2011 International Conference on Signal, Image Processing and Applications
With workshop of ICEEA 2011
IPCSIT vol.21 (2011) © (2011) IACSIT Press, Singapore

Efficient Framework for Ensuring the Effectiveness of Information Security in Cloud Computing

Karunanithi. D [1+] and Kiruthika. B [2]

[1, 2] Department of Information Technology, Hindustan University, Chennai, India

Abstract. The overall objective of security, private and trust challenges arise from the technological underpinnings of cloud computing is a principle to guide decisions and achieve rational outcomes to confirm that users of cloud environments are given total protections, to strengthen and stabilize a world leading cloud ecosystem. Cloud computing is increasingly subject to interest from individuals who have the authority to set the policy framework of an organisation and regulatory authorities. Hence, our concern is that currently a number of challenges and risks in respect of security, privacy and trust exist that may damage the fulfilment of these policy and so we upgrade in various implementations of cloud computing .The overall strategic goal is to avoid interoperability barriers and cases of technological lock-ins that may undermine the development of new cloud-based services.

Keywords: Cloud Computing, Security, Privacy and Trust

1. Introduction

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 [1]. The literature identifies four different broad service models for cloud computing:

1. Software as a Service (SaaS), where applications are hosted and delivered online via a web browser offering traditional desktop functionality, eg, Google Docs, Gmail and MySAP [3].

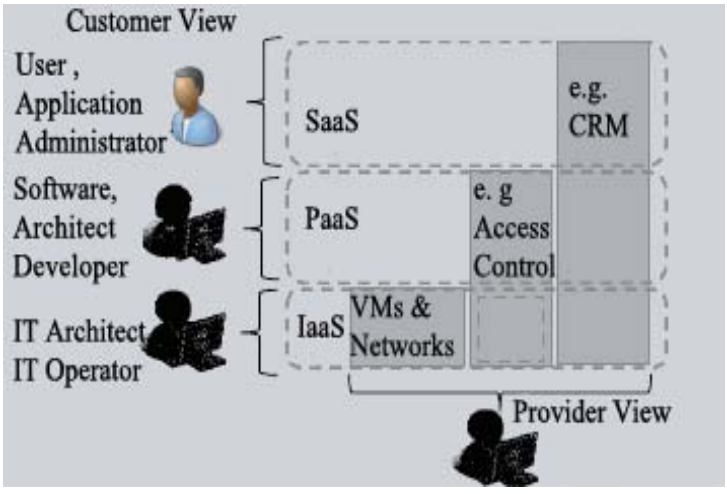

Fig 1: XaaS Stack Views

2. Platform as a Service (PaaS), where the cloud provides the software platform for systems (as opposed to just software), the best current example being the Google App Engine [6].

3. 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. Current examples are Amazon Elastic Compute Cloud (EC2), Simple Storage Service (S3) and SimpleDB [3].

[+] Corresponding author. Tel.: + 91-9445753975
E-mail address: karunanithid@gmail.com

4. Hardware as a Service (HaaS), where the cloud provides access to dedicated firmware via the Internet, eg, XEN and VMWare [7].

2. Scope and Evolution of Cloud

1. Private clouds, services are provided exclusively to trusted users via a single-tenant operating environment. Essentially, an organisations data centre delivers cloud computing services to clients who may or may not be in the premises [11].

2. Public clouds, are the opposite: services are offered to individuals and organizations 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 [8].

3. Inter Clouds, Combining both private and public cloud service offerings [2].

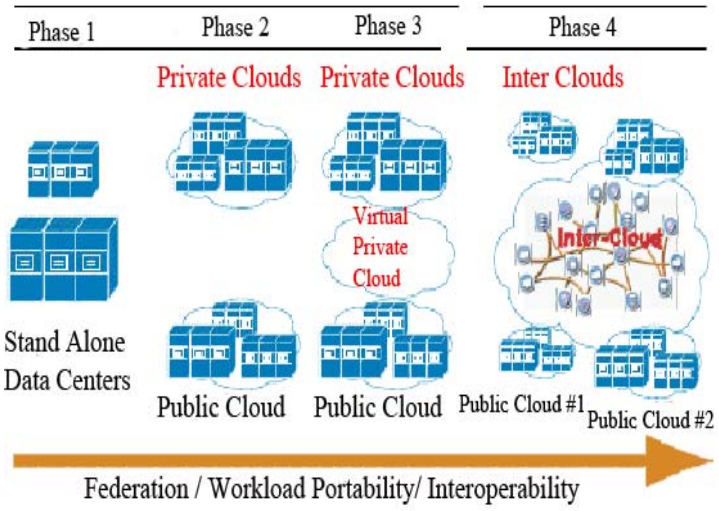

Fig 2: Evolution of Cloud

3. Architecture of Cloud Computing

The cloud computing architecture of a cloud solution is the structure of the system, which comprises on-premise and cloud resources, resources, services, middleware, and software components, geo-location, the externally visible properties of these, and the relationship between them. The term also refers to documentation of a system‘s cloud computing architecture. Documenting facilities communication between stakeholders, documents early decisions about high level design components and patterns between project [13].

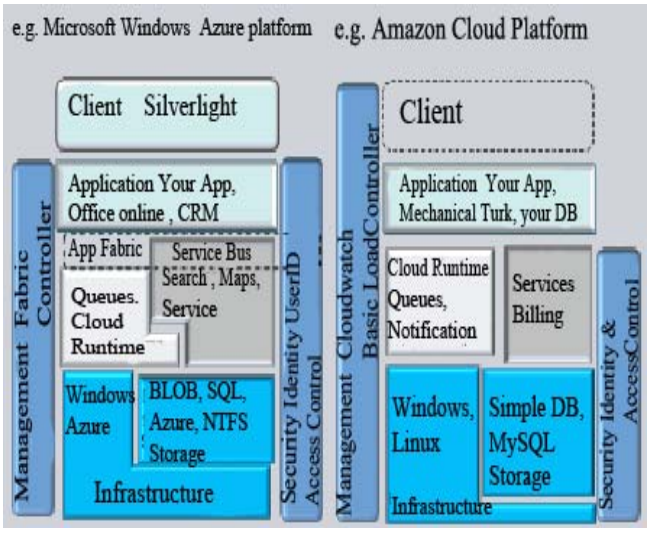

Fig 3: Cloud Reference Architecture

3.1. Reference architecture

Basis for documentation, stakeholder and team communication, payment, contract and cost models [13].

3.2. Technical architecture

Structuring according to XaaStack, adopting cloud platform paradigms, structuring cloud services and cloud components, showing relationships and external endpoints, middleware and communication, management and security [16].

3.3. Deployment Operation Architecture:

Geo-location check, operation and monitoring [10].

4. Defining Security, Privacy And Trust

Before assessing the literature dealing with security, privacy and trust in the cloud, it is important to define these terms because their currency and usage can change radically in different contexts: Security concerns the confidentiality, availability and integrity of data or information. Security may also include authentication and non-repudiation. Privacy concerns the expression of or adherence to various legal and non-legal norms regarding the right to private life. In the European context this is often understood as compliance with European data protection regulations. Although it would be highly complex to map cloud issues onto the full panoply of privacy and personal data protection regulatory architectures, the globally accepted privacy principles give a useful frame: consent, purpose restriction, legitimacy, transparency, data security and data subject participation. Trust revolves around assurance‘ and confidence that people, data, entities, information or processes will function or behave in expected ways. Trust may be human to human, machine to machine (eg, handshake protocols negotiated within certain protocols), human to machine (eg, when a consumer reviews a digital signature advisory notice on a website) or machine to human (eg, when a system relies on user input and instructions without extensive verification). At a deeper level, trust might be regarded as a consequence of progress towards security or privacy [15].

5. Major Issues and Challenges

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 determining and sanctioning cyber-crime in the cloud and finally difficulties in determining applicable law and jurisdiction [15].

6. Chosen Approach to Address these Risks

The main security/privacy and trust issues ultimately addressed:

1. From a legal perspective, eg, via: Specific contracts, including service level agreements, maintenance agreements, auditing rights, etc. Compliance controls, external legal audits [3].

2. From a technical perspective, eg, via: Establishing technical guidelines such as incident handling protocols, logging obligations, security metrics, etc. Testing periods and/or trial phases during implementation External technical audits [11].

3. From an operational perspective, eg, via: Migration planning, including staff training, Risk Assessment, including lock-in, incident management planning, Etc, Implementing contingency and/or continuity plans, external operational audits [4].

7. Implementations

The 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 [8].

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 [16].

7.1. 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 [14].

7.2. 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 [5].

7.3. 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 [3].

8. Arising Issues

Area/ Technological or legal domain	**Security**	**Privacy**	**Trust**
Virtualization	Integrity	Segregation of personal data on shared infrastructure	Compromised virtual machines/ hypervisors permit loss of trust
Web services	Integrity and Confidentiality	Security and Confidentiality	Interoperability (in the context of identity and access management)
Service-orientated Architectures	Integrity	Safeguards against unlawful intrusions in the personal sphere	The reliance of distributed systems on different security credentials
Web application frameworks	Integrity and Availability	Existence and effectiveness of privacy protection laws/principles	Trust across distributed environments
Encryption in the cloud context	Confidentiality	Security and Confidentiality	Compromised virtual machines/ hypervisors permit loss of trust
Applicable law (data/service location)	Trust across distributed computing environments	Existence and effectiveness of privacy protection laws/principles	Existence of a clear legal framework as a basis for the service
Data protection and privacy	Obligation to implement secure data processing approaches	Compliance with privacy Principles	Confidence in data protection practices
Protection of intellectual property rights	Confidentiality and availability (data portability)	Obligation to implement private data processing approaches	Confidence in the security/confidentiality of data entrusted to the cloud
Security obligations and cybercrime	Confidentiality, availability and integrity; effective law enforcement	Safeguards against unlawful intrusions in the personal sphere	Balancing privacy safeguards with the need for security
Accountability and liability	Accountability for security breaches and incidents	Accountability for data leaks: can incidents be identified and sanctioned?	Trust that instruments for restitution and sanction will work
Harmful and illegal content	Availability: can the cloud identify and respond to such content?	Safeguarding communications secrecy	Trust in jurisdictions to apply transparent standard or approach to illegal content

			(applicable laws)
Scope and quality of services (SLAs)	Transparency and security metrics are needed to ensure that security targets are met	Existence of a clear legal framework as a basis for the service	Assurance and commitments between two parties
Validity and consent	Transparency and Accountability	Transparency must be ensured. Consent from consumers must be free, specific and informed	Assurance and commitments between two parties must be clear and enforceable

9. Conclusion

Successfully addressing the challenges identified in this study should not be considered an endpoint but rather a process. Security is very important when the internet is involved as the internet creates anonymity and removes boundaries. Cloud computing exists on the internet backbone and gives users the ability to connect from anywhere. Hence, security in cloud computing is a vital consideration. The security goals of confidentiality, integrity and availability are commonly used in the field of security and we applied them here to security in cloud computing [9].

10. References

[1] Amazon Web Services, '*Overview of Security Processes'*, August 2010. As of November 2010: http://awsmedia.s3.amazonaws.com/pdf/AWS_Security_Whitepaper.pdf.

[2] www.ct.siemens.com. Dr. Gerald Kaefer gerald.kaefer@siemens.com Siemens AG, CTTDEIT1 Corporate Technology, Global Technology Field System Architecture and Platforms Otto-Hahn-Ring 6 81739 Munich, Germany.

[3] Armbrust, Michael et al., 'Above the Clouds: *A Berkeley View of Cloud Computing'*, University of California at Berkeley, Technical Report No. UCB/EECS-2009-28, 10 February 2009. As of 25 November 2010: http://www.eecs.berkeley.edu/Pubs/TechRpts/2009/EECS-2009-28.pdf

[4] Creese, Sadie, Mike Auty, Michael Goldsmith & Paul Hopkins, Inadequacies of Current Risk Controls for the Cloud, forthcoming (to appear in the proceedings of the CloudCom 2010 conference).

[5] European Network and Information Security Agency (ENISA), *Cloud Computing: Benefits, risks and recommendations for information security*, 2009a. As of 25 November 2010: http://www.enisa.europa.eu/act/rm/files/deliverables/cloud-computing-riskassessment/at_download/fullReport

[6] Article 29 Data Protection Working Party & Working Party on Police and Justice, '*The Future of Privacy: Joint contribution to the Consultation of the European Commission on the legal framework for the fundamental right to protection of personal data*',WP168, 2009. As of 25 November 2010 *http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2009/wp168_en.pdf*

[7] Amazon, AWS and EC2 resources, Google App Engine articles, The Open Group, The Open Group Architecture Framework (TOGAF), Definition of the term "Architectural Principle", *http://www.opengroup.org/architecture/togaf8-doc/arch/chap29.html*.

[8] Birman, Ken, Gregory Chockler & Robbert van Renesse, '*Toward a Cloud Computing Research Agenda'*, ACM SIGACT News, 2009/40(2).

[9] European Network and Information Security Agency (ENISA), 'Position Paper: *Web 2.0 Security and Privacy'*, December 2008.

[10] M. Jensen, J. Schwenk, N. Gruschka, and L. L. Iacono, "*On Technical Security Issues in Cloud Computing*," in Cloud Computing, 2009. CLOUD '09. IEEE International Conference on, 2009, pp. 109-116.

[11] Loud Security Alliance, "*Security Guidance for Critical Areas of Focus in Cloud Computing V2.1*", Dec. 2009.

[12] W. Itani, A. Kayssi, and A. Chehab, "Privacy as a Service: Privacy- Aware Data Storage and Processing in Cloud Computing Architectures," in Dependable, Autonomic and Secure Computing, 2009. DASC '09. Eighth IEEE International Conference on, 2009, pp.711-716

[13] IBM, IBM Point of View: Security and Cloud Computing, ftp://ftp.software.ibm.com/common/ssi/sa/wh/n/tiw14045usen/TIW14045USEN HR.PDF, 2009.

[14] CiscoCloudComputing_WP.pdf http://pdftop.net/preview/

[15] Sun_CloudComputing.pdf http://pdftop.net/preview/