International Journal of Computer Science and Engineering (IJCSE)
ISSN 2278-9960
Vol. 2, Issue 3, July 2013, 123-130
© IASET

International Academy of Science, Engineering and Technology
Connecting Researchers; Nurturing Innovations

SECURITY CHALLENGES IN PUBLIC CLOUD- A SURVEY

ARCHANA PANDITA

Department of Computer Science and Engineering, Birla Institute of Technology Offshore Campus Rak Al-Khaimah, United Arab Emirates

ABSTRACT

Cloud computing is a new way of delivering computing services ranging from data storage and processing to software, such as email handling. These services are now available right away, commitment-free and on-demand. Cloud computing is a approach of computing over the internet. The word cloud is an allegory for Internet. It is a new way for the delivery of IT services on the internet. The main attractions in Cloud computing are its usability and cost-effectiveness. The common characteristics most shared are scalability of vastly available and reliable collective computing resources, secure access to metered services from nearly anywhere, and displacement of data from inside to outside the organization. While aspects of these characteristics have been realized to a certain extent, cloud computing remains a work in progress. This publication provides an overview of the infrastructure to a public cloud environment and security and privacy challenges related to public cloud computing and considerations that should be taken when outsourcing data, applications, and infrastructure to a public cloud environment are also pointed out

KEYWORDS: Cloud Computing, Public Cloud Computing Infrastructure, Establishing Requirements, Security and Privacy Challenges

INTRODUCTION

Cloud computing is being paid a great deal of attention both in academics and industries, from research scholars to users. Cloud computing is a subscription based service which provides networked storage space and computer resources. It is a computing paradigm, where a large pool of systems is connected in private or public networks, to provide dynamically scalable infrastructure for application, data and file storage.

With the dawn of this technology, the application hosting, storage, delivery and cost of computation are reduced appreciably. Without worrying about any management or maintenance of actual resources, database resources can be accessed through internet remotely with Cloud computing for as long as needed. The basic cloud computing model is shown below

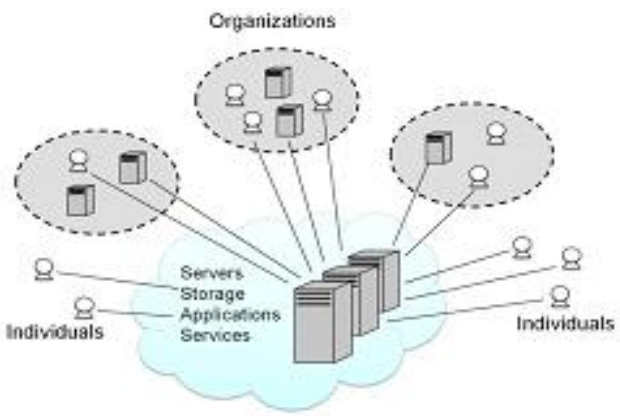

Figure 1: Basic Cloud Computing Model

Taxonomy can be divided into the following types:

- Public clouds: where the IT capabilities that are offered by cloud providers to any customers over the internet.
- Private clouds: where IT capability is offered to a select group of consumers who are part of an enterprise. The cloud service provider may be an internal IT organization (i.e., the same organization as the consumer) or a third party.
- Hybrid clouds: in which the environment is created through the usage of a combination of private and public cloud offerings by an organization.
- Internal clouds: is a subset cloud is an IT capability offered as a service by an IT organization to its own business.
- External clouds: is IT capability offered as a service to a business that is not hosted by its own IT organization. An external cloud can be public or private, but must be implemented by a third party.

From a point of view of architectural service layers based on the services provided using the cloud model, the ecosystem can be broadly divided into three:

- ***Software as a Service (SaaS):*** forms the top layer featuring a complete application provided in a multitenant environment. One prominent example of SaaS is Sales force.
- ***Platform as a Service (PaaS):*** providing a development and deployment middleware layer. Key Players include the Microsoft Azure platform as well as Google App Engine.
- ***Infrastructure as a Service (IaaS):*** the lowest layer delivering services like compute storage and network. One prominent example of IaaS is Amazon EC2 service. The work reported here mainly deals with the IaaS service delivery model. [1]

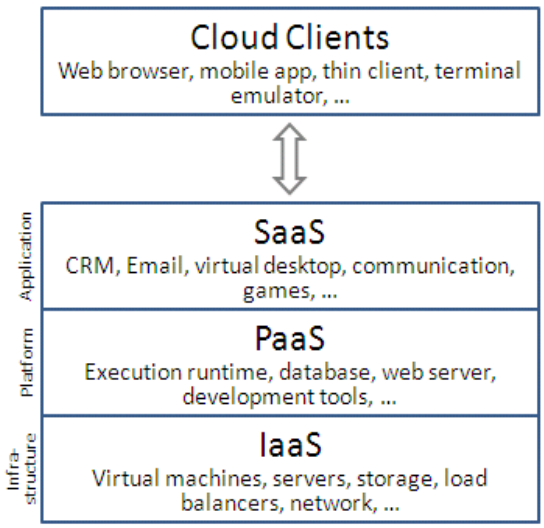

Figure 2: Cloud Computing Service Model Architecture

While the biggest obstacle facing public cloud computing is security, the cloud computing paradigm provides opportunities for innovation in provisioning security services that hold the prospect of improving the overall security of some organizations. The biggest beneficiaries are likely to be smaller organizations that have limited numbers of information technology administrators and security personnel, and lack the economies of scale available to larger organizations with sizeable data centers. Besides its many potential benefits for security and privacy, public cloud computing also brings with it potential areas of concern, when compared with computing environments found in traditional

data centers. Although the emergence of cloud computing is a recent development, insights into critical aspects of security can be gleaned from reported experiences of early adopters and also from researchers analyzing and experimenting with available cloud provider platforms and associated technologies. The sections below highlight privacy and security-related issues that are believed to have long-term significance for cloud computing.

PUBLIC CLOUD COMPUTING-INFRASTRUCTURE

A public cloud computing is one based on the standard cloud computing model, in which a service provider makes resources, such as applications and storage, available to the general public over the Internet. Public cloud services may be free or offered on a pay-per-usage model. The public cloud delivers chosen set of standardized business process, application and infrastructure services on a flexible price per use basis. Multiple occupancy is a main characteristic of public cloud services. Owned and operated by third parties Public Clouds deliver higher economics of range to customers, as the infrastructure costs are distributed among a mix of users, giving each individual client a pretty low cost, These are also called provider Clouds. SaaS (Software as a service) business models and public clouds go together and allow companies to control shared IT resources and services.

"Public" does not mean "free". Public cloud providers possibly will put forward some services free of charge, but in general they charge enough to at least cover their costs. Also, "public" does not mean that user data is visible to the public. Cloud providers put into practice security mechanisms to keep data access properly controlled. The main benefit of using a public cloud, as opposed to creating a private cloud, is easy and inexpensive set-up. The provider has done the work needed to create the cloud; the consumer just needs to do a small additional amount to configure the resources to be used.

In [2] author describes a private cloud as a Virtual private cloud, mainly where the third party is a public cloud provider that dedicates a part of its cloud infrastructure to public use and part to private use. The subsistence of other applications running in the cloud should be apparent to both cloud architects and end users in case a public cloud is implemented with data locality, performance and security in consideration. Certainly, one of the benefits of public clouds is that they can be greatly larger than a company's private cloud, offering the ability to scale up and down on demand, and shifting infrastructure risks from the enterprise to the cloud provider, if even just for the short term. Creating a virtual private data centre; portions of a public cloud can be engraved out for the special use of a single client. A virtual private datacenter gives customers superior visibility into its infrastructure rather than being restricted to deploying virtual machine images in a public cloud. Now customers can manipulate servers, storage systems, network devices, and network topology and virtual machine images as well. Creating a virtual private data center with all components located in the same capacity helps to lower the issue of data locality because bandwidth is abundant and typically free when resources are connecting within the same capacity.

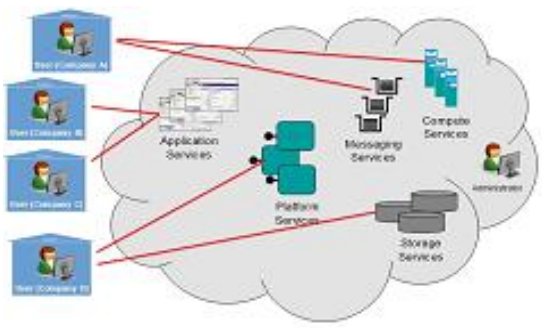

Figure 3: A Public Cloud

ESTABLISHING REQUIREMENTS

The requirements are conditions that the solution must or should meet. Requirements that are specific to, or affected by, cloud computing are functionality, supplier choice, performance, manageability, security, and regulatory compliance. Different requirement areas may have greater or lesser importance depending on whether you are considering IaaS, PaaS, or SaaS. The requirements in these areas are summarized in the table.[3]

Table 1: Cloud Ccomputing Requirements Areas

Area	Requirements
Functionality	Service Functionality Backup Bulk Data Transfer
Supplier Choice	Supplier Choice
Performance	Availability Reliability Recoverability Responsiveness Throughput
Manageability	Configurability Reporting Fault Management
Security	End User Access Control Supplier Access Control Resource Partitioning Logging Threat Response
Compliance	Compliance with regulations

- Service Functionality are the requirements for what the system should do. They are considered as overall solution requirements when establishing the aptness of a Cloud solution.
- Regular backups enable data to be recovered in the event of system failure. They can also be useful when users wish to correct mistakes that they have made.
- Some cloud suppliers provide bulk data transfer facilities, for example using physical transfers on disk packs.
- Supplier choice will strengthen your hand considerably in negotiations.
- Making it a requirement that there should be other similar suppliers that you could move to if necessary will enable you to have a viable exit strategy.
- *Availability*, or *uptime*, is the proportion of the time that a system is available for use. It is typically measured in 9s. A "Five 9s" system is up 99.999% of the time – a little over five minutes per year downtime. Planned, scheduled outages for maintenance are typically excluded.
- In the world of electronic components, reliability of repairable components is expressed as a combination of two parameters: mean time between failures (MTBF) and mean time to repair (MTTR).
- Recoverability is the ability to recover from a failure. It is measured in terms of recovery time objective (RTO) and recovery point objective (RPO). RTO determines how quickly the system needs to be fully operational; RPO determines how much data loss can be tolerated.
- Throughput is the amount of work that a computer can do in a given time period. It is normally calculated as transactions-per-second. For systems processing bulk data, such as audio or video servers, it is measured as a data

rate (e.g. Megabytes per second). Web server throughput is often expressed as the number of supported users – though clearly this depends on the level of user activity, which is difficult to measure consistently.

- Response time is the time taken for the system to respond to input. It can be specified as an average with an allowance for variability, for example, "an average of 300 ms with no more than 1% of responses taking more than 800 ms".
- On demand self service is a necessary characteristic of cloud computing. Consumers can provision capabilities without requiring human interaction with the service provider.
- The reports on system usage and performance must give enough information for your purposes.
- Diagnosis as well as correction of faults in the service will be the provider's responsibility. You require adequate procedures to enable you to report faults and check the progress that has been made in fixing them. You may wish to require web or telephone helpdesk and support to be accessible.
- Where cloud services are simply used to replace a component of a conventional IT architecture, the end user access control requirements are similar to those of the conventional architecture.
- Provider Access Control is the ability of system administrators and the staffs which are given special privileges to access restricted information, even when there is no business reason for them to do so, has long been an issue.
- An inference of resource pooling on public cloud is that the applications and data may be sharing resources with other programs that could have been written and deployed by anyone else. Cloud suppliers have mechanisms to ensure that the programs are securely partitioned.
- A user activity log is extremely valuable in the event of a security breach, and can also be significant for normal activity. It provides an audit trail that helps the system manager to establish what damage has been done, re-secure the system, and take measures to prevent future breaches of the same kind. It may be required to act in accordance with legislation, but you may well want one in any case to meet a business need to keep track of user access. This should be specified as a requirement.
- If a security breach is there, much of the remedial and corrective work must be done by the service provider. You should make it a requirement that the supplier has procedures that meet your requirements.
- Many legal regulations prohibit using the Cloud as-is. For example, the EU Data Protection Directive 95/46/EC impose restrictions on where personal data can be held. Apart from the legal regulations, contractual or moral obligations may require you to take care that information is kept confidential, or to guarantee that it is not lost or destroyed.

SECURITY AND PRIVACY CHALLENGES

As with any emerging information technology area, cloud computing should be approached cautiously with due thought to the sensitivity of data. Planning helps to make certain that the computing environment is secure and is in obedience with all relevant organizational policies and that data privacy is highly maintained. It also helps to ensure that the organization is deriving full benefit from information technology expenses. The security objectives of an organization are main factors for making decisions about outsourcing information technology services and specifically for decisions about transitioning organizational data, applications, and other resources to a public cloud computing environment. The

information technology governance practices of the organizations that affect to the policies, procedures, and standards for application development and service provisioning, as well as the design, implementation, monitoring of deployed or engaged services and testing should be extended to cloud computing environments.

To make the most of effectiveness and reduce costs, security and privacy must be considered from the initial planning stage at the start of the systems development life cycle. Attempting to address security after implementation and deployment is very difficult, expensive and risky. Although the emergence of cloud computing is a recent development, insights into critical aspects of security is revealed from experiences of early adopters and also from researchers which analyze and experiment with available cloud provider platforms and related technologies. Because cloud computing include service oriented architecture, virtualization, Web 2.0, and utility computing, many of the privacy and security issues involved can be viewed as known problems transmitting in a new setting.

Governance: Governance implies control and oversight over policies, procedures, and standards for application development, as well as the design, implementation, testing, and monitoring of deployed services. With the wide availability of cloud computing services, lack of organizational controls over employees engaging such services arbitrarily can be a source of problems. While cloud computing simplifies platform acquisition, it doesn't alleviate the need for governance; instead, it has the opposite effect, amplifying that need. Failure of Governance Includes, vulnerable systems could be deployed the-legal regulations could be ignored, charges could amass quickly to unacceptable levels, resources could be used for unsanctioned purposes, or other untoward effects could occur.

Compliance: Compliance involves conformance with an established specification, standard, regulation, or law. Various types of security and privacy laws and regulations exist within different countries at the national, state, and local levels, making compliance a potentially complicated issue for cloud computing. Challenges

- Data location challenges include whether sufficient safeguards are in place, whether legal and regulatory compliance requirements are being met, whether the laws in the jurisdiction where the data was collected permit the flow, whether the laws at them destination present additional risks or benefits
- Laws and Regulations challenges include, Different laws in different parts of the world making it difficult for moving data across borders.
- E-Discovery challenges include, how are document holds enforced; metadata protected; information searched for and retrieved?

Trust: Under the cloud computing paradigm, an organization relinquishes direct control over many aspects of security and, in doing so, confers an unprecedented level of trust onto the cloud provider.

Challenges

- Insider Access--Implement Insider Threat Intelligence with focus on all aspects of company's people, processes, and technology to create a definitive roadmap that is unique to company's business environment.
- Data Ownership--Contract should state clearly that the organization retains ownership over all its data, data cloud provider acquires no rights or licenses through the agreement to use the data for its own purposes, including intellectual property rights or licenses
- Liability and Performance --Terms of the agreement should be clear before transition into cloud Visibility--Organizations should have control over the aspects of the means of the visibility, such as threshold of alerts and

notifications or the level of detailed and scheduled reports, to accommodate it needs. Should have some visibility into security controls and processes employed by cloud provider and their performance over time

- Risk Management--Organization should ensured that security controls are implemented correctly, operate as intended ad meet its security requirements to deal with Risk Management

Architecture: The architecture of the software systems used to deliver cloud services comprises hardware and software residing in the cloud. The physical location of the infrastructure is determined by the cloud provider as is the implementation of the reliability and scalability logic of the underlying Support framework. Virtual machines often serve as the abstract unit of deployment and are loosely coupled with the cloud storage architecture. Applications are built on the programming Interfaces of Internet-accessible services, which typically involve multiple cloud components Communicating with each other over application programming interfaces. Many of the simplified interfaces and service abstractions belie the inherent complexity that affects security. Challenges:

- Virtual Network Protection Traffic over virtual networks may not be visible to security protection devices on the physical network, such as network-based intrusion detection and prevention systems Duplication of the physical network protection capabilities may be required on the virtual network
- Ancillary data cloud providers hold significant details about the service user's accounts that could be compromised and used in subsequent attacks. Ancillary data held by IaaS cloud providers is virtual machine images, promptly report security breaches occurring not only in the data the cloud provider holds for its subscribers, but also the data it holds about its subscribers Image repositories must be carefully managed and controlled to avoid problems.
- Client side protection maintaining physical and logical security over clients can be troublesome, especially with embedded mobile devices such as smart phones. security patches and updates for system components and add-ons are not as frequent; organizations need to review existing measures and employ additional ones, if necessary, to secure the client side, encrypt network exchanges and protect against keystroke logging
- Server side Protection Preventing holes or leaks between the composed infrastructures is a major concern with hybrid clouds, because of increases in complexity and diffusion of responsibilities; Following organizational policies and procedures, hardening of the operating system and applications should occur to produce virtual machine images for deployment. Provision security for the virtualized environments in which the images run

Identity and Access Management: Data sensitivity and privacy of information have become increasingly an area of concern for organizations and unauthorized access to information resources in the cloud is a major concern.

One recurring issue is that the organizational identification and authentication framework may not naturally extend into the cloud and extending or changing the existing framework to support cloud services may be difficult [4]. The alternative of employing two different authentication systems, one for the internal organizational systems and another for external cloud-based systems, is a complication that can become unworkable over time. Identity federation, popularized with the introduction of service oriented architectures, is one solution that can be accomplished in a number of ways, such as with the Security Assertion Markup Language (SAML) standard or the OpenID standard.

- **Authentication.** A growing number of cloud providers support the SAML standard and use it to administer users and authenticate them before providing access to applications and data. SAML request and response messages are typically mapped over the Simple Object Access Protocol (SOAP), which relies on the eXtensible Markup

Language (XML) for its format. SOAP message security validation is complicated and must be carried out carefully to prevent attacks. For example, XML wrapping attacks have been successfully demonstrated against a public IaaS cloud [5]. XML wrapping involves manipulation of SOAP messages.

- **Access Control.** SAML alone is not sufficient to provide cloud-based identity and access management services. The capability to adapt cloud subscriber privileges and maintain control over access to resources is also needed. Messages transmitted between XACML entities are susceptible to attack by malicious third parties, making it important to have safeguards in place to protect decision requests and authorization decisions from possible attacks, including unauthorized disclosure, replay, deletion and modification.[6]

CONCLUSIONS

Cloud computing promises to have far-reaching effects on the systems and networks of organizations. Emphasis on the benefits of public cloud computing, however, tend to overshadow some of the fundamental security and privacy concerns organizations have with these computing environments. Many of the features that make cloud computing attractive can also be at odds with traditional security models and controls. Attaining high-assurance qualities in implementations has been an elusive goal of computer security researchers and practitioners. Nevertheless, public cloud computing is a compelling computing paradigm that agencies need to incorporate as part their information technology solution set. Accountability for security and privacy in public clouds remains with the organization. Organizations must ensure that any selected public cloud computing solution is configured, deployed, and managed to meet the security, privacy, and other requirements of the organization. Organizational data must be protected in a manner consistent with policies, whether in the organization's computing center or the cloud. The organization must ensure that security and privacy controls are implemented correctly and operate as intended.

REFERENCES

1. Deepika Patidar, P S Patheja and Akhilesh A.Waoo, *An Efficient Approach for Cloud Computing based on Hierarchical Secure Paravirtualization System Resource Model*, International Journal of Applied Engineering Research, ISSN 0973-4562 Vol.7 No.11, 2012.
2. http://www.opengroup.org/cloud/cloud/what.htm
3. Cloud Computing for Business, The open group guide, 2010
4. Richard Chow et al., Controlling Data in the Cloud: Outsourcing Computation without Outsourcing Control, ACM Workshop on Cloud Computing Security, Chicago, Illinois, November 13-13, 2009, Chicago, Illinois, USA
5. Sebastian Gajek, Meiko Jensen, Lijun Liao, and Jörg Schwenk, Analysis of Signature Wrapping Attacks and Countermeasures, IEEE International Conference on Web Services, Los Angeles, California, July 2009
6. Yared Keleta, J.H.P. Eloff, H.S. Venter, Proposing a Secure XACML Architecture Ensuring Privacy and Trust, Research in Progress Paper, University of Pretoria, 2005,

   <URL:http://icsa.cs.up.ac.za/issa/2005/Proceedings/Research/093_Article.pdf>.