ISSN No. 0976-5697

Volume 4, No. 3, March 2013 (Special Issue)

International Journal of Advanced Research in Computer Science

REVIEW ARTICLE

Available Online at www.ijarcs.info

Cloud Computing: A Journey towards its Security Issues

Manisha Raj
M Tech Scholar, Department of Computer Science,
Arya College of Engineering & IT Jaipur, India
manisha.raj86@gmail.com

Prof. Shiv Kumar
Professor, Department of Computer Science
Arya College of Engineering & IT Jaipur, India
shiv@aryacollege.in

Abstract: Cloud computing can be defined as a model for enabling ubiquitous, convenient, on-demand network access to a shared pool of computing resources(eg: networks, servers, storage, applications and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction. Security remains the top concern for cloud adoption.

In a cloud computing environment, the entire data resides over a set of networked resources, enabling the data to be accessed through virtual machines. Since these data-centers may be located in any part of the world beyond the reach and control of users, there are multifarious security and privacy challenges that need to be understood and addressed. Some of the security risks in cloud computing includes data integrity, data intrusion, service availability, Multi-tenancy etc. These issues need to be addressed with respect to security and privacy in cloud computing environment. This paper aims to highlight the security concerns and analyze the numerous unresolved issues threatening the cloud computing adoption.

Keywords: ubiquitous, on-demand, security risks, multifarious, threatening

I. INTRODUCTION

Cloud computing is Internet-based computing, whereby shared resources, software and information are provided to computers and other devices on demand. may be familiar with services that involve cloud computing. Some web-based email services are examples of cloud computing implementations. Other examples are web-based document storage, editing and collaboration tools. Cloud computing services are also used for web commerce. Increasingly web applications are making use of cloud computing, and many contemporary websites use and integrate a number of cloud computing services. Wikipedia defines cloud computing as:“the delivery of computing as a service rather than a product, whereby shared resources, software and information are provided to computers and other devices”. Cloud computing provides computation, software, data access, and storage services that do not require end-user knowledge of the physical location and configuration of the system that delivers the services[1]. Typical cloud computing providers deliver common business applications online that are accessed from another Web service or software like a Web browser, while the software and data are stored on servers. The two most significant components of cloud computing architecture[2] are front end and back end. The front end is the part seen by the client, i.e. the computer user. This includes the client’s or computer and the applications used to access the cloud via a user interface such as a web browser. The backend of the cloud computing architecture is the ‘cloud’ itself, comprising various computers, servers and data storage devices.

Concept of this new trend started from 1960 used by telecommunication companies until 1990 offered point to point data circuits and then offered virtual private networks. But due to network traffic and make network bandwidth more efficient introduced cloud to both servers and infrastructure. The development[3] of this Amazon played vital role by making modern data centers. In 2007 Google, IBM and many remarkable universities and companies adopted it. And in 2008 Gartner highlighted its characteristics for customer as well service providers.

There is a critical need to securely store, manage, share and analyze massive amounts of complex (e.g., semi-structured and unstructured)data. So It is important that clouds be secure. The major security challenge with clouds is that the owner of the data may not have control of where the data is placed. This is because if one wants to exploit the benefits of using cloud computing, one must also utilize the resource allocation and scheduling provided by clouds. Therefore, we need to safeguard the data in the midst of untrusted processes.

Clouds aim to power the next generation data centers by architecting them as a network of virtual services (hardware, database, user-interface, application logic) so that users are able to access and deploy applications from anywhere in the world on demand at competitive costs depending on users QoS (Quality of Service) requirements. Cloud computing infrastructures are quite flexible.

In the model of cloud computing, the local computing and storage resources are moved into the cloud. So those from a business point of view do not need to buy expensive servers, and to employ professionals who deploy and maintain the IT infrastructure. Only need to pay a low rental cost to the cloud service provider, thereby reducing the enterprise’s purchase cost and operation cost. Especially for small-scale enterprises, it is undoubtedly beneficial.

CONFERENCE PAPER
II International Conference on
“Advance Computing and Creating Entrepreneurs (ACCE2013)”
On 19-20 Feb 2013
Organized by
2nd SIG-WNs, Div IV & Udaipur Chapter , CSI , IEEE Computer Society Chapter India Council ,
IEEE Student Chapter Geetanjali Institute of Technical Studies, Udaipur, Rajasthan, India

II. CLOUD DEPLOYMENT MODELS

There are four deployment models for cloud services, with derivative variations that address specific requirements:

A. *Public:*

The cloud infrastructure is made available to the general public or a large industry group and is owned by an organization selling cloud services. It describes cloud computing in the traditional mainstream sense, whereby resources are dynamically provisioned on a fine-grained, self-service basis over the Internet, via web applications/web services, from an off-site third-party provider who shares resources and bills on a fine-grained utility computing basis. It is typically based on a pay-per-use model, similar to a prepaid electricity metering system which is flexible enough to cater for spikes in demand for cloud optimization.[5] Public clouds are less secure than the other cloud models because it places an additional burden of ensuring all applications and data accessed on the public cloud are not subjected to malicious attacks.

B. *Private:*

The cloud infrastructure is operated solely for a single organization. It may be managed by the organization or a third party, and may exist on-premises or off-premises. It is a new term that some vendors have recently used to describe offerings that emulate cloud computing on private networks. It is set up within an organization’s internal enterprise datacenter. In the private cloud, scalable resources and virtual applications provided by the cloud vendor are pooled together and available for cloud users to share and use[6]. It differs from the public cloud in that all the cloud resources and applications are managed by the organization itself, similar to Intranet functionality. Utilization on the private cloud can be much more secure than that of the public cloud because of its specified internal exposure. Only the organization and designated stakeholders may have access to operate on a specific Private cloud.

C. *Hybrid:*

The cloud infrastructure is a composition of two or more clouds (private, community, or public) that remain unique entities but are bound together by standardized or proprietary technology that enables data and application portability (e.g., cloud bursting for load-balancing between clouds). It is a private cloud linked to one or more external cloud services, centrally managed, provisioned as a single unit, and circumscribed by a secure network [7]. It provides virtual IT solutions through a mix of both public and private clouds. Hybrid Cloud provides more secure control of the data and applications and allows various parties to access information over the Internet. It also has an open architecture that allows interfaces with other management systems. Hybrid cloud can describe configuration combining a local device, such as a Plug computer with cloud services. It can also describe configurations combining virtual and physical, collocated assets -for example, a mostly virtualized environment that requires physical servers, routers, or other hardware such as a network appliance acting as a firewall or spam filter. Figure 1 gives the details of cloud deployment models.

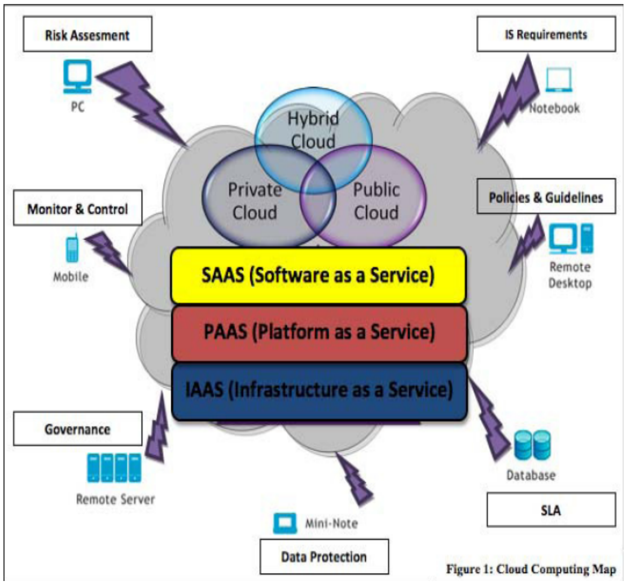

Figure 1: Cloud Deployment model

D. *Community:*

The cloud infrastructure is shared by several organizations and supports a specific community that has shared concerns (e.g., mission, security requirements, policy, or compliance considerations). It may be managed by the organizations or a third party and may exist on-premises or off-premises.

III. FLAVOURS OF CLOUD COMPUTING

Cloud service delivery is divided among three archetypal models and various derivative combinations. The three fundamental classifications are often referred to as the “SPI Model,” where ‘SPI’ refers to Software, Platform or Infrastructure (as a Service) respectively.

A. *SaaS:*

SaaS, stands for Software as a Service[4], where applications are hosted and delivered online via a web browser offering traditional desktop functionality for example Google Docs, Gmail, MobileMe, Zoho and MySAP etc. 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. Sometimes it is referred to as “on Demand Software service”. SaaS is becoming an increasingly prevalent delivery model as underlying technologies that support web services and service-oriented architecture (SOA) mature and new developmental approaches become popular.

B. PaaS:

PaaS, stands for Platform as a Service, where the cloud provides the software platform for systems (as opposed to just software), the best current example being the Google App Engine, Microsoft Azure, Force.com. The capability provided to the consumer is to deploy onto the cloud 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[5].

C. IaaS:

IaaS stands for infrastructure as a Service, where a set of virtualized computing resources, such as storage and computing capacity, are hosted in the cloud; customers deploy and run their own software stacks to obtain services. IaaS consist of servers, storage, security, databases and other peripherals. is a single tenant cloud layer where the Cloud computing vendor's dedicated resources are only shared with contracted clients at a pay-per-use fee.

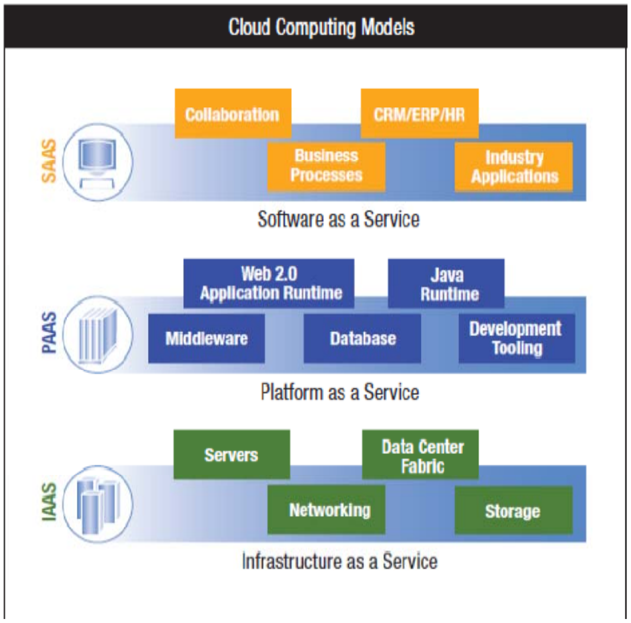

Figure 2 : Cloud computing service delivery models

This greatly minimizes the need for huge initial investment in computing hardware such as servers, networking devices and processing power[6]. They also allow varying degrees of financial and functional flexibility not found in internal data centers or with collocation services, because computing resources can be added or released much more quickly and cost-effectively than in an internal data center or with a collocation service Current examples are Amazon Elastic Compute Cloud (EC2), Simple Storage Service (S3), Rackspace Mosso offering, Sun's cloud service, Terremark cloud offering and Simple DB. Figure 2 gives the detail of cloud service delivery models.

IV. CLOUD COMPUTING BENEFITS

Cloud computing is enabling the enterprise to:

A. Expand scalability – By utilizing cloud computing, IT staff can quickly meet changing user loads without having to engineer for peak loads.

B. Lower infrastructure costs – With external clouds, customers do not own the infrastructure. This enables enterprises to eliminate capital expenditures and consume resources as a service, paying only for what they use. Clouds enable IT departments to save on application implementation, maintenance and security costs, while benefiting from the economies of scale a cloud can offer compared to even a large company network.

C. Increase utilization – By sharing computing power between multiple clients, cloud computing can increase utilization rates, further reducing IT infrastructure costs.

D. Improve end-user productivity– With cloud computing, users can access systems, regardless of their location or what device they are using (e.g., PCs, laptops, etc.).

E. Improve reliability– Cloud computing can cost-effectively provide multiple redundant sites, facilitating business continuity and disaster recovery scenarios.

F. Increase security– Due to centralization of data and increased security-focused resources from cloud computing providers, cloud computing can enhance data security. Cloud computing can also relieve an IT organization from routine tasks, including backup and recovery. External cloud service providers typically have more infrastructure to handle data security than the average small to midsize business.

***G. Gain access to more sophisticated applications* –** External clouds can offer CRM and other advanced tools that were previously out of reach for many businesses with smaller IT budgets.

H. Downsize the IT department– By moving applications out to a cloud, IT departments can reduce the number of application administrators needed for deployment, maintenance and updates. It departments can then reassign key IT personnel to more strategic tasks.

***I. Save energy* –** Going "green" is a key focus for many enterprises. Clouds help IT organizations reduce power, cooling and space usage to help the enterprise create environmentally responsible datacenters[8].

V. CHALLENGES OF EXISTING CLOUD COMPUTING

We must address some challenges that cloud computing poses before we can recognize its full value. These include:

A. Lack of interoperability– The absence of standardization across cloud computing platforms creates unnecessary complexity and results in high switching costs. Each compute cloud vendor has a different application model, many of which are proprietary, vertically integrated stacks that limit platform choice. Customers don't want to be locked into a single provider and are often reluctant to relinquish control of their mission-critical applications to hosting service providers.

B. Application Compatibility – Most of the existing public compute clouds are not interoperable with existing applications and they limit the addressable market to those willing to write new applications from scratch.

C. Difficulty in meeting compliance regulations– Regulatory compliance requirements may limit the use of the shared infrastructure and utility model of external cloud computing for some environments. Achieving compliance often requires complete transparency of the underlying IT infrastructure that supports business-critical applications, while cloud computing by design places IT infrastructure into a 'black box' accessible only through well-defined interfaces[8]. As a result, internal compute clouds may be a better solution for some applications that must meet stringent compliance requirements.

D. Inadequate security– By design, cloud vendors typically support multi-tenancy compute environments. IT managers must look for a balance between the security of an internal, dedicated infrastructure versus the improved economics of a shared cloud environment. Security can be a key inhibitor to adoption of cloud computing

VI. CLOUD PRIVACY & SECURITY ISSUES

Security controls in cloud computing are, for the most part, no different than security controls in any IT environment. However, because of the cloud service models employed, the operational models, and the technologies used to enable cloud services, cloud computing may present different risks to an organization than traditional IT solutions. Following are some issues that can be faced while implementing cloud services:

A. Privacy Issues:

It is the human right to secure his private and sensitive information. In cloud context privacy occur according to the cloud deployment model [9].

a. Lack of user control:

In SAAS environment service provider is responsible to control data. Now how customer can retain its control on data when information is processed or stored. It is legal requirement of him and also to make trust between customer and vendor [10] . In this new paradigm user sensitive information and data is processed in 'the cloud' on systems having no any, therefore they have danger of misuse, theft or illegal resale.

b. Unauthorized Secondary Usage:

One of the threats can occur if information is placed for illegal uses. Cloud computing standard business model tells that the service provider can achieve profits from authorized secondary uses of users' data, mostly the targeting of commercials [11]. Now a days there are no technological barriers for secondary uses.

c. Data Proliferation:

One of the attribute of cloud is Data proliferation and which involves several companies and is not controlled and managed by the data owners. Vendor guarantee to the ease of use by copy data in several datacenters. This is very difficult to ensure that duplicate of the data or its backups are not stored or processed in a certain authority, all these copies of data are deleted if such a request is made.

d. Dynamic provision:

Cloud has vibrant nature so there is no clear aspect that which one is legally responsible to ensure privacy of sensitive data put by customer on cloud [11].

B. Security Issues:

Conventional infrastructure security controls designed for dedicated hardware do not always map well to the cloud environment. Cloud architectures must have well-defined security policies and procedures in place. Realizing full interoperability with existing dedicated security controls is unlikely; there has to be some degree of compatibility between the newer security protections specifically designed for cloud environments and traditional security controls. Some security concerns are described below:

a. Access:

It has the threat of access sensitive information. The risk of data theft from machine has more chances in cloud environment data stored in cloud a long time duration any hacker can access this data [12].

b. Control over data lifecycle:

To ensure the customer that it has control over data, if it remove or delete data vendor cannot regain this data. In cloud IAAS and PAAS models virtual machine are used that process and then media wiped but still there is no surety that next user cannot get that data [11].

c. Availability and backup:

There is no any surety of availability and back up of data in this environment. In business backup is one of the important consideration [12].

d. Multi-tenancy:

It is feature of SAAS that one program can run to multiple machines. CSP use multi-tenant application of cloud to reduce cost by using virtual machine but it increase more vulnerability [12].

e. Audit:

To implement internal monitoring control CSP need external audit mechanism .But still cloud fails to provide auditing of the transaction without effecting integrity [13].

C. Trust:

Trust is very necessary aspect in business. Still cloud is fail to make trust between customer and provider. So the vendor uses this marvelous application should make trust.Weak trust relationship and lack of customer trust cause many problems during deployment of cloud services [14].

VII. MITIGATION STEPS

This section includes mitigation steps and some solution to overcome the issues discussed in previous section. It provides guidelines to the companies that offer cloud services .It will helpful to them to make proper strategy before implementing cloud services[15].

a. Build up an iterative policy for relocation from traditional environment to Cloud environment
b. As this upcoming trend reduce cost but be careful to select possible solutions to avoid problems in this computing and calculate the effect on the system just not consider the outlay.
c. Providers should be aware regarding new changes and assure that customers access privileges are limited.
d. Cloud is a shared pool of resource. Discover the linked service providers that wants to connected to particular Cloud service provider to query, which provider has right to use facts and data .
e. System for monitoring should be request for exclusion
f. Service provider should tell customer for managing polices for security beside provider's owned policies, with in the duration of services.
g. Make it sure, that the data being transferred is protected and secured by standard security techniques and managed by appropriate professionals.

VIII.SOLUTIONS

This section includes solutions that are helpful to the cloud customer and companies offer services in with secure and trusty environment.

A. Data Handling Mechanism:

a. Classify the confidential data
b. Define the geographical region of data
c. Define policies for data destruction

B. Data security mitigation:

a. Encrypting personal data
b. Avoid putting sensitive data on cloud

C. Design for policy:

a. Fair information principles are applicable

D. Accountability:

a. For businesses having data lost, leakage or privacy violations is catastrophic
b. Accountability needs in legal and technical
c. Audit needed in every step to increase trust

IX. CONCLUSION

It is certain that cloud computing is predominantly dominating the present enterprise business computing with its tempting financial benefits. At the same time, due to the open & public nature of cloud, it equally attracts the attention of attackers on par with customers (sometimes in leading count), which append more severe security challenges & risks to it. At the same time, the amounts of investment made by these cloud vendors are also significantly high. The paper addresses the issues that can arise during the deployment of cloud services. After identify these problems some steps are explained to mitigate these challenges and solutions to solve the problems.

X. REFERENCES

[1] http://en.wikipedia.org/wiki/Cloud_computing

[2] Rajat Jain, Deepti Mathur, Kalpit Mathur " Cloud Computing Architecture" ICACTEA-2011)

[3] Janakiram MSV Cloud Computing Strategist; (2010), "Demystifying the Cloud: An introduction to Cloud Computing", Version 1.0 – March.

[4] F. A. Alvi, B.S Choudary ,N. Jaferry , E.Pathan,(2011) "A review on cloud computing security issues and challanges" IEEE 2011 44th Hawaii International Conference on System Sciences (HICSS), pp1, 4-7 Jan. 2011.

[5] Cloud Security Alliance, December 2009

[6] Kuyoro S. O., Ibikunle F. & Awodele O., "cloud computing security issues and challanges", International Journal of Computer Networks (IJCN),Volume (3) : Issue (5) : 2011

[7] Global Netoptex Incorporated. "Demystifying the cloud. Important opportunities, crucial choices." pp4-14. Available: http://www.gni.com [Dec. 13, 2009].

[8] A Review of cloud computing, security implications, and best practices by VM Ware.

[9] Grobauer, B.; Walloschek, T.; Stocker,E.;(2011), "Understanding Cloud Computing Vulnerabilities", Security & Privacy, IEEE, Vol 9, pp 50.

[10] Gansen Z; Chunming R; Jin L; Feng Z; Yong T; (2010),,"Trusted Data Sharing over Untrusted Cloud Storage Providers",2010 IEEE Second International Conference on Cloud Computing Technology and Science (CloudCom), pp 97, Nov. 30 2010-Dec. 3 2010.

[11] Kresimir P; Zeljko H; (2010), "Cloud computing security issues and challenges", MIPRO 2010, May 24-28, 2010, Opatija, Croatia.

[12] Jensen, M.; Schwenk, J.; Gruschka, N.; Iacono, L.L.; (2010), "On Technical Security Issues in Cloud Computing", IEEE International Conference on Cloud Computing, 2009. CLOUD '09, pp 109, 21-25 Sept.2009. 5708519 Searchabstract

[13] Jansen, W.A.; (2010), " Cloud Hooks: Security and Privacy Issues in Cloud Computing5719001 IEEE 2011 44th Hawaii International Conference on System Sciences (HICSS), pp1, 4-7 Jan. 2011.

[14] Tian L.Q; NI Y,LING; (2010) , “Evolution of user Behavior Trust in Cloud Computing”, 2010 International Conference on Computer Application and System Modeling (ICCASM 2010),Vol. 7,pp V7-567, 22-24 Oct. 2010.

[15] F. A. Alvi1, B.S Choudary ,N. Jaferry , E.Pathan “A review on cloud computing security issues & challanges”