

# Conceptual Information of Cloud Computing & Migration with Its Security Approaches

Renuka Bareth<sup>1</sup> Rakesh Patel<sup>2</sup> Meenu Rani Dey<sup>3</sup>

<sup>1,3</sup>Student <sup>2</sup>Lecturer

<sup>1,2,3</sup>Department of Information Technology

<sup>1,2,3</sup>Kirodimal Institute of Technology, Raigarh (C.G.), India

**Abstract**— Cloud computing is a new paradigm that combines several computing concepts and technologies of the Internet creating a platform for more agile and cost-effective business applications and IT infrastructure. The adoption of Cloud computing has been increasing for some time and the maturity of the market is steadily growing. Security is the question most consistently raised as consumers look to move their data and applications to the cloud. In these paper we will see the basic concept of cloud computing, simple form of cloud computing, cloud service modle, architecture cloud characteristics, cloud migration and some security points by which the data migration will become more secure.

**Key words:** cloud service model, simple form of cloud computing, basic concept of cloud computing

## I. INTRODUCTION

The Cloud computing is a general term used to describe a new class of network based computing thattake place over the internet. These platform hide the complexity and details of underlying infrastructure from users and applications by providing very simple graphical interface. A key differentiating element of a successful information technology (IT) is its ability to become a true, valuable, and economical contributor to cyber infrastructure. “Cloud” computing embraces cyber infrastructure, and builds upon decades of research in virtualization, distributed computing, “grid computing”, utility computing, and, more recently, networking, web and software services. It implies a service oriented architecture, reduced information technology overhead for the enduser, greater flexibility, reduced total cost of ownership, on demand services and many other things. “Cloud computing” is the next natural step in the evolution of on-demand information technology services and products. To a large extent, cloud computing will be based on virtualized resources.

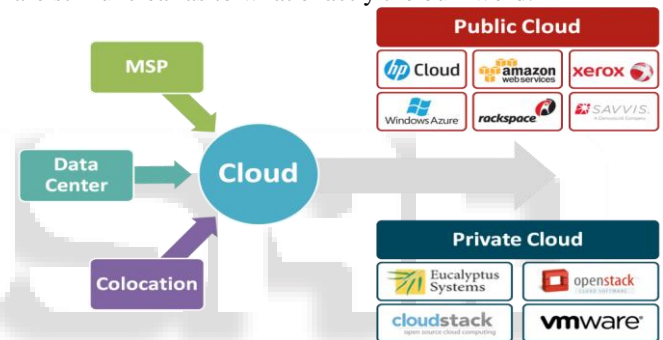


## II. BASIC CONCEPT OF CLOUD COMPUTING

“Cloud computing” is the next natural step in the evolution of on-demand information technology services and products. To a large extent, cloud computing will be based on virtualized resources”.

The economic case for cloud computing has gained widespread acceptance. Cloud computing providers can build large datacenters at low cost due to their expertise in organizing and provisioning computational resources. The economies of scale increase revenue for cloud providers and lower costs for cloud users. The resulting on-demand model of computing allows providers to achieve better resource utilization through statistical multiplexing, and enables users to avoid the costs of resource over-provisioning through dynamic scaling.

“Cloud computing” actually means. In its simplest form, the principle of Cloud computing is the provision of computing resources via a network. Cloud computing services such as Amazon EC2 and Windows Azure are becoming more and more popular but it seems many people are still unclear as to what exactly the buzzword.



## III. SIMPLE FORM OF CLOUD COMPUTING

### A. Cloud Computing:

IT resources and services that are abstracted from the underlying infrastructure and provided on demand and at scale in a shared multitenant and elastic environment—represents a paradigm shift from which both enterprise IT and service providers can benefit.

According to the definition of cloud computing from the National Institute of Standards and Technology (NIST), IT services that are delivered as cloud services offer:

- A pay-as-you-go model with minimal or no initial costs
- Usage-based pricing, so that costs are based on actual usage
- Elasticity, so that users can dynamically consume more or less resources
- Location independence, high availability, and fault tolerance
- Ubiquitous access to services, where users can access services from any location using any form factor.



A cloud can provide IT infrastructure services such as servers, storage, network and network services, or infrastructure as a service (IaaS); an application deployment platform with application services such as databases, or platform as a service (PaaS); or subscription-based software applications, or software as a service (SaaS).

Today, service providers, who already excel at provisioning, managing, and scaling services for multiple customers, are providing offerings based on IaaS in which the enterprise uses the pay-as-you-go compute infrastructure from the service provider. A cloud provided by a service provider is known as a public cloud.

In addition, some enterprises are choosing to build a private cloud—enterprise IT infrastructure services, managed by the enterprise, with cloud computing qualities: self-service, pay-as-you-go chargeback, on-demand provisioning, and the appearance of infinite scalability. reference:-(migration of enterprise apps to cloud white paper.

#### IV. CLOUD SERVICE MODELS

##### Description of Cloud Service Models

###### A. Cloud Software As A Service (SaaS):

Use provider's applications over a network.

###### B. Cloud Platform As A Service (PaaS):

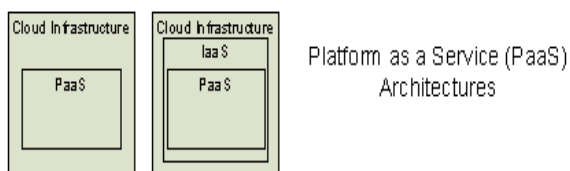
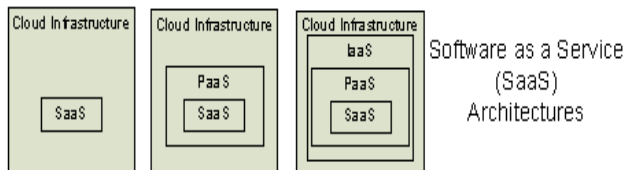
Deploy customer-created applications to a cloud.

###### C. Cloud Infrastructure As A Service (IaaS):

Rent processing, storage, network capacity, and other fundamental computing resources.

To be considered "cloud" they must be deployed on top of cloud infrastructure that has the key characteristics.

##### Cloud Service Architecture:



#### V. ESSENTIAL CLOUD CHARACTERISTICS

- On-demand self-service
- Ubiquitous network access
- Resource pooling
  - Location independence
  - Homogeneity
- Rapid elasticity
- Measured service



- On-demand self-service. A consumer can unilaterally provision computing capabilities, such as server time and network storage, as needed automatically without requiring human interaction with each service's provider.
- Ubiquitous network access. Capabilities are available over the network and accessed through standard mechanisms that promote use by heterogeneous thin or thick client platforms (e.g., mobile phones, laptops, and PDAs).
- Resource pooling. The provider's computing resources are pooled using a homogenous infrastructure to serve all consumers using a multi-tenant model, with different physical and virtual resources dynamically assigned and reassigned according to consumer demand. There is a sense of location independence as the customer generally has no control or knowledge over the exact location of the provided resources but may be able to specify location at a higher level of abstraction (e.g., country, state, or datacenter). Examples of resources include storage, processing, memory, network bandwidth, and virtual machines.
- Rapid elasticity. Capabilities can be rapidly and elastically provisioned, and in some cases automatically, to quickly scale up and rapidly released to quickly scale down. To the consumer, the capabilities available for provisioning often appear to be infinite and can be purchased in any quantity at any time.
- Measured Service. Cloud systems automatically control and optimize resource use by leveraging a metering capability at some level of abstraction appropriate to the type of service (e.g., storage, processing, bandwidth, and active user accounts). Resource usage can be monitored, controlled, and reported providing transparency for both the provider and consumer of the utilized service.



## VI. COMMON CLOUD CHARACTERISTICS

- Massive scale
- Virtualization
- Non-stop computing
- Free software
- Geographic distribution
- Service oriented software
- Autonomic computing
- Advanced security technologies

### A. Massive Scale:

Cloud implementations, regardless of the deployment model, tend to be as large as possible in order to take advantage of economies of scale. Large cloud deployments can often be located next to cheap power and real estate to lower costs. They often take advantage of bulk commodity hardware purchases and streamlined datacenter technologies (e.g., contain based data centers). To improve effectiveness, large cloud deployments may be located near high speed Internet hubs.

### B. Virtualization:

Virtualization is a critical element of most cloud implementations and is used to provide the essential cloud characteristics of location independent resource pooling and rapid elasticity. Virtualization, when used in the cloud paradigm, enables data centers to increase their server utilization from a typical 10% to an ideal 80% thereby producing significant cost savings. This said, other techniques (such as software sandboxing in a PaaS model) can provide similar benefits although they are less used.

### C. Non-Stop Computing:

Cloud implementation (especially SaaS and PaaS) often enable a characteristic of non-stop computing. This means that cloud applications can take advantage of the abstraction of the cloud distributed software layer from the hardware to enable an application to remain active at all times even through upgrades. In this model there are no scheduled maintenance downtimes for applications.

### D. Free Software:

The massive scale of many clouds combined with the need for many software licenses encourages the use of free software in the development of cloud architectures. By free software we mean software that is one of the following: open source, a product that is free to the cloud developer (e.g., a software company usually includes its own products

in its cloud offerings), or very cheaply licensed (possibly due to open source competition).

### E. Geographic Distribution:

Cloud systems that are built on the concept of resource pooling may not have separate backup sites. Instead, cloud providers often rely on unused cloud capacity to provide disaster recovery capabilities. To make this work cloud providers not only need significant unused capacity but must have their resource pool geographically distributed so that a single data center disaster will not cause outage.

### F. Service Oriented Software:

As noted in the cloud definition, “cloud software takes full advantage of the cloud paradigm by being service oriented with a focus on statelessness, low coupling, modularity, and semantic interoperability.” This is an important characteristic for cloud applications in order for them to fully leverage the location independent resource pool and rapid elasticity capabilities. Clouds can run applications that do not have this characteristic, but such applications will be isolated workload instances for which the cloud cannot provide the same reliability and scalability that service oriented application are provided.

### G. Autonomic Computing:

Cloud implementations often have automated systems to enable their management and security. This characteristic enables them to be massive and complex and yet still be cost effective. According to IBM [see auto slide] autonomic computing has four properties: self-healing, self-configuration, self-optimization, and self-protection. Clouds may exhibit all of these properties. Self-healing may happen when a physical server or storage device fails and the cloud automatically replicates the associated processes or data to other devices. Self-configuration happens when a customer provisions a process instance or a virtual machine and the management and security configurations are set up automatically. Self-optimization may happen when a cloud dynamically relocates processes and/or storage to optimize cloud usage and service delivery. Lastly, the self-protection property may exist in clouds and leverage the overall automation and homogeneity. However, this property does not commonly exist in advanced forms that aren't available using traditional computing models.



## VII. ADVANCED SECURITY TECHNOLOGIES

Cloud implementations often contain advanced security technologies. The homogenous resource pooled nature of the cloud enables cloud providers to focus all their security resources on securing the cloud architecture. At the same time, the automation capabilities within a cloud combined with the large focused security resources usually result in advanced security capabilities. These capabilities are often necessary because the multi-tenant nature of clouds increased the threat exposure compared to traditional computing models. **Cloud migration definition:-**A cloud migration process is a set of migration activities carried to support an end-to-end cloud migration. Implications of definition to be considered: initial requirements and expectation elicitation tools for automated migration of IT art effect plans for the deployment of new cloud services decommissioning of old infrastructure.



## VIII. BENEFITS OF CLOUD MIGRATION

There are many benefits that explain why to migrate to clouds Cost savings, power savings, green savings, increased agility in software deployment. Cloud security issues may drive and define how we adopt and deploy cloud computing solutions Cloud Deployment Models.

### A. Private Cloud:

Private cloud. The cloud infrastructure is operated solely for an organization. It may be managed by the organization or a third party and may exist on premise or off premise.

### B. Community Cloud:

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

### C. Public Cloud:

The cloud infrastructure is made available to the general public or a large industry group and is owned by an organization selling cloud services.

### D. Hybrid Cloud:

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).

## IX. CLOUD COMPUTING SECURITY

### Analyzing Cloud Security

#### A. Some Key Issues:

- Trust, multi-tenancy, encryption, compliance.
- Clouds are massively complex systems can be reduced to simple primitives that are replicated thousands of times and common functional units.
- Cloud security is a tractable problem



## X. THERE ARE BOTH ADVANTAGES AND CHALLENGES

### A. General Security Advantages:

- Shifting public data to a external cloud reduces the exposure of the internal sensitive data
- Cloud homogeneity makes security auditing/testing simpler
- Clouds enable automated security management
- Redundancy / Disaster Recovery

### B. General Security Challenges:

- Trusting vendor's security model
- Customer inability to respond to audit findings
- Obtaining support for investigations
- Indirect administrator accountability
- Proprietary implementations can't be examined
- Loss of physical control

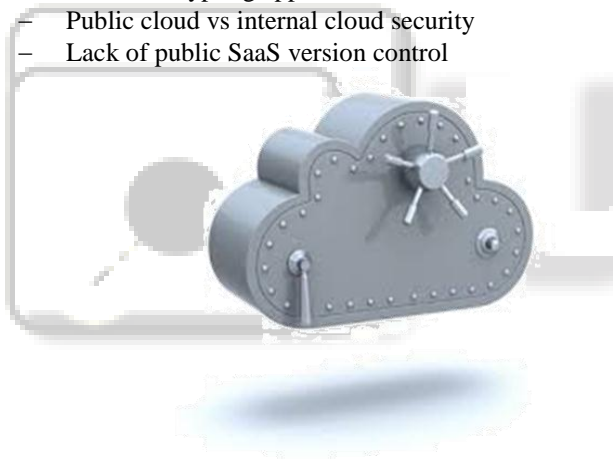
### C. Cloud Security Advantages:

- Data Fragmentation and Dispersal
- Dedicated Security Team
- Greater Investment in Security Infrastructure
- Fault Tolerance and Reliability
- Greater Resiliency
- Hypervisor Protection Against Network Attacks
- Possible Reduction of C&A Activities (Access to Pre-Accredited Clouds)
- Simplification of Compliance Analysis
- Data Held by Unbiased Party (cloud vendor assertion)
- Low-Cost Disaster Recovery and Data Storage Solutions
- On-Demand Security Controls
- Real-Time Detection of System Tampering
- Rapid Re-Constitution of Services

- Advanced Honeynet Capabilities

#### D. Cloud Security Challenges:

- Data dispersal and international privacy laws
  - EU Data Protection Directive and U.S. Safe Harbor program
  - Exposure of data to foreign government and data subpoenas
  - Data retention issues
- Need for isolation management
- Multi-tenancy
- Logging challenges
- Data ownership issues
- Quality of service guarantees
- Dependence on secure hypervisors
- Attraction to hackers (high value target)
- Security of virtual OSs in the cloud
- Possibility for massive outages
- Encryption needs for cloud computing
  - Encrypting access to the cloud resource control interface
  - Encrypting administrative access to OS instances
  - Encrypting access to applications
  - Encrypting application data at rest



### XI. SECURITY ISSUES IN PUBLIC, PRIVATE AND HYBRID CLOUDS

While cloud models provide rapid and cost-effective access to business technology, not all of these services provide the same degree of flexibility or security control. In most organizations, data protection levels vary depending on the use of technology.

#### A. Public Cloud:

Public clouds (or external clouds) describe 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 or web services, from an off-site, third-party provider who shares resources and bills on a fine-grained, utility-computing basis. In a public cloud, security management day-to-day operations are relegated to the third party vendor, who is responsible for the public cloud service offering.

#### B. Private Cloud:

Private clouds differ from public clouds in that the network, computing, and storage infrastructure associated with private clouds is dedicated to a single organization and is not shared with any other organizations (*i.e.*, the cloud is dedicated to a single organizational tenant). The security management and day-to-day operation of hosts are relegated to internal IT or to a third party with contractual SLAs. By virtue of this direct governance model, a customer of a private cloud should have a high degree of control and oversight of the physical and logical security aspects of the private cloud infrastructure.

#### C. Hybrid Cloud:

A hybrid cloud environment consisting of multiple internal and/or external providers is a possible deployment for organizations. With a hybrid cloud, organizations might run non-core applications in a public cloud, while maintaining core applications and sensitive data in-house in a private cloud. Providing security in a private cloud and a public cloud is easier, comparing with a hybrid cloud since commonly a private cloud or a public cloud only has one service provider in the cloud. Providing security in a hybrid cloud consisting of multiple service providers is much more difficult especially for key distribution and mutual authentication. Also for users to access the services in a cloud, a user digital identity is needed for the servers of the cloud to manage the access control. While in the whole cloud, there are many different kinds of clouds and each of them has its own identity management system. Thus a user who wants to access services from different clouds needs to have multiple digital identities from different clouds, which will lead to inconvenience for users. Using federated identity management, each user will have his unique digital identity and with this identity, he/she can access different services from different clouds.



### XII. APPROACHES OF MIGRATION PROCESSES

There are different approaches in which the authors analyze and define migration processes or recommend guides of migration to Cloud computing. A set of points to consider when making the decision to migrate a project to an external cloud, which are as follows:

- (1) an established vendor with a track record;
- (2) Does the project really need to be migrated?;
- (3) Consider data security;
- (4) Data transfer;
- (5) Data storage and location;
- (6) Scaling;
- (7) Service level guarantees;
- (8) Upgrade and maintenance schedules;
- (9) Software architecture; and
- (10) Check with the lawyers. Other important steps, shown in

that can be taken in preparation for Cloud computing adoption are: (i) Identify all potential opportunities for switching from existing computing arrangements to cloud services; (ii) Ensure that in-house infrastructure complements cloud-based services; (iii) Develop a cost/benefit and risk evaluation framework to support decisions about where, when, and how cloud services can be adopted; (iv) Develop a roadmap for optimizing the current ICT environment for adoption of public and/or private cloud services; (v) Identify which data cannot be held in public Cloud computing environments for legal and/or risk-mitigation reasons; (vi) Identify and secure in-house competencies that will be required to manage effective adoption of cloud services; (vii) Designate a cross-functional team to continually monitor which new services, providers, and standards are in this space, and to determine if they affect the roadmap; (viii) Evaluate technical challenges that must be addressed when moving any current information or applications into a cloud environment; (ix) Ensure that the networking environment is ready for Cloud computing. Reference [26] defines the points to take into account in the migration such as (i) Deciding on the applications and data to be migrated; (ii) Risk mitigation; (iii) Understanding the costs; (iv) Making sure the regulatory things are handled; (v) Training the developers and staff. A phased strategy for migration is presented in [27] where the author describe a step by step guide with six steps given as such; (1) Cloud Assessment Phase; (2) Proof of Concept Phase; (3) Data Migration Phase; (4) Application Migration Phase; (5) Leverage of the Cloud; (6) Optimization Phase. In this strategy some security aspects are indicated and some correct security best practices are defined such as safeguard of credentials, restricting users to resources, protecting your data by encrypting it at-rest (AES) and in-transit (SSL) or adopting a recovery strategy. The alternative migration strategies which Gartner [28] suggests IT organizations should consider are: (i) Rehost, *i.e.*, redeploy applications to a different hardware environment and change the application's infrastructure configuration; (ii) Refactor, *i.e.*, run applications on a cloud provider's infrastructure; (iii) Revise, *i.e.*, modify or extend the existing code base to support legacy modernization requirements, then use rehost or refactor options to deploy to cloud; (iv) Rebuild, *i.e.*, Rebuild the solution on PaaS, discard code for an existing application and re-architect the application; (v) Replace, *i.e.*, discard an existing application (or set of applications) and use commercial software delivered as a service.

As we can see, the approaches of migration process identify and define a set of steps or points to follow and consider in the migration to Cloud which can be used for our propose of migrating security aspects to Cloud, but the initiatives do not consider security or only specific security aspects that do not guarantee a full migration process of all security features of the legacy systems and it is this aspect which we want to achieve.

### XIII. CONCLUSION

The benefits of Cloud computing are the first weapon when organizations or companies are considering moving their applications and services to Cloud, analyzing the advantages that it entails and the improvements that they can get. If the

customers decide to incorporate their businesses or part of them to the Cloud, they need to take into account a number of risks and threats that arise, the possible solutions that can be carried out to protect their applications, services and data from those risks, and some best practices or recommendations which may be helpful when the customers want to integrate their applications in the Cloud. In addition, organizations or customers require guidelines or processes which indicate the steps necessary and advisable to follow, the techniques most suitable, the most appropriate mechanisms and the technologies to implement the successful migration of all security aspects of their systems to the Cloud, with the purpose of having complete assurance that their systems, data and assets are ensured in the same form as in their own organization or company. For future work, we will carry out a systematic review of the literature in a formal way, extending the search to migration processes from legacy systems to Cloud computing, searching initiatives of Cloud-related technologies, such as SOA, Web services, Grid or virtual machines, and always considering security aspects in this search.

### REFERENCE

- [1] A Security Approach For Data Migration In Cloud Computing Virendra Singh Kushwah\*, Aradhana Saxena\*\*
- [2] Economic Importance Of Animals Husbandry Management System Through The Cloud Computing Renuka Bareth1, Rakesh Patel2, Meenu Rani Dey3
- [3] What's New About Cloud Computing Security? Yanpei Chen Vern Paxsonrandy H. Katz
- [4] Effectively And Securely Using The Cloud computing paradigm.
- [5] Effectively And Securely Using The Cloud Computing Paradigm Peter Mell, Tim Grance Nist, Information Technology Laboratory 8-12-2009)