ISSN:2231-0711

Present Trends of Data Protection Policies in Cloud Computing

Shri. RK. Bigensana Singh*, Dr. Lakshmi Prasad Saikia **

*MTech (CSE) 5th Semester, Assam Down Town University, Panikhaiti, Assam, India
**Professor & HOD, Computer Sc. Dept., Assam Down Town University, Panikhaiti, Assam, India

Abstract: Cloud Computing is an emerging technology of sharing computational resources through a network may be LAN, MAN, WAN or the Internet. The resources which can share on Cloud are Software, Platform, Data Storage & Infrastructure. There are two parties involved in this technology – (i) Cloud Service Provider (CSP) (ii) Cloud Consumer (CC). CSP develops necessary infrastructure to facilitate the service and CC uses the services through network connection. Cloud Computing makes outsourcing of computing environment for an individual or an enterprise so that they can avoid committing large capital outlays when purchasing & managing software and hardware as well as dealing with the operational overhead therein. Although cloud computing's benefits are tremendous, data security and protection is one of the major concern in Cloud Computing. Both the parties – CSP and CC need to understand the possible loopholes and need to strictly follow the recommended do's and don'ts to protect data and make is secure. In this paper, we present various do's and don'ts frame-worked by different leading organizations to become the cloud computing environment fully secure and trustworthy.

Index Terms: Cloud Computing, Data Encryption, Data at Rest, Data in motion

I. Introduction

Cloud Computing is use of internet-based/network-based service to support business process. It is to rent IT-Services on a utility like basis. Attributes of Cloud Computing are Rapid deployment, Low startup costs/capital investments, Costs based on usage or subscription, Multi-tenant sharing of services/resources. And, the following are the essential characteristics "on-demand self-service", "Ubiquitous network access", "Location independent resource pooling", "Rapid elasticity" and "Measured service". It can also defined as a compilation of existing techniques and technologies, packaged within a new infrastructure paradigm that offers improved scalability, elasticity, business agility, faster startup time, reduced management costs, and just-in-time availability of resources [8].

If an organization or individual is planning to purchase Cloud Service then, the organization or individual need to know "the type of service(s) like to get from CSP", "advantages and disadvantages of Cloud Computing" and "Privacy, Security and Terms & Conditions". To use this service, the organization or individual need to have "A Computer/laptop/smart phone or other applicable devices" and "Reliable Internet connection (for cloud services through internet)".

There are three Delivery/Service Models of Cloud Computing they are:

a) SaaS (Software as a Service):
Providing software/ applications as a service

b) PaaS (Platform as a Service):
Providing platform as a service

c) IaaS (Infrastructure as a Service) :
Providing virtual environment of infrastructure as a service

And, Cloud Computing has four Deployment Models. They are:

a) Private cloud – privately setup & owned cloud within the Organization.

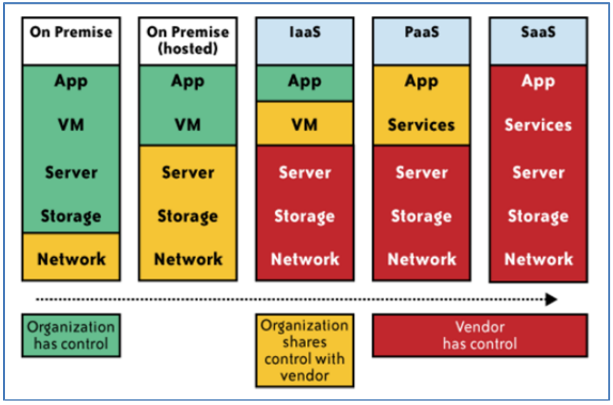
b) Community cloud – Cloud developed for a group of People.

c) Public cloud – Cloud developed for use by pubic on payment basis over the internet.

d) Hybrid cloud – An integrated cloud utilising both private and public clouds to perform distinct functions within the same organisation.

Major Advantages of Cloud Computing are "Low Cost", "Reliability", "Manageability", "Flexibility", and "Scalability". Cloud Computing has the disadvantages of "Lack of Privacy", "Limited Control", "Lack of Transparency", "Downtime" and another major concern of **Data Security/ Protection.**

Cloud computing gives a major impact to the governance structure of IT Organization. Following figure shows the impact of Cloud Computing on the governance of IT organization [7].



II. CLOUD COMPUTING & DATA SECURITY

Data are at the core of information security concerns for any organization – whatever the form of infrastructure used. Data Security is one of the most difficult task to implement in cloud computing. Different forms of attacks in the application side and in the hardware components are possible. Local complex data management system is outsourced to the Cloud Service Providers (CSP) to get cloud computing advantages. Such Data items may include emails, personal health record, photo albums, confidential tax documents, financial transactions etc. Once such data is out of physical possession, its confidentiality and integrity can be at risk. Followings are the type of Risk on Data in cloud Computing:

a) Risk of theft or unauthorized disclosure of data which may leads to Loss on Confidentiality.
b) Risk of tampering or unauthorized modification of data which may leads to Loss of Integrity.
c) Risk of loss or unavailability of data i.e. Non-availability.

The above mentioned risk applies to:

a) Data at Client's Device(Local Host which connects to the Cloud)
b) Data in motion (when data is being transferred over some form of communication link)
c) Data at rest (when data is held by the Cloud Service Provider in some form)

Level of impact to the organization of the above three risk can be elaborated as follows:

a) Risk Type: **Loss of Confidentiality**

Impact Level	**Elaboration**
Low	The unauthorized disclosure of information could be expected to have a limited adverse effect on organizational operations, organizational assets, or individuals.
Moderate	The unauthorized disclosure of information could be expected to have a serious adverse effect on organizational operations, organizational assets, or individuals.
High	The unauthorized disclosure of information could be expected to have a severe or catastrophic adverse effect on organizational operations, organizational assets, or individuals.

b) Risk Type: **Loss of Integrity**

Impact Level	**Elaboration**
Low	The unauthorized modification or destruction of information could be expected to have a limited adverse effect on organizational operations, organizational assets, or individuals.
Moderate	The unauthorized modification or destruction of information could be expected to have a serious adverse effect on organizational operations, organizational assets, or individuals.
High	The unauthorized modification or destruction of information could be expected to have a severe or catastrophic adverse effect on organizational operations, organizational assets, or individuals.

c) Risk Type: **Non-Availability**

This risk can be assessed as per CSP's stated level of availability.

III. DATA PROTECTION POLICIES AT CLOUD CONSUMER's DEVICE

Local host machines/Client's Devices which connect to Cloud are to be treated as part of the cloud infrastructure. They are not outside the security perimeter. While cloud consumers worry about the security on the cloud provider's site, they may easily forget to harden their own machines. The lack of security of local devices can provide a way for malicious services on the cloud. With mobile devices, the threat may be even stronger. Users may misplace or have the device stolen from them. Security mechanisms on handheld gadgets are often times insufficient compared to say, a desktop computer which may provides a potential attacker an easy avenue into a cloud system. If a user relies mainly on a mobile device to access cloud data, the threat to availability is also increased as mobile devices malfunction or are lost.
Hence, Local host machines/Client's Devices that access the cloud should have

- Strong authentication mechanisms
- Tamper-resistant mechanisms
- Strong isolation between applications
- Methods to trust the OS
- Cryptographic functionality when traffic confidentiality is required.

IV. DATA PROTECTION POLICIES WHEN DATA IS IN MOTION.

Data is travelled through a communication channel when CC uses the cloud service. For Community, Public &

Hybrid clouds, the main communication channel is through internet. The Internet is, in every sense, a public network. Anyone and everyone is on it, making it a hotbed for all kinds of scam and hacking activity. Professional hackers from around the world are available for hire as sort of high-tech hit men. Secrets aren't secret on the Internet unless they're securely encrypted. Even a private Multiprotocol Label Switching (MPLS) network also traverses a network that carries traffic from thousands of other users, including traffic from other carriers. With more companies facing the real and growing threat of data theft, along with increased regulatory pressure to protect their data, encryption of data in motion has gone from a "nice-to-have" technology to a necessity.

Security standards to consider for protecting of data which is in motion are frame worked in draft ISO 27017 standards. They are:

- To use of HTTPS (Hyper Text Transfer Protocol Secure) for regular connections cloud service customers over internet to cloud services.
- To use of SFTP (Secure File Transfer Protocol) for bulk data transfer.
- To use of VPN using IPSec or SSL (Virtual Private Network using IP Security or Secure Service Layer Protocol) preferably for connections from employees to the customer to the cloud Service.
- Facilitating Group encryption by CSP

The last one is generally based on purpose- built encryption appliances deployed to all linked sites. These appliances are under the control of a central manager. Group policies specify what traffic to secure, how to secure it, and which enforcement points should use the rule.

Group policies also specify which encryption and authentication algorithms to use and how often to rotate the keys. The central manager generates keys and securely distributes the keys and group policies to encryption appliances.

V. Data Protection Policies When Data Is At Rest.

Data are stored in virtualized pool of storage hosted by the third parties. The same hardware is used to store data from different customers. It may be possible that, strict security measures are not taken up by CSP to prevent unauthorized access, copying, using or modifying personal information. In the virtualized multi-tenant environment, SW bugs and newly identified security vulnerabilities are the major threats. Multi-tenancy also opens doors for potential privacy leaks. One of such case may be side channel attack. One of the best Solution for data protection & Security when data is at rest is Encryption of Data. There are several Symmetric (*only one key is used to encrypt & decrypt data*) data encryption algorithms and Asymmetric (*two keys –public & private keys used, public key is used to encrypt data and Private keys is used to decrypt data*) data encryption algorithms.

Some of the Security tips for protecting data at rest are:

- Identify sensitive data and encrypt it before uploading to Cloud.
- The algorithm chosen for encryption should be recommended by a standard such as the US FIPS 140-224.
- Encryption keys should be handled appropriately. The keys should not be stored alongside the data.
- For IaaS and PaaS, it may be the case that the keys are stored by the customer and passed to the application as required.
- For SaaS, encryption is more in the hands of the provider, in which case appropriate assurance should be sought about key handling.
- Cloud service customers should inquire if their prospective cloud service providers support KMIP (Key Management Interoperability Protocol which provides a standardized way to manage encryption keys across diverse infrastructures.

VI. Conclusion

The Simplest way for data protection is encryption before outsourcing the data. However, difficulty arises while deploying traditional data utilization services such as - plaintext keyword search or query over database. Also, downloading all data for decryption locally is impractical due to huge bandwidth cost as well as time consumption.

Hence, both the parties – CSP and Cloud Consumers need to understand the possible loopholes and need to strictly follow the recommended do's and don'ts to protect data and make is secure. Many research works also remained to become the public cloud environment fully secure and trustworthy.

References

[1] Cloud Standards Customer Council, "Security for Cloud Computing - Ten Steps to Ensure Success Version 2.0, March, 2015" http://cloudcouncil.org/Security_for_Cloud_Computing_Version_2.pdf

[2] ISO/IEC 27017 — Information technology — Security techniques — Code of practice for information security controls based on ISO/IEC 27002 for cloud services (DRAFT) http://www.iso27001security.com/html/27017.html

[3] Department of Defense (DoD), US Govt. "CLOUD COMPUTING SECURITY REQUIREMENTS GUIDE (SRG)" Version 1, Release 1, 12 January 2015 https://info.publicintelligence.net/DoD-CloudSecurity.pdf

[4] The BlackBox.Com – "The key to protecting data in motion**"**, 724-746-5500|blackbox.com http://www.blackbox.com/go/EncrypTight

[5] Randeep Kaur & Supriya Kinger, "Analysis of Security Algorithms in Cloud Computing" IJAIEM, Volume 3-Issue 3rd March-2014 (2319 – 4847)

[6] Mandeep Kaur & Manish Mahajan "Using encryption Algorithms to enhance the Data Security in Cloud Computing" IJCCT Volume 01 – No.12, 3rd Jan-2013 (2278-9723)

[7] Tim Mather and Subra Kumaraswamy, "Cloud Security and Privacy", ISBN-13: 978-0596802769

[8] P. Mell and T. Grance "The NIST Definition of Cloud Computing", US National Institute of Science and Technology 2011

http://csrc.nist.gov/publications/nistpubs/800-145/SP800-145.pdf

[9] Cloud Security Alliance - "Security Guidance for Critical Areas of Focus in Cloud Computing V2.1", December 2009 https://cloudsecurityalliance.org/csaguide.pdf

[10] wikipedia. org- "Cloud Computing" https://en.wikipedia.org/wiki/Cloud_computing

AUTHORS

Shri. RK Bigensana Singh, MCA, Perusing MTech(CSE) at Assam Down Town University, Guwahati, India.

Dr. Lakshmi Prasad Saikia, PhD, Professor & HOD, Dept. of Computer Sc. & Engg., Assam Down Town University, Guwahati, India