ISSN:2320-0790

An International Journal of Advanced Computer Technology

Review of Potential Threats on Cloud Computing

Dr. Ananthi Seshasaayee[1], Sreevidya Subramanian[2]

[1]Associate Professor & Head, Dept. of Comp Sci.,
Quaid-E-Millath College, Chennai.
[2]Research Scholar, Vels University, Chennai

Abstract: Cloud Computing is the evolution, over the past 20+ years, of a continuous trend towards the industrialization of IT. This is in part due to the popularity of outsourcing and hosting of increasingly industrialized service definitions and cost structures & pricing. This has also spurred dramatic growth in popularity and use of both internet and corporate wide intranets as trusted delivery models. But are they safe and secure for storing confidential information? How can we make sure that the client has total control over their data on the cloud? Is it true that in order to reduce the cost of operation and efficiency, we have to comprising giving away sensitive data? This paper does an in-depth study of the recurring vulnerabilities.

Keywords: DLP, SaaS, Cloud, Grid

I. INTRODUCTION

Today, cloud computing systems are providing a wide variety of services and interfaces to enable vendors to rent out spaces on their physical machines at an hourly rate for a tidy profit. The services that are provided by these vendors can vary from dynamically virtual machines to flexible hosted software services.

With the emergence of cloud computing, multibillion dollar organizations like IBM, Amazon, Google and Ebay have already invested in cloud technology.

Despite recent headlines about cloud breaches that affect millions of customers, clouds are here to stay—because doing business in them has many cost-saving benefits and can give even the smallest company a competitive edge. Recent Researches show that "the global market for cloud computing will grow from $40.7 billion in 2011 to more than $241 billion in 2020[1]."

II. CLOUD CHARACTERISTICS

The following are the most important characteristics of a cloud environment.

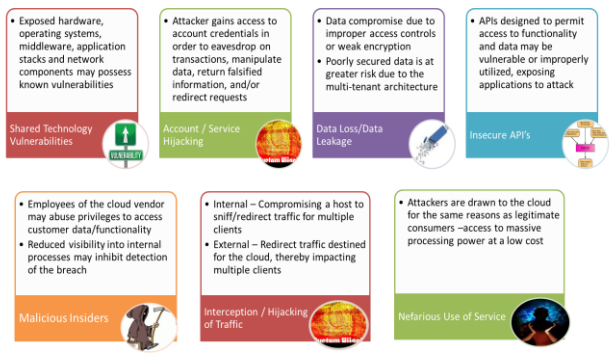
- On-demand self-service
- Ubiquitous network access
- Location independent resource pooling
- Rapid elasticity
- Measured service[2]

Four Deployment Models of Cloud*[3]*

Model	**Definition**
Private Cloud	Enterprise owned or Leased
Community Cloud	Shared Infrastructure for a specific community
Public Cloud	Sold to Public, established on a mega scale infrastructure
Hybrid Cloud	Composition of two or more cloud deployment models.

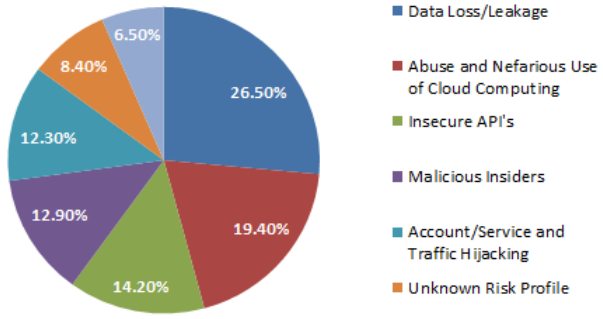
III. CLOUD THREATS & VULNERABILITIES

The CSA Top Threats Working Group, which conducted a cloud threats survey with a group of industry experts, have identified the below as the top nine notorious threats of cloud computing.
Out of these the top three threats this year were data breaches, data loss and account hijacking. In 2010[4], the top three were abuse of cloud services, insecure interfaces and APIs, and malicious insiders. Those three are still on the list but have fallen (7, 4, 6, respectively) in 2013.



Step	Explanation
Incursion	Hackers gain remote access to the network.
Discovery	Hackers map out the company's systems and scan for confidential / sensitive data.
Capture	Attackers take control of key systems and collect exposed data as it flows through these systems.
Exfiltration	The Stolen data is sent out the front door to external servers under control of the attacker.

With response to a short survey we had conducted to understand the overall Response from IT Consultants on Various Threats identified by Cloud Security Alliance resulted in a response below:



The total number of incidents[5] reported by CSP's are collated as given below:

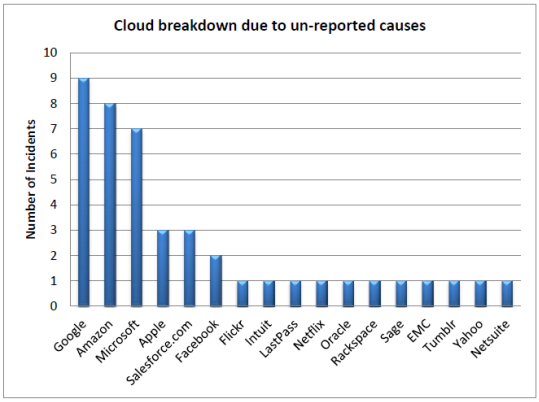


Figure 1: Number of incidents reported by cloud service providers

Let us look in to the top three threats for 2013 and proposal of mitigation strategies to resolve them.

A. Data Loss / Leakage

BYOD, cloud computing and social media have a common thread – they all create data repositories that have been geared towards the non-IT consumer, where governance, management and retention have taken a backseat to ease of use.

Hackers typically breach a cloud infrastructure using a four-step process that closely resembles the plan of attack used to breach a traditional enterprise IT environment. They are given below:

However, data stored in the cloud can be lost due to reasons other than malicious attackers. Any accidental deletion by the cloud service provider, or worse, a physical catastrophe such as a fire or earthquake, could lead to the permanent loss of customers' data unless the provider takes adequate measures to backup data.

A.A.1 Top Incidents for Data Breach:

Google Lawsuit / Security Breach

Large corporations, like Google, have come under heavy fire with regard to data collection and privacy.

Recently, the European Union has come after Google[6] with sanctions for breaching data protection laws. The search engine giant is known for having amassed one of the largest customer databases ever known with data such as full names, phone numbers, addresses, credit card numbers, search query logs, phone calls made, contact lists, etc.

Google's Internal Security Breach Raises Questions About Trust and the Cloud

Facebook – Data Loss/ Breach incident

It wouldn't be fair to forget to mention Facebook, which has had its fair share of privacy blunders, something that cannot go unnoticed when you are the world's largest social networking platform.

On Friday June 21st 2013, Facebook apologized to its users for a flaw in its system that allowed people to view private phone numbers and email addresses[7].

A.A.2 Top Incidents for Data Loss:

Amazon EC2 Cloud Services

In addition to taking down the sites of dozens of high-profile companies for hours (and, in some cases, days), Amazon's huge EC2 cloud services crash permanently destroyed some data. The data loss was apparently small relative to the total data stored, but anyone who runs a web site can immediately understand how terrifying a prospect any data loss is (And a small loss on a percentage basis for Amazon [8], obviously, could be catastrophic for some companies).

Swissdisk suffers catastrophic failure

US cloud storage supplier SwissDisk has suffered a catastrophic hardware failure resulting in users being unable to access their data. After first saying emergency maintenance was underway and that users could "rest assured that (their) data is safe [9]," SwissDisk support sent an e-mail on Saturday, October 18, to its users which said:

Attention SwissDisk Users, We regret to inform you that due to an unplanned and unforeseen catastrophic hardware failure caused by multiple simultaneous events the engineering staff was unable to restore the SwissDisk file server to it's previous status.

A.A.3 Mitigation Strategies for Data Breach and Loss:

Data Retention Policy Guidelines:

- Identify Age of Data stored
- Identify Stale Data
- Automated classification of data (based on the content type).
- Automatically archive or delete data that is meets your retention guidelines
- Automatically migrate data that is stale but contains sensitive information to a secure folder or archive within customer premises or with in an environment with limited access to non-privileged users.
- Make sure your solution can provide evidence (e.g. reports) of your defensible data retention and disposal policy.

Risk Assessments Guidelines:

The level of risk is estimated on the basis of the likelihood of an incident scenario, mapped against the estimated negative impact. The likelihood of an incident scenario is given by a threat exploiting vulnerability with a given likelihood. These are mainly:

- Classify the risks in to three categories Organizational Risks, Technical Risks and Legal Compliance Risks.
- Each Risks to be mapped against the following Risk Domains:
    - Probability of Recurrence
    - Business Impact
    - Reference to established Vulnerability
    - Risk Level
    - Mitigation Possibility
- Prepare a Roadmap for Maturity considering the implementation of mitigations identified in the assessment.
- Follow up, Validate and Sign off the implemented mitigation strategy.

Resilient Environment Guidelines

This is generally made up of two important operatives:

- Business Continuity in case of natural calamities or unknown source of problems – Make sure to have the BCP established which is validated by SME's. Twice a year BCP testing is a recommended approach.
- Disaster Recovery in case of Outages – Establish a DR setup preferably on a Private cloud environment and make sure to exercise DR Drills at least once per year.

Developing a contingency plan and exit strategy for the above two operations will benefit most enterprises from falling in to the Snake-Pit.

B. *Account Hijacking*

Account or service hijacking is not new. Attack methods such as phishing, fraud, and exploitation of software vulnerabilities still achieve results. Credentials and passwords are often reused, which amplifies the impact of such attacks. Cloud solutions add a new threat to the landscape.

If an attacker gains access to your credentials, they can eavesdrop on your activities and transactions, manipulate data, return falsified information, and redirect your clients to illegitimate sites. Your account or service instances may become a new base for the attacker. From here, they may leverage the power of your reputation to launch subsequent attacks.

B.A.1 Top Incidents for Account Hijacking:

BT email accounts hacked

Following a surge in complaints in February 2013[10], about email account hijacking incidents, BT has decided to drop Yahoo as its email partner for its broadband subscribers.

All BT broadband customers are automatically given a Yahoo Mail account, which means it will move six million accounts to the new email system. Customers will be able to keep their existing inbox and folders but will be prompted to change their password, according to BT.

Also, after 17 June, BT will begin to deleting any BT Yahoo email accounts that have not been accessed within 150 days of that date.

DreamHost Database Hack Forces Mass Password Reset

A malicious attacker gained access to a database which contained unencrypted FTP and shell passwords. DreamHost claims this was a legacy table which they had not previously deleted. They claim there are no more legacy tables with unencrypted passwords. DreamHost reset all FTP and shell access passwords. DreamHost claims the attacker did not access billing or other personal information.

Guidelines to Mitigate Account Hijacks

- Establishing high-level information security policies for protecting data
- Establishing more granular compliance-related policies for specific departments, such as finance and human resources[11]
- Establishing processes for auditing and improving policy effectiveness
- Restrict unauthorized users from accessing sensitive data by using components and methods like Governance, Risk and Compliance.
- Revoke user access on a regular basis for those who are no longer associated with the enterprise.
- Establish a fool proof intrusion detection engine (IDE)
- Conduct regular Audits[12] –e.g. CloudAudit providers are on the rise these days.
- single sign-on/off
- A single identity directory for all services
- Access control policy enforcement which comply with the company's security baseline requirements. These requirements are to be established according to the characteristics of the user profile and permission. The minimum requirements settled should be: updated antivirus and updated OS[13].
- Secure Cryptographic Key management [14].
- Identity provisioning and de-provisioning [15]

C. *Insecure Interfaces and APIs*

Attackers over the past three years have begun to actively target the digital keys used to secure the Internet infrastructure. Stuxnet's creators stole code-signing keys and then used them to allow the malware to more easily evade host-based security. An alleged Iranian hacker broke into a partner of registry Comodo and bought Secure Sockets Layer (SSL) keys for major domains to eavesdrop on activists. And unknown attackers stole important information on RSA's SecureID token[16], a device that generates one-time keys to strengthen online security.
So-called API keys are used by Web and cloud services to identify third-party applications using the services. If service providers are not careful, an attacker with access to the key can cause a denial-of-service or rack up fees on behalf of the victim.

C.A.1 Top Incidents for Insecure APIs

As more and more organizations tap into single sign-on (SSO) schemes through Web services providers such as Google and Facebook, new research suggests that they must better plan how they implement SSO APIs lest they leave users open to attack. New findings by Microsoft Research found troubling logic flaws in SSO for Facebook, Google ID, PayPal, and other Web services that threaten a large number of users online.

Guidelines to Mitigate Insecure APIs

- To guide designer to follow robust principles for designing their Interfaces.
- Establish proper version control for the custom code played out in the cloud.
- Enforce Code Policy by restricting malware functionality on the cloud.
- Stress the CSP's to have a completely integrated design which looks out for the potential malwares and provide KPI reporting on the malwares identified, so that the business can take appropriate decisions.
    - Identify the Custom code
    - Analyze the risks
    - Apply security countermeasures
    - Conduct post-run evaluations

IV. CONCLUSION

One must know the importance of what you have to consider when moving to the cloud environment. Enterprises should know their Risk Matrix well in advance where they clearly define the risks involved in outsourcing their data to another vendor but maintaining the operational rights with them.

A mere cloud certification is not enough for any provider to qualify storing customer data. All Enterprises must establish a matrix for their Risks, code changes, user management policies, KPIs, SLAs and agree with Data Management and Retention mechanisms before moving on to cloud.

Once after migrating to cloud, enterprises should also establish standards and policies to evaluate low-value assets for which same level of security controls are not needed and can skip many of the recommendations — such as on-site inspections, discoverability, and complex

encryption schemes. A high-value regulated asset might entail audit and data retention requirements. For another high-value asset not subject to regulatory restrictions, you might focus more on technical security controls.

V. REFERENCES

[1] http://www.cio.com/article/680673/Forrester_Public_Cloud_Growth_to_Surge_Especially_SaaS.

[2] E. Brown, "NIST issues cloud computing guidelines for managing security and privacy," National Institute of Standards and Technology Special Publication 800-144, January 2012.

[3] Security Guidance for Critical Areas in Cloud Security by Cloud Security Alliance Available: https://downloads.cloudsecurityalliance.org/initiatives/guidance/csaguide.v3.0.pdf

[4] "Top threats to cloud computing," in Cloud Security Alliance, 2013.

[5] Cloud Security Alliance. (2010). Top Threats to Cloud Computing (V2.0). Available: https://cloudsecurityalliance.org/topthreats/csathreats.v2.0.pdf

[6] http://readwrite.com/2010/09/16/googles-internal-security-brea - Google Lawsuit and the trust in cloud.

[7] Privacy in the Cloud: Google Lawsuits, Facebook Data Breach, NSA Leaks - http://blog.malwarebytes.org/whats-in-the-news/2013/06/privacy-in-the-cloud-google-lawsuits-facebook-data-breach-nsa-leaks/

[8] Lightning strikes Amazon cloud (honest). Available: http://www.theregister.co.uk/2009/06/12/lightning_strikes_amazon_cloud/

[9] Catastrophic Hardware Failure at Swissdisk http://www.theregister.co.uk/2009/10/19/swissdisk_failure/.

[10] http://www.telegraph.co.uk/finance/newsbysector/epic/btdota/10089355/BT-dumps-Yahoo-email-after-hacking-claims.html

[11] P. M. a. T. Grance, Effectively and Securely Using the Cloud Computing Paradigm (V0. 25), US National Institute of Standards and Technology, 2009.

[12] Zhou M, Zhang R, Xie W, Qian W, Zhou A (2010) Security and Privacy in Cloud Computing: A Survey. Proceedings IEEE Sixth International Conference on Semantics, Knowledge and Grids 2010:106-112

[13] NIST Recommended Security Controls for Federal Information Systems (SP800-53)

[14] NIST SP 800-30 Risk Management Guide for Information Technology Systems

[15] OATH- http://www.openauthentication.org

[16] Justify Identity Management Investment with Metrics, by Roberta J. Witty, Kris Brittain and Ant