Volume 3, Issue 4, April 2013 ISSN: 2277 128X

International Journal of Advanced Research in Computer Science and Software Engineering

Research Paper

Available online at: www.ijarcsse.com

Data Security: Cloud Data Storage in Organization

Ms. Shubhra Saggar
Research Scholar , Singhania University.
Faculty, Guru Nanak Institute of Manegment, New Delhi, India.

Dr. R.K. Datta
Director, M.E.R.I.T.
New Delhi, India.

Abstract: Cloud computing is the use of computing resources, including both hardware and software, that are made available over the Internet by a subscription-based service provider. Because cloud computing is Internet-based, it offers several advantages over more traditional access to a company's data and software. Cloud computing delivers the potential for efficiency, cost savings and improved performance to governments, organizations, private and individual users. The general counsel of the multinational company or organizations is concerned about data privacy and data protection. However along with these advantages, storing a large amount of data including critical information on the cloud motivates highly skilled hackers thus creating a need for the security to be considered as one of the top issues while considering Cloud Computing. Today, issues of risk, data privacy, and compliance are the chief inhibitors to most organizations for adoption of cloud services. In this paper, we investigated the problem of data security in cloud data storage, which is essentially a distributed storage system.

Keywords: Data Centralization ,Distributed Denial of Service (DdoS), Data Segregation, Logging, Identity management

I. Introduction

In the last few years, cloud computing has grown from being a promising business concept to one of the fastest growing segments of the IT industry. It is providing unlimited infrastructure to store and execute customer data and program. As customers you do not need to own the infrastructure, they are merely accessing or renting; they can forego capital expenditure and consume resources as a service, paying instead for what they use. " A Cloud is a type of parallel and distributed system consisting of a collection of inter-connected and virtualized computers that are dynamically provisioned and presented as one or more unified computing resource(s) based on service-level agreements established through negotiation between the service provider and consumers."

A. Benefits of Cloud Computing :

Here are six benefits of Cloud computing:

- **Reduced Cost**
  It reduced the cost of organizations money and paid incrementally.
- **Increased Storage**
  Organizations can store more data than on private computer systems.
- **Highly Automated**
  No longer do IT personnel need to worry about keeping software up-to-date.
- **Flexibility**
  Cloud computing offers much more flexibility than past computing methods.
- **More Mobility**
  Employees can access information wherever they are, rather than having to remain at their desks.
- **Allows IT to Shift Focus**
  No longer having to worry about constant server updates and other computing issues, government organizations will be free to concentrate on innovation.

B. General models of cloud computing

IaaS (Infrastructure as a Service), PaaS (Platform as a Service), and SaaS (Software as a Service) are three general models of cloud computing

C. Infrastructure as a Service (IaaS):

The capability provided to the consumer is to provision processing, storage, networks, and other fundamental computing resources where the consumer is able to deploy and run arbitrary software, which can include operating systems and applications. The consumer does not manage or control the underlying cloud infrastructure but has control over operating systems, storage, deployed applications, and possibly limited control of select networking components.

D. Platform as a Service (PaaS):

The capability provided to the consumer is to use the provider's applications running on a cloud infrastructure. The applications are accessible from various client devices through a thin client interface such as a web browser (e.g., web based email). The consumer does not manage or control the underlying cloud infrastructure including network, servers, operating systems, storage, or even individual application capabilities, with the possible exception of limited user specific application configuration settings.

E. Software as a Service (SaaS):

The capability provided to the consumer is to deploy onto the loud infrastructure consumer-created or acquired applications created using programming languages and tools supported by the provider. The consumer does not manage or control the underlying cloud infrastructure including network, servers, operating systems, or storage, but has control over the deployed applications and possibly application hosting environment configurations.

II. Security a major Concern:

Cloud computing environment is generally assumed as a potential cost saver as well as provider of higher service quality. Security, Availability, and Reliability are the major quality concerns of cloud service users, suggests that security in one of the prominent challenge among all other quality challenges.

Each of these models possesses a different impact on application security.There is a number of security issues associated with cloud computing but these issues fall into two broad categories: Security issues faced by cloud providers and security issues faced by their customers.

A. Security assurance from Cloud provider:

Though people doubt cloud computing, clouds tend to be more secure than the traditional business models. Clouds offer real-time backup which results in less data loss. In case of outage, your customers can use the backup servers that sync with the main ones as soon as they are up. Your business gets maximum uptime without any loss of data during the transitions. Other than this, clouds are less prone to hacks and Distributed Denial of Service (DdoS) attacks as people don't know the whereabouts of your data.

Data theft attacks are amplified if the attacker is a malicious insider. This is considered as one of the top threats to cloud computing by the Cloud Security Alliance. While most Cloud computing customers are well-aware of this threat, they are left only with trusting the service provider when it comes to protecting their data. The lack of transparency into, let alone control over, the Cloud provider's authentication, authorization, and audit controls only exacerbates this threat

Cloud Provider claims:

- A good security resume are establish by them.
- Excellent backup facility.
- Customer data is not known to competent or hacker.
- Cloud provider on demand can provide password or biometric authentication thereby decreasing the chances of security part.

B. *Security advantages in Cloud Environments:*

Data Centralization: In a cloud environment, the service provider takes care of storage issues and small business need not spend a lot of money on physical storage devices. Also, cloud based storage provides a way to centralize the data faster and potentially cheaper. This is particularly useful for small businesses, which cannot spend additional money on security professionals to monitor the data.

- **Incident Response:** IaaS providers can put up a dedicated forensic server that can be used on demand basis. Whenever a security violation takes place, the server can be brought online. In some investigation cases, a backup of the environment can be easily made and put onto the cloud without affecting the normal course of business.
- **Forensic Image Verification Time:** Some cloud storage implementations expose a cryptographic check sum or hash. For example, Amazon S3 generates MD5 (Message-Digest algorithm 5) hash automatically when you store an object. Therefore in theory, the need to generate time consuming MD5 checksums using external tools is eliminated.
- **Logging:** In a traditional computing paradigm by and large, logging is often an afterthought. In general, insufficient disk space is allocated that makes logging either nonexistent or minimal. However, in a cloud, storage need for standard logs is automatically solved.

C. Security Disadvantages in Cloud Environments:

Cloud computing paradigm also introduces some key security challenges.

- **Data Location:** In general, cloud users are not aware of the exact location of the datacenter and also they do not have any control over the physical access mechanisms to that data. Most well-known cloud service providers have datacenters around the globe. Some service providers also take advantage of their global datacenters. However, in some cases applications and data might be stored in countries, which can judiciary concerns. For example, if the user data is stored in X country then service providers will be subjected to the security requirements and legal obligations of X country. This may also happen that a user does not have the information of these issues.

- **Investigation:** Investigating an illegitimate activity may be impossible in cloud environments. Cloud services are especially hard to investigate, because data for multiple customers may be co-located and may also be spread across multiple datacenters. Users have little knowledge about the network topology of the underlying environment. Service provider may also impose restrictions on the network security of the service users.
- **Data Segregation:** Data in the cloud is typically in a shared environment together with data from other customers. Encryption cannot be assumed as the single solution for data segregation problems. In some situations, customers may not want to encrypt data because there may be a case when encryption accident can destroy the data.
- **Long-term Viability:** Service providers must ensure the data safety in changing business situations such as mergers and acquisitions. Customers must ensure data availability in these situations. Service provider must also make sure data security in negative business conditions like prolonged outage etc.
- **Compromised Servers:** In a cloud computing environment, users do not even have a choice of using physical acquisition toolkit. In a situation, where a server is compromised; they need to shut their servers down until they get a previous backup of the data. This will further cause availability concerns.
- **Regulatory Compliance:** Traditional service providers are subjected to external audits and security certifications. If a cloud service provider does not adhere to these security audits, then it leads to obvious decrease in customer trust.
- **Recovery:** Cloud service providers must ensure the data security in natural and man-made disasters. Generally, data is replicated across multiple sites. However, in the case of any such unwanted event, provider must do a complete and quick restoration.

III. How Cloud Storage Works

A typical cloud storage system architecture includes a master control server and several storage servers. Once we gathered enough stuff, we have to find places to store all of it. If we were to update that routine today, we could make the same observation about computer information. It seems that everyone with a computer spends a lot of time acquiring data and then trying to find a way to store it.

For some computer owners, finding enough storage space to hold all the data they've acquired is a real challenge. Some people invest in larger hard drives. Others prefer external storage devices like pen drives or compact discs. Desperate computer owners might delete entire folders worth of old files in order to make space for new information. But some are choosing to rely on a growing trend: cloud storage.

While cloud storage sounds like it has something to do with weather fronts and storm systems, it really refers to saving data to an off-site storage system maintained by a third party. Instead of storing information to your computer's hard drive or other local storage device, you save it to a remote database. The Internet provides the connection between your computer and the database.

IV. Data Security In Cloud Computing

It is understandable that prospective cloud adopters would have security concerns around storing and processing sensitive data in a public or hybrid or even in a community cloud. Compared to a private data center, these concerns usually center on two areas:

- Decreased control by the owning organization when data is no longer managed within an organization's premises Securing the Cloud
- Concern by the owning organization that multitenancy clouds inherently pose risks to sensitive data

In both cases, the potential risk of data exposure is real but not fundamentally new. This is not to say that cloud computing does not bring unique challenges to data security.

Data privacy is an issue of concern for companies, their IT professionals and legal departments, whether files stay on-site or are stored electronically with a cloud computing provider. For organization considering cloud computing options, it is particularly important to carefully evaluate the provider's policies and procedures to ensure that they provide sufficient safeguards to protect confidential data. The company's lawyers and IT professionals should develop an understanding of the technology so that they can make informed decisions about whether cloud computing provides the level of protection they require.

One specific risk is that electronically stored information (ESI) may be co-mingled with the ESI of another company or of a separate but related corporate entity. Such situations can make it difficult to determine what entity has "possession, custody, or control" of the data and is under an obligation to preserve or produce the data. Moreover, if a cloud computing provider stores data in multiple servers around the world, ESI may be split up among jurisdictions with different data protection and transfer laws, making it difficult to keep track of how to access and retrieve data, and how to keep data private and secure.

ESI stored with a cloud computing provider can also present challenges to the discovery process in litigation. If a company has contracted with a cloud computing provider to maintain and hold its ESI, the company does not have direct control over, or possession of, the ESI. For purposes of discovery, however, the company still has a duty to preserve and produce that data, as long as it has the practical ability to do so.

V. Cloud Computing Providers and Key Features

Many big names have been offering cloud computing services as well as smaller more specialized vendors. Cloud-hosted services have also become a great way for businesses to cut costs, through SaaS monthly subscription vs. outright purchasing software. Some of the important factors to consider when investing in the cloud include: Platform ,Key features Scalability/Flexibility , Security , Reliability .

Below is a comparison of different features and key aspects for some of the top cloud computing companies.

Table 1 : Comparison of different features and key aspects for some of the top cloud computing companies.

Cloud Name	*Platform*	*Key feature*	*Scalability/Flexibility*	*Security*	*Reliability*
Sun Microsystems Sun Cloud	*MySQL, OpenSolaris, VirtualBox, NetBeans IDE.*	*More available applications than any other open OS.*	*Network-scale computing. Scale, reconfigure, or repurpose your infrastructure*	*Offers open-source utilities to encrypt data as well as Hardened OpenSolaris for Amazon EC2.*	*MySQL cluster offers 99.999% availabilty.*
Amazon EC2	*Red Hat Enterprise Linux, Windows Server 2003 R2, 2008 and 2008 R2, Oracle Enterprise Linux, OpenSolaris, openSUSE Linux, Ubuntu Linux, Fedora, Gentoo Linux, Debian.*	*Designed to make web-scale computing easier for developers.*	*Automatic scaling. Highly - increase or decrease capacity within minutes.*	*Web service interfaces to configure firewall settings that control network access to and between groups of instances.*	*99.95% availability. A few performance-related outages over the past few yea*
Google App Engine	*Windows, Mac OS X, Linux/Other Platforms.*	*No limit to the free trial period if you do not exceed the quota alotted.*	*Automatic scaling. "Massively scalable" App Engine datastore and services.*	*Same security, privacy and data protection policies as Google Apps.*	*Generally 100% available, but not guarenteed at 100%. Transparent uptime visual offered.*
Microsoft Azure	*In addition to managed code languages supported by .NET, Azure will support more programming languages and development environments in the near future.*	*Currently offering a "development accelerator" discount plan. 15-30% discount off consumption charges for first 6 months.*	*Automatic scaling and highly scalable. Open platform supports both Microsoft and non-Microsoft languages and environments.*	*Multiple levels of security at Microsoft-quality scale.*	*Fabric Controller technology reroutes work instantaneously if a server goes down; 99.9% - 99.95% uptime.*

VI. Managing Risks

The use of cloud computing should not fundamentally change the way a company handles ESI. No matter where the ESI resides, a company is responsible for being aware of the information that it creates and for governing that information in accordance with applicable business and legal requirements. It is important that the company be familiar with and closely monitor how its information is stored, retrieved, retained and disposed of by its cloud provider. A company should also develop effective procedures for auditing such activities by its cloud provider. At a minimum, the company should make sure it is capturing sufficient data when information is created (including what the information is, who created it, and for what purpose) to properly govern it. Before signing a service contract with a cloud computing provider, a company should be sure that the contract contains provisions protecting the organization interests and its need to comply with data privacy requirements. Just to introduce how the cloud deserves a place in our current education institution, it's important to reiterate the education philosophy. Its essence is knowledge. It's this knowledge which brings advancement, achievement and success. However, there are several things which make these parameters unattainable. In blunt language, this is failure. Small classrooms, lack or resources, short-handed staff, lack of adequate teachers…the list is endless. One way or the other, cloud computing can be utilized to improve education standards and activities. The end result will be to curb the above problems and instead, boost performance.

A. Security system as a user

Consider the following items when negotiating a service contract with Provider:

- **Access:** The education institution should have the right to access all ESI "on demand" and in a specified format that is easy to use.
- **Control:** The education institution should have the ability to reasonably direct actions of the provider to preserve and produce ESI.
- **Cooperation:** The provider should be willing to comply with the education institution directions regarding its ESI and to comply with any and all legal holds.
- **Speed:** The provider should agree to cease any data destruction in a timely manner and to produce data with sufficient speed to meet the education institution obligations.
- **Metadata:** The education institution should inquire as to the form or format in which data will be stored and returned for production during litigation, including whether metadata will be intact.
- **Costs:** Beyond the subscription price for the service, the contract should address the costs of potential production, as well as potential indemnification policies and attorneys' fees should the cloud provider's failure to comply with the contract terms result in liability for the education institution.
- **Transparency:** The contract should address confidentiality, data integrity and availability issues, including whether data will be commingled with the data of other cloud customers.
- **Jurisdiction:** The education institution should discuss with the provider where the data will be maintained and should consider whether production of the data might require compliance with data transfer laws or international privacy laws.
- **Ownership:** The contract should clearly state that the education institution owns the data.
- **Security:** The education institution should inquire about the security measures that the provider has in place to protect data privacy and attorney-client privilege and whether the company will be informed in the event of a security breach.
- **Policies:** The education institution should determine whether the provider's policies and procedures could impede the company's obligations to preserve, collect and produce ESI during litigation.
- **Disaster Recovery:** The education institution should have contingency plans in the event the provider was to suffer a server crash or other data loss or go bankrupt or out of business. The contract should stipulate that its provisions will remain in force if the provider is acquired by another company.

B. Security system as a Provider

- **Identity management:** Every enterprise will have its own identity management system to control access to information and computing resources. Cloud providers either integrate the customer's identity management system into their own infrastructure, sing federation or SSO technology, or provide an identity management solution of their own.
- **Physical and personnel security:** Providers ensure that physical machines are adequately secure and that access to these machines as well as all relevant customer data is not only restricted but that access is documented.
- **Availability:** Cloud providers assure customers that they will have regular and predictable access to their data and applications.
- **Application security:** Cloud providers ensure that applications available as a service via the cloud are secure by implementing testing and acceptance procedures for outsourced or packaged application code. It also requires application security measures be in place in the production environment.

- **Privacy:** Finally, providers ensure that all critical data (results, students personal data , for example) are masked and that only authorized users have access to data in its entirety. Moreover, digital identities and credentials must be protected as should any data that the provider collects or produces about customer activity in the cloud.
- **Legal issues:** In addition, providers and customers must consider legal issues, such as Contracts and E-Discovery, and the related laws, which may vary by country.

VII. Conclusion:

To ensure the correctness of users data in cloud data storage, the best way to manage the data privacy and security risks associated with cloud computing is to gain a comprehensive understanding of how the company plans to use cloud computing and to establish procedures and contract terms with the cloud computing provider that meet the company's data security and privacy needs. Before establishing your cloud infrastructure, it's important to be familiar with technologies and products used for storage management, protection and disaster recovery. You should ensure that your service provider is performing backups as often as necessary to meet contracted Recovery Point Objectives ,which is what an organization determines is an "acceptable loss" in a disaster situation. Cloud computing as an exciting development is a significant alternative today's educational perspective. Students and administrative personnel have the opportunity to quickly and economically access various application platforms and resources through the web pages on-demand. This automatically reduces the cost of organizational expenses and offers more powerful functional capabilities.

References

1) Gens, F.: IT Cloud Services User Survey, part 2: Top Benefits and Challenges (2008)
2) John, H.: Security Guidance for Critical Areas of Focus in Cloud Computing (2009), http://www.cloudsecurityalliance.org/guidance/ (Accessed 2 July 2009)
3) Kevin Fogarty, *Top Cloud Computing Security Risk: One Company Gets Burned*, Network World, July 14, 2010, http://www.networkworld.com/news/2010/071410-topcloud-computing-security-risk.html.
4) John Markoff, *Cyberattacks on Google Said to Hit Password System*, NY Times, June 28, 2010, *available at* http://www.nytimes.com/2010/04/20/technology/20google.html?sudsredirect=true.
5) John D. Sutter, Twitter Hack Raises Questions About "Cloud Computing," CNN, July 16, 2009, http://www.cnn.com/2009/TECH/07/16/twitter.hack/index.html.
6) Amazon. Amazon Elastic Compute Cloud(EC2),2010 /http://www.amazon.com/ ec2/S [accessed: 10December2009].
7) Attanasio CR.Virtual machines and data security. In: Proceedings of the workshop on virtual computer systems. NewYork,NY,USA:ACM;1973.p.206–9.
8) Auger R.SQLInjection,2009 /http://projects.webappsec.org/SQL-InjectionS [accessed on:15February2010].
9) Basta A,HaltonW.Computersecurityandpenetrationtesting. DelmarCengage Learning 2007.
10) Bernard Golden.Definingprivateclouds,2009 /http://www.cio.com/article/ 492695/ Defining _Private Clouds_Part_OneS [accessed on:11January2010].
11) Boss G,MalladiP,QuanD,LegregniL,HallH. Cloudcomputing,2009,p.4 /http://www.ibm.com/ developerswork/websphere/zones/hipods/library.htmlS [accessedon:18October2009].
12) Clavister.Securityinthecloud,ClavisterWhitePaper /http://www.it-wire.nu/ members/ cla69/ attachments/ CLA_WP_SECURITY_IN_THE_CLOUD.pdfS [accessed on:21October2009].
13) Cloud SecurityAlliance.Guidanceforidentity& accessmanagementV2.1,2010a /http://www. Cloudsecurity alliance.org /guidance/csaguide-dom12-v2.10.pdfS [accessed on:9May2010].
14) Cloud SecurityAlliance.Securitybestpracticesfor cloudcomputing,2010b /http://www. cloudsecurityalliance.orgS [accessed on:10April2010].
15) Descher M,MasserP,FeilhauerT,TjoaAM,HuemerD. Retainingdatacontroltothe client in infrastructure clouds. In: International conference on availability, reliability andsecurity, ARES'09,2009,p.9–16.
16) Kaufman LM. Data security in the world of cloud computing, security and privacy. IEEE 2009;7(4):61–4.
17) Lo H, Wang R, Garbani J-P, Daley E, Iqbal R, Green C, Forrester report. The State of Enterprise Software: 2009.
18) Raj H, Nathuji R, Singh A, England P. Resource management for isolation enhanced cloud services. In: Proceedings of the 2009 ACM workshop on cloud computing security, Chicago, Illinois, USA, 2009, p. 77–84.
19) Seccombe A, Hutton A, Meisel A, Windel A, Mohammed A, Licciardi A, et al. Security guidance for critical areas of focus in cloud computing, v2.1. CloudSecurityAlliance, 2009, 25 p.
20) Wang C,WangQ,RenK.Ensuringdatastoragesecurityin cloudcomputing, Cryptology ePrintArchive,Report,2009 /http://eprint.iacr.org/S [accessed: 18 October2009].
21) Zalewski M.Browsersecurityhandbook,2009 /http://code.google.com/p/brow sersec/S [accessed on:19February2010].

