the Data Protection Directive in Article 8 "personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, trade-union membership and the processing of data concerning health or sex life". Unless the fact that people disclose these data voluntarily in social networks and Internet forums, there is a higher risk associated with the processing of e.g. the health records in a hospital compared to the processing of customer addresses and payment details as needed e.g. for a web shop. For the processing of these categories of data it would be advisable to use an internal system or at least a community cloud to reduce the risk. The measures described in this paper have the intention to reduce the risk concerning the processing of standard personal data as described above with "a level of security appropriate to the risks represented by the processing and the nature of the data to be protected" as it is described in the Data Protection Directive Article 17, 1.

In Section I "principles relating to data quality" Article 6 (b), (d) demands from a technical perspective that data is only processed for legitimate purposes and that data can be rectified and erased. Similar requirements result from Article 12 (a), (b) "right of access", where the data subject has the right that the data controller communicates "an intelligible form of the data undergoing processing" and the right of "rectification, erasure and blocking of data". Even if in Article 12 only the data controller is addressed, the data controller would need to demand appropriate requirements from the data processor in form of a contract, even if the data processor is not addressed in the Directive. The obligation for such a contract is mentioned in Article 17, 3. These requirements are mainly to be fulfilled on the database and application layer since data is stored in the form of databases and hence these requirements can only be realised there. The only requirement that needs to be realised on the IaaS layer is *(1) deletion of all data when virtual instances are no longer needed.*

The next group of requirements are addressing confidentiality and security of processing. In Article 16 concerning the confidentiality of processing the data controller and data processor are directly addressed "any person acting under the authority of the controller or of the processor, including the processor himself,

who has access to personal data must not process them except on instructions from the controller". Hence *(2) access to personal data has to be restricted and processing of data must be controlled* by every party involved in data processing and therefore also by the IaaS provider. Concerning the security of processing in Article 17, 1 the data controller is obliged to "implement appropriate technical and organizational measures to protect personal data against accidental or unlawful destruction or accidental loss, alteration, unauthorized disclosure or access ... and against all other unlawful forms of processing". Article 17, 2 states that "the controller must, when processing is carried out on his behalf, choose a processor providing sufficient guarantees in respect of the technical security measures and organizational measures governing the processing to be carried out, and must ensure compliance with those measures". These requirements must according to Article 17, 3 be "governed by a contract". The IaaS Provider has to ensure *(3) personal data has to be protected against accidental or unlawful destruction or accidental loss, alteration, unauthorized disclosure or access* and *(4) compliance according to the technical and organisational measures has to be ensured.*

The last technical requirement that can be derived from the Data Protection Directive is based on Chapter IV "transfer of personal data to third countries". Hence the IaaS cloud provider must allow *(5) restrictions concerning the location of processing.* This has to be combined with a check concerning the legislation of the country where the provider resides. An example for this issue is the Patriot Act as mentioned e.g. in the data use limits of Microsoft Online Service [14].

3.2 Requirements derived from the E-Privacy Directive

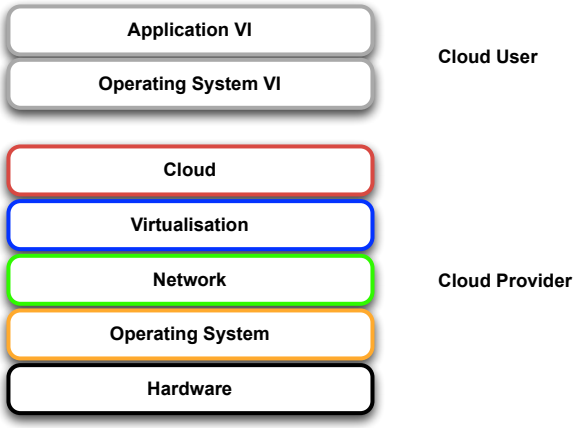
The E-Privacy Directive addresses providers of public communication services. Similar to the Data Protection Directive in Article 4, 1 "the provider of a publicly available electronic communications service must take appropriate technical and organisational measures to safeguard security of its services" which is amended in Article 4, 1(a) (according to the amendment 2009/136/EC) such that the measures "shall ensure that personal data can be accessed only by authorised personnel for legally authorised purposes" and "protect personal data stored or transmitted against accidental or unlawful destruction, accidental loss or alteration, and unauthorised or unlawful storage, processing, access or disclosure". There also the "implementation of a security policy with respect to the processing of personal data" is demanded. If the service provider employs an IaaS cloud service the requirements (2), (3) and (5) from the section about the Data Protection Directive should be fulfilled to build a communication service which is compliant. From the implementation of the security policy further requirements concerning the IaaS cloud provider may arise which could not be described on this general level.

Additionally, in Article 4 there are regulations concerning data breaches where there exists in the amendment 2009/136/EC Article 4.3 the possibility instead of informing the users about data breaches apply technological measures that "shall render the data unintelligible to any person who is not authorised

to access it". There in the realisation of the communication service appropriate encryption has to be employed. This has to be done at the application and database layer. Also encryption at the file system level is done inside the operating system in the virtual instance and is not in the responsibility of the IaaS provider. The provisions of Article 5, 1 "prohibit listening, tapping, storage or other kinds of interception of communications and the related traffic data by persons other than the users, without the consent of the users allowed" and of Article 6 concerning traffic data need to be realised already at the application level. There concerning the deletion of traffic data it would be advisable that the IaaS provider fulfils requirement (1) deletion of all data when virtual instances are no longer needed. Also Article 8 and 9 address technical requirements concerning the communication service, but all these requirements need to be realised by the applications of the communication service.

4 Prototype

The prototype described in this paper is an IaaS cloud service based on the open source cloud stack Eucalyptus [8]. Eucalyptus is a mature cloud computing stack which is widely used and e.g. integrated in the Ubuntu Linux distribution. Eucalyptus uses Xen [15] as a virtualisation layer and VDE (Virtual distributed Ethernet) [16] for the realisation of virtual network connections.



The cloud provider is responsible for the technology stack from the hardware up to the cloud layer which is in the case of this prototype Eucalyptus. The cloud user is responsible for the operating system of the virtual image and for the application. In the context of the European Data Protection directive it is important to be able to impose restrictions concerning the locations where data is processed. There Eucalyptus offers the concept of a cloud which consists of several clusters representing different locations. Clusters are a concept similar to Amazons availability zones. Each cluster is controlled by a cluster controller (CC)

and manages a group of assigned node controllers (NC), where virtual instances for cloud users are generated. The whole cloud infrastructure is controlled by the cloud controller (CLC).

The IaaS technology stack consists of the hardware, the operating system, the network, the virtualisation and the cloud layer. The cluster and cloud controller communicate with the virtual instances over a virtual private network. Via another virtual network connection also the public network connection to the virtual instance is realised. Therefore the virtual instances are already adequately separated from other instances apart from bugs in Xen or VDE. Hence the role of other cloud users as adversaries would be interesting with a focus on security issues of the technology stack. The access to the virtual instances is controlled via a public-key infrastructure. Only the cloud user and the cluster controller for internal purposes can access the virtual instance over the cloud infrastructure. But with root access to the operating system of the node controllers the administrators of the cloud provider can also get access to the virtual instances.

Santos et al. [17] investigated how virtual machines can be protected against the administrators of the cloud provider under the assumption that the administrator has root access to the system. They propose an approach using TPM technology (Trusted Platform Module). In contrast to this approach which makes assumptions about the hardware platform of the cloud service, it is investigated here how this can be accomplished via automated procedures and operational processes accompanied with an approach for monitoring and auditing.

5 Technical and Organisational Measures Addressing the Requirements Identified

In the section about legal requirements there were 5 requirements derived concerning an IaaS cloud service as data processor:

(1) Deletion of all data when virtual instances are no longer needed
(2) Access to personal data has to be restricted and processing of data must be controlled
(3) Personal data has to be protected against accidental or unlawful destruction or accidental loss, alteration, unauthorized disclosure or access
(4) Compliance according to the technical and organisational measures has to be ensured
(5) Restrictions concerning the location of procession

Requirement (5) is already fulfilled by the prototype. The other requirements are addressed by the following approach: The operation of a cloud is a highly industrialised form of IT operation. Therefore most operational tasks should be accomplished in the form of automated procedures. The tasks where this is not possible must be organised with the help of processes. Hence administrative access to the system in general is only needed in very restricted situations. The normal operation of the cloud should need no administrator interaction. The

focus of the work of administrators is to develop, test and maintain automated procedures. These automated procedures are transferred to the production in form of a change or the deployment of a new release.

All tasks must be controlled via monitoring to allow for regular audits. The Federal Office for Information Security in Germany (BSI) recommends to use an IT service management framework as ITIL or CoBIT in their recommendations for cloud computing providers [18] as a basis for ISO 27000 resp. IT-Grundschutz. Hence we assume that the IT operation of the cloud service is implemented according to the IT Infrastructure Library (ITIL) which is a best practice framework for IT service management. See [19] concerning notions of IT service management according to ITIL. We claim that through the following technical measurements, where this is not possible organisational measurements accompanied by auditing an IaaS cloud provider fulfils the above named requirements. That means that associated risks are reduced in an adequate manner.

(T) Technical measurements
  (T1) Automated procedures
  (T2) Restrict privileged access to the system where possible
(O) Organisational measurements
  (O1) IT service management (especially change management is important)
  (O2) Four-eyes principle
  (O3) Segregation of duties
  (O4) Software engineering methodologies (e.g. model driven development)
(A) Auditing
  (A1) Logging
  (A2) Cryptographic measures (e.g. checksums)
  (A3) Monitoring, automated auditing

In the following operational tasks of the cloud provider are investigated. Since for cloud computing it is important to profit of the economy of scale it is assumed that a group of administrators of the cloud provider will be responsible for the IT operation of the cloud service. These are in the following named *administrators*. Because there are several administrators it can be assumed that a segregation of duties is possible.

What are the operational tasks to deliver virtual instances in form of a cloud service to cloud users? A short overview is given here. The detailed analysis follows afterwards. To build up the infrastructure administrators need to *add and remove systems*. For updates and patches it is necessary to *change systems*. Beside that it is needed to realise standard administrative tasks as *monitoring* of the whole technology stack, *backup* the node controllers. If needed, it must be possible to *restore* a system from the backup. In the case of an incident[1] *troubleshooting* has to be done. For the tasks add system and change system, images resp. packages have to be provided.

1. Add, remove systems

[1] An unplanned interruption to an IT service or a reduction in the quality of an IT service. [19]

2. Change systems
3. Monitoring, backup, restore
4. Troubleshooting

A. Provide image
B. Provide package

5.1 Add, Remove Systems

As an example for a system a node controller is used. What are the necessary steps to add a system (here a node controller is used) to the cloud infrastructure?

- **A change is initiated** with technical details as MAC address, the role of the system, i.e. node controller or cluster controller, etc.. The technical details can be extracted from the change for automated procedures described in the next steps and for *auditing* purposes.
- **The new system is placed in the data centre.** Because of the *segregation of duties* between the administrators it is assumed that an administrator that has access to the data centre do not has any other administrative access to the systems.
- **The system is installed.** This can be realised as an *automated procedure*. The MAC address is added to the DHCP configuration and the system is added to the configuration of the boot server. The system boots the designated image. The integrity of the image can be verified by the use of *checksums*.
- **Add the system to the cloud configuration.** This can be also realised with an *automated procedure*.

All steps in the above workflow beside the initial placement of the system in the data centre can be automated. Since the result of each step can be checked by comparing configuration files or by using commands for monitoring and can be documented in log files, the whole workflow can be checked against the initial change in an automated auditing process. In the following we describe how images which are needed also here can be realised in this model.

Provide Image An important step to build up the cloud infrastructure are operating systems images. An *image* is a collection of software packages accompanied by configuration changes. They are needed in the task add system for node controllers and cluster controllers. beside that the cloud provider has to provide operating system images for the creation of virtual images by cloud users. Also a special image is needed to delete all data of a virtual instance after the cloud user has finished to use it according to Article 12 (b) of the Data Protection Directive. To provide an image the following steps need to be performed:

- **Plan image** Select packages and plan configuration changes, document the image. This step can only be checked by the *four-eyes principle* and should be documented in the form of a change.

- **Build image** This can be realised by an *automated procedure* based on the documentation. The images is built from packages which are provided from a central repository. The checksums of the packages can be used for verification.
- **Test the image with respect to the documentation** An install of the image is provided and the result is tested against the initial documentation with the help of tools to analyse the system.
- **Create checksum** *(automated procedure)*
- **Deploy image on boot server** *(automated procedure)*
- **Regularly check the integrity of the image by verifying the checksum** *(automated procedure)*

For the tasks which cannot be automated, the risk can be reduced by using the four-eyes principle and by relying on the segregation of duties, i.e. that the person that plans an image does not perform the checks. These elements can be assured via rigorous application of change management. It now has to be explained how the basic building blocks for images, the packages, could be realised in this model.

Provide Package Packages are the basic building blocks of operating system images. Most packages used to build up images are standard software packages as e.g. MySQL, package consisting of system utilities, etc. But a package can also consist of individual software as e.g. a collection of scripts. Similar to the creation of images, the package is planned. But afterwards the software needs to be implemented which is a *manual process* where the risk can only be reduced by rigorous software engineering methodologies. An important approach there is model driven development (see France and Rumpe [20] for an overview) where the aim is to generate code from a model, e.g. in UML or SysML. This approach is often used for embedded systems. Then as before a checksum is created and the package is deployed to the repository. The integrity of the package can be verified by an automated procedure on a regular basis.

5.2 Change Systems

In contrast to standard IT operation a system is in this industrialised form of cloud computing only changed in form of an update. This can be a *minor update* where only some updated packages have to be integrated and a reboot is not needed or in the form of a *major update* where the whole image is changed. Hence the case of a major update is already described in the task *add, remove system* where also a new image is installed.

5.3 Monitoring, Backup, Restore

The standard tasks monitoring, backup and restore are usually realised in an automated way. For backups of systems access restrictions have to be realised

and restore processes need to be confirmed by a change since a restore should normally not occur in a cloud service providing virtual instances. There the measures for availability should be focussed.

5.4 Troubleshooting

This is beside software development the task where manual intervention is needed. But manual intervention can be accompanied by the four-eyes principle and logging of all administrative actions. Based on these logs the operation can be reviewed afterwards. With these procedural measures it is possible to reduce the risk.

5.5 Auditing

The documentation of the processes and the log files of IT operations are a basis for auditing. In the prototype process mining according to van der Aalst [21] is used for auditing. This is an approach where log files and other data can be after the transformation to the XML file format XES used as a basis for auditing purposes. These measures can be complemented with an audit of the cloud service focusing on privacy, e.g. a Privacy Impact Assessment of the Information Commissioners Office in the UK [22] or the European Privacy Seal [23]. In [24] a tool based approach is proposed for PIAs in a cloud computing environment.

A different approach proposed by Neisse et.al [25] is to use a cloud certification system based also on TPM that detects unintended or malicious modifications of the cloud infrastructure It guarantees to service providers at runtime the detection of unintended or malicious modifications of cloud infrastructure configurations.

6 Remaining Risks

Several administrative tasks as *provide OS images*, *implementation of automated procedures* and also *update systems* are based on software which is implemented resp. selected and configured by the cloud provider. Change management and release management processes can only reduce the risk that someone tries to manipulate code or that software has vulnerabilities.

But because of the standardised cloud architecture software resp. hardware bugs and errors in configurations have greater impact (e.g. the Amazon EC2 and Amazon RDS Service Disruption in the US East Region [26]). To reduce the impacts it is possible to use cloud services that employ different technologies or an intercloud where this is realised. But there the problem is that most cloud providers do not disclose their technology since it is their intellectual property.

Another risk is that in the case of troubleshooting no access restrictions can be applied. The risk is reduced by logging actions and the four-eyes principle, but it is not possible to avoid it in general.

In this paper the focus is on administrative roles. Hence attacks as e.g. Distributed Denial of Service attacks (DDoS) need to be addressed by additional measures. Another risk that needs to be accounted for is governmental access to data. E.g. companies from the U.S. are giving government entities access to user data based on legal requirements based on the Patriot Act, even if it is stored in Europe. This is documented for example in the data use limits of Microsoft Online Service [14].

7 Related Work

There are already various approaches addressing security and privacy by proposing a trusted technology stack or the use of TPM (Trusted Platform Module) technology. The measurements for the administrative level could be combined with these approaches. Concerning the focus of security of IaaS cloud services Santos et al. [17] investigated how virtual machines can be protected against the administrators of the cloud provider under the assumption that the administrator has root access to the system. Here TPM is used. On the other hand, the cloud provider needs assurance about the integrity of the virtual machines and can provide this also as a service to cloud users. Christodorescu et. al. [27] propose for this aim an approach of secure introspection of virtual instances by cloud providers. Another approach which addresses security and privacy in cloud computing is from Doelitzscher et al. [28]. There a six-layer security model for cloud computing consisting of risk analysis, security guidelines, QoS monitoring, data encryption, logging, encrypted communication is proposed.

These approaches focus mainly on technical measures, which result in adaptation resp. development of new cloud management software. In the prototype presented here, we concentrate on existing technologies and use a combination of organisational, procedural and technical measures accompanied with an approach for auditing these measures to realise privacy requirements.

With a focus on SaaS cloud services Pearson et al. [29] investigated as example services sales data analysis, mining multiple databases, customized end user services and proposed a privacy manager software on the client as a central component. In [30] they used also a combination of a procedural and a technical approach to assure accountability for large organisations in a general cloud computing scenario. In the prototype investigated here additionally processes of IT service management and the possibilities to restrict access to the production environment by automation and further control by audits on the basis of log files are discussed.

8 Conclusion

In this paper a prototype for an IaaS cloud service based on a standard cloud stack is investigated with a focus on technical and operational measurements. Measures as the segregation of duties, automation of administrative tasks, IT service management processes, the employment of cryptography and auditing

are applied. These considerations concerning system operation are a basis for compliance with the Data Protection Directive 95/46/EC, resp. the E-Privacy Directive integrated in a more general concept based on ISO 27000 resp. IT-Grundschutz. Future work will be based on this prototype and extend the investigation to PaaS and SaaS cloud services. Another interesting direction for research is the composition of cloud services out of services of different cloud providers and the investigation of processes for data processing of cloud users incorporating cloud services.

References

[1] M. Armbrust, M. Fox, A. Griffith, R. et al. Above the Clouds: A Berkeley View of Cloud Computing. UCB/EECS-2009- 28, EECS Department, University of California, Berkeley, 2009. http://www.eecs.berkeley.edu/Pubs/TechRpts/2009/EECS-2009-28.pdf

[2] P.Mell, T. Grace, The NIST Definition of Cloud Computing (Draft), National Institute of Standards and Technology, January 2011, http://csrc.nist.gov/publications/drafts/800-145/Draft-SP-800-145_cloud-definition.pdf

[3] A.Lenk , M. Klems , J. Nimis , S. Tai , T. Sandholm, What's inside the Cloud? An architectural map of the Cloud landscape, Proceedings of the 2009 ICSE Workshop on Software Engineering Challenges of Cloud Computing, p.23-31, May 23-23, 2009.

[4] W.A. Jansen, Cloud Hooks: Security and Privacy Issues in Cloud Computing, Proceedings of the 44th Hawaii International Conference on System Sciences, 2011.

[5] R. Chow, P. Golle, M. Jakobsson, E. Shi, J. Staddon, R. Masuoka, J. Molina, Controlling data in the cloud: outsourcing computation without outsourcing control, Proceedings of the 2009 ACM workshop on Cloud computing security, 2009.

[6] Cloud computing risk assessment. European Network and Information Security Agency. November 20, 2009 http://www.enisa.europa.eu/act/rm/files/deliverables/cloud-computing-risk-assessment/at_download/fullReport.

[7] Amazon, Case Studies http://aws.amazon.com/solutions/case-studies/

[8] Eucalyptus, http://open.eucalyptus.com/

[9] D. Nurmi, R. Wolski, C. Grzegorczyk, G. Obertelli, S. Soman, L. Youseff, D. Zagorodnov, Eucalyptus: A technical Report on an Elastic Utility Computing Architecture Linking your Programs to Useful Systems, UCSB Computer Science Technical Report Number 2008-19, 2008, http://www.cs.ucsb.edu/research/tech_reports/reports/2008-10.pdf.

[10] Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data, http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:31995L0046:EN:HTML

[11] Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:32002L0058:EN:HTML

[12] Craig Gentry, Fully homomorphic encryption using ideal lattices, Symposium on the Theory of Computing (STOC), 2009, pp. 169-178.

[13] R. Leenes, Who Controls the Cloud?, In: 6th IDP Conference. Cloud Computing: Law and Politics in The Cloud [online monograph]. IDP. Revista de Internet, Derecho y Politica. No. 11. UOC, 2010.
[14] Microsoft Online Services, Data use limits, http://www.microsoft.com/online/legal/v2/?docid=23
[15] http://xen.org/
[16] http://vde.sourceforge.net/
[17] N. Santos, K.P. Gummadi, R. Rodrigues, Towards trusted cloud computing, HotCloud'09 Proceedings of the 2009 conference on Hot topics in cloud computing, 2009.
[18] BSI, Security recommendations for cloud computing providers, https://www.bsi.bund.de/DE/Themen/CloudComputing/Eckpunktepapier/Eckpunktepapier_node.html, 2011.
[19] ITIL IT Service Management-Glossary of Terms and Definitions, OGC, 2007, http://www.itsmfi.org/content/itil-v3-glossary-acronmys-pdf.
[20] R. France, B. Rumpe. Model-driven Development of Complex Software: A Research Roadmap. In 2007 Future of Software Engineering (FOSE '07). IEEE Computer Society, Washington, DC, USA, 37-54, 2007.
[21] W.M.P. van der Aalst. Process Discovery: Capturing the Invisible. IEEE Computational Intelligence Magazine, 5(1):28-41, 2010.
[22] Information Commissioners Office, Privacy Impact Assessment Handbook, 2009, http://www.ico.gov.uk/upload/documents/pia_handbook_html_v2/index.html.
[23] European Privacy Seal, https://www.european-privacy-seal.eu/
[24] D. Tancock, S. Pearson, A. Charlesworth, A Privacy Impact Assessment Tool for Cloud Computing, Proceeding CLOUDCOM '10 Proceedings of the 2010 IEEE Second International Conference on Cloud Computing Technology and Science IEEE, 2010.
[25] R. Neisse, D. Holling, A. Pretschner, Implementing Trust in Cloud Infrastructures, CCGrid 2011 11th IEEE/ACM International Symposium on Cluster, Cloud and Grid Computing, IEEE, 2011.
[26] Amazon, Summary of the Amazon EC2 and Amazon RDS Service Disruption in the US East Region http://aws.amazon.com/de/message/65648/
[27] M. Christodorescu, R. Sailer, D. L. Schales, D. Sgandurra, D. Zamboni, Cloud security is not (just) virtualization security: a short paper, Proceeding CCSW '09 Proceedings of the 2009 ACM workshop on Cloud computing security, 2009.
[28] F. Doelitzscher, C. Reich, and A. Sulistio, Designing Cloud Services Adhering to Government Privacy Laws, 2010 10th IEEE International Conference on Computer and Information Technology, 2010.
[29] S. Pearson, Taking account of privacy when designing cloud computing services, Proceedings of the 2009 ICSE Workshop on Software Engineering Challenges of Cloud Computing, p.44-52, May 23-23, 2009.
[30] S. Pearson, A. Charlesworth, Accountability as a Way Forward for Privacy Protection in the Cloud, Proceedings of the 1st International Conference on Cloud Computing, December 01-04, 2009.