This product is part of the RAND Corporation technical report series. Reports may include research findings on a specific topic that is limited in scope; present discussions of the methodology employed in research; provide literature reviews, survey instruments, modeling exercises, guidelines for practitioners and research professionals, and supporting documentation; or deliver preliminary findings. All RAND reports undergo rigorous peer review to ensure that they meet high standards for research quality and objectivity.

TECHNICAL REPORT

The Cloud

Understanding the Security, Privacy and Trust Challenges

Neil Robinson, Lorenzo Valeri, Jonathan Cave, Tony Starkey
(RAND Europe)

Hans Graux
(time.lex)

Sadie Creese, Paul Hopkins
(University of Warwick)

Sponsored by the European Commission
Directorate General Information Society and Media

RAND EUROPE

time.lex

THE UNIVERSITY OF WARWICK

The research described in this report was sponsored by the European Commission Directorate General Information Society and Media.

Published 2011 by the RAND Corporation
1776 Main Street, P.O. Box 2138, Santa Monica, CA 90407-2138
1200 South Hayes Street, Arlington, VA 22202-5050
4570 Fifth Avenue, Suite 600, Pittsburgh, PA 15213-2665
Westbrook Centre, Milton Road, Cambridge CB4 1YG, United Kingdom
RAND URL: http://www.rand.org
RAND Europe URL: http://www.rand.org/randeurope
To order RAND documents or to obtain additional information, contact
Distribution Services: Telephone: (310) 451-7002;
Fax: (310) 451-6915; Email: order@rand.org

Executive Summary

Our research investigated the security, privacy and trust aspects of cloud computing and determined whether these were sufficiently distinct to warrant public policy intervention. On the whole, cloud computing brings into acute focus many security and privacy challenges already evident in other domains such as outsourcing or behavioural advertising.

Defining cloud computing

For the purposes of this study, we adopt a definition of cloud computing proposed by the US National Institute for Standards and Technology (NIST) in 2009:

> *Cloud computing is a model for enabling convenient, on-demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction*.

The literature identifies four different broad service models for cloud computing:

- *Software as a Service (SaaS)*, where applications are hosted and delivered online via a web browser offering traditional desktop functionality
- *Platform as a Service (PaaS)*, where the cloud provides the software platform for systems (as opposed to just software)
- *Infrastructure as a Service (IaaS)*, where a set of virtualised computing resources, such as storage and computing capacity, are hosted in the cloud; customers deploy and run their own software stacks to obtain services.
- *Hardware as a Service (HaaS)*, where the cloud provides access to dedicated firmware via the Internet

Cloud computing offerings also differ by scope. In private clouds, services are provided exclusively to trusted users via a single-tenant operating environment. Essentially, an organisation's data centre delivers cloud computing services to clients who may or may not be in the premises. Public clouds are the opposite: services are offered to individuals and organisations who want to retain elasticity and accountability without absorbing the full costs of in-house infrastructures. Public cloud users are by default treated as untrustworthy. There are also hybrid clouds combining both private and public cloud service offerings.

Issues, challenges and concerns

We identified a number of issues in the **literature** relating to technological and legal challenges confronting privacy, security and trust posed by cloud computing. Regarding the challenges in the technological underpinnings of cloud computing, we note evidence stemming from: virtualisation (e.g. vulnerabilities in hypervisors could have potential widespread effects on data integrity and confidentiality); whether grid computing models can afford the appropriate level of interoperability ; if Web Services will be effective for identity management in the cloud; establishing trust when using Service Orientated Architectures and web application frameworks and finally whether current technical methods of encryption will remain viable to achieve confidentiality. There are a number of challenges posed by a range of legal and regulatory frameworks relevant to cloud computing. These include the viability of legal regimes which impose obligations based on the location of data; the ex-ante definition of different entities (such as distinguishing between data controllers and processors); establishing consent of the data subject; the effectiveness of breach notification rules; the effectiveness of cyber-crime legislation in deterring and sanctioning cyber-crime in the cloud and finally difficulties in determining applicable law and jurisdiction. From an operational perspective, the study uncovered issues relating to the effectiveness of existing risk governance frameworks, whether cloud customers can meet their legal obligations when data or applications are hosted overseas, how to be compliant and accountable when incidents occur; whether data will be locked into specific providers; the complexities in performing audit and investigations; how to establish the appropriate level of transparency and finally measuring security of cloud service provision.

The **case studies** identified a number of challenges relating to cloud service provision from recent real-world instances. These include the immature and exploratory nature of cloud computing deployments; the necessity that those using cloud services should be versed in their tolerance for risk prior to migrating to the cloud; how to balance the business benefits of cloud computing with achieving security and privacy obligations; the need to integrate cloud security into existing security measures; the importance of understanding untoward dependencies created by cloud computing deployments and finally that tailored and specific security agreements can be achieved but only if the cloud user has sufficient negotiating power.

These identified real-world concerns were supplemented by additional material gathered at an **Expert Workshop**. Participants commented that it was difficult to achieve a high degree of accountability or transparency in the cloud; that there was little awareness raising for either cloud customers or private citizens; little established guidance on expectations for cloud users in meeting their legal obligations and finally lack of harmonisation of relevant legal and regulatory frameworks, potentially presenting an impediment to realising the economic and social benefits of cloud computing for Europe.

Recommendations

Our recommendations are orientated around four themes of current opportunities for policy action:

- **Compliance** - *Greater harmonisation of relevant legal and regulatory frameworks* to be better suited to help provide for a high level of privacy, security and trust in cloud computing environments. For example: *establishing more effective rules for accountability and transparency* contributing to a high level of privacy and security in data protection rules and *expansion of breach notification regimes* to cover cloud computing providers.
- **Accountability** – Improvement of rules enabling cloud users (especially consumers) to *exercise their rights* as well as *improvement of models of Service Level Agreements (SLAs)* as the principle vehicle to provide accountability in meeting security, privacy and trust obligations.
- **Transparency** –improving to way in which levels of security, privacy or trust afforded to cloud customers and end-users can be discerned, measured and managed, including *research into security best practices, automated means for citizens to exercise rights* and *establishment of incident response guidelines*.
- **Governance** – The *European Commission could act as leading customer* by deploying cloud computing solutions as part of its e-Commission initiative and indirectly supporting the improvement of existing operational risk control frameworks. Research funding could be assigned to *improving Security Event and Incident Monitoring* in the cloud amongst other things.