Available online at http://www.journalcra.com

International Journal of Current Research
Vol. 4, Issue, 11, pp. 121-125, November, 2012

INTERNATIONAL JOURNAL OF CURRENT RESEARCH

ISSN: 0975-833X

RESEARCH ARTICLE

IMPLEMENT CLOUD COMPUTING MODEL FOR BUSINESS INFORMATION SYSTEM SECURITY

[1]Dr. Bharat Mishra, and [2]Vivekanand Mishra

[1]Mahatma Gandhi Chitrakoot Gramodaya Vishwavidyalaya Chitrakoot Satna (M.P.)
[2]Vindhya Institute of Technology and Science, Satna (M.P.)
**Corresponding author:* bm_cgv@rediffmail.com , vm0133@gmail.com

ARTICLE INFO

Article History:
Received 5th August, 2012
Received in revised form
27th September, 2012
Accepted 14th October, 2012
Published online 21th November 2012

Key words:
Flexibility
Web-accessed
Highly scalable,
Availability etc.

ABSTRACT

Cloud computing is one of today's most attractive technology areas due to its many advantages like Highly scalable, on-demand, web-accessed IT resources with major cost / cash and flexibility. Various companies around the world adapting cloud computing as a means to increasing efficiency and reducing cost of their IT services. In this research paper efforts have been made to analyze the use of hybrid cloud computing model with security and scalability in business information system. There are many challenges in using cloud computing. The main challenges are security and because all essential services are generally outsourced to a third party. The outsourcing makes it harder to maintain data integrity and privacy, support data and service availability etc. Using public cloud model only in the business is very risky because of its security reasons and using private cloud only will not solve our purpose because in that case we will not be able to use advantages of public cloud model. To solve these security problems in business information system we can use hybrid cloud computing model where we can use advantages of public cloud and security of private cloud, in which we can elect to store highly sensitive data of the company in the private storage cloud and less sensitive data in public storage cloud. This research paper focused upon the security problems in business information system. Research suggests a hybrid cloud computing model where converging advantages of public cloud and security of private cloud can be used.

Copy Right, IJCR, 2012, Academic Journals. All rights reserved.

INTRODUCTION

Cloud computing is the technology that enables the functionality of an IT infrastructure, IT platform or an IT product to be exposed as a set of services in a seamlessly scalable model so that the consumers of these services can use what they really want and pay for only those services that they use (pay per use). Computing is being transformed to a model consisting of services that are commoditized and delivered in a manner similar to traditional utilities such as water, electricity, gas, and telephony [1]. Using this model user can access services as per their requirement without knowing that where the services are hosted and how they are delivered. The cloud model represents nothing less than a fundamental change to the economics of computing and the location of computing resources [2]. With the growth in Internet usage, the proliferation of mobile devices and the need for energy and processing efficiency, the stage has been set for a different computing model – the idea of computing as a utility.

Cloud computing

Definition

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 [3]. Cloud computing technology enables the IT functionality to be exposed as service in a multi-tenant manner. The enabling technology includes (but not limited to) virtualization, grid technologies, SaaS (Software as a service) enabled application platform (SEAP), Service Oriented Architecture (SOA), Metering tools and technologies etc. Cloud services are provided by the cloud vendor and that can be used by the cloud consumer on a pay per use basis. These service exposed as industry standard interfaces like web services (using Service Oriented Architecture SOA [4]) or REST [5] services or any proprietary services. Cloud computing is a computing paradigm, where a large pool of systems are connected in private or public networks, to provide dynamically scalable infrastructure for application, data and file storage. With the advent of this technology, the cost of computation, application hosting, content storage and delivery is reduced significantly. Cloud computing is a practical approach to experience direct cost benefits and it has the potential to transform a data center from a capital-intensive set up to a variable priced environment.

Cloud computing models

Public Clouds

Public clouds are most often hosted away from customer premises, and they provide a way to reduce customer risk and cost by providing a flexible, even temporary extension to enterprise infrastructure. Public cloud services are the services

those are available to clients from a third party service provider via the Internet. A public cloud does not mean that a user's data is publicly visible; public cloud vendors typically provide an access control mechanism for their users. Public clouds provide an elastic, scalable, cost effective means to deploy solutions.

Private Clouds

A private cloud offers many of the benefits of a public cloud computing environment, such as being elastic and service based. The difference between a private cloud and a public cloud is that in a private cloud-based service, data and processes are managed within the organization without the restrictions of network bandwidth, security exposures and legal requirements that using public cloud services might entail. In addition, private cloud services offer the provider and the user greater control of the cloud infrastructure, improving security and resiliency because user access and the networks used are restricted and designated.

Hybrid Clouds

A hybrid cloud is a combination of a public and private cloud that interoperates. In this model users typically outsource non critical information and processing to the public cloud, while keeping critical services and data in their control. The companies see the public nature of cloud as a big issue for adoption. Control of IT in case of using cloud computing remains with the third party (provider), which increases the threat to public cloud's adoption. With an aim to tackle the challenges of public cloud a concept of in-house private clouds started. However though private clouds are supposed to emulate the public cloud functionalities, they introduce their own shortcomings of scalability and up-front costs. To handle the challenges of public cloud and use the advantages of private cloud a hybrid approach can be used that allow us to adopt the public cloud partially, deploying only those services which are suitable and less critical. The highly sensitive and critical data and services can be deployed on private (Internal) cloud. The success of this hybrid approach depends on how public and private cloud interacts and works together in union.

Many Flavors of Cloud Computing

Software as a Service (SaaS)

Software as a service model offers application as a service to the consumer on demand. Through SaaS, companies can access applications and large amounts of virtual computing power without buying it. Rather, the application is hosted offsite by some other company, which cuts maintenance headaches and most of the setup costs for users. "You're getting all the functionality but none of the headaches of running the IT infrastructure in-house. No upgrades, no contract renewals, no security issues: The provider manages your service. You pay based on how much computing you use." [6]. By purchasing SaaS from third party companies can focus on their main work like expending business and improving services without requiring an IT overhaul. SaaS allows SMBs to avoid hiring extensive IT staffs, managing software upgrades, or staying current with the latest releases – and it can unleash new capabilities because it evolves as their businesses evolve, Aoki says [7]

Platform as a Service (PaaS)

Platform as a service model offers a hosting environment for applications to the consumer on demand. The consumer controls the applications that run in the environment (and possibly has some control over the hosting environment). The platform is typically an application framework. Platform as a Service (PaaS) helps developers in creating and delivering business applications on-demand. As Platform-as-a-Service (PaaS) is available as a service, the developer get full control of the application development and and deployment. Developer can build enterprise-class applications quickly, built-in services (including analytics, globalization, security, mobility and compliance), development as a service, application exchanges, user interface as a service and integration as a service. It also enables developers to create custom web applications and deliver it quickly, as many of the hassles like setting up hosting, servers, databases, user interaction process and frameworks are prepackaged.

Infrastructure as a Service (IaaS)

Infrastructure as a service offers computing resources such as processing power, storage, networking components or middleware to consumer on demand. The consumer can control the operating system, storage, deployed applications and possibly networking components such as firewalls and load balancers, but not the cloud infrastructure beneath them. Infrastructure-as-a-Service provides virtual server instances with unique IP addresses and blocks of storage on demand. Customers use the provider's application program interface (API) to start, stop, access and configure their virtual servers and storage. In the enterprise, cloud computing allows a company to pay for only as much capacity as is needed, and bring more online as soon as required. Because this pay-for-what-you-use model resembles the way electricity, fuel and water are consumed, it's sometimes referred to as utility computing.

Data as a Service (DaaS)

Data as a service offers data in various formats and from various sources could be accessed via services by users on the network, in a transparent, logical or semantic way. Users could, for example, manipulate remote data just like operate on a local disk or access data in a semantic way in the Internet.[8]

Hardware as a Service (HaaS)

Hardware as a Service offers hardware virtualization, IT automation, and usage metering and pricing, users could buy IT hardware - or even an entire data center - as a pay-as-you-go subscription service. The HaaS is flexible, scalable and manageable to meet clients needs [9].

Cloud Computing Benefits

Significant Cost Reduction

Companies can reduce ICT capital expenditures and decrease ongoing operating expenditures by paying only for the services they use and, potentially, by reducing or redeploying their ICT staffs.

Easy to implement

Without the need to purchase hardware, software licenses, or implementation services, an organization can deploy cloud computing rapidly.

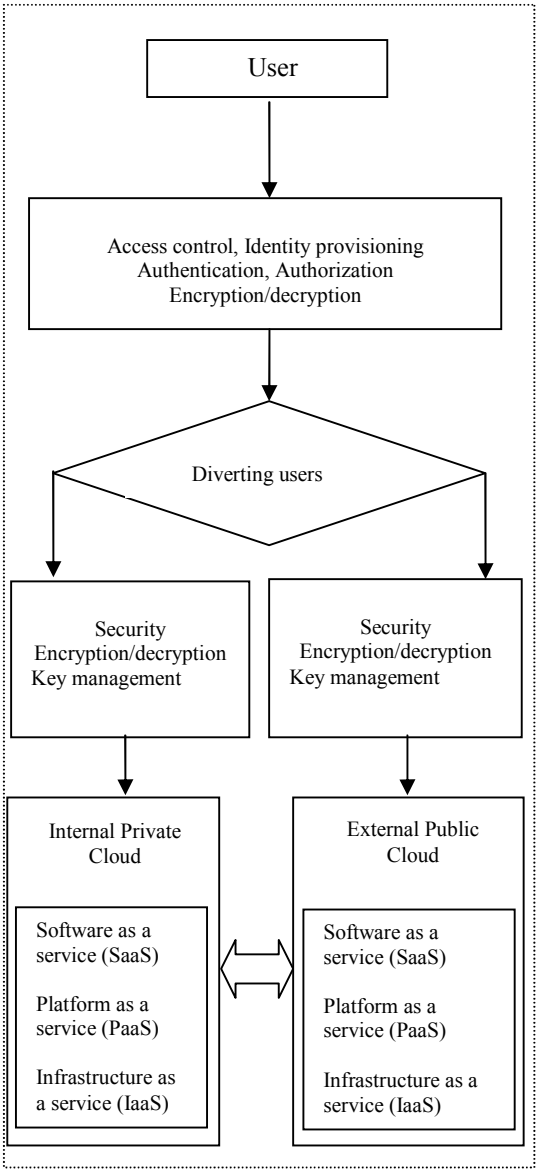

Fig (1) Hybrid cloud computing model for business information system

Elastic scalability

Elasticity is defined as the ability to scale resources both up and down as needed. To the consumer, the cloud appears to be infinite, and the consumer can purchase as much or as little computing power as they need. This is one of the essential characteristics of cloud computing.

Increased Flexibility

Cloud computing offers more flexibility (on demand) in matching ICT resources to business functions than past computing methods. It can also increase staff mobility by enabling access to business information and applications from a wider range of locations and/or devices.

Access anywhere

Cloud can be accessed from a single computer or network. It can also be accessed from a portable devices to use applications and documents from cloud.

Quality of Service

Cloud computing provides reliable services to the clients. It also provides large storage and computing capacity, and 24/7 service and up-time.

Sustainability

The poor energy efficiency of most data centers, due to substandard design or inefficient asset utilization, is now understood to be environmentally and economically unsustainable. Cloud service providers, by using economies of scale and their capacity to manage computing assets more efficiently, can consume far less energy and other resources than traditional data center operators.

Sharing Application and documents

Cloud computing allows the users to access applications and documents from anywhere in the world, facilitating group collaboration on documents and projects.

Security in Cloud computing

Cloud computing shifts most of the control over data and operations from the client organization to their cloud providers. The client organizations must establish trust relationships with their service providers through service level agreement (SLA) and understand how these providers implement, deploy, and manage security. This relationship between cloud service providers and consumers is critical because the cloud service consumer is still ultimately responsible for compliance and protection of their critical data, even if that workload had moved to the cloud. In fact, some organizations choose private or hybrid models over public clouds because of the risks associated with outsourcing services [10].

Authorization

It is important for client organizations that only authorized users have access to the data and tools that they need, and unauthorized access should be blocked. Larg number of users access the cloud environments, so these controls are even more critical. In addition, clouds introduce a new tier of privileged users: administrators working for the cloud provider. Privileged-user monitoring, including logging activities, becomes an important requirement. Identity federation and rapid on boarding capabilities must be available to coordinate authentication and authorization with the enterprise back-end or third-party systems. A standards-based, single sign-on capability is required to simplify user logons for both internally hosted applications and the cloud, allowing users to easily and quickly leverage cloud services.

Security of Data and information

Data is the most important part of organizations. Data protection is the most important security issue of these organizations. Typical concerns include the way in which data is stored and accessed, compliance and audit requirements, and business issues involving the cost of data breaches, notification requirements, and damage to brand value. All sensitive or regulated data needs to be properly segregated on the cloud storage infrastructure, including archived data. Encrypting and managing encryption keys of data in transit to the cloud or data at rest in the service provider's data center is critical to protecting data privacy and complying with compliance mandates. The encryption of mobile media and the ability to securely share those encryption keys between the cloud service provider and consumer is an important and often overlooked need. Because moving large volumes of data quickly and cheaply over the Internet is still not practical in many situations, many organizations must send mobile media, such

as an archive tape, to the cloud provider. It is critical that the data is encrypted and only the cloud provider and consumer have access to the encryption keys.

Application Security

Clients typically consider cloud application security requirements in terms of image security. All of the typical application security requirements still apply to the applications in the cloud, but they also carry over to the images that host those applications. The cloud provider needs to follow and support a secure development process. In addition, cloud users demand support for image provenance and for licensing and usage control. Suspension and destruction of images must be performed carefully, ensuring that sensitive data contained in those images is not exposed. Defining, verifying, and maintaining the security posture of images in regards to client-specific security policies is an important requirement, especially in highly regulated industries. Organizations need to ensure that the Web services they publish into the cloud are secure, compliant, and meet their business policies. Leveraging secure-development best practices is a key requirement.

Server and Network Security

In the shared cloud environment, clients want to ensure that server, network and client are properly isolated and that no possibility exists for data or transactions to leak from one tenant domain into the next. To help achieve this, clients need the ability to configure trusted virtual domains or policy-based security zones. Detection and Prevention systems to be built into the environment. The concern is not only intrusions into a client's trusted virtual domain, but also the potential for data leakages and for *extrusions*, that is, the misuse of a client's domain to mount attacks on third parties. Moving data to external service providers raises additional concerns about internal and Internet-based denial of service (DoS) or distributed denial of service (DDoS) attacks. In a shared environment, all parties must agree on their responsibilities to review data and perform these reviews on a regular basis. The organization must take the lead in terms of contract management for any risk assessments or controls deployment that it does not perform directly.

Physical Infrastructure

The cloud's infrastructure, including servers, routers, storage devices, power supplies, and other components that support operations, should be physically secure. Safeguards include the adequate control and monitoring of physical access using biometric access control measures and closed circuit television (CCTV) monitoring. Providers need to clearly explain how physical access is managed to the servers that host client workloads and that support client data.

Hybrid cloud model for Business Information System

Figure 1 shows the proposed model of hybrid cloud computing for business information system. In this model we will discuss all the basic security points those should be considered when using hybrid cloud model for business.

Access control

On internet 69% of online users are using some form of cloud computing [11] out of which many users accessing business data and information from the cloud. Managing access control and identity in business information system is a great challenge. Following four major functions are essential for successful and effective identity management in cloud computing [12].

Identity Provisioning

The secure and timely management of on-boarding (provisioning) and off-boarding (de provisioning) of users in the cloud is called identity provisioning. The rights and attributes of each person who accesses business information system continually change as roles, rules, and policies changes within the organization. The challenge is compounded during mergers and acquisitions, and when sharing IT privileges with other organization and clients.

Authentication

Authenticating users in a trustworthy and manageable manner is very important in cloud computing. The organization must address authentication-related challenges such as credential management, strong authentication (typically defined as multi-factor authentication), delegated authentication, and managing trust across all type of cloud services.

Authorization

The requirements of authorization usually derive directly from the hierarchy, organization, and specifics of the environment in which is deployed. It is common for companies with more than few employees to categorize them according to the roles they possess. The requirements for user profiles and access control policy vary depending on whether the user is acting on their own behalf (such as a citizen) or as a member of organization. The access control requirements include establishing trusted user profile and policy information, using it to control access within the cloud service, and doing this in an auditable way.

Differentiating users

On the basis of access control rights user should be differentiated and diverted to access private or public cloud. Private cloud contains critical and very sensitive information due to that all users can not be directed to private cloud. Only the users those are authorized to access private cloud can be directed to private cloud they can also access public cloud, rest users those are not authorized to access private cloud can be directed to public cloud they can access public cloud only.

Data and information security

Security and data protection is the core principal of the business information system. Cloud customers and providers need to guard against data loss and theft. Today, encryption of personal and enterprise data is strongly recommended, and in some cases mandated by laws and regulations around the world. Cloud customers want their providers to encrypt their data to ensure that it is protected no matter where the data is physically located. Likewise, the cloud provider needs to protect its customer's sensitive data. Following two functions are important to manage security of the data on cloud computing.

Encryption

Before transferring data on the cloud it should be encrypted. Encryption keys should securely manage to prevent misuse or disclosure. Key management methodology can be used to

secure key distribution. Keys should be recycled from time to time and old keys should be destroyed [13]. Encryption is the most important part of the cloud security. Encryption on the data can be used at various places [14], For example, data in transit, data at rest and data in memory or process. Encrypting and managing encryption keys of data in transit to the cloud or at rest in the service provider's data center are critical to protect data privacy and comply with compliance mandates [15]. The encryption of mobile media and the ability to securely share those encryption keys between the cloud service provider and consumer is an important and often overlooked need. Because moving large volume of data quickly and cheaply over the Internet is still not practical in many situations, many organizations must send mobile media, such as an archive tape, to the cloud provider. It is critical that the data is encrypted and that only the cloud provider and client have access to the encryption keys.

Internal cloud

Data privacy and security related challenges cannot be ignored for a large category of the business scenario where customer information and business critical intelligence is involved [16]. By building private enterprise cloud, organization can keep the sensitive data within their control boundaries and allow them to use existing infrastructure effectively.

External cloud

External or public clouds are owned and operated by third parties; they deliver superior economies of scale to customers, as the infrastructure costs are spread among a mix of users, giving each individual client an attractive low-cost, "Pay-as-you-go" model [17]. All customers share the same infrastructure pool with limited configuration, security protections, and availability variances. These are managed and supported by the cloud provider.

Communication Security

Data and information should be properly protected when communication is going on between internal and external cloud. It is important to ensure that access to the internal infrastructure is only possible through secure communications. Date or information should be encrypted using encryption key before Communicating between public and private cloud. At the destination data can be decrypted using decryption key.

Conclusion

Cloud computing has become very popular in the last few years and has become a new trend in the IT industry. As its popularity has increased very fast, it has to overcome a lot of issues and faces many challenges. Especially in hybrid cloud environments, incompatibilities between the available cloud solutions prevent a broad adoption throughout all businesses. Using hybrid cloud computing we can use advantages of both private and public clouds for business information system. Using hybrid cloud computing also changes the management process, culture of the organization, relationship between the organization and customers. These changes will make it easier for organization and clients to make good cloud-sourcing decisions and transitions in the future. Our hybrid cloud model for business information system will provide organizations with a simple, cost-effective and secure way to provision IT services, irrespective of where the services are hosted or provisioned. The hybrid cloud enables standardization at new levels which reduces IT complexity, and in the end provides a more reliable, secure and feature rich IT service resource for clients.

REFERENCES

[1] Haridayal Singh Shekhawat, DR. Durga Prasad Sharma (2010). Hybrid cloud computing model for business information system security. ISSN: 0975 – 6728| NOV 09 TO OCT 10 | Volume 1, Issue 1.

[2] R.K.Buyya , Cloud computing and emerging IT platforms: Vision, hype, and reality for delivering computing as the 5th utility,http://www.elsevier.com/wps/find/journaldescription.cws_home/505611/description#description

[3] N.G. Carr, "The many ways cloud computing will disrupt IT," InfoWorld, March 25, 2009. [Online].Available: http://www.tmcnet.com/usubmit/2009/03/25/4084363.htm

[4] National Institute of Standards and Technology (NIST) Definition of Cloud Computing, http://csrc.nist.gov/groups/SNS/cloud-computing/

[5] The open group service oriented architecture. http://www.opengroup.org/projects/soa

[6] REST – Representational State Transfer. http://www.ics.uci.edu/filding/pubs/dissertation/top.html

[7] Cloud Computing: The Evolution of Software-as-a-Service http://knowledge.wpcarey.asu.edu/article.cfm?articleid=1614

[8] Cloud Services and SaaS: A Smarter Way to do Business http://newsroom.cisco.com/dlls/2010/ts_032910.html

[9] The Cumulus Project: Build a Scientific Cloud for a Data Center http://www.cca08.org/papers/Paper29-Lizhe-Wang.pdf

[10] Here comes HaaS, http://www.roughtype.com/archives/2006/03/here_comes_haas.php

[11]Cloud Security Guidance, IBM Recommendations for the Implementation of Cloud Security, http://www.redbooks.ibm.com/redpapers/pdfs/redp4614.pdf

[12] IIT Hyderabad, Cloud Computing For EGovernance, http://search.iiit.ac.in/uploads/CloudComputingForEGovernance.pdf

[13] Security Guidance for Critical Areas of Focus in Cloud Computing V2.1 http://cloudsecurityalliance.org/csaguide.pdf

[14] Cryptography as a service, http://www.infoassurance.org/Public%20Docs/ISSA_Cryptography as a Service.pdf

[15]Cloud computing information assurance framework, http://www.enisa.europa.eu/act/rm/files/deliverables/cloud-computing-information-assurance-framework.pdf

[16] IBM Point of View: Security and Cloud Computing, ftp://public.dhe.ibm.com/common/ssi/sa/wh/n/tiw14045usen /TIW14045USEN_HR.PDF

[17] Realizing value proposition of cloud computing. http://www.infosys.com/cloud-computing/white-papers/documents/realizing-value-proposition.pdf

[18] Cloud Computing – An Overview http://www.thbs.com/pdfs/Cloud-Computing-Overview.pdf

****