Compliance Auditing in Future Web-based Infrastructures

Jonathan Sinclair
SAP Research Belfast
The Concourse, Titanic Quarter
Belfast, BT3 9DT
jonathan.sinclair@sap.com

Benoit Hudzia
SAP Research Belfast
The Concourse, Titanic Quarter
Belfast, BT3 9DT
benoit.hudzia@sap.com

Maik Lindner
SAP Research Palo Alto
3475 Deer Creek Road
Palo Alto, 94304
m.lindner@sap.com

Alan Stewart
School of EEECS
Queen's University Belfast
Belfast, BT7 1NN
a.stewart@qub.ac.uk

Terry Harmer
Belfast e-Science Centre
School of EEECS
Queen's University Belfast
Belfast, BT7 1NN
t.harmer@besc.ac.uk

John Stewart
SAP Research Belfast
The Concourse, Titanic Quarter
Belfast, BT3 9DT
jo.stewart@sap.com

ABSTRACT

Businesses today are required to comply with a litany of legislation, regulations and standards. However, with an increasing utilisation of the internet for delivering products as services, challenges arise in assessing and maintaining compliance. We propose to discuss an architecture that attempts to leverage the dynamism of service-based infrastructures in order to process the real-time compliance state of a system.

Keywords

compliance, auditing, enterprise cloud computing, data protection

1. INTRODUCTION

Fortune 1000 companies can spend up to £3.4million/annum in order to implement governance compliance policies [7]. Even in a slow economy, companies still place compliance and security at the top of their IT process requirements [5]. All organizations that collect and use personal data must comply with data-protection compliance laws [3, 11]. Possible consequences for breaching compliance are imprisonment or large financial fines [9]. Business processes involving IT must have auditing and compliance capabilities [4]. In most companies compliance audits are carried out in a relatively static environment in which processes are often carried out on a single system, within a company's domain. However, as technologies and business processes evolve so to must compliance; ideally compliance should be treated in a technology agnostic way – consequently, the enforcement of regulations [8] may also need to evolve.

2. MOTIVATION

The use of internet for delivering IT services is increasing rapidly. This growth is supported through the advancement of web-based infrastructures. The wide-spread availability of on-demand computing resources has resulted in the treatment of computational services as a 5th household utility (after water, electricity, gas and telephony) [1, 2]. There are consequential challenges arising from the use of on-demand services; in particular, information assurance and the ability to assess and maintain compliance in distributed web-based infrastructures (such as clouds) are required. In such environments system locality, size and availability can be altered dynamically to meet a company's requirements. This dynamism introduces additional complexity to compliance auditing [12, 13]. In order for organizations to use Cloud infrastructures effectively these compliance, regulation, governance and security challenges need to be addressed. Enterprises are under increasing pressure to improve return on investment (ROI) whilst maintaining both legal and regulatory compliance. Moreover, as the number of regulations an organisation has to comply with increases so too does the complexity of auditing IT services. Therefore automation of procedures that process the data of organisations has come under increasing scrutiny as a result. In order to audit and certify data storage and access arrangements it is important to establish evidence for compliance verification [6]. The development of internet-based IT infrastructures may result in current auditing standards becoming obsolete. Auditors have traditionally relied on SAS 70 [10] reports to audit and gain assurance that proper controls are in place. However a number of factors have contributed to the need for new standards:

- The globalization of information technology and the practice of outsourcing business processes has generated the need for an international auditing standard.
- A dynamic regulatory landscape may create the need for additional information about internal control of financial reporting.
- U.S. convergence with international standards.

In this paper, we examine legal-technical issues that arise in compliance analysis on web-based infrastructures; examples of such issues are the physical locality of data (data-protection act), jurisdictional consequences / conflicts, disaster recovery and breach of privacy liability.

3. DISCUSSION

The compliance challenges introduced by cloud computing model are loosely associated with data and security challenges. These challenges can be categorised as follows:

- Data Locality
- Data Retention
- Data Accesibility
- Data Integrity
- Data Backup / Recovery

These challenges are defined by the legislation and regulation imposed on businesses. Compliance has to be enforced in all aspects of the service lifecycle to maintain assurance, from deployment time legal implications such as cross-jurisdiction and availability, through to maintaining performance and enabling disaster recovery / backup. Legal and regulatory specifications are defined from tangelible specifications that deal with the handling, usage, storage, transfer and the availability of data.

A solution to develop a real-time monitoring and compliance auditing service is proposed whereby requirements from these legal specifications are mapped onto parts of Service Level Agreements (SLAs). Such mappings must be consistent with the legal, regulatory and geographical constraints that arise in a cloud context. Optimisation is brought about by imposing stricter auditing conditions, especially with reference to locality. For example, data-protection laws may restrict the geographic regions in which a cloud-based service can run. The consequences of complying with conflicting legal requirements may be increased cost and reduced flexibility. We propose to leverage the information provided by SLAs as an input for generating auditing policies derived from compliance specifications. Currently work on SLA's only considers the benefits to be gained from cloud and the non-functional requirements defined by the organisation. However, as described the legal responsibility of ensuring compliance is upheld has equal value to the organisation. We further analyse how SLA's are re-negotiated in order to satisfy conflicting legal requirements in order to meet the legal obligation of the consumer. SLA re-negotiation can be evaluated in terms of its detriment of cloud benefits in terms of flexibility and cost.

4. CONCLUSION

We identified how cloud benefits do not come without their cost and that companies are becoming increasing vigilant in assuring they meet compliance. The complexity of distributed systems and the flexibity of the cloud computing models poses challenges when monitoring and assuring compliance is met. Therefore in our discussion we describe the requirements of a real-time monitoring and compliance auditing service and briefly describing how rules will be derived and defined in an SLA. This forms the foundation for current and further research into a compliance-driven auditing architecture for distributed systems.

5. ACKNOWLEDGMENTS

This work was done and funded as part of the EU FP7 OPTIMIS project.

6. REFERENCES

[1] C. Baumann, P. Peitz, O. Raabe, and R. Wacker. Compliance for service based systems through formalization of law. In J. Filipe and J. Cordeiro, editors, *Proceedings of the 6th International Conference on Web Information Systems and Technology*, volume 2, pages 367–371, Valencia, Spain, April 2010. INSTICC Press.

[2] R. Buyya, C. S. Yeo, and S. Venugopal. Market-oriented cloud computing: Vision, hype, and reality for delivering it services as computing utilities. In *HPCC '08: Proceedings of the 2008 10th IEEE International Conference on High Performance Computing and Communications*, pages 5–13, Washington, DC, USA, 2008. IEEE Computer Society.

[3] A. Cavoukian. Privacy in the clouds, a white paper on privacy and digital identity: Implications for the internet. Information and Privacy Commissioner of Ontario, Canada, 2009.

[4] D. Flint. Law shaping technology: Technology shaping the law. *International Review of Law, Computers & Technology*, 23 , 1:5–11, 2009.

[5] A. Joint, E. Baker, and E. Eccles. Hey, you, get off of that cloud? *Computer Law and Security Review*, 25:3, 2009.

[6] L. M. Kaufman. Data security in the world of cloud computing. *Security and Privacy, IEEE*, 7, 4:61–64, 2009.

[7] M. Knights. It shoulders new laws load [it legislation guide]. *Engineering and Technology, IET*, 5:49 – 52, 2010.

[8] S. Levi and K. Riedel. Cloud computing. *Practical Law the Journal*, 2010:8, 2010.

[9] B. News. Previous cases of missing data, 12 2009.

[10] A. I. of Certified Public Accountants: Auditing Standards Board. Statement on auditing standards no. 70: Service organizations, 1992.

[11] L. Sotto, B. Treacy, and M. McLellan. Privacy and data security risks in cloud. *Computing Electronic Commerce & Law Report*, 15:186, 2010.

[12] M. Vouk. Cloud computing: Issues, research and implementations. *Computing and Information Technology, IEEE*, 16:235–246, 2008.

[13] H. Wang. Privacy-preserving data sharing in cloud computing. *Journal of Computer Science and Techonology*, 25, 3:401–414, 2010.