International Journal of Advanced Computer Research (ISSN (print): 2249-7277 ISSN (online): 2277-7970)
Volume-2 Number-2 Issue-4 June-2012

Cloud Computing Issues-A Survey

M.Malathi
Associate Professor, Department of Computer Science Engineering,
Indra Ganesan College of Engineering, Tiruchi, India.

Abstract

Cloud Computing is being adopted by many companies because of its capacity to use computing and storage resources on a metered basis thereby reducing the investments in infrastructure. With all its benefits, cloud computing also brings along concerns about the security, privacy and jurisdiction because of its size, structure, and geographical dispersion. This paper tries to explore these concerns and gives suggestions which may help companies to take security initiatives before they actually move into the cloud.

Keywords

Confidentiality, integrity, availability, privacy, access control, contracts, jurisdiction

1. Introduction

Cloud computing is a model for enabling convenient, on-demand network access to a shared pool of configurable and reliable computing resources that can be rapidly provisioned and released with minimal consumer management effort or service provider interaction [1]. There are number of choices that a consumer can use to take advantages of the benefits of cloud computing. These choices comprise the cloud delivery models SaaS, PaaS, Iaas and the private, community, public and hybrid cloud deployment models. The combinations selected and their implementations are a function of the types of applications involved, storage needs, time needs, scaling requirements, and the cost associated with it.
But companies need to take some precautions about security, privacy and jurisdiction issues before they enjoy the advantages of the cloud. This paper presents various issues related to the cloud and provides suggestions to come over it. Section 2 gives the Literature review. Section 3 describes the security issues. Section 4 raises concerns about privacy. Section 5 gives jurisdiction issues and solutions and conclusion is drawn.

2. Literature Review

In 2010 Minqi et al in their paper 'Security and Privacy in Cloud Computing: A Survey [2]', have given their opinions regarding cloud computing. They have addressed various problems related to data availability, integrity and privacy. In 2012 Rohit et al presented security issues in their work [3]. In 2009 Pearson has discussed the ways in which these issues can be handled [4]. In 2011 Wang Ziydan has given some suggestions and methods to overcome these concerns [5]. But they have not given importance to jurisdiction. As the customers do not know where their data is jurisdiction also plays an important role. In 2012 Malathi et al in their paper addressed these issues [6].But suggestions for improving confidentiality, integrity and availability had not been given. This paper addresses all these issues and has given solutions for companies to take precautions before they put their data in to the cloud.

3. Security Issues

Confidentiality: Confidentiality refers to the prevention of unauthorized disclosure of information. Confidentiality in cloud systems is related to the areas of intellectual property rights, covert channels, traffic analysis, encryption and inference.

- Intellectual property rights: Rights to intellectual property are covered by copy right laws, which are granted for new inventions.
- Covert channels: It is an unintended communication path that enables the exchange of information. Covert channels are created through timing of messages or inappropriate use of storage mechanisms.
- Traffic analysis: It is a breach of confidentiality that is accomplished by analyzing the volume, rate, source and destination locations of the traffic.
- Encryption: Converting the messages so that they cannot be read by unauthorized person. The encryption algorithm and the keys should be such that it should take a lot of effort to decrypt the algorithm.

- Inference: Ability of a person to use information of less security to uncover information that is protected at higher level.

There are two approaches to solve these problems. One is physical isolation and the other is cryptography. Virtual local area networks and network middle boxes should be deployed to achieve the virtual physical isolation [7].Encrypted storage provides security for the data stored in the cloud. This approach is used by TC3[8], a healthcare company when moving their HIPAA compliant application to AWS.

Integrity: Integrity requires that data should not be modified by unauthorized persons, and unauthorized modification of data should not be made by authorized persons. To provide integrity two techniques can be followed. One is RAID (Redundant Array of Independent Disks)like technique and the other is Digital Signature. For example Zetta[9] provides Zetta system for storage service on demand. Zetta implements RAIN-6(Redundant Array of Independent Nodes-6) in its Zetta system for the primary data hosting service. RAIN-6 is similar to RAID-6 which provides data integrity by data placement in terms of node striping. Digital signature is another technique where data is divided into a set of blocks and when a block is physically stored on, a digital signature is attached to it providing integrity.

Availability: Availability should ensure timely access to cloud data and resources by authorized persons. Two strategies, hardening and redundancy are mainly used to enhance the availability of the Cloud system, or applications hosted on it. Many Cloud Computing system vendors provide Cloud infrastructures and platforms based on virtual machines. For example Amazon Web Services provide EC2, S3 entirely based on the virtual machine called Xen[10]. Cloud depends on virtualization to tie commodity personal computers or servers together and to provide a scalable, robust system. Thus this virtual machine is always available to use. As for redundancy, large Cloud Computing system vendors like Amazon, Google offer geographic redundancy in their Cloud Systems, enabling high availability. Google File System (GFS) developed by Google set 3 as the default number of replications for each object it stores which enhances the availability of the system[11].

Cloud security services: Services that should be provided by the cloud for the above are

- Authentication: Ensures persons are the ones who claim to be.
- Authorization: Refers to rights and privileges given to individuals for particular resources.
- Auditing: For the inspection of people who are logging in and the resources they use. Companies use two basic methods, System audits and monitoring.

These methods can be employed by cloud customer and the cloud provider. System audit is a onetime audit or periodic event to evaluate security. Monitoring refers to ongoing activity that examines either the system or the users, such as intrusion detection.

Accountability: It is the ability to determine the actions and behaviors of a single individual with in a cloud system and to identify that particular individual. It is related to the concept of nonrepudiation where an individual cannot deny sending a message. Accountability can be achieved by attaching digital signature.

Relevant cloud security principles:
Cloud Security principles that have to be followed are

- Least privileges: A person or a process should be given the minimum privileges and resources for minimum period of time to complete a task. It prevents unauthorized access to sensitive information.

- Separation of Duties: An authorization requires signature of more than one individual and decryption key should be with different reliable persons.

- Defense in depth: It is the application of multiple layers where the lower layer provides security to the upper layer.

- Fail safe: If a cloud fails, the security and its data should not be compromised. If system recovery is not automatic, only the system administrator should access the failed system and the other users.

- Complete mediation: Every request by a subject to an object should undergo complete authentication procedure. Complete mediation entails the following: Identification of the entity making the access request, verification that the request has not changed since its initiation, application of the appropriate authorization procedures. re-examination of previously authorized requests by the same entity [12].

- Psychological Acceptability: It refers to the user friendly nature of user interface without complex instructions.

Proper design of a cloud based IT system should also meet the following requirements. Secure access from remote locations, a distributed architecture with no single point of failure, integral redundancy of applications and information, geographical description.

Access Control: Access control is necessary to preserve the confidentiality, integrity and availability of cloud data. The concepts defined for access control are

- Threat: An event or activity that has potential to cause harm to the information systems and networks.

- Vulnerability: Lack of safety measures that can be exploited by threat, causing harm to the information systems and networks.

- Risk: The potential for harm or loss to an information system or network. The probability that a threat will may occur.

Controls are implemented to mitigate risks and reduce potential for loss. There are two important concepts. One is separation of duties and the other is privilege of duties. Separation of duties requires an activity or process to be performed by two or more entities for successful operation. So the only way that a security policy can be violated is, if there is collusion among the entities. Privilege of duties can be accomplished by controls. Control measures can be administrative, technical and physical in their implementation. Administrative controls include policies and procedures, security awareness training, background checks, work habit checks and increased supervision. Technical controls involve the restriction of access to systems and information. Examples are encryption, smart cards, access control lists and transmission protocols. Physical controls can be locking server rooms or laptops the protection of cables, the separation of duties and the backing up of files. Controls provide accountability for individuals who are accessing sensitive information in a cloud environment. So this accountability is accomplished through access control mechanisms that require identification and authentication and through the audit function.

Models for Controlling Access: Controlling access by a subject to an object requires access rules. These rules can be classified as Mandatory, Discretionary Non-Discretionary access control [13].

- Mandatory access control: The authorization of a subject's access to an object depends on labels, which indicate the subject's clearance, and the classification or sensitivity of the object. An individual can get a clearance of confidential, secret or top secret and can get access to documents below his or her specified clearance level.

- Discretionary Access control: With this control, the subject has access with in certain limitations to an object based on access control lists.

- Non-Discretionary Access control: A central authority determines which subjects can have access to certain objects based on the organizational security policy. The access controls can be role based or task based.

Single Sign On: When users must remember numerous passwords and IDs, they might take shortcuts in creating them that could leave them to exploitation. In SSO security, a user provides one ID and password per work session and is automatically logged on to all the required applications. SSO can be implemented by using scripts that replay the users multiple logins or by using authentication servers to verify a user's identity, and encrypted authentication tickets to permit access to system services. SSO can be implemented on web applications residing on different servers in the same domain by using non-persistent, encrypted cookies on the client interface.
Another solution is to build a secure credential for each user on a reverse proxy that is situated in front of the web server. The credential is then presented each time a user attempts to access protected web applications.

4. Privacy issues

One area that is greatly affected by cloud computing is privacy. A successful identity theft exploit can result in a privacy loss that affects a company due to loss of credibility, confidence and negative publicity. A person's right to privacy comes under the following principles.

- Notice: With respect to the collection, use and disclosure of Personally Identifiable Information.
- Choice: To opt out or opt in regarding disclosure of PII to third parties.
- Access: By consumers to their PII to permit and review and correction of information.
- Security: To protect PII from unauthorized disclosure.
- Enforcement: Of applicable privacy policies and obligations.

There are various laws, legislation and acts that should be applicable to the cloud. The various acts that exist for privacy should apply to a cloud also. Some of them are The Cable Communication Policy Act [14], The Children's Online Privacy Protection Act, Customer Proprietary Network Information rules, The Financial services Modernization Act and The Telephone Consumer Protection Act. But most important of them is Health Insurance Portability and Accountability Act [15].

The protection from disclosure and misuse of an individual's medical information is a prime example of a privacy law.

Generally these policies cover the following areas. Statement of the organization's commitment to privacy, the type of information collected such as names, addresses, credit card information, phone nos and so on, retaining and using email correspondence, information gathered through cookies and Web server logs, and how that information is used, how information is shared with affiliates and strategic partners, mechanisms to secure information transmissions, such as encryption and digital signatures.

The measures to be taken by an organization to comply with privacy policies are procedures for review of the organization's compliance with the privacy policy, evaluation of information protection practices, means for the user to access and correct PII held by organization, rules for disclosing PII to outside parties, providing PII that is legally required.

5. Jurisdiction issues

A key issue often ignored by companies in evaluating the value of the cloud is Jurisdiction. Generally, a company doing business in a particular geographic area will be subjected to jurisdiction in that area. This typically means that a company is responsible for producing its documents without regard to where the documents are physically stored, provided they are the company's documents or the company has control over the documents. However, because a company using cloud storage will place its documents in a different physical location from the office of that company, several new questions may arise [16].

By storing documents in a cloud located in a different place from the company's offices, does the company agree to jurisdiction rules in that location? Is the company considered to be doing business in that location merely because it locates documents there? States have laws governing privacy and confidentiality that can lead to major problems for violating those laws. With cloud computing, the important question is, which jurisdiction does a company belong? There are three possibilities.

Because of the physical storage of documents in a particular location, the documents can be governed by the law of the state in which they are physically located or by the location of the company possessing them or by the laws of the state where cloud service provider resides. If the government wishes to review, or even seize, the records located in the cloud does it have the power to do so? If there is a dispute over that issue, which court would have jurisdiction? It is important to remember that law enforcement and government agencies may have difficulty using their authorized powers if they are outside of their jurisdictional limits. More complications arise when the documents are stored in another country. Confidentiality and privacy laws vary greatly from country to country.

Another potential area for disputes involves intellectual property rights, which can vary from country to country. Affiliated companies may go for different locations for data storage and maintenance that leads to another complication. Copyright rules differ from country to country. The applicable law is determined by where the software is created. Accordingly, cloud computing shows uncertainty and has the potential for future disputes concerning.

Some of these issues can be addressed in the cloud computing contract. Companies must retain ownership and control of their data. Agreements can be made concerning the jurisdiction disputes over the data. If developers on a cloud computing project are scattered around the world, the rules can be a combination of domestic law, foreign law and international laws. Exploring this, needs a good understanding of the conflict of laws and principles that govern international transactions. When information might be stored in the ‘‘cloud’’ somewhere and cloud computing services are consumed somewhere, there is a risk that the courts could claim jurisdiction based on the location of the consumer/customer. Operators of cloud computing sites might be able to control their jurisdictional risks to a certain degree by preventing customers in certain jurisdictions from accessing the services.

Through contractual measures [16] a company can protect itself against some of the risks. Another option available for service providers in order to limit cloud computing risks is to ensure that their contracts with IT services vendors limit the scope of subcontracting [17].

This can be done by including in a contract, a list of prohibited subcontractors and by limiting subcontracting to a list of pre-approved subcontractors. The advantage of limiting subcontracting from the customer’s perspective is that subcontractors are known to operate or use servers in jurisdictions of concern, and then the customer has a certain degree of control over data flows in the cloud. Similarly, a customer could ask the service provider not to use servers located in particular countries of concern. In case of disputes data can be shifted from one location to another location.

6. Conclusion

Issues related to security and privacy and jurisdiction when designing and using cloud services are studied and suggestions are given to overcome these issues. A Cloud solution provider must ensure that customers can continue to have the same security and privacy controls over their applications and services by following some standard security techniques, privacy policies. Jurisdiction issues also have been covered because they play a prominent role in cloud computing. In future, more security strategies have to be developed to achieve data confidentiality, availability, and integrity as well as to enhance the privacy acts and jurisdictional laws.

References

[1] National Institute of Standards and Technology, http://csrc.nit.gov/groups/cloud computing.
[2] Minqi Zhou et al “Security and privacy in cloud computing: A survey”, proceedings of Sixth international conference on semantics, knowledge and grids, .978-0-7695-4189-1/10, 2010.
[3] Rohit et al, “A Survey on security issues in cloudcomputing” proceedings of IEEE second international conference on cloud computing technology and science (cloud com) at S Indianapolis, 2012.
[4] S. Pearson, “Taking Account of Privacy when Designing Cloud Computing services”, CLOUD’09, Vancouver, Canada, May 23, 2009.
[5] Wang ziyaden,”Security and Privacy issues in cloud computing” proceedings of International Conference on computational and informational sciences(ICCIS)Chengdu, china,2011.
[6] Malathi et al “A study on security, Privacy and jurisdiction issues” proceedings of 4th International Conference on Science, Engineering and Technology, Vellore, May 2012.
[7] M.Ambrust et al, “Above the clouds: A Berkeley view of Cloud Computing”, University of California,Berkeley, Tech.Rep. 2009.
T.HealthCare, “TC3 HealthCare”
[8] http://www.tc3healthcare.com/, 2008.
[9] Zetta, “zetta: Enterprise Cloud storage on Demand”, http://www.zetta.net/,2008.
[10] GNU,”XEN”, http://www.xen.org/2008.
[11] Ghemovat et al, “The Google File System” in the proceedings of the 19th symbosium on operating System Principles, pp 29-43, 2003.
[12] Ronald L Krutz and Russell Dean Vines “CLOUDSECURITY A Comprehensive Guide to Secure Cloud Computing” Page no 68.
[13] Ronald L Krutz and Russell Dean Vines”CLOUDSECURITY A Comprehensive Guide to Secure Cloud Computing” Page 212.
[14] Parsons, Patrick, and Rob Frieden. The cable and satellite television industries. Boston, MA: Allyn and Bacon, 1998.
[15] Dwyer III, Samuel J., Alfred C. Weaver, and Kristen Knight Hughes. "Health Insurance Portability and Accountability Act." Security Issues in the Digital Medical Enterprise (2004).
[16] Daniel Garrie: Who has Legal Jurisdiction in the Cloud? 18 August 2010 http://www.Gplus.com/cloud still too dark for legal information.
[17] Jan Kyer, Gabriel Where in the cloud is my data?Jurisdictional issues with cloud computing, stern, 30, March, 2011 www.fasken.com.

Malathi received the BE degree in Electricals and Electronics Engineering in Madurai Kamaraj University, Tamilnadu and ME degree in Computer Science Engineering in Vinayaka Mission University Salem. Her research interests include Network Security and Cryptography and Security in Cloud Computing and she is a member of IEEE. Currently she is working as Associate Professor in Indra Ganesan College of Engineering, Tiruchi, India.