Name of the Candidate: NAGENDRA CHARY KOTTHOJU

Research Area : Cloud Computing

Proposed Title : Security deployment in Cloud Computing

Topics covered in the Research proposal :

1. Introduction

2. Objectives
    - 2.1 Core Objectives
    - 2.2 Cloud Computing Strategy Objectives
    - 2.3 Cloud Economics

3. Comparative study
    - 3.1 Cloud Computing versus Grid Computing
    - 3.2 Clouds vs. Traditional Hosting

4. Assumptions
    - 4.1. Cloud is best for all applications
    - 4.2. Cloud is cheaper than managed hosting
    - 4.3 Decision time
    - 4.4 Buying from Cloud means you don't need networking people any more
    - 4.5 Operating costs will be more predictable
    - 4.6 The cloud will be manageable

5. Hypothesis to be considered

6. Related work:
    - 6.1. History
    - 6.2. Characteristics
    - 6.3. Service models
    - 6.4. Deployment models

7. Security in Cloud Computing

8. Conclusion

9. Bibliography

1. Introduction

Cloud Computing is a new computing paradigm in which the Internet is used to deliver reliable IT services to the customers.

It is a form of Parallel and Distributed system where the resources are shared dynamically and services are provided to the customers on demand. Thus, the users has to pay only for the duration they utilize the resources as it is called "Pay-per-Usage"[1].

According to National Institute of Standards and Technology (NIST), Cloud Computing is defined as "A model for enabling convenient, on-demand network access to a shared pool of configurable computing resources that can be rapidly provisioned and released with minimal management effort or service provider interaction".

2. Objectives of Cloud Computing

2.1 Core Objectives:

The Core objectives and principles that cloud computing must meet to be successful are:

- Security
- Scalability
- Availability
- Performance
- Cost-effective
- Acquire resources on demand
- Release resources when no longer needed
- Pay for what you use
- Leverage others' core competencies
- Turn fixed cost into variable cost

Cloud computing has the potential to create irreversible changes in how computers are used around the world. "Cloud computing technology's objective is to move any application stored on a computer to a remote location, eliminating all the standard components, including operating systems and hard drives, which are necessary in today's computers and make them accessible online through a standard browser".

Over recent years, research shows that there is higher growth in Cloud Computing among companies with higher revenues. This is because of lower costs, economically scalable and easier to budget. It is clear that Cloud Computing has number of attractive aspects which are driving its adoption.

2.2 Cloud Computing Strategy Objectives:

Business and/or IT Objectives are used to establish the Cloud Computing Strategy Objectives. These objectives will vary depending on the Sponsor of Cloud Computing.

For example:

♣ Cost Reduction Objectives are the most immediate, i.e. move, transition, switch or introduce a narrow set of applications and/or workloads to the Cloud to save or avoid IT costs and move the percentage of IT spend on the Cloud to 25% of the total spend.

♣ Transformation Objectives are more long term, i.e. build a smarter, more agile business by transforming the percentage of IT spend on Cloud Computing Services...steadily. The strategy is to eliminate the fixed costs for IT, i.e. Depreciation of the Data Center Infrastructure; reduce related IT staffing; reduce the number of IT Vendors; and convert IT into a variable operating cost, while making the business processes more efficient and effective.

♣ Innovation Objectives to create a sustainable competitive advantage, that achieves superior performance relative to the other industry players, are the ultimate fundamental aim of an enterprise.

2.3 Cloud Economics:

- Estimates vary widely on possible cost savings
  "If you move your data center to a cloud provider, it will cost a tenth of the cost." – Brian Gammage, Gartner Fellow.
- Use of cloud applications can reduce costs from 50% to 90% - CTO of Washington D.C.
- IT resource subscription pilot demonstrated a 28% cost savings - Alchemy Plus cloud (backing from Microsoft).
- "Using Cloud infrastructure saves 18% to 28% before considering that you no longer need to buy peak capacity" – George Reese, founder Valtira and enStratus.
- When implementing Cloud you must consider other costs which may not be apparent today.

3. Comparative Study

3.1 Cloud Computing versus Grid Computing:

Cloud computing is based on grid computing, and allows users to access shared servers, which distribute resources, software and data on demand.

Cloud is interactive in that you can get resources on demand via self service. Grid is batch in that you submit jobs to a job queue after obtaining the credentials from some authority to do so. The code you run on the grid waits in that queue until there are sufficient resources to execute it.

Grid computing is where more than one computer coordinates to solve a problem together. Cloud computing is where an application doesn't access resources it requires directly, rather it accesses them through something like a *service*.

A *cloud* would usually use a grid. A grid is not necessarily a cloud or part of a cloud. On the other hand, Grid computing is a backbone of cloud computing.

3.2 Clouds vs. Traditional Hosting:

- Three distinct characteristics that differentiate clouds from traditional hosting
  - It is sold on demand
    - Typically by the minute or the hour
  - It is elastic
    - A user can have as much or as little of a service as they want at any given time
  - The service is fully managed by the provider
    - The consumer needs nothing but a personal computer and Internet access.

4. Assumptions in the Cloud Computing

4.1 Cloud is best for all applications:

There are certain applications that are better for the burst-ability and elasticity of cloud like file sharing, social media, testing and development, e-mail and server virtualization. At the same time there are many other applications where they require significant diligence due to the hierarchical nature of their architecture like legacy enterprise commercial off-the-shelf (COTS) applications. These applications might be a good fit for the cloud, but traditional hosting may be more practical and cost-effective. Thus it is important to carefully evaluate the costs associated with transitioning to the cloud and be realistic about what you are trying to achieve.

4.2 Cloud is cheaper than managed hosting:

It is true that in the cloud you pay for only what you need to use — avoiding the need to engineer your infrastructure, managed hosting environment and additional software component that providers deliver to users to enable self-management, faster provisioning and granular control. This means that the same configuration consuming the same amount of resources for the same period of time is going to cost more in the cloud than it would in a dedicated environment. Cost savings are realized by leveraging dedicated hosting for predictable workloads and the cloud for variable workloads. Be sure to fully understand the ongoing usage and access fees associated with the infrastructure you are deploying to avoid any additional charges.

4.3 Decision time:

There are several important questions that must be answered as you develop your cloud strategy. Do you *really* need to move to the cloud? If so, which applications should be moved? And should those applications be hosted in a private cloud, with more security, reliability and support? Or Whether your work load is better suited for a cheaper, less regulated public cloud option? What types of templates should you start with, and who on your team will be responsible for the on-demand management of these resources?

It is important to know the answer for of these questions, as it helps to align with a service provider that offers hands-on consultative support to deploy a right model. A provider that is equipped to assess your workload history with you and talk through

potential solutions, leveraging their experience in terms of business goals, configuration development and the physical migration itself is best.

4.4 Buying from Cloud means you don't need networking people any more:

In the Cloud environment, we don’t require any application engineers. "Are you sure about that? If that is the case, Would you leave everything to third parties and be relaxed? Thus indirectly, you might not have any control over your strategy? The cloud operators would have to be really trustworthy. How many would you trust?".

4.5 Operating costs will be more predictable:

In theory, cloud computing will be more affordable because it stops IT from being a difficult, capital expenditure and converts it into a compliant and reliable operating cost. But the problem is, Once you take on one of these new systems, the initial costs will be more than you expected. For example, client server architecture ended up costing 10 times as much to manage.

4.6 The cloud will be manageable:

Yes, it’s true the Cloud will be manageable, but you won't be able to see everything that goes on in your cloud as you loose vicinity over the data and the resources.

5. Hypotheses related to Cloud Computing

The following are some of the hypotheses related to Cloud Computing:

- An organization can use its existing infrastructure simultaneously with cloud resources with relative ease
- Cloud computing environments provide ways to continuously update the amount of resources allocated to an organization and
- It is possible to move an application's resources between cloud computing providers, with varying levels of effort required.

Cloud Computing is not a completely new concept; it has intricate connection to the relatively new but established Grid Computing paradigm, and other relevant technologies such as utility computing, cluster computing, and distributed systems in general.

6. Related Work

6.1 History of Cloud Computing:

The underlying concept of Cloud Computing dates back to the 1960’s, when John Mc Carthy opined that “Computation may someday be organised as a public utility”.

Basic idea of Cloud Computing was derived from telecommunications companies who made a radical shift from point-to-point data circuits to virtual private network services in 1990's.

For the first time the term in its current context was used in 1997 by Prof Ramnath Chellappa where he defined it as "A new computing paradigm where the boundaries of computing will be determined by the economic rationale rather than technical limits alone". From 1999 till 2011, many companies like Salesforce, Amazon, Google, Microsoft, VMware and many others have joined Cloud Computing.

In this year, Geeknet Media launched first web site dedicated to Cloud Computing, Slashcloud. Like, many companies are joining the cloud because of its enormous advantages.

Future of Cloud Computing:

The main factor that is driving demand for Cloud Computing is the explosive growth of data.

According to projections by Century Link, by 2015, world will see a four-fold increase in the amount of data being created and replicated. Once it becomes real, we need a way to store the data securely and allow end-users to access it efficiently.

6.2 Characteristics:

The Key characteristics of Cloud Computing are as follows:

*Multi-tenancy***:** It enables sharing of resources and costs across a large pool of users thus allowing for centralization of infrastructure and utilization and efficiency improvements.

*On-Demand self services***:** Computer services such as email, network service and applications can be provided without requiring human interaction with each service provider. Currently, Microsoft, Google, IBM are providing these services.

*Reliability***:** If multiple redundant sites are used, reliability improves, which makes Cloud Computing suitable for business continuity and also disaster recovery.

*Managed Metering***:** Cloud Computing manages and optimizes the services by using metering concept. In this way, consumers are billed for services according to how much they have actually used during the billing period.

Security: Security is often as good or better than traditional systems, because providers are able to devote resources to solve security issues that many customers cannot afford.

*Rapid elasticity***:** The services of Cloud Computing can be rapidly and elastically provisioned. To the consumer, the capabilities available often appear to be unlimited and can be purchased in any quantity at any time.

6.3 Service Models:

The main goal of Cloud Computing is to develop a complete architecture to meet IT needs. Companies will no longer have to allocate large percentage of resources and time to building and maintaining complex IT infrastructure.

Mainly there are three types of Cloud Computing services. They are :
Infrastructure-as-a-Service(IaaS),
Platform-as-a-Service(PaaS),
Software-as-a-Service(SaaS).

Fig1 shown below illustrates the service models. IaaS is the basic and lowest service model in the technology stack[2].

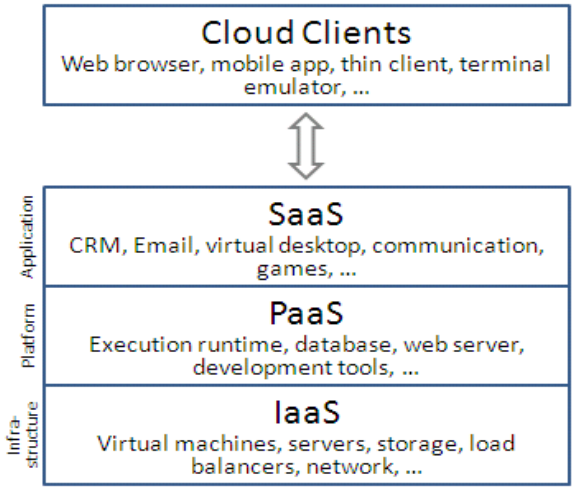

Fig 1. Service models

Software-as-a-Service(SaaS) – In this model, cloud providers install and operate application software in the cloud and cloud users access the software from cloud clients. The services run on top of a cloud infrastructure, which is invisible for the customer. Thus when the software is hosted off-site, the customer doesn't have to maintain it. The cloud users do not have to acquire the software rather they make payments based on usage i.e., Pay-per-Use model. Also, it supports multi-tenant, which means software can be shared amongst more than one user but logically it's unique for each user.

Platform-as-a-Service(PaaS) – In this model, cloud providers deliver a computing platform typically including Operating System, execution environment, database and Webserver. Application developers can develop and run their software on a cloud platform without the cost and complexity of buying and managing the underlying hardware and software layers.

PaaS services include application design, development, testing, deployment and hosting. Other services include team collaboration, security, integration, scalability, storage and versioning.

Infrastructure-as-a-Service(IaaS) – In this, cloud providers offer computers as physical or more often as virtual machines, firewalls, load balancers and networks.

IaaS providers supply these resources on demand from their large pools installed in data centers.

SaaS, PaaS are providing applications to customers, whereas IaaS doesn't. It simply offers the hardware so that the organization can put whatever they want onto it. Rather than purchase and having to pay for the data center space, the service provider rents those resources.

6.4 Deployment Models:

Deployment models for Cloud Computing can differ depending on the requirements. Four models have been identified, each with specific characteristics which supports the needs of the services and users of the clouds. Fig2 illustrates the models.

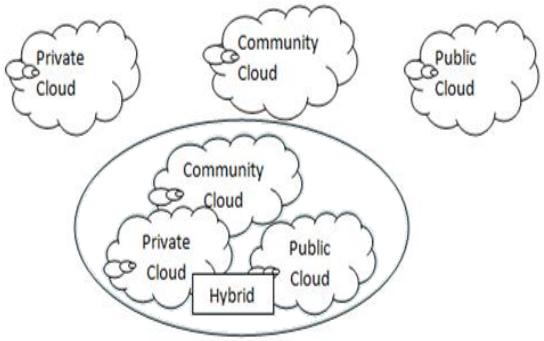

Fig 2. Deployment models

Public cloud – Public cloud applications, storage and other resources are made available to the general public by a service provider. These services are free or offered on basis of pay-per-usage. The infrastructure is located on the premises of the provider, who also owns and manages the cloud infrastructure. In this, direct connectivity is not offered, users can access only via internet. Also, public cloud users are considered to be untrusted, which means they are not tied to the organization as employees and the user has no contractual agreements with the provider.

Private cloud – The infrastructure of a private cloud is operated solely by a single organization, whether managed internally or by a third-party and hosted internally or externally. As private clouds run in service of a single organization, resources are not shared by other entities. Also, private cloud users are considered as trusted by the organization, in which they are either employees or have contractual agreements with the organization.

Community cloud – Community cloud shares infrastructure between several organizations from a specific community with common concerns like security, compliance, jurisdiction etc, whether managed internally or by a third party, and hosted internally or externally. Community users are also considered as trusted by the organizations that are part of the community.

Hybrid cloud – Hybrid clouds are combination of two or more clouds (private, public or community), that remain unique entities but are bound together, offering the benefits of multiple deployment models. Each part of a hybrid cloud is connected to the other by a gateway, controlling the applications and data that flow from each part to the other. In this, users may be trusted or untrusted. Thus, untrusted users must be prevented to access the confidential data and resources of the private cloud and as well as community parts of the hybrid cloud.

7. Security in Cloud Computing

Cloud Computing users work with applications and data that are often located off-premise. Thus, many users and organizations are not comfortable with the idea of storing their valuable information on systems which they do not control. There is lack of knowledge on how Cloud Computing impacts the confidentiality of data stored, processed and transmitted in the cloud environments. Thus, some sort of security mechanism is needed to ensure the client that their data is safeguarded.

A recent survey of IEEE and CSA (Cloud Security Alliance) indicates that many organizations are interested to deploy cloud environments but they need solution for security.

The key security issues that were been identified are:

Identity and Access Management:

IAM is heart of Information security that provides an adequate level of protection to data and resources by enforcing rules and policies such as authentication, authorization and auditing methods. In this system, many challenges exist such as avoiding duplication of identities,attributes and credentials[3].

The increase in interaction with third parties and growth in number of applications and other technology portfolios, has led to the need for solutions that allow for a single logon to gain access to multiple resources without having to re-authenticate.

The main approaches used for managing identity with IAM are Open Authentication (OAuth) protocol, Security Assertion markup Language (SAML) and WS-Trust.

Trust and Assurance:

Cloud Computing provides ways that enable large-scale data sharing and interoperations among resources that may be located on different networks [4]. Therefore, security becomes a major importance in cloud infrastructure; to ensure only the right authorized people get access to it. Therefore, cloud-computing environments should have trust amongst themselves because cloud users change dynamically.

Data Protection:

Data stored in the cloud typically resides in a shared environment collocated with data from other customers.

Data Isolation: Data can take many forms. Access controls are one means to keep data away from unauthorized users; encryption is another. Access controls are typically identity-based, which makes authentication of the user's identity an important issue in Cloud Computing.

Currently, the responsibility for cryptographic key management falls mainly on the cloud service subscriber. Protecting data in use is an emerging area of cryptography with few practical results to offer, leaving trust mechanisms as the main safeguard.

Data Location: One of the most common compliance issues facing an organization is data location [5]. The main characteristic of many Cloud Computing services is that the detailed information of the location of an organization's data is unavailable or not disclosed to the service subscriber. This situation makes it difficult to ascertain whether sufficient safeguards are in place and whether legal and regulatory compliance requirements are being met. External audits and security certifications can, to some extent, alleviate this issue, but they are not a panacea. Once information crosses a national border, it is extremely difficult to guarantee protection under foreign laws and regulations.

Architecture:

The systems architecture used to deliver cloud services comprises hardware and software residing in the cloud. The physical location of the infrastructure is determined by the service provider. Virtual machines (VMs) typically 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 and typically involve multiple intercommunicating cloud components.

8. Conclusion

Cloud Computing is still a new and evolving paradigm where computing is regarded as on-demand service. Once the organization takes decision to move to the cloud, it loses control over its data. Thus, the amount of protection needed to secure data is directly proportional to the value of the data.

Security of the cloud relies on trusted computing and cryptography. Organizational data must be protected in a manner consistent with policies. No standard service contract exists till date that covers the ranges of cloud services available and the needs of different organizations. Interoperability is also an important problem unless an agreement is met, before implementation. Also, the migration to a cloud environment is concerned with risk management. The risks must be carefully balanced against the available safeguards and expected benefits. An appropriate balance between the strength of controls and the relative risk associated with data and programs must be ensured. Meanwhile the IT teams and end user companies, organizations should significantly redesign their security architecture to cope up with the existing problems and benefit from the Cloud Computing paradigm. The proposed research could enable to develop an authentication model that provides end to end security for cloud providers and users.

9. Bibliography

[1] V. Sandhya, "A Study on Various Security Methods in Cloud Computing", International Journal of Advanced Research in Computer Science, Volume 2, No.6, Nov-Dec 2011.

[2] Subedari Mithila, P. Pradeep Kumar, "Data Security through Confidentiality in Cloud Computing Environment", Subedari Mithila et al, / (IJCSIT) International Journal of Computer Science and Information Technologies, Vol. 2 5) , 2011, 1836-1840.

[3] Sameera Abdulrahman Almulla, Chan Yeob Yeun " Cloud Computing Security Management", July 2011, IEEE 4th International conference on Cloud Computing, CLOUD 2011.

[4] Z. Shen, L. Li, F. Yan, and X. Wu, "Cloud Computing System Based on Trusted Computing Platform", (ICICTA) IEEE Conferences, 942 - 945 (2010).

[5] B. R. Kandukuri, R. Paturi V, A. Rakshit, "Cloud Security Issues", IEEE International Conference on Services Computing, Bangalore, India, September 21-25, 2009.

[6] T. Mather, S. Kumarasuwamy, and S. Latif, "Cloud Security and Privacy", O'Rielly, ISBN: 978-0-4596- 802769, 2009.

[7] J. Wei et al., "Managing Security of Virtual Machine Images in a Cloud Environment", ACM Cloud Computing Security Workshop, Nov. 13, 2009,Chicago, IL.

[8] Mahmoud K.I Umar , Xiaochun Cheng, "A Security Design for Cloud Computing: An Implementation of an On Premises Authentication with Kerberos and IPSec within a Network", International Journal of Advanced Research in Computer Science, Vol 3, No 1, Jan-Feb 2012.

[9] Pankaj Patidar, Arpit Bhardwaj, "Network Security through SSL in Cloud Computing Environment", International Journal of Computer Science and Information Technologies, Vol 2 (6), 2011, 2800-2803.