Inspira- International Journal of Advance Research in Commerce, Management & Social Science
ISSN : ……, Volume 01, No. 01, October - December, 2017, pp. 39-44

SECURITY ISSUES AND CHALLENGES OF PORTING SERVICES OVER CLOUD NETWORK

Dr. Navneet Sharma*
Dr. R.K. Tailor**

Abstract

Information technology plays an important role in each sector. Cloud computing is an emerging and increasingly critical part of a modern economy. It is a general term for delivering hosted services over the internet to remotely store, process and share digital data. Cloud computing and its services are very much focus to new environment in the IT community and various services which are provided by the cloud. Services i.e. Software as a service (SAAS), Platform as a service (PAAS), Infrastructure as a service (IAAS) reduce IT expenditures, increase network flexibility, and streamline communication infrastructure. It has various advantages when we talk about services but when we think about porting from one service provider to another service provider then it may face various problems and security issues related to porting the data and application services. This becomes a challenge in the cloud as the data is stored on a service providers cloud and when we port the data and application from one cloud service provider along with other service provider. The challenge arise that the same data and application is to be available ensure that data of this kind is only used for the purpose set out and agreed, as it can easily be pooled with other service provider. The major issue relating to porting is understanding who is responsible for data availability and security. In IAAS, the borders are clear, but in PAAS they are more blurred. Service provider is responsible for protecting the infrastructure components, but all instance and application security is up to user level. If we are using a managed database environment, the service provider will also be responsible for the availability of the database, but it will not provide protection against confidentiality and integrity threats. In this paper we focus on some challenges and security issues . these are application lock in, processing incompatibility and conflicts

* Senior Assistant Professor, Department of CS & IT, The IIS University, Jaipur, Rajasthan.

** Senior Assistant Professor, Department of Accounting & Taxation, The IIS University, Jaipur, Rajasthan.

causing disruption of services, costly data migration or data conversion, application re-engineering, original data format etc.

Keywords: *PAAS, IAAS, SAAS, Cloud Models, Hybrid, Infrastructure, Portability.*

Introduction

Cloud computing is an immerging issue for using the services as pay per use. Using cloud computing services we can reduce IT expenditures, increase network flexibility, and streamline communication infrastructure. It encompasses any subscription -based service that in real time over the Internet, extends its existing capabilities. various services which are provided by the cloud. Services i.e. Software as a service (SAAS), Platform as a service (PAAS), Infrastructure as a service (IAAS) reduce IT expenditures. A Cloud Computing platform is to be made operationally secure, all the issues potentially posing a threat to the confidentiality, integrity and availability of the data stored there needs to be examined. Besides a well-structured procedural model for all IT processes. The major issue with businesses to look to cost-effective and efficient solutions to satisfy their hardware, software, communications, and IT needs. However, unlike other industries having simply to deal with the risk inherent in any strategic business decision, cloud computing is presented with unique challenges. Particular problems must be addressed before any business makes the leap to the cloud. In the cloud, questions of data storage and protection, consumer privacy, and what law and jurisdiction govern cannot be ignored. Even more crucial is recognizing that state and local governments are slow to react to market shifts and technological innovation and porting over cloud services which leaves cloud providers with few laws and ground rules to guide their behavior and business relationships. Contract formation, analysis, review, and negotiations are therefore critical for any cloud users and their service providers.

Cloud computing is a new trend in computer environment .use of cloud and protecting the Data over cloud is a vital issue in this area. Clouds have no limitations or restrictions and the data can be physically available anywhere in the world. So this trend raises serious issues and challenges regarding services provided by the cloud service providers and user's data protection and portend of data over cloud network.

There are different types of cloud models used for various services :

Private— It is exclusively used with one organization. It may be managed by the organization or a third party and exist on-premises or off-premises.

Public— It is made for public or a large group of users and is owned by an organization.

Hybrid— It is a combination of private and public cloud models and used by a single organisation.

Community— It is developed to share with many organizations that want to share the common environment.

Challenges and Security Issues in Cloud Acceptance and Portability

The current issue over cloud computing is portability of services which are provided by service providers are satisfactory or not or there should be some regulatory issues and challenges faced by the users. In the networked cloud environment, businesses and individuals are as concerned about maintaining access to their data and their online profile as they are about maintaining their telephone number. Data portability is the term

used most often when referring to an individual's management of their digital information and is a mechanism for sharing data seamlessly between platforms, services and applications transferring data easily between platforms, services and applications or from one to another is really so easy as it seems. Data portability, like number portability has the potential to promote competition in communications and cloud service providers because it would remove existing barriers in the cloud to end users' ability to easily change services and their service providers. The challenging aspect of cloud computing is the security issues that have come out on a growing scale that need to be solved to promote the wider service of cloud computing In addition to addressing regulatory barriers to the development of cloud computing, current consumer concerns are another barrier to the take-up of cloud services. Limited understanding about how cloud computing works and concerns about relevant protections for personal data use are current identifiable concerns.

The main barriers to engagement with cloud computing can be categorized as:

Security, privacy and the management of user's data ,vendor lock-in, specifically concerns about interoperability and portability between cloud computing services, and loss of control of an individual's or a firm's data ,data autonomy—the ownership of data and access to data stored in countries, other than the one where the end user resides, including redress mechanisms.

Security, Privacy and Data Protections

Cloud computing illustrates the growing level of interconnection between users and services. The amount and types of information stored, shared and analyzed in the cloud are far greater than the name and address that was once available to the average telecommunications provider. As a result, the amount of information available to service providers is becoming increasingly detailed.

Vendor Lock-in, Portability and Ease of Switching Providers

A common feature of public cloud computing services, such as webmail, content sharing and storage, is the use of proprietary standards and service agreements. Proprietary standards may limit a business or an individual's ability to easily transfer their data, or may prevent them accessing their content via other services. Email is a very common cloud service and a customer can migrate to a new provider and a new address. In this case, the customer or the customer's correspondents may be aware of the implications of different data requirements such as addresses, earlier emails and attachments. There are degrees of difficulty with other types of cloud computing services. For example, a consumer who has stored their music collection in one cloud service may be unable to easily transfer the entire collection to another. This can be because they do not have a copy of the music files on their own computer or device, or the files are in a proprietary technical standard that is incompatible with those used elsewhere. Currently, there is no open standard or technical specification that ensures data portability between data controllers.29 Data portability is a prerequisite for users of cloud computing services, if they are to have an ongoing choice between providers for a range of services, but the challenge of providing data portability is different with each cloud service type.

At present, the lack of interoperable technical standards between cloud computing services means that users may risk losing their content and media if they change services. For both business and consumers, this is an increasingly high barrier as social and professional lives move online.

Data Sovereignty and Redress

Cloud computing service providers are often based internationally and national economy-wide legislation, such as privacy, may not capture providers based in other jurisdictions. Cloud providers based in international jurisdictions may be subject to local legislation and this has raised concerns about end users' ability to manage access to their personal information in accordance with the protections available in their home country

Contracts and Commercial Transactions

The primary source of legal and business obligations of providers of cloud-based services is the customer contract. Quality of service, profitability, and the outcome of all legal issues flow a cloud service provider's commercial arrangements and terms of contract. Service level and performance, best practices, liability, risk management and allocation, vendor lock-in and the strength of both parties' obligations hinge on the cloud computing service contract.

Data Breaches

Data breaches mainly violate two security properties of data which are the integrity and confidentiality. The breach behavior may come from inside employee who operates the data intentionally or unintentionally, or from outside malicious hacker. Data breaches have been reported to the top ten threats in cloud computing security alliance

Data Security

Customers and providers of cloud services are especially concerned over data protection, and knowing how best to comply with laws imposing data security requirements and standards on cloud service providers and their customers is essential. With the increase of electronic data and malicious actors attempting to access valuable information, service providers and business customers must provide for the physical, operational, and programmatic security of their data.

Data Privacy

Compliance with laws governing the privacy of customer data is a serious responsibility for any cloud provider. Especially it is more concern with porting of data from different cloud networking Data privacy is addressed in multiple federal, state, and international laws including the Electronic Communications Privacy Act (ECPA), the legal environment for the cloud industry is in a state of change and often saddled with outdated laws and rules. Cloud computing and a cloud provider's particular customer base means that there is never a one-size-fits-all approach to data privacy and customer confidentiality.

Data Locality

In a SAAS model of a cloud environment the customer does not know where the data is stored, which may be an issue. Extraterritorial or dispersed geographical storage can impact the ability of customers to establish an audit trail for purposes of satisfying regulatory compliance and legal obligations, which rely on verifying where data is located, accessed, or altered. One of the top security concerns of enterprises are the

physical location of the data that are being stored in the cloud especially if they are located in another country the laws of the host country of the equipment apply to the data on the system and it could be a big concern if the host country does not have ample laws to protect sensitive data or if the host nation becomes hostile or when the government of the hosting nation changes and become unfriendly.

Data Remanence

Data remanence is the residual representation of data that have been in some way nominally erased or removed. In private cloud it causes minimal security threats; however in public cloud it can cause severe security issues because of the open environment, especially in an IAAS model. Deleting of data files from digital devices may look like the best way to protect data from security breaches, but that simple act may not be enough. Virtually all digital devices utilize built in data storage. This issue of data remanence remained the worries to the organization after the deletion of the data. This issue needs a wise solution to be proven by the cloud service providers to ensure that the data that has been removed is free from the attackers in the future

Intellectual Property

Cloud computing touches on a number of intellectual property issues, and the protection of trade secrets, confidential information, copyright, and trademarks in the cloud has to be maintained. When we think about porting of data from one cloud network to another network When different software are involved in any porting of data and services , the licensing, use, and ownership of both software as a service (SaaS) and data stored on the cloud become critical. For customers who rely on the cloud, warranties and indemnification regarding the infringement of third-party intellectual property rights are important considerations. Some cloud service providers must also arrange for the sub-licensing of software to their customers in porting of software and platform.

Regulatory Matters

Cloud service providers must comply with international laws and regulations as well as applicable industry standards. However, complying with the current ground rules that implicate the cloud is only half the story. The cloud industry is relatively young, and the laws and rules bearing on the business and operations of cloud-based service providers are still in flux as legislators come to grips with the technology of the cloud. In an background of regulatory indecision, the aid of experienced counsel is an absolute requirement in order to stay abreast of changes in the cloud's legal and regulatory issues.

Conclusion

Cloud computing, is not a new idea which is rising in eminence. Cloud computing represents a range of communications services, which are moving beyond traditional business models and capitalizing on changing consumer behavior. This is due to the growing success of the apps market and the ongoing demand by consumers and business for access to their content and media anywhere and on any device. The cloud industry is diverse and globalised and as the market is growing there are some barriers and limitations arise in terms of service providing and especially in porting of services and

data. It illustrates many of the concerns being expressed by consumers around the privacy, security and management of their personal information in a globalised information economy when they want to port the cloud network and services.

Costumers and service providers are more concerned with transparency of data management and the privacy practices of cloud services and porting of services, which inhibits their take-up and engagement with cloud computing. Strengthening consumer confidence in the use of cloud computing is likely to require further action from both industry and governments. Such action would address global governance arrangements for cloud computing services and about data security and data availability over porting of cloud network. The ease of switching cloud providers and transferring data, along with assurances about relevant protections for personal information in an information economy. Cloud computing and poring of cloud network services are currently subject to regulatory measures, as well as emerging international standardization. Reducing regulatory complexity, while also balancing consumer personal data protections and service providers porting regulation and data transparency is an early area for action that would emphasize a more secure and confident environment for cloud computing and portability of cloud computing.

References

- ATSE, Cloud Computing: opportunities and challenges for Australia, p. 2.
- KPMG, Modeling the Economic Impact of Cloud Computing, p. 8.
- ATSE, Cloud Computing: opportunities and challenges for Australia, p. 2.
- KPMG, Modeling the Economic Impact of Cloud Computing, p. 8.
- ATSE, Cloud Computing: opportunities and challenges for Australia, p. 2.
- http://www.cloudsecurity.org, accessed on April 10, 2009. Cloud Security Alliance.
- http://www.cloudsecurityalliance.org .
- Cloud Security Alliance The Notorious Nine: Cloud Computing Top Threats in 2013.

❖❖❖