Advances in Computer Science and Information Technology (ACSIT)
p-ISSN: 2393-9907; e-ISSN: 2393-9915; Volume 3, Issue 5; July-September, 2016, pp. 409-412
© Krishi Sanskriti Publications
http://www.krishisanskriti.org/Publication.html

Security Secrecy and Reliability Challenges Stemming from Technological Underpinnings of Cloud Computing

Harpreet Kaur[1] and Ashish Kumar Bajpai[2]

[1]Dept of Computer Science S.R. Govt College (W), ASR
[2]Dept of Computer Science Govt. College, Mohali
E-mail: [1]harpreetsethi.27@gmail.com, [2]contact.bajpai@gmail.com

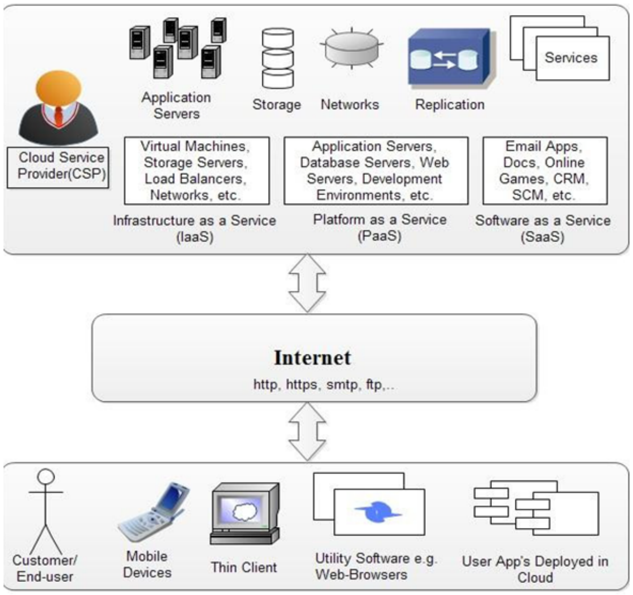
Abstract—*Cloud computing is a model for enabling convenient, on-demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction an analysis of the technological challenges of cloud computing and associated services, and will support the argument that the benefits of using clouds hinge on finding appropriate technological answers to the security, secrecy and reliability challenges. The starting point of this analysis is that cloud technologies are on the whole not new, but that their development has been revitalized by cloud computing.*

Keywords*: Cloud Computing, On-Demand Network, Pool, Associated Services, Cloud Hinge, Revitalized.*

1. INTRODUCTION

Clouds are a large pool of easily usable and accessible virtualised resources (such as hardware, development platforms and/or services). These resources can be dynamically reconfigured to adjust to a variable load (scale) allowing also for an optimum resource utilisation. This pool of resources is typically exploited by a paper-use model in which guarantees are offered by the Infrastructure Provider by means of customised service level agreements. Cloud computing is the latest approach to provide computing infrastructure, with the purpose to shift the location of the computing infrastructure to the network in order to reduce the cost of management and maintenance of hardware and software resources. All

These resources are provided as services to customers an as-needed basis. Companies are moving to the cloud according to a study by the Pew Internet & American Life Project, 66 percent of Americans are connected to the Web for some kind of cloud services as online hard drive back up to store files and personal photos, Blogs, wikis and social networks. It provides an analysis of the technological challenges of cloud computing and associated services, and will support the argument that the benefits of using clouds hinge on finding appropriate technological answers to the security, secrecy and reliability challenges.


Application Servers
Storage
Networks
Replication
Services
Cloud Service Provider(CSP)
Virtual Machines, Storage Servers, Load Balancers, Networks, etc.
Application Servers, Database Servers, Web Servers, Development Environments, etc.
Email Apps, Docs, Online Games, CRM, SCM, etc.
Infrastructure as a Service (IaaS)
Platform as a Service (PaaS)
Software as a Service (SaaS)
Internet
http, https, smtp, ftp,..
Customer/ End-user
Mobile Devices
Thin Client
Utility Software e.g. Web-Browsers
User App's Deployed in Cloud

The Cloud

2. CHARACTERIZED SECURITY, SECRECY AND RELIABILITY

It is important to define these terms because their currency and usage can change radically in different contexts. This document uses the following concepts.

- **Security**

It concerns the confidentiality, availability and integrity of data or information. Security may also include authentication and non-repudiation.

➢ **Secrecy**

It concerns the expression of or adherence to various legal and nonlegal norms. In the European context this is often understood as compliance with European data protection regulations 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. •

➢ Reliability

It revolves around 'assurance' and confidence that people, data, entities, information or processes will function or behave in expected ways. Reliability maybe 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 web site) 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 objectives.

3. SERVICE MODELS FOR CLOUD COMPUTING:

3.1 Software as a Service (SaaS)

SaaS where applications are hosted and delivered online via a web browser offering traditional desktop functionality, eg, Google Docs, Gmail and My SAP.

3.2 Platform as a Service (PaaS)

PaaS where the cloud provides the software platform

For systems (as opposed to just software), the best current example being the Google App Engine.

3.3 Infrastructure as a Service (IaaS)

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)10 and Simple DB.

3.4 Hardware as a Service (HaaS),

HaaS where the cloud provides access to dedicated firmware via the Internet, eg, XEN and VMWare.12

4. CHALLENGES WITH RESPECT TO SECURITY, SECRECY AND RELIABILITY OF CLOUD COMPUTING

The main considerations in respect of the security, secrecy and reliability challenges associated with the technological or legal domains constituting cloud computing. This is populated from the review of this study and reflects key concerns noted from the desk research:

Table 1: Challenges of Cloud Computing

AREA	SECURITY	SECRECY	RELAIBILTY
Virtualisation	Integrity	Segregation Of Personal Data On Shared Infrastructure	Compromised Virtual Machines
Grid Technologies	Availability		Interoperability
Web Services	Integrity And Confidentiality	Security And Reliability	
Services Oriented Architecture	Secrecy		The Reliance Of Distributed System On Different Security Credentials
Web Applications Framework	Secrecy And Availability		Trust Across Distributed Environments
Encryption In The Cloud Context	Reliability	Secrecy And Reliability	
Data Protection And Privacy	Obligation To Implement Securing Data Processing Approaches	Compliance With Secrecy Principles	Confidentiality
Protection Of Intellectual Property Rights	Confidentiality And Availability		Confidentiality In The Security Of Data Entrusted To The Cloud
Electronic Communication In The Cloud		Safeguarding Communication Secrecy	Protection Against Eavesdropping
Security Obligations And Cybercrimes	Confidential Availability And Integrity ,Effective Law Enforcement	Safeguards Against Unlawful Intrusions In The Personal Sphere	Balancing Privacy Safeguards With The Need For Security

This table is intended as a short checklist of areas to be covered in cloud deployments, and is used to support the analysis of areas, and specifically to determine to what extent each case study has been able to find appropriate answers to the legal and technical challenges in their respective domains. It should be noted, however, that this list is mostly valid with respect to public cloud systems (where specific data or services are outsourced to a third-party service provider), but much less so in the case of private cloud systems (which are deployed, operated and controlled by the us. The use of cloud technologies may still cause technical and security challenges, but to a lesser extent since they can be managed internally. Internal cloud computing deployments represent limited issues in respect of new legal or operational challenges.

4.1 Challenges with Operational services Of Cloud Computing

Depending on the cloud service the evidence from our study noted that the following operational challenges are of relevance:

- Data or services may be (or become) hosted from another country, even without the end user necessarily being aware.
- Infrastructure may be shared with other customers, leading to data segregation concerns.
- Incidents may cause service interruptions without it being evident where the problem lies, and thus how it may be addressed.
- Data withdrawal might be difficult, in the sense that it can be hard to determine for a cloud user whether deleted data was actually removed from the provider's systems, or whether it was merely made inaccessible to the user.
- Auditing and investigations may be more challenging, due to the complexity of the system (e.g. use of virtualisation technologies may make it harder to determine where data is located, and which systems may be audited without accessing another cloud user's data).

None of these challenges is strictly unique to cloud services: traditional outsourcing models can also be confronted with these same issues. However, the fact that cloud models combine all of these elements and a layer of technical complexity means that they are viewed as more problematic.

5. SECURITY, SECRECY AND RELIABILITY CHALLENGES STEMMING FROM TECHNOLOGICAL UNDERPINNINGS OF CLOUD COMPUTING

The technological challenges of cloud computing and associated services, and will support the argument that the benefits of using clouds hinge on finding appropriate technological answers to the security, privacy and trust challenges. The starting point of this analysis is that cloud technologies are on the whole not new, but that their development has been revitalised by cloud computing. There are number of challenges for security, secrecy and trust from the underlying technological drivers of cloud computing can be distilled, namely virtualisation technology, grid computing, web services, service-orientated architectures, web application frameworks and encryption.

5.1 The linchpin of trust: the hypervisor

Virtualisation is a key component in the provision of cloud infrastructure services (computation and data storage) as it enables providers to marry efficient use of hardware resources and multiple customers by using the same physical machine for different applications (as demonstrated by Amazon's EC2 offering).

Virtualisation is not a new idea and indeed there is already a range of different concepts of virtualisation ranging from the process level execution of a Java program within a Java Virtual Machine, to the system level virtualisation execution of an operating system such as Windows 2003 within a virtual machine monitor environment like VMware. While there are varying definitions of virtualisation, its importance in cloud computing focuses specifically on system level virtualisation and predominately what is often referred to as full or native hardware virtualisation. In this type, a virtual machine monitor (or hypervisor) replicates the physical machine logically, enabling multiple guest virtual machines (containing one of a number of different operating systems) to run independently.

5.2 Security Aspects of Virtualisation

The security aspects covered by the virtualization literature are primarily in two areas:

- The First area examines the problems in isolation and the occurrence of vulnerabilities within the configuration and development of hypervisors and how they may be exploited. In this instance, the ability to assure the hypervisor is critical in determining the level of confidence and trust placed in the security solutions.
- The second area, which examines the potential challenges for providing current security controls to a virtualized environment, also requires that there is confidence in the integrity of its behavior as well as its ability to monitor at a granular and appropriately detailed level security event data.

The main key security and trust themes from this study are:

- Assurance of the hypervisors' ability to isolate and establish trust for guest or hosted virtual machines is critical, as this forms the root node for multitenant machine computing and thus could prove to be a single point of failure, since the hypervisor can potentially modify or intercept all guest OS processing.
- The same properties of the hypervisor, which enable it to inspect and monitor all processing within and between guest OSs, give the potential for enhanced security monitoring, but will require that current security controls
- Based on dedicated appliances can be migrated to virtual machine architectures. They could also lead to a potential loss of individual customer privacy and security.
- For economic purposes, the ability of large-scale instances of virtual machines to be dynamically moved and re-provisioned is vital. It is unclear at this point how

adequate the lifecycle management of those instances between hardware and across clouds is, and whether trust can be established to an adequate level, if at all.

6. CONCLUSIONS

Cloud providers have to safeguard the Privacy and Security of personal and confidential data of organizations and users to provide and support trustworthy cloud computing services. There are number of challenges for security, secrecy and trust from the underlying technological drivers of cloud computing can be distilled, namely virtualisation technology, grid computing, web services, service-orientated architectures, web application frameworks and encryption. There are various technologies of cloud that safe our all environment instead that issues behind here but the solutions with the various protocols are also been there.

REFERENCES

[1] Jingwei Huang and David M Nicol, “Trust mechanisms for CloudComputing”, Journal of Cloud Computing: Advances, Systems and Applications 2013, 2:9, Springer Open Journal.[5] Rashmi, Dr.G.Sahoo, Dr.S.Mehfuz, “Securing Software as a Service

[2] Model of Cloud Computing: Issues and Solutions”, International Journal on Cloud Computing: Services and Architecture (IJCCSA), Vol.3, No.4, August 2013.

[3] [Zhou M, Zhang R, Xie W, Zhou A (2010) “Security and Privacy in cloud computing: a Survey”, In 6t international conference on semantics knowledge and grid(Ningbo, China, 2010), pp 105-112.

[4] Mell, Peter and Tim Grance, ‘The NIST Definition of Cloud Computing’, National Institute of Standards and Technology, 2009a. As of 25 November 2010:http://www.*csrc.nist.gov/groups/SNS/cloud-computing/cloud-def-v15.doc*

[5] Mell, Peter & Tim Grance, ‘Effectively and Securely Using the Cloud Computing Paradigm’. Presentation, NIST Information Technology Division, 2009b.

[6] Mills, Laurin H., ‘Legal Issues Associated with Cloud Computing’, presentation, May 2009. As of 25 November 2010: http://www.secureit.com/resources/Cloud%20Computing%20Mills%20Nixon%20Peabody%205-09.pdf

[7] Murty, James, *Programming Amazon Web Services: S3, EC2, SQS, FPS, and SimpleDB*, Sebastopol, CA: O'Reilly, 2008.Nature ‘web matters’, 2000. As of 25 November 2010: http://www.nature.com/nature/webmatters/grid/grid.html

[8] Nelson, Michael R., ‘The Cloud, the Crowd, and Public Policy’, *Issues in Science and Technology*, 2009/Summer:71–76. As of 25 November 2010: http://cct.georgetown.edu/Nelson%20Cloud%20Article.pdf

[9] NIST, ‘Recommended Security Controls for Information Systems’, Special Publication 800-31-1, 2005, National Institute of Standards and Technology.

[10] Nurmi et al., ‘The Eucalyptus Open-Source Cloud Computing System’, *J. Phys.: Conf. Ser.* 2009/180:012051. As of 25 November 2010:

http://open.eucalyptus.com/documents/ccgrid2009.pdf

[11] OECD, ‘Briefing Paper for the ICCP Technology Foresight Forum: Cloud Computing and Public Policy’, DSTI/ICCP(2009)17, 2009.

[12] O’Malley, Owen, ‘Hadoop World: Security and API Compatibility’, presentation, 2009.As of 25 November 2010:

[13] B. Emmerson, M2M: the internet of 50 billion devices, Huawei Win–Win Mag. J. (4) (2010) 19–22.

[14] D. Boswarthick, O. Elloumi, O. Hersent, M2M Communications: A Systems Approach, first ed., Wiley Publishing, 2012.

[15] O. Hersent, D. Boswarthick, O. Elloumi, The Internet of Things: Key Applications and Protocols, second ed., Wiley Publishing, 2012