Original Research Paper Computer Science

DATA SEQUESTRATION ISSUES AND CHALLENGES IN CLOUD COMPUTING: AN ANALYSIS AND REVIEW

Rachana C R Associate Professor & Head, DoS in Computer Science, Pooja Bhagavat Memorial Mahajana Education Centre.

Dr. ReshmaBanu Professor & Head, Department of I S E, GSSSIETW Mysore, Karnataka, India.

ABSTRACT Cloud computing is a model for enabling ubiquitous, 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. The cloud enables companies to share, store and consume resources easier, at a lower cost and with greater flexibility. The risk of data loss, and concerns about data privacy and regulatory compliance exist, making security risks the single biggest factor holding back faster adoption of cloud computing. Traditional security tools have not been designed for cloud environments and their unique challenges. The need to secure cloud access from anywhere across highly dynamic, virtual cloud environments is the increasing concern of cloud security experts. This paper focuses on data security issues in the cloud and the factors affecting cloud security.

KEYWORDS : Cloud security, Health care Data Breach, Data Breach cost, Integrity.

I. Introduction

Cloud Computing is a computational paradigm as well as distribution architecture. The main objective is to provide secure, quick, convenient data storage and net computing service, with all computing resources visualized as services and delivered over the Internet. [2,3]

Several authors [13-15] agree security concerns are among one of the biggest issues that will enable growth in cloud computing services. The use of public clouds demands tighter restrictions on cloud providers to incorporate into their service models. Legal complications that cloud providers must adhere to are yet to be standardized and as a result remain the biggest obstacle to continued substantial growth of the cloud model [14].

Further challenges include loss of control over IT services, disaster recovery, and insider threats and so on.

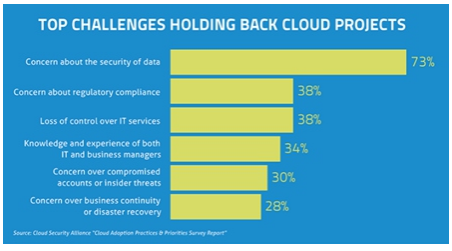

Fig. 1: Challenges in adoption of cloud service and products.

To understand the best about Adoption of cloud in business, the service and deployment models need to be reviewed.

II. Cloud Service Models:

Infrastructure as a Service (IaaS) - In IaaS, generally the service provider offers a Virtual Machine platform and underlying infrastructure with CPU, memory, storage, and networking. Enterprises then deploy their Virtual Machines into this environment. The enterprise retains control of operating systems (OS), storage data, and applications.

Platform as a Service (PaaS) - In PaaS, the enterprise retains control of applications and limited control over application hosting environment configurations. Otherwise, the enterprise relies on the service provider to provide security.

Software as a Service (SaaS) - In SaaS, the enterprise retains control of only limited user specific application configuration settings. In SaaS models, the enterprise relies on the service provider to provide security. The level of abstraction increases as cloud customers migrate from IaaS to SaaS delivery models, hence responsibility is handed to cloud providers to handle the SaaS model [11]. Furthermore [12] discuss SaaS architecture through multi-tenant utilization as it shares common resources and underlying instances of both database and object code.

III. Cloud Deployment Models:

Private Cloud: The NIST definition is: the cloud infrastructure is provisioned for exclusive use by a single organization comprising multiple consumers (e.g., business units). It may be owned, managed, and operated by the organization, a third party, or some combination of them, and it may exist on or off premises. Private clouds are a choice for companies that already own data centre and developed IT infrastructure and have particular needs around security or performance.

Public cloud: The NIST definition is: the cloud infrastructure is provisioned for open use by the general public. It may be owned, managed, and operated by a business, academic, or government organization, or some combination of them. It exists on the premises of the cloud provider and is a form of providing public cloud services and a Cloud Service Providers business model.

Hybrid Cloud: The NIST definition for Hybrid Cloud is: the cloud infrastructure is a composition of two or more distinct cloud infrastructures (private, community, or public) that remain unique entities, but are bound together by standardized or proprietary technology that enables data and application portability (e.g., cloud bursting for load balancing between clouds). Hybrid cloud, while the most complicated configuration to manage, is also the most economical model for modern companies.

Community Cloud: The NIST definition is – The cloud infrastructure is provisioned for exclusive use by a specific community of consumers from organizations that have shared concerns (e.g., mission, security requirements, policy, and compliance considerations). It may be owned, managed, and operated by one or more of the organizations in the community, a third party, or some combination of them, and it may exist on or off premises. [8]

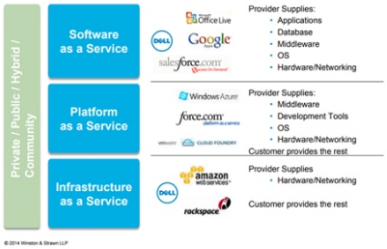

Fig. 2: Cloud service and Deployment models.

IV. Cloud Security

Confidentiality is one of the three pillars of the traditional information security model, along with availability and integrity. In terms of availability, cloud services can be provided on a 24x7 basis and cloud services providers invest heavily in business continuity and disaster recovery capabilities, providing guarantees over data recoverability and the uptime of the service.

Confidentiality can be assured by security controls such as those placed over access rights, the use of strong authentication methods, and encryption for data both when in transit and at rest. For ensuring the integrity of data, tools can be used to prove that no data has been altered, which is backed up by management reports and audit trails of all actions taken [1].

Security provided by the Cloud is stronger than what businesses can achieve with their legacy systems. This is because Cloud service providers are more focused on data protection, providing several high-end security features such as biometric identification, surveillance cameras and redundant power sources, than individual businesses.

Analyst firm Gartner estimates that the market for Cloud-based security services will grow 25 percent in 2018 and reach nearly $9 billion globally by 2020.[18]

Worldwide Cloud-Based Security Services Forecast by Segment (Millions of Dollars)

Segment	2016	2017	2018	2019	2020
Secure email gateway	654.9	702.7	752.3	811.5	873.2
Secure web gateway	635.9	707.8	786.0	873.2	970.8
IAM, IDaaS, user authentication	1,650.0	2,100.0	2,550.0	3,000.0	3,421.8
Remote vulnerability assessment	220.5	250.0	280.0	310.0	340.0
SIEM	286.8	359.0	430.0	512.1	606.7
Application security testing	341.0	397.3	455.5	514.0	571.1
Other cloud-based security services	1,051.0	1,334.0	1,609.0	1,788.0	2,140.0
Total Market	**4,840.1**	**5,850.8**	**6,862.9**	**7,808.8**	**8,923.6**

IDaaS = identity and access management as a service
Note: Numbers may not add to totals shown due to rounding.
Source: Gartner (June 2017)

Table 1: World-wide cloud based security forecast

To manage cloud security in today's world, a solution is required to address the threats posing in enterprise data and infrastructure [24]:

- **Changing attackers and threats:**

Threats are no longer the purview of isolated hackers looking for personal fame. More and more, organized crime is driving well-resourced, sophisticated, targeted attacks for financial gain.

- **Evolving architecture technologies:**

With the growth of virtualization, perimeters and their controls within the data centre are in flux, and data is no longer easily constrained or physically isolated and protected.

- **Consumerization of IT:**

As mobile devices and technologies continue to proliferate, employees want to use personally owned devices to access enterprise applications, data, and cloud services.

- **Dynamic and challenging regulatory environment:**

Organizations and their IT departments face ongoing burdens of legal and regulatory compliance with increasingly prescriptive demands and high penalties for noncompliance or breaches.

V. Data Breach in Cloud

A data breach is when an unauthorized hacker or attacker accesses a secure database or repository. Data breaches typically target logical or digital data and are often conducted over the Internet or a network connection. A data breach may result in data loss, including financial, personal and health information. For example, a hacker's data breach of a network administrator's login credentials can result in access of an entire network.

Internet security firm Symantec reveals in their annual 'Internet Security Threat Report' that India has been placed at 5th position globally in terms of data breach and exposed digital identities. The report found that globally, 1.1 billion identities of citizens were exposed via data breach, across various types of websites and portals. In total, there were 1209 data breaches across the world, which resulted in the exposure of these 1.1 billion identities. Interestingly, while the number of data breaches reduced from 1211 in 2015 to 1209 in 2016, the number of identities exposed has almost doubled from 563 million in 2015 to 1.1 billion in 2016. US is the country which experienced maximum number of data breach, as the report discovered 1023 cases of a hack, originating in U.S.[5] as shown in figure 3.

Fig. 3: Data Breach statistics of past three years

Across the globe, companies are losing a huge amount of money because of data breaches. According to a Study conducted by Ponemon Institute on cost of data breach, the participating 419 companies lost USD 3.63 million on an average in FY2017. The per capita cost of data breaches was found to be the highest in the US (USD 225) and Canada (USD 190) owing largely to high detection, notification and post data breach response cost. On the other hand, companies in Brazil (USD 79) and India (USD 64) incur lowest per capita data breach cost. Per capita cost implies total cost divided by the total number of data breaches. The average total cost attached to data breaches as shown in figure 4.

Fig. 4: Average total Cost of Data Breaches

Recently Apple suffered the largest high-profile cloud security breach due to the victims involved. Many of the victims initially thought that someone had hacked their individual phones. Instead, the iCloud service they used for personal storage had been compromised. In response, Apple urged users to employ stronger passwords and introduced a notification system that sends alerts when suspicious account activity is detected. [4]

Data breaches in health care industry are on the rise. In the world of black market, medical information has a higher value than credit card information. One reason medical data is coveted by thieves is

that it has more lasting value than other types of information. Once the thieves get their hands on it, it's difficult for the victim to do anything to protect themselves. While a stolen credit card can be cancelled and fraudulent charges disputed, the process for resolving medical ID theft is not as straightforward.

According to the Office of Civil Rights (OCR), over 322 healthcare data breach cases were reported in 2016. These are only the cases that involved more than 500 records each. The year closed with more than 16 million records exposed, primarily from healthcare providers. In fact, the healthcare industry is the most vulnerable industry to privacy breaches. [9]

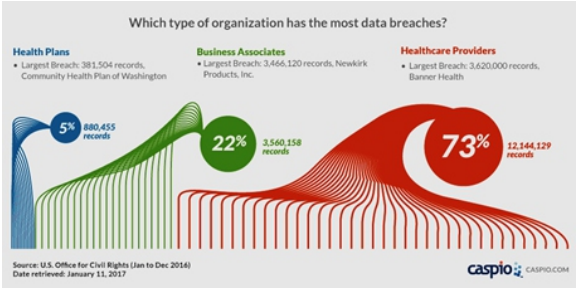

Fig. 5: Healthcare providers experienced the most data breaches in 2016.

When corporate and customer data is not stored in an onsite data centre, IT managers need to know that they will still have control of the data. Although security and privacy concerns around hybrid cloud services are similar to those of traditional IT services, they tend to escalate with the fear of external control over organizational assets and the potential for mismanagement of those assets. [23]

The information below is provided by the European Network and Information Security Agency. It outlines the way that responsibility for security should be divided between the customer and the provider of the service. This information refers primarily to the division of responsibilities for Software as Service offerings, where more of the security requirements are delegated to the service provider than for platform- or infrastructure as-a-service offerings. [1]

Customer responsibilities:

- Compliance with data protection laws in terms of the data that it collects and processes.
- Maintenance and manageability of identity management system and authentication platform.
- Service Provider responsibilities:
- Physical infrastructure security and availability
- Patch management and hardening procedures
- Security platform configuration
- Systems monitoring
- Security platform maintenance
- Log collection and security monitoring

VI. Conclusion

Almost every organisation, whatever its size or line of business, is dependent on technology. The threat is increasingly sophisticated attacks from criminals looking to compromise the sensitive information that they contain. In terms of information security, many large enterprises have commonly used the services of specialised contractors and service providers. In the age of cloud computing, those services are available to organisations of any size and make enterprise-grade security available to even the smallest organisation. The right measures of security provided to data in the cloud will reap benefits to the organization.

REFERENCES

[1] Fran Howarth, Best practices for cloud security, A White Paper by Bloor Research, January 2012.
[2] Zhao G, Liu J, Tang Y, Sun W, Zhang F, Ye X, Tang N: Cloud Computing: A Statistics Aspect of Users, First International Conference on Cloud Computing (CloudCom), Beijing, China. Heidelberg: Springer Berlin; 2009:347–358.
[3] Zhang S, Zhang S, Chen X, Huo X: Cloud Computing Research and Development Trend. In Second International Conference on Future Networks (ICFN'10), Sanya, Hainan, China. Washington, DC, USA: IEEE Computer Society; 2010:93–97.
[4] https://www.storagecraft.com/blog/7-infamous-cloud-security-breaches/
[5] http://trak.in/tags/business/2017/04/27/1-1b-identities-leaked-data-breach-email/
[6] DATA STORY: The millions lost by companies every year due to data breaches, Sep 04, 2017 01:13 PM IST | Source: Moneycontrol.com
[7] https://m.acc.com/chapters/houst/upload/FINAL-ACC-Cloud-Computing-CLE-Sept-2014_2.pdf
[8] Cloud Strategy Partners, LLC., Cloud Service and Deployment Models, IEEE Cloud Computing tutorial, IEEE eLearning Library.
[9] http://blog.caspio.com/healthcare-data-breaches/
[10] David Kolevski, Katina Michael, Cloud Computing Data Breaches-A socio-technical review of literature.
[11] J. R. Winkler, Securing the cloud: cloud computing security techniques and tactics. Burlington, MA: Elsevier, 2011.
[12] B. R. Rimal, et al., "Chapter 2. A Taxonomy, Survey, and Issues of Cloud Computing Ecosystems," in Cloud Computing: Principles, Systems and Applications, N. Antonopoulos and L. Gillam, Eds., ed London, UK: Springer-Verlag, 2010, pp. 21-46.
[13] S. Y. Esayas, "A walk in to the cloud and cloudy it remains: The challenges and prospects of 'processing' and 'transferring' personal data," Computer Law & Security Review, vol. 28, pp. 662-678, 2012.
[14] N. J. King and V. T. Raja, "Protecting the privacy and security of sensitive customer data in the cloud," Computer Law & Security Review, vol. 28, pp. 308-319, 2012.
[15] N. Kshetri, "Privacy and security issues in cloud computing: The role of institutions and institutional evolution, "Telecommunications Policy, vol. 37, pp. 372-386, 2013.
[16] http://resources.infosecinstitute.com/hackers-selling-healthcare-data-in-the-black-market/#gref
[17] http://www.healthcareitnews.com/slideshow/biggest-healthcare-breaches-2017-so-far?page=2
[18] http://www.veritis.com/blog/companies-enhance-investments-cloud-security-measures/
[19] Worldwide and Regional Public IT Cloud Services 2011–2015 Forecast, IDC, June 2011.
[20] I DG Research, "CIO Global Cloud Computing Adoption Survey," January 2011.
[21] John Pescatore, "Key Issues for Securing Public and Private Cloud Computing", Gartner Research,2011.
[22] Patrick Thibodeau , "Cloud Security Fears Exaggerated, Says Federal CIO," Computerworld, July 28, 2011. (http://news.idg.no/cw/art.cfm?id=62DE7B46-1A64-67EA-E4E3D0EB9C453EC5)
[23] https://ww2.frost.com/files/1614/2113/3098/Whitepaper-VMware Bluelock Security In The Hybrid Cloud.pdf
[24] Planning Guide-Cloud Security-Seven Steps for Building Security in the Cloud from the Ground Up Sponsors of Tomorrow.™, Intel IT Centre, MAY 2012.