Towards a Self-protecting Cloud

Anthony Sulistio[1] and Christoph Reich[2]

[1] Dept. of Service Management & Business Processes,
HPC Center Stuttgart (HLRS), Germany
[2] Cloud Research Lab, Hochschule Furtwangen University, Germany
sulistio@hlrs.de, rch@hs-furtwangen.de

Abstract. Small and Medium-sized Enterprises (SMEs) are the backbone of a nation's economy. In order to remain competitive and become a market leader in this globalization era, SMEs need to look into innovative IT solutions. One of these IT solutions is cloud computing, where it delivers Infrastructure, Platform, and Software as a Service (IaaS, PaaS, and SaaS) on a simple pay-per-use basis. Nevertheless, enterprises are sceptical about adopting the cloud, because of the risks involved in outsourcing services into the cloud.

To reduce the barrier for SMEs, this paper proposes a solution towards a two step service migration approach, 1) pre-defined Service-Level Agreement templates and 2) risk analyses, combined with a *self-protecting* cloud service that monitors, for example, the pre-defined privacy regulations and privacy protection measures.

Keywords: self-protecting, cloud, privacy.

1 Introduction

Cloud computing enables SMEs to avoid over-provisioning of IT infrastructure and training personnel to become experts in administration of IT infrastructures. Further, SMEs can take advantage of cloud computing if the IT capacity needs to be increased on the fly. This increase is typically needed for services which are only requested for a certain period of time. By leveraging cloud computing, SMEs can also reduce time to market for new products and services.

Although cloud computing provides the aforementioned advantages, SMEs are quite slow in adopting cloud solutions into their existing production system and/or migrating their applications to the cloud. Barriers towards the cloud are complexity of their services, integration problems, cloud specific Service Level Agreements as well as security and privacy concerns [1][2]. SMEs do not have the necessary resources and expertise in cloud migration and choosing which cloud technologies are most suitable for their needs [3]. Moreover, questions have been raised about the privacy of data stored in the cloud and how cloud providers could guarantee them, as stated in [4]. In [5], some of the identified privacy issues for cloud computing are data access, data breaches and data recovery. Businesses are responsible for the data that will be outsourced, and therefore must know the type of data to be outsourced (e.g., personal data, confidential data), the legal

R. Meersman et al. (Eds.): OTM 2013, LNCS 8185, pp. 395–402, 2013.

regimes their outsourcing providers are subject to, the risk of losing data and the quality of the outsourced service during the decision of outsourcing a service into the cloud. Gathering this information can be difficult and time-consuming, if the providers do not make public all the situations in which personal data is made available to government or law enforcement bodies (e.g., with respect to the US Patriot Act). The lack of clarity may prompt some companies to bring data back under their direct control.

To address these aforementioned problems, this paper contributes by introducing the following approaches. First, to reduce the barrier for service migration into the cloud a two stage migration strategy is introduced with a) pre-defined Service-Level Agreement (SLA) templates and b) a risk analyses. Second a *self-protecting* cloud service monitors the specified privacy issues and privacy protection measures.

The rest of this paper is organized as follows. Section 2 mentions the related work. Section 3 describes the cloud migration strategy in details, whereas Section 4 explains the self-protecting cloud service. Finally, Section 5 concludes the paper and provides future works.

2 Related Work

This section first starts with the privacy-related standards, regulations, and policies. Then, this section discusses papers stating important issues of privacy if services are outsourced, and presents an overview of a privacy preserving in cloud computing.

There are several legislations for data protection that need to be considered, which depend on the data domain, and the countries of the cloud customer and the cloud provider are based on. The US takes a sector-based approach (e.g. Children's Online Privacy Protection Act (COPPA) or Health Insurance Portability and Accountability Act (HIPPA)), whereas in Asian countries like Singapore, Hong Kong, and Malaysia case-based emerging laws are relevant. Other countries like Canada and Argentina have their own special data protections laws. There are many similarities among these laws due to the OECD guidelines [6] on these issues.

The longest established and strictest data protection laws in effect are the one enacted by the European Union (EU). The Data Protection Directive 95/46/EC [7] applies throughout the EU. Currently at the time of the writing, the European Commission works on a proposal for a General Data Protection Regulation [8], that is likely to take until 2016. One of the key themes of the proposed regulation is accountability (i.e., taking responsibility for your data processing), the right to be forgotten, notification of data breaches to the regulators and data protection officers for SMEs that employ more than 250 people.

According to Sotto et al. [9], storing data in the cloud may elicit various federal and state privacy and data security law requirements, such as US HIPPA and EU Data Protection Directive. For example, Articles 25 and 26 of the EU Data

Protection Directive prohibit transfers of personal data to countries outside of European Economic Area (EEA), unless these countries have an adequate level of data protection [10]. Thus, privacy and data security laws present a significant challenge for cloud providers to comply with. As a result, the cloud providers are unable to provide SMEs with an assurance.

Betge-Brezetz et al. [11] proposes a solution where cloud users enabled to control their data storage, processing and movement in the cloud. The approach is based on a paradigm of sticking policies to data and encapsulating sensitive information in a Privacy Data Envelope (PDE) structure before uploading it in the cloud.

A general discussion about privacy issues can be found in [12], where the main privacy issues in data outsourcing are addressed, ranging from data confidentiality to data utility. It is also illustrated which main research directions are being investigated for providing effective data protection to externally stored data and as well as how to enable querying on such data.

Recently, there have been several publications discussing data privacy in relation to cloud storage. Joseph et al. [13] discuss key privacy issues in the context of cloud computing, and analyze the various works being done to solve the issues in privacy, in order to ensure privacy of outsourced data on cloud storage. Anil et al. [14] survey and compare different types of techniques used to enhance the security of data stored in cloud environment.

There are several different approaches addressing the privacy-preservation problem. Sayi et al. [15] tackle the issue by proposing a vertical fragmentation to a relation, where the fragment that is assigned to the cloud server contains maximum data without violating privacy. Privacy is expressed in terms of a set of confidentiality constraints and represented as a graph where the nodes are the attributes and the links represent paired confidentiality. With the graph coloring approach, the amount of data stored and/or the workload at the data owner such that there is no violation of data confidentiality is minimized.

On the other hand, a privacy-preserving access control mechanism is proposed by Jiazhu et al. [16] to provide a guaranteed secure access to outsourced data while preserving privacy of access control policies and users IDs.

Wang et al. [17] states requirements for secure third party auditor: 1) the auditor should be able to efficiently audit the cloud data storage without demanding the local copy of data 2) the auditing process should bring in no new vulnerabilities towards user data privacy.

3 A Cloud Migration Strategy

From the related work complex issues regarding data privacy and protection arise, which significantly hinder the cloud adoption rate by SMEs. In order to reduce the barrier for adopting and migrating applications to the cloud, a two-stage migration strategy is proposed. In the first stage the customer can choose from domain specific Service-Level Agreement (SLA) templates, and then perform a risk analysis in the second stage.

The first stage of the migration strategy is to allow the SMEs to choose a pre-defined domain specific SLA template that is suitable for their applications, such as in the area of e-Learning, Product Lifecycle Management, e-Science, SaaS, etc. For example, if a user selects the e-Science criteria, a specific template for e-Science applications like Computational Fluid Dynamics (CFD) and Finite Element Method (FEM) is available to choose, as shown in Figure 1. This SLA template will eventually correspond to an image template with specific software packages or libraries and configurations when running on the cloud.

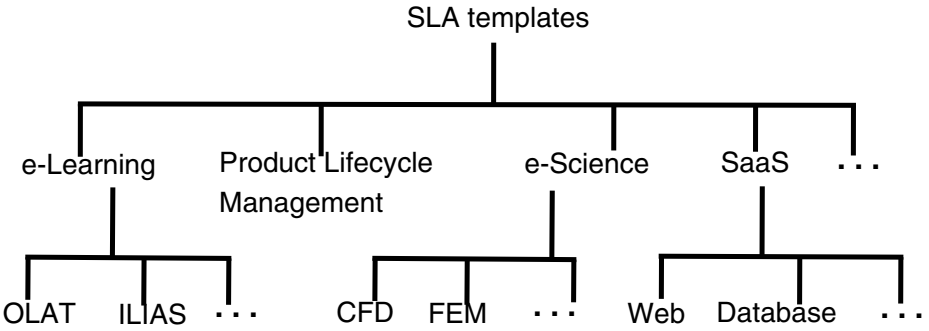

Fig. 1. Pre-defined SLA templates

After choosing the SLA template, a comparison table of various cloud providers will be displayed, as shown in Table 1. This table shows how well this application will run and what risks are considered. The SLA templates are living documents that constantly need to be updated and improved. Thus, for each criterion, an automated performance evaluation tool needs to be used across all cloud providers. Moreover, to avoid vendor lock-in, cloud providers that provide interoperability will be considered.

The second stage of the migration strategy aims to provide a detailed risk analysis of the chosen SLA template, by providing a *what-if* scenario. The risk analysis is based on existing security catalogs (e.g., ISO 27001), and considering several factors like factual knowledge (e.g., the location of the cloud infrastructure),

Table 1. An example of a comparison table for various cloud providers

Risk Categories	Amazon Web Services	Flexiscale	Microsoft Azure	...
Total cost / hour	4 Euros	4 Euros	5 Euros	
Security	Good	Satisfactory	Satisfactory	
Privacy	Good	Good	Good	
Best Practices (ITIL)	Level 3	Level 5	Level 2	
Interoperability	Satisfactory	Good	Good	
...				

customer surveys or questionnaires (e.g., Gartner and 451 Group), cloud samples (such as measurement of software versions, and security incidents), and best IT practice fulfillment like Information Technology Infrastructure Library (ITIL) [18] stated in levels (Level 0 = no to Level 5 = ITIL certified). Moreover, the user can modify the input SLA parameters (shown in Table 1). This approach will greatly facilitate the migration to the cloud because it allows an overview of the total costs, functionalities and associated risks to the SMEs.

The data privacy risk is expressed in three levels (i.e., Good, Medium, Bad) and evaluated according to historical data (e.g., data breach incidences) while considering used cryptographic methods for data transfer and storage. If the suitable provider (the one with the best fitting SLA with a minimum risk) is found, a privacy self-protecting service will be deployed on the chosen cloud provider to protect the data privacy.

The next step is to protect the migrated service during runtime by self-protection.

4 A Self-protecting Cloud Service

After a cloud provider has been selected, privacy needs to be monitored and the appropriate actions shall be performed when privacy incidences occur. This can be achieved by a *privacy self-protecting* cloud service with a control system that performs independent compliance checks of external and internal regulations, as shown in Figure 2. The control system leverages the MAPE-K (Monitor, Analyze, Plan, Execute, and Knowledge) reference model [19]. The key characteristics of autonomic computing are self-healing, self-configuring, self-optimizing and self-protecting [20]. The focus in this work is on the self-protection of a system, where systems safeguard the private or confidential information.

In the MAPE-K Loop reference model, the privacy related criteria are monitored during the Monitor and Analyse phases, using a knowledge base containing various information, such as data access rules, etc. and the automated privacy measures (like anomaly metric) are implemented in the Plan and Execute phases.

The *Privacy API* module contains a sensor and an executor, as illustrated in Figure 2. The sensor provides an input of sensor data for the Monitor phase in the control system, whereas the executor enables security actions in order to protect the customer application. For this purpose, an interconnected artificial neural network of the self-protecting *Service* module is installed to detect a potential security breach, where the same customer is running several services in the same cloud environment. Moreover, through an interconnected network the anomaly detection rate will be improved over time as more users using the service.

Through a web browser or calling directly via web services of the control system's API, the knowledge base can be updated at any time, and the selected security parameters can be monitored visually, as depicted in Figure 2. Moreover, in this figure, the *Enterprise Integrator* module enables the integration of cloud services into the user's business infrastructure through a Virtual Private Network (VPN) tunnel. As a result, this approach is intended to ensure the integrity, availability and confidentiality of the data and functions of the cloud service.

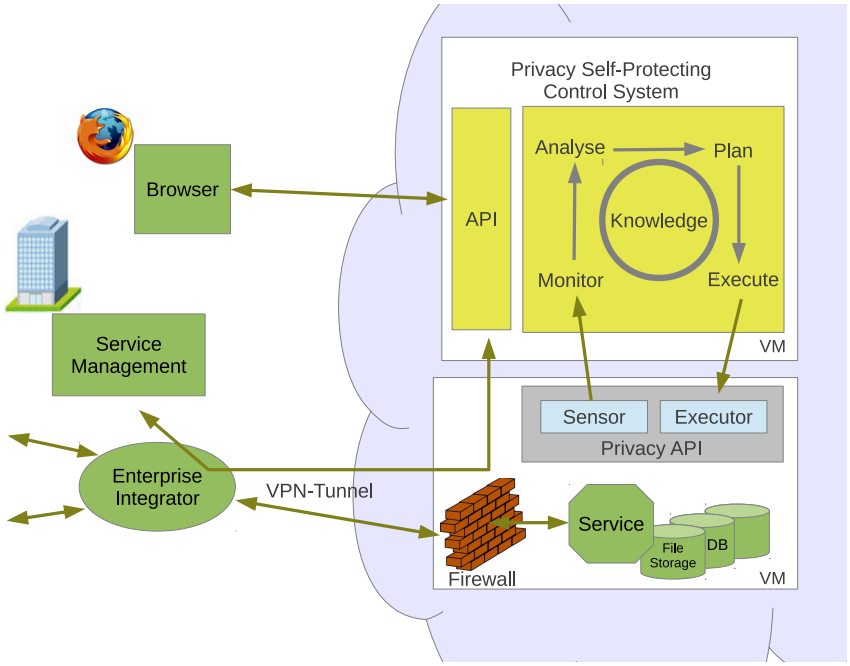

Fig. 2. The Architecture Overview

Towards Self Protecting Privacy

For private or confidential data safeguarding, companies define privacy policies that comprises various privacy rules, such as:

- only specific group has access to the data,
- gives alarm if data breaches occurred,
- data location only at predefined region,
- only encrypted data should be stored, and
- access of data only by a specific service.

Each of these rules specify on how various pieces of information need to be handled, and are individually defined by each cloud customer. The cloud's multi-tenancy character needs a scalable and effective implementation of these rules. It is essential to have in place a system for an automated enforcement of various privacy rules. The MAPE-K loop is therefore designed as following:

- *Knowledge:* The knowledge base contains the tenant-based privacy protection policies. Also, the knowledge about policy enforcement tools has to be known. It is intended to use existing tools (e.g., Intrusion Detection System or Intrusion Prevention System) and integrate them, if a policy rule implies it. Moreover, the knowledge base has information such as data access rules, log file formats, service configurations, cloud-specific facts (e.g.,

virtualization technology, firewall API), etc. which is needed for the analysis and planing phases.
- *Sensor/Actor:* Application Programming Interface (API) transformation between the tools and the phases (Analysis and Planning). For each existing tool, there will be one specific sensor/actor.
- *Analysis:* The data of the tools are analyzed and the appropriate plan is triggered. For example, a tool signals data breach and unauthorized access. As a result, it will trigger an alarm for data leakage.
- *Plan:* There are different executable plans, such as different notification levels (info, alarm), firewall reconfiguration (block traffic), data restore, etc.

5 Conclusion and Future Work

This paper proposes a solution towards a *self-protecting* cloud to reduce the barrier for cloud adoption by Small and Medium-sized Enterprises (SMEs). This can be done by having two approaches, i.e. by having a migration strategy with predefined Service-Level Agreement (SLA) templates, and a self-protecting cloud service that monitors the specified security criteria and security measures.

In order to find the "suitable" cloud environment for IT services, an SLA analysis of various cloud providers are evaluated and analyzed by using pre-defined SLA templates and service-specific SLA specifications. Moreover, a detailed risk analysis is used to determine an overview of the total costs, the risks and the long-term benefit to SMEs.

After a cloud provider has been selected, a *self-protecting* cloud service with a *self-securing* control system oversees safety criteria compliance and performs independent safety measurements. This approach is intended to ensure the integrity, availability and confidentiality of the data and functions of the cloud service.

As for future work, an implementation of the self-protecting cloud service will be done as a proof of concept.

References

1. CISCO Systems Inc.: Planning the migration of enterprise applications to the cloud, http://www.cisco.com/en/US/services/ps2961/ps10364/ps10370/ps11104/Migration_of_Enterprise_Apps_to_Cloud_White_Paper.pdf
2. Jansen, W.A.: Cloud hooks: Security and privacy issues in cloud computing. In: HICSS, pp. 1–10. IEEE Computer Society (2011)
3. MacInnes, B.: Leading the SME to cloud, http://www.microscope.co.uk/feature/Leading-the-SME-to-cloud
4. Ren, K., Wang, C., Wang, Q.: Security challenges for the public cloud. IEEE Internet Computing 16(1), 69–73 (2012)
5. Winkler, J.R.V.: Securing the Cloud: Cloud Computer Security Techniques and Tactics. Syngress Publishing (2011)
6. OECD: OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data. OECD Publishing (February 2002)

7. Data Protection Directive 95/46/EC: Data Protection Directive 95/46/EC, http://europa.eu/legislation_summaries/information_society/data_protection/l14012_en.htm
8. European Commision: General data protection regulation, http://ec.europa.eu/justice/data-protection/document/review2012/com_2012_11_en.pdf
9. Sotto, L.J., Treacy, B.C., McLellan, M.L.: Privacy and Data Security Risks in Cloud Computing. In: Electronic Commerce & Law Report (February 2010)
10. Council Directive 2002/58/EC: On the protection of individuals with regard to the processing of personal data and on the free movement of such data. Official Journal L 281, pp. 31–50 (October 24, 1995)
11. Betge-Brezetz, S., Kamga, G.B., Ghorbel, M., Dupont, M.P.: Privacy control in the cloud based on multilevel policy enforcement. In: 2012 IEEE 1st International Conference on Cloud Networking (CLOUDNET), pp. 167–169 (2012)
12. Samarati, P., di Vimercati, S.D.C.: Data protection in outsourcing scenarios: issues and directions. In: Proceedings of the 5th ACM Symposium on Information, Computer and Communications Security, ASIACCS 2010, pp. 1–14. ACM, New York (2010)
13. Joseph, N.M., Daniel, E., Vasanthi, N.A.: Article: Survey on privacy-preserving methods for storage in cloud computing. In: IJCA Proceedings on Amrita International Conference of Women in Computing - 2013 AICWIC(4), pp. 1–4. Foundation of Computer Science, New York (2013)
14. Anil, S.L., Thanka, R.: A survey on security of data outsourcing in cloud. International Journal of Scientific and Research Publications (IJSRP) 3 (2013)
15. Sayi, T., Krishna, R., Mukkamala, R., Baruah, P.K.: Data outsourcing in cloud environments: A privacy preserving approach. In: 2012 Ninth International Conference on Information Technology: New Generations (ITNG), pp. 361–366 (2012)
16. Jiazhu, D., Shuangyan, L., Hongxia, L.: A privacy-preserving access control in outsourced storage services. In: 2011 IEEE International Conference on Computer Science and Automation Engineering, CSAE, vol. 3, pp. 247–251 (2011)
17. Wang, C., Wang, Q., Ren, K., Lou, W.: Privacy-preserving public auditing for data storage security in cloud computing. In: Proceedings of the 29th Conference on Information Communications, INFOCOM 2010, pp. 525–533. IEEE Press, Piscataway (2010)
18. ITIL: ITIL - IT Infrastructure Library, http://www.itil-officialsite.com/home/home.aspx
19. Menascé, D.A., Kephart, J.O.: Guest editors' introduction: Autonomic computing. IEEE Internet Computing 11(1), 18–21 (2007)
20. IBM: An architectural blueprint for autonomic computing, http://www-03.ibm.com/autonomic/pdfs/AC%20Blueprint%20White%20Paper%20V7.pdf