IJISET - International Journal of Innovative Science, Engineering & Technology, Vol. 1 Issue 6, August 2014.
www.ijiset.com
ISSN 2348 – 7968

A review on Data Damage Avoidance in Cloud Computing

Deepika Trivedi[1], Shipra Dubey[2] and Suman Bhajia[3]

[1] Department of Computer Science / Arya Institute of Engineering & Technology, Jaipur, Rajasthan 302012/ India

[2] Department of Computer Science, Banasthali University, Jaipur, Rajasthan / India

[3] Department of Computer Science / Arya Institute of Engineering & Technology, Jaipur, Rajasthan 302012/ India

Abstract

Cloud defines the use of a collection of services, applications, information, and infrastructure. It is like a group of resources and services accessible in a pay asyou go fashion. Services like computation, network, and information storage. This paper mostly emphasis on the foremost security anxieties about cloud computing. In today's business world, many administrations practice Information Systems to accomplish their complex and business precarious information. The essential to defend such a key component of the organization cannot be over highlighted. Data Damage/Leakage Anticipation has been originate to be one of the operative ways of preventing Data Loss. DLP solutions detect and preventing lawful efforts to copy or send sensitive data, both intentionally or/and unintentionally, without authorization, by people who are authorized to access the complex information. DLP is designed to detect potential data breach incidents in appropriate method and this occurs by observing data.

Keywords: *Data leakage, DLP, Information Systems and Sensitive data1.*

1. Introduction

Rendering too many latest reviews, more than 70 percent of IT and business professionals are consuming cloud applications in both personal and enterprise occupied environments. Recollect the last time you uploaded the financial report or that important presentation to Dropbox since you wanted to transfer it to your tablet to look well ready during your board meeting? Or that colleague uploading an important, confidential proposal document to Skydrive to download it later at home to go the extra mile and work during the weekend? These are just two of many very common innocent use cases that leverage the instant sharing of any data content to company/home PC, laptop, or mobile phones, and unlimited storage of files by, in many cases, a simple click of a button.

Data Damage Avoidance on the cloud is not a new assessment. You may remember online services like Slideshare, Slidesix, Slideboom, etc. that allow you to upload presentations and share them with the world. Today, with so many cloud services and SaaS applications like DropBox, Skydrive, Google Drive, iCloud, Office365, Salesforce, etc., possibilities of sharing data are endless. However, most of the time, security is the last variable considered, especially if you think about the difficulty of tracing and detecting very sensitive data leakage or worse the lack of encryption used when storing sensitive data in the cloud. The truth is that nobody is monitoring cloud-based applications.

2. Why is the Cloud creating so much Safety Thrill?

- ✓ Cloud Services are increasing in both personal and enterprise employed environments.
- ✓ Permits limitless storage of files by a simple click of a button.

ISSN 2348 – 7968

- ✓ Relaxed to access by employees from their company PC, laptop or mobile phone
- ✓ Permits immediate sharing of any data and sensitive content to third parties
- ✓ Allows storage of unencrypted complex data
- ✓ Problematic to hint and detect data outflow
- ✓ Virtual storage spaces are here to stay
- ✓ It is the IT safety problem for network administrators

3. How to protect your company data against the Cloud Threat?

The Content-Aware Data Loss Prevention solution for Cloud Services by Endpoint Protector got everything covered through:

- The Content Aware Protection feature, which enables a detailed and in depth inspection, detection, blocking and reporting of all sensitive content transferred to Cloud Services like:
  - Dropbox
  - iCloud
    - Google Drive
    - SugarSync
    - Microsoft SkyDrive
    - Etc....

Allowing you to know at any time who, how and what data goes out (or tried to get out) towards the cloud.

- The Device Control feature, which adds additional protection by controlling how and what sensitive company data content stored on removable (e.g. USB Drive) and mobile devices can reach the virtual space.
- The Enforced Encryption feature, which offers automatic military-grade encryption of all data copied on removable storage devices.

How it works?

- User attempts to upload a file to a cloud service
- Content is inspected before upload to the cloud
- If sensitive content is detected, violating a policy, the incident is reported and/or blocked

ISSN 2348 – 7968

- Data transfer is stopped to protect company information and logged for later auditing

4. Recognize the data sources, movement and endpoint

The key to start resolving the problematic is to have a clear sympathetic of what information is really most momentous to the business. This generally gets talented with a data calculation, which must include data detection and data fingerprinting that provides a better understanding as to where, who, when and in what format the information is being generated and in what devices it is being stored. In addition, identifying the cloud services currently being used and the type of data that is being moved to the cloud is an significant step during this process.

5. Enforce security as everybody's responsibility

Once the data organization determination has been done and it is properly documented, awareness is the key ingredient in making security everybody's responsibility. Many organizations develop awareness programs in which they incorporate regular and nonstop communication to share IT security policy particulars like data classification criteria, common threats, who to contact, tools, etc. Moreover, many organizations supplement this exertion with annual consciousness sessions in which employees or associates not only join a meeting but also sign the actual data classification policy adhering to protecting confidential information.

6. Select the accurate tool for you

DLP facilities work essentially by classifying evidence that desires to be threatened, indexing it and securing it. The DLP system can prevent, for example, sensitive data, such as customer credit card information, from being downloaded onto an employee's USB drive.

Once the type of facts that is dangerous for your association, business necessities to inhibit data damage anticipation, as well as the regulations requirements have been identified; it will be time to define, through a risk-based approach, the use cases your company needs to focus on. Tools usually focus on providing the same standard procedure, generally providing continuous monitoring. Thus, when the user attempts to upload a file to a cloud service, the tool inspects the content before uploading to the cloud. If sensitive content is detected, violating a policy, the incident is reported and/or blocked. Therefore, data transfer is stopped to protect company information and logged for later auditing. Evaluating the technical protocols that the DLP solutions support is essential. While some applications use HTTP/HTTPS to upload information, others use secure RDP. On the other hand, based on the specific use cases, at some point you may want to evaluate encryption solutions for data at rest or in transit. Many times, rather than spending a great deal of effort on a DLP initiative, a good encryption strategy may work.

In regard to the delivery model, there are some variations in the DLP tools. Some tools leverage the cloud to store the metadata associated to the events that are being captured. While they provide real-time monitoring and great

ISSN 2348 – 7968

dashboards that can be accessed from anywhere, their offerings usually articulate the value in simplifying the network and reducing the total cost of ownership. However, some security practitioners would rather keep the information on premise since they consider it is inefficient to copy all the data into the cloud for analysis.

7. Harmony your DLP Policy

Deliver conspicuousness! Permitting upper administration and the main investors to see and appreciate the results attained for the carrying out of the DLP process and tools is vital. Make sure they clearly understand the value that the initiative generates. This will undoubtedly help you to gain even more support and credibility, but most prominently, it will make them aware of the implications of the use of cloud services and applications. This is the way to inspiration the management team to think about security before accepting new technologies for either operational and/or financial effectiveness.

8. Conclusion

Data leak prevention (DLP) is a complement of technologies intended at stemming the loss of delicate information that occurs in enterprises across the sphere. By engaged on the location, organization and nursing of information at rest, in use and in motion, this solution can go far in helping an enterprise get a handle on what information it has, and in stopping the numerous leaks of information that occur each day. DLP is not a plug-and-play solution. The fruitful execution of this technology needs important groundwork and hard-working continuing preservation. Originalities looking for to incorporate and appliance DLP should be ready for an important effort that, if done appropriately, can momentously decrease danger to the group. Those implementing the solution must take a strategic approach that discourses risks, impacts and modification steps, along with suitable authority and guarantee actions.

References

[1] Wang Zhiying, Ren Jiangchun, Wu Jiangjiang, Cheng Yong and Mei Songzhu,"
The Application of Chinese Wall Policy in Data Leakage Prevention" in International Conference on Communication Systems and Network Technologies,2012.

[2]Charles PEREZ, Babiga BIRREGAH, Marc LEMERCIER, "The Multi-layer imbrication for dataleakage prevention from mobile devices"in IEEE 11th International Conference on Trust, Security and Privacy in Computing and Communications,2012.

[3]Zhang Xiaosong , Liu Fei , Chen Ting , LiHua , "Research and Application of the
Bijayalaxmi Purohit, Pawan Prakash Singh/ International Journal of Engineering Research and Applications (IJERA) ISSN: 2248-9622www.ijera.comVol.3, Issue 3, May-Jun 2013, pp.1311-13161316| P a g eTransparent Data Encpryption In Intranet Data Leakage Prevention" in Internationa Conference on Computational Intelligence and Security,2009.

[4]Janusz Marecki, Mudhakar Srivatsa, Pradeep Varakantham,"A Decision Theoretic Approachto Data Leakage Prevention "in IEEE International Conference on Social Computing / IEEE International Conference on Privacy, Security, Risk and Trust.

[5]M. Srivatsa, P. Rohatgi, S. Balfe, and S. Reidt, "Securing information flows: A metadata framework," in Proceedings of 1st IEEE Workshop on Quality of Information for Sensor Networks (QoISN), 2008.

ISSN 2348 – 7968

[6]D. Roberts, G. Lock, and D. Verma, “Holistan: A Futuristic Scenario for International Coalition Operations,” in In Proceedings of Fourth International Conference on Knowledge Systems for Coalition Operations (KSCO), 2007.

[7]Zhao Yong, Liu Jiqian, Han Zhen,Shen Changxiang, ”The Application of Information Leakage Defendable Model in EnterpriseIntranet”, In: Journal of Computer Research and Development, pp761-767 2007 44(5)

[8]Wang Lei, ZHUANG Yi, Pan Long-ping, ”Design and implementation of file watching system based on mandatory accesscontrol”, In: Computer Application. Vol.26 No.12 Dec.2006

[9] Lei Zheng, Zhao-feng Ma, Ming Gu, ”Techniques of File SystemFilter Driverbased and Security-enhanced Encryption System”, In:Journal of Chinese Computer Systems.Vol28.no.7,July 2007[10] Shufen Liu, Zhagxiang Zhang, Yaorui Cui, Lin tao Wu;”A Newinformation Leakage Defendable Model ” In: Computer-Aided Industrial Design and Conceptual Design, 2008. CAID/CD 2008. 9thInternational Conference on,pp:109-112, Nov. 2008

[11] Microsoft Corporations: “Using Encrypting File System”, published: November ,2005

[12]Ulf T. Mattsson, CTO Protegrity, “A Practical Implementation of Transparent Encryption and Separation of Duties in EnterpriseDatabases, Protection against External and Internal Attacks on Databases”, In: E-Commerce Technology, 2005. CEC 2005. SeventhIEEEInternational Conference on, pp:559