SURVEY ON VARIOUS ATTRIBUTES AND UTILITIES OF CLOUD COMPUTING FOR CURRENT BUSINESS MODELS

SWETA RAMESH[a1], VINEET AGRAWAL[b] AND RAJESH KESHAVRAO DESHMUKH[c]

[abc]Department of CSE, S.S.I.P.M.T., Raipur, Chhattisgarh, India

ABSTRACT

The computational world has become large and complex. Cloud computing has emerged as a popular computing model in the field of Information Technology. Advancements in cloud computing has resulted in handling of large amount of data and services. In this paper, we present a survey of cloud computing, highlighting its key concepts, architectural, deployment model, security factors and the cloud services. The aim of this paper is to provide a better understanding of the cloud services.

KEYWORDS: Cloud Computing, Cloud, Saas, Paas, Iaas, Cloud Services, Cloud Architecture, Cloud Model, Public Cloud, Private Cloud, Hybrid Cloud, Community Cloud, Cloud Challenges

Cloud computing is a complete new technology. It is the development of parallel computing, distributed computing grid computing, and is the combination and evolution of Virtualization, Utility computing [1], Software-as-a-Service (SaaS), Infrastructure-as-a-Service (IaaS) and Platform-as-a-Service (PaaS). To users, cloud computing is a Pay-per-Use-On-Demand mode that can conveniently access shared IT resources through the Internet [2]. Where the IT resources include network, server, storage, application, service and so on and they can be deployed with much quick and easy manner and least management and also interactions with service providers. Google, Amazon, Yahoo and alternative web service suppliers, IBM, Microsoft and alternative IT vendors have imply their own cloud computing strategy [3].

ARCHITECTURE

Cloud computing architecture refers to the components and subcomponents required for cloud computing [4]. These components typically consist of a front end platform (fat client, thin client, mobile device), back end platforms (servers, storage), a cloud based delivery, and a network (Internet, Intranet). Combined, these components make up cloud computing architecture.

Cloud Computing architecture comprises of many cloud components, which are loosely coupled. We can broadly divide the cloud architecture into two parts:

- Front End
- Back End

Each of the ends is connected through a network, usually Internet.

The front end refers to the client part of cloud computing system. It consists of interfaces and applications that are required to access the cloud computing platforms, Example - Web Browser.

The back end refers to the cloud itself. It consists of all the resources required to provide cloud computing services. It is the responsibility of the back end to provide built-in security mechanism, traffic control and protocols. It comprises of huge data storage, virtual machines, security mechanism, services, deployment models, servers, etc [5].

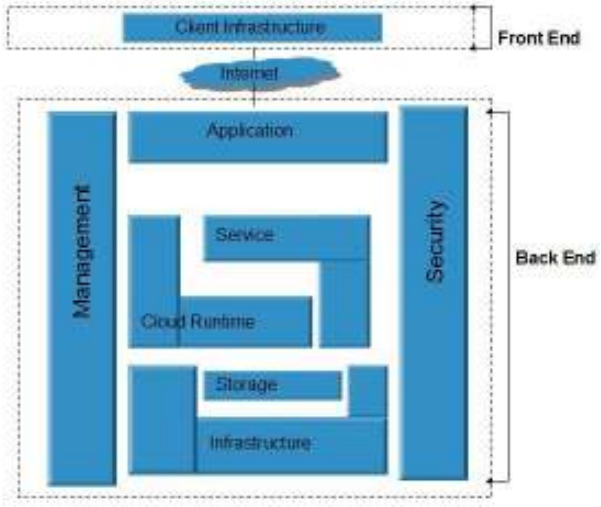

Figure 1: Cloud computing architecture – front end and back end

Architectural layers of cloud computing [6]:

The architecture of a cloud computing can be categories into four layers:

The Physical layer, the infrastructure layer, the platform layer and the application layer**:**

[1]**Corresponding author**

The Hardware Layer

The hardware layer is responsible for dealing with the physical assets of the cloud, including routers, servers, switches, cooling systems and power.

The Infrastructure Layer

The infrastructure layer is also called as virtualization layer. The infrastructure layer makes a pool of storage capacity and computing resources by partitioning the physical resources using virtualization technologies such as KVM and VMware.

The Platform Layer

The platform layer based on top of the infrastructure layer, and this layer comprises of operating systems and requisition structures.

The Application Layer

The application layer comprises of the actual cloud provisions, for e.g. Business Applications, Multimedia & Web Services.

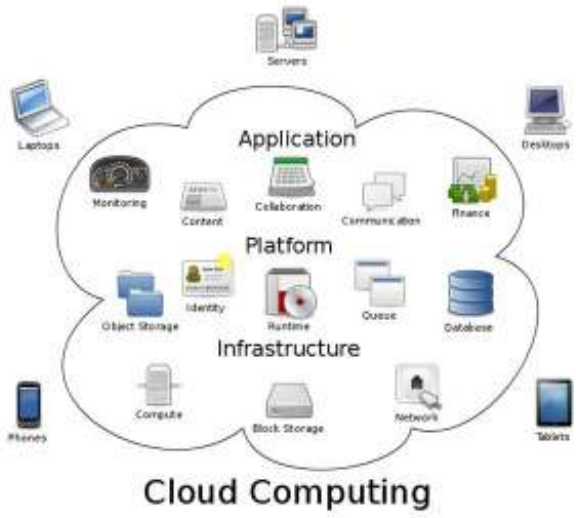

Figure 2: Cloud Computing Architecture

CLOUD SERVICES

Cloud computing system can be divided into two sections: the front end and the back end. Cloud service models are commonly divided into SaaS, PaaS, and IaaS.

Software as a Service (SaaS)

Cloud consumers release their applications in a hosting environment, which can be accessed through networks from various clients. SaaS uses the web to deliver applications that are managed by a third-party vendor and whose interface is accessed on the clients' side. Most SaaS applications can be run directly from a web browser without any downloads or installations required, although some require plug-ins [7]. SaaS is a bit like public transport. Cheap, someone else takes care of pretty much everything; you just get to use it.

SaaS Characteristics [7]**:**

- Software is hosted on a remote server and is always accessible through a web browser over Internet.
- Application is managed from a central location.
- Application users don't need to worry about hardware, software updates and patches.
- Any integration with the third party applications are done through APIs.
- Web access to commercial software.
- Software is managed from a central location.
- Software delivered in a "one-to-many" model.
- Users not required handling software upgrades and patches.
- Application Programming Interfaces (APIs) allow for integration between different pieces of software [8].

Where SaaS Makes Sense:

Cloud computing generally and SaaS in particular, is a rapidly growing method of delivering technology. That said, organizations considering a move to the cloud will want to consider which applications they move to SaaS. As such there are particular solutions we consider prime candidate for an initial move to SaaS:

- Applications where there is significant interplay between the organization and the outside world. For example, email newsletter campaign software.
- Applications that have a significant need for web or mobile access. An example would be mobile sales management software.
- Software that is only to be used for a short term need. An example would be collaboration software for a specific project.
- Software where demand spikes significantly, for example tax or billing software used once a month.

Where SaaS May Not be the Best Option

While SaaS is a very valuable tool, there are certain situations where we believe it is not the best option

for software delivery. Examples where SaaS may not be appropriate include:

- Applications where extremely fast processing of real time data is required.
- Applications where legislation or other regulation does not permit data being hosted externally.
- Applications where an existing on-premise solution fulfills all of the organization's needs.

Some of the popular SaaS products are Salesforce, Google Apps, NetFlix, WebEx, GotoMeeting and DropBox.

Platform as a Service (PaaS)

PaaS is a development platform supporting the full "Software Lifecycle" which allows cloud consumers to develop cloud services and applications (e.g. SaaS) directly on the PaaS cloud. **PaaS** is a bit like getting a cab. You get in and choose where you want to go to and how to get there. Keeping the car running and figuring out the details is up to the driver. Developers work on PaaS platform and concentrate on software application building without having to worry about software updates, operating systems, load balancing, storage, or other details related to infrastructure.

PaaS Characteristics

- Built on top of virtualization technology – you can demand for resources as per your need and scale up/ down as per the requirement.
- Provides varying services to facilitate development, testing, deployment and hosting of software applications in integrated development environment.
- Multiple users can utilize the same development application.
- Integrated web services and databases.
- Billing and subscription is managed by tools
- Services to develop, test, deploy, host and maintain applications in the same integrated development environment. All the varying services needed to fulfill the application development process.
- Built in scalability of deployed software including load balancing and failover.

Where PaaS Makes Sense

- PaaS is especially useful in any situation where multiple developers will be working on a development project or where other external parties need to interact with the development process.
- It is proving invaluable for those who have an existing data source – for example sales information from a customer relationship management tool, and want to create applications which leverage that data.
- Finally PaaS is useful where developers wish to automate testing and deployment services.

Where PaaS May Not be the Best Option

There are certain situations where PaaS may not be ideal, examples include:

- Where the application needs to be highly portable in terms of where it is hosted.
- Where proprietary languages or approaches would impact on the development process.
- Where a proprietary language would hinder later moves to another provider – concerns are raised about vendor lock-in.
- Where application performance requires customization of the underlying hardware and software.

Some examples of PaaS include Google App Engine, Microsoft Azure Services, and the Force.com platform.

Infrastructure as a Service (IaaS)

Cloud consumers directly use IT infrastructures (processing, storage, networks and other fundamental computing resources) provided in the IaaS cloud. Virtualization is extensively used in IaaS cloud in order to integrate/decompose physical resources in an ad-hoc manner to meet growing or shrinking resource demand from cloud consumers. With **IaaS**, it's like leasing a car. Keeping the car repaired is someone else's problem, you just need to supply it with fuel (setting it up, maintaining software, etc.) and you get to go pretty much wherever you want to. IaaS model delivers Cloud Computing infrastructure including servers, storage, network and operating systems an on-demand service. For organizations it means that instead of purchasing the whole infrastructure, they simply buy those resources as a service on demand.

Characteristics of IaaS

As with the two previous sections, SaaS and PaaS, IaaS is a rapidly developing field. That said there are some core characteristics which describe what IaaS is. IaaS is generally accepted to comply with the following;

- Resources are distributed as a service.

- Allows for dynamic scaling.
- Has a variable cost, utility pricing model.
- Generally includes multiple users on a single piece of hardware.

Where IaaS Makes Sense

IaaS makes sense in a number of situations and these are closely related to the benefits that Cloud Computing bring. Situations that are particularly suitable for Cloud infrastructure include:

- Where demand is very volatile – any time there are significant spikes and troughs in terms of demand on the infrastructure.
- For new organizations without the capital to invest in hardware.
- Where the organization is growing rapidly and scaling hardware would be problematic.
- Where there is pressure on the organization to limit capital expenditure and to move to operating expenditure.
- For specific line of business, trial or temporary infrastructural needs.
- Where IaaS May Not be the Best Option:
- While IaaS provides massive advantages for situations where scalability and quick provisioning are beneficial, there are situations where its limitations may be problematic. Examples of situations where we would advise caution with regards IaaS include:
- Where regulatory compliance makes the off-shoring or outsourcing of data storage and processing difficult.
- Where the highest levels of performance are required, and on-premise or dedicated hosted infrastructure has the capacity to meet the organization's needs [9].

There are a plethora of IaaS providers out there from the largest Cloud players like Amazon Web Services and Rackspace to more boutique regional players.

Figure 3: Cloud Services

CLOUD DEPLOYMENT MODEL

Public cloud

A public cloud is basically the internet. Service providers use the internet to make resources, such as applications (also known as Software-as-a-service) and storage, available to the general public, or on a 'public cloud. Examples of public clouds include Amazon Elastic Compute Cloud (EC2), IBM's Blue Cloud, Sun Cloud, Google AppEngine and Windows Azure Services Platform.

For users, these types of clouds will provide the best economies of scale, are inexpensive to set-up because hardware, application and bandwidth costs are covered by the provider. It's a pay-per-usage model and the only costs incurred are based on the capacity that is used.

There are some limitations, however; the public cloud may not be the right fit for every organization. The model can limit configuration, security, and SLA specificity, making it less-than-ideal for services using sensitive data that is subject to compliancy regulations.

Private Cloud

Private clouds are data center architectures owned by a single company that provides flexibility, scalability, provisioning, automation and monitoring. The goal of a private cloud is not sell "as-a-service" offerings to external customers but instead to gain the benefits of cloud architecture without giving up the control of maintaining your own data center.

Private clouds can be expensive with typically modest economies of scale. The most advantage here is that it's easier to manage security, maintenance and upgrades and conjointly provides additional management over the preparation and use. This is usually not an option for the average Small-to-Medium sized business and is most typically put to use by large enterprises. Private clouds are driven by concerns around security and compliance, and keeping assets within the firewall [10].

Community Cloud

A community cloud is a collaborative effort made for sharing infrastructure between multiple organizations. A community cloud is similar to a public cloud except that its access is limited to a specific community of cloud consumers.

The community cloud may be jointly owned by the community members or by a third-party cloud provider that provisions a public cloud with limited access. The member cloud consumers of the community typically share the responsibility for defining and evolving the community cloud.

Membership in the community does not necessarily guarantee access to or control of all the cloud's IT resources. Parties outside the community are generally not granted access unless allowed by the community.

Hybrid Cloud

Hybrid cloud is a combination 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).

By using a Hybrid approach, companies can maintain control of an internally managed private cloud while relying on the public cloud as needed. For instance during peak periods individual applications, or portions of applications can be migrated to the Public Cloud. This will also be beneficial during predictable outages: hurricane warnings, scheduled maintenance windows, rolling brown/blackouts.

The ability to maintain an off-premise disaster recovery site for most organizations is impossible due to cost. While there are lower cost solutions and alternatives the lower down the spectrum an organization gets, the capability to recover data quickly reduces. Cloud based Disaster Recovery (DR)/Business Continuity (BC) services allow organizations to contract failover out to a Managed Services Provider that maintains multi-tenant infrastructure for DR/BC, and specializes in getting business back online quickly.

APPLICATIONS

There are a few applications of cloud computing as follows:

1. Cloud computing provides dependable and secure data storage center.
2. Cloud computing can realize data sharing between different equipments.
3. The cloud provides nearly infinite possibility for users to use the internet.
4. Cloud computing does not need high quality equipment for the user and it is easy to use.

CHARACTERISTICS

1. The infrastructure that is mostly provided by a third-party is accessed with the assistance of web. Price is reduced to a major level because the infrastructure is provided by a third-party.
2. Less IT skills are needed for implementation.
3. Reliable services are often obtained by the employment of multiple sites that is appropriate for business continuity and disaster recovery.
4. Sharing of resources and prices amongst an outsized assortment of users.
5. Maintenance is simpler.
6. Pay per use facility.
7. Performance is often monitored and so it's ascendible.
8. Security is often pretty much as good as or higher than ancient systems.

CHALLENGES

Data Breaches

Due to vast amount of data stored on cloud servers, provider becomes an attractive target. The severity of potential damage tends to depend on the sensitivity of the data expose. When data breach occurs, companies may incur fines or they may face lawsuits or criminal charges. Indirect effects like brand damage and loss of business can impact organizations.

Compromised Credentials And Broken Authentication

Organizations often struggle with identity management as they try to allocate permissions

appropriate to user's job role. They sometimes forget to remove user access when a job function changes or a user leaves the organization. Multifactor authentication systems like OTP, phone based authentication, and smartcard protects cloud services because they make it harder for attackers to log in with stolen passwords.

Hacked Interfaces And API

IT team uses API's and interfaces to manage and interact with cloud services. The security and availability of cloud services from authentication and access control to encryption and activity monitoring depends on the security of the API.

Account Hijacking

Phishing, fraud and software exploits are still successful, and cloud services and a new dimension to the threat because attackers can eavesdrop on activities, manipulate transactions and modify data too.

Malicious Insiders

The insider threat has many faces – a current or former employee, a system admin, or a business partner. The malicious agenda ranges from theft to revenge. An insider can destroy the whole infrastructure or even manipulate the data.

Permanent Data Loss

Malicious hackers have been known to permanently hack and delete the cloud data to harm business, and cloud data centers re as vulnerable to natural disasters and any other.

Shared Technology- Shared dangers

Cloud service providers share infrastructure, platform and application, an if a vulnerability arises in any of these layers, it affects everyone. A single vulnerability can lead to compromise across an entire provider's cloud.

Cloud Service Abuse

Cloud services can be used to conduct nefarious activities such as using cloud resources to break an encryption key to launch an attack. Customers should make sure providers offers a mechanism to report abuse. Cloud service abuse can result in service availability issues and data loss.

CONCLUSION

Cloud computing provides various sorts of service to make our lives easier through different kinds of services like PAAS, SAAS and IAAS. However, each has its own attributes and utilities. Hence the choice between these three will be dependent on the demand of the business.

REFERENCES

https://www.linkedin.com/topic/paas-%26-iaas

http://www.ijarcce.com/upload/2015/october-15/IJARCCE%2015.pdf

https://www.researchgate.net/profile/Anurag_Jain15/publication/264435521_Survey_Paper_on_Cloud_Computing/links/53df522e0cf2cfac99296fac.pdf

https://www.simplilearn.com/cloud-computing-architecture-article

https://www.coursehero.com/file/16701781/cloud-computing-architecturepdf/

http://www.academia.edu/14401386/Survey_Paper_on_Cloud_Computing

https://www.linkedin.com/topic/paas-%26-iaas

http://www.c-sharpcorner.com/UploadFile/370e35/windows-azure-cloud-computing-services/

http://www.cloudcomputingtraining.co.in/understanding-the-cloud-computing-stack-saas-paas-iaas/

http://escale-it.com/cloud-solutions/