Moving from Legacy Systems to Cloud Computing

A Tata Communications White Paper

Table of Contents

1 Executive Summary

Many companies continue to have questions about having their infrastructure or applications deployed on a cloud computing architecture, despite the proven savings and business advantages cloud computing can provide. This paper addresses some common technology and deployment concerns, and makes suggestions on how companies can more easily migrate comfortably to using cloud-based computing more effectively in their business. In particular this paper outlines and discusses common concerns, such as cloud security, flexibility, the ability to migrate away from cloud computing if necessary, managing cloud environments and ensuring service levels are maintained. The paper also focuses on types of cloud architectures, including when they are each most commonly used, and migration strategies for companies with deeply entrenched legacy applications, as well as companies with basic IT requirements to transfer to a cloud platform. Finally, the paper outlines briefly Tata Communications' extensive experience in global network computing and managed services, and how this expertise serves as the basis for its cloud computing service offerings.

2 Introduction

2.1 Definition of Cloud Computing

Cloud computing is a model for enabling convenient, on-demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction. This cloud model promotes availability and is composed of **five essential characteristics, three service models, and four deployment models.**

2.2 Essential Characteristics:

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.

Broad 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 to serve multiple 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 in that 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.

Rapid elasticity. Capabilities can be rapidly and elastically provisioned, in some cases automatically, to quickly scale out and rapidly released to quickly scale in. To the consumer, the capabilities available for provisioning often appear to be unlimited 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.

Source: Cloud Security Alliance, 2009, "Security Guidance for Areas of Focus in Cloud Computing V2.1"

Corporations worldwide are adopting cloud computing as the main computing platform for conducting their day-to-day business. They have abandoned or severely cut back on capital expenditures and maintenance for onsite servers, storage devices, business applications, and backup devices such as tape and optical drives. By eliminating hardware or software acquisition and maintenance costs, companies realize a substantial savings when moving to a cloud based architecture.

While the savings can be promising, many corporate IT directors have valid concerns about the cloud computing trend, including that of entrusting key corporate assets to a new way of deployment that they aren't completely familiar with, and comfortable implementing on a company-wide basis.

A complete examination of cloud computing strengths and weaknesses allows corporate IT managers to better determine whether cloud computing is a viable option for all, or select parts, of their business needs.

2.3   Cloud Computing Business Advantages

Cloud computing evolved from early Internet commerce sites. As corporations began to realize significant savings in shared infrastructure / application environments, a number of vendors began to offer these online resources to customers. Cloud computing has matured significantly since those early days and can now demonstrate a greater number of key advantages for businesses including lower hardware and software costs, less management overhead, and predictable, utility-based pricing of services. However, although cloud computing provides a variety of benefits, it has its challenges as well.

3 The Move to Cloud Computing: Addressing Potential Concerns

Despite clear economic, managerial, and functional advantages to using cloud computing for corporate computing, many IT managers and business executives may still have unresolved issues in moving their business functions to a third party location. Most of these potential fears involve security, availability, flexibility and control, quality of service, or the long-term protection of valuable data. Others are concerned that the connection to the offsite cloud will not perform consistently or that their entire business would rely on network connections that may go down at any time. Every company should fully address these issues, and understand the pros and cons, before migrating specific IT functions and applications to a cloud platform.

3.1 Cloud Security

Companies considering cloud computing should look carefully at the security and reliability of potential service providers. Most cloud computing vendors make security a top priority. Since many service providers began their businesses as online commerce providers, they have ample experience, tools, and equipment in securing online data from unauthorized use and in making certain that access to that data is highly secured as well. Cloud computing providers offering SaaS and IaaS services routinely ensure that company data is segregated through firewall and password access.

Another layer of protection for businesses using cloud computing is private network or VPN and/or IPSec connections to their cloud. This technology ensures that the entire connection from the offsite worker's desktop to the cloud network is safe from data capture or interception of any kind.
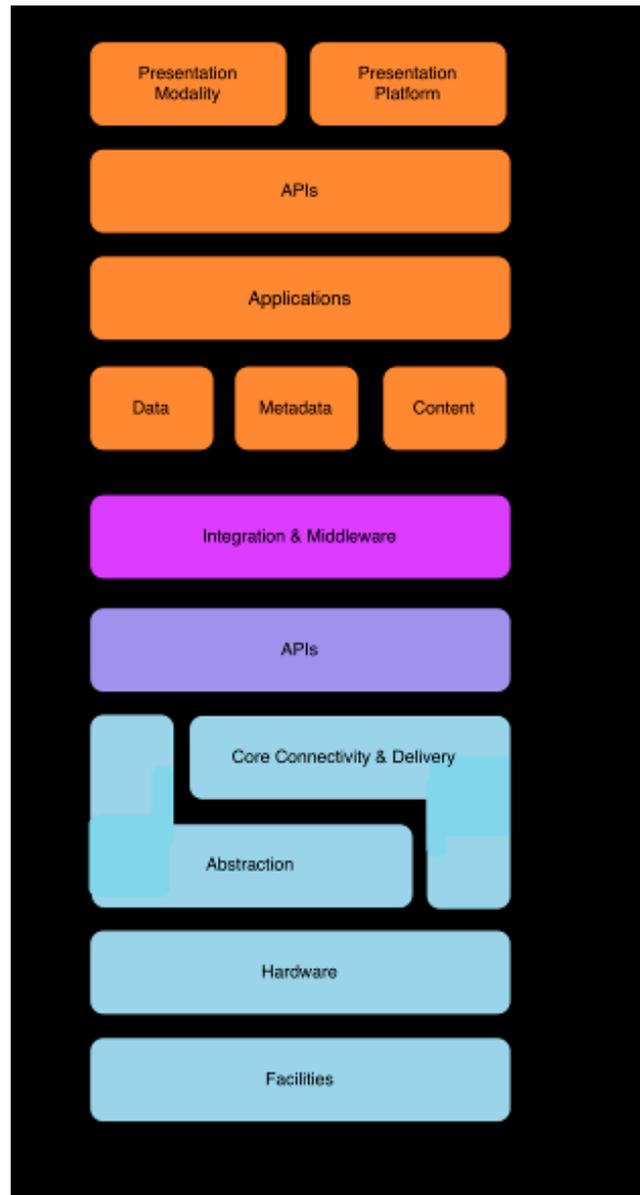
Figure 1. Cloud Computing Stack. Source: Cloud Security Alliance, 2009, "Security Guidance for Areas of Focus in Cloud Computing V2.1"

Some providers use multiprotocol label switching (MPLS) networks that can route traffic dynamically. These are both highly reliable and highly secure.

3.2 High Availability

The most complete cloud computing facilities are routinely protected from equipment failures and outages using redundant network switches, servers, and storage facilities. In particular, the use of offsite backup and redundant servers and storage facilities make these well-equipped cloud computing facilities less vulnerable to disaster, local catastrophe, or malicious attack.

The best cloud computing providers also see to it that customers can have fully redundant IP connections to the cloud, protecting access in the event that a local disaster or equipment failure drops carrier access to the cloud platform. Using MPLS also adds an additional layer of reliability and performance to cloud access.

3.3 Guaranteed Service Levels

Rightfully, corporations should be concerned with the level of service that cloud computing providers can actually guarantee. In most cases these vendors can only control SLAs on their cloud platform, leaving the service level of access to the cloud to a third-party service provider. Therefore, it is important that businesses get SLA guarantees from the provider from the company environment / desktop to their cloud provider to ensure that the business has the best possible access and uptime for the services in the cloud. If the cloud is up and running, but access to it is down due to an unreliable connectivity provider, the entire business may as well be closed.

While having SLAs is important, it is also important to define how and when a SLA truly goes "into effect."   A SLA does not necessarily affect the actual operations; its terms and conditions are only recited when things go awry, and it typically does not protect a business from loss of system uptime. Similarly, an SLA will not prove an effective tool for managing a cloud provider. It will still be a prerequisite, and the SLA offered by the cloud provider under consideration should be consistent with what others provide. Is uptime exclusive of scheduled maintenance? Is there a cap to service credit? While payment should cover the cost of the lost service, do not expect business losses owing to the downtime to be covered. It is also important to understand not just the contractual entitlements, but the course of action to seek a remedy. Does the provider offer a 24-hour help line? In the end, the quality of the uptime is directly related to the sophistication of the IT department, not the strength of the SLA. Choosing an IaaS or SaaS provider that employs best practices in design and operations and promotes transparency offers the greatest assurance of performance.

3.4 Flexibility

Most companies are concerned about the flexibility and response times associated with change requests that may come in. Since most migrations to the cloud today are in a shared environment, there will be some flexibility to get the full business / financial advantages, and as cloud computing continues to mature, cloud computing companies can offer even greater flexibility to their customers.

3.5 Managing a Cloud Infrastructure

Many corporate IT managers are reluctant to commit to cloud computing because it also commits them to managing the new cloud infrastructure. While this may suit some IT departments, most companies are better served moving to a fully managed cloud environment. Fully managed cloud environments should monitor performance, application availability, routine backup and archiving, storage, memory and server provisioning, and other security, performance, and protections tasks. For most companies, 24X7 support and technical assistance is mandatory. Companies should read the fine print to make certain the level of management, service, and support they require are provided by the cloud vendor, and whether these are part of the paid service or layered on as extra charges to the company.

3.6 An Escape Hatch

A full commitment to cloud computing often seems risky to any company. Many CIOs fear that if the platform does not work out, it could literally ruin their credibility. For this reason, companies should make certain that any potential cloud computing partner has a fully documented path for not only migrating applications and systems on to their platform, but also has defined policies and procedures, in the event that a customer wants to disengage specific deployments from the cloud provider.

3.7   Deciding on a Cloud Service Model

Once all uncertainties have been addressed, and IT and management are committed to a cloud computing implementation, it is time to decide on the best way to migrate to a cloud-based business. There are many competing definitions of what cloud computing truly is. The definition published by the Cloud Security Alliance is the most comprehensive and serves as the industry's guideline. [See page 2]. A true cloud computing platform can offer a number of different service models to businesses, each with its strengths and weaknesses in serving as a solid platform for business computing tasks, and each affords businesses the opportunity to move from small cloud implementation to very large-scale cloud deployments.

Service Models

Software as a Service (SaaS). This model enables the customer to access the cloud provider's applications running on a cloud infrastructure, from various client devices through a thin client interface such as a web browser (e.g., web-based email). The customer 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.

Platform as a Service (PaaS). This model enables customers to deploy onto the cloud infrastructure customer-created or acquired applications created using programming languages and tools supported by the provider. The customer 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.

Infrastructure as a Service (IaaS). This model enables provisioning of processing, storage, networks, and other fundamental computing resources, where the customer is able to deploy and run arbitrary software, which can include operating systems and applications. The customer does not manage or control the underlying cloud infrastructure but has control over operating systems, storage, deployed applications, and possibly limited control of select networking components (e.g., host firewalls).

Source: Cloud Security Alliance, 2009, "Security Guidance for Areas of Focus in Cloud Computing V2.1"

3.7.1 Advantages of Software as a Service

Software as a service (SaaS) enables companies to offload what were traditionally in- house applications to a third-party provider. Many strategic SaaS suppliers offer monthly usage of their software, with easy methods for uploading and downloading data. Typically, SaaS is on a shared environment, with multiple companies using the same foundational infrastructure, with clear segregation of data and access. The primary advantage of using SaaS based business services are that customers pay only for the users that they have. Companies are not responsible for software upgrades or maintenance. SaaS, therefore, has turned out to be the most practical first step for companies migrating from legacy to cloud computing, provided that the SaaS vendor can ultimately accommodate a full cloud-based business infrastructure.

Millions of Dollars
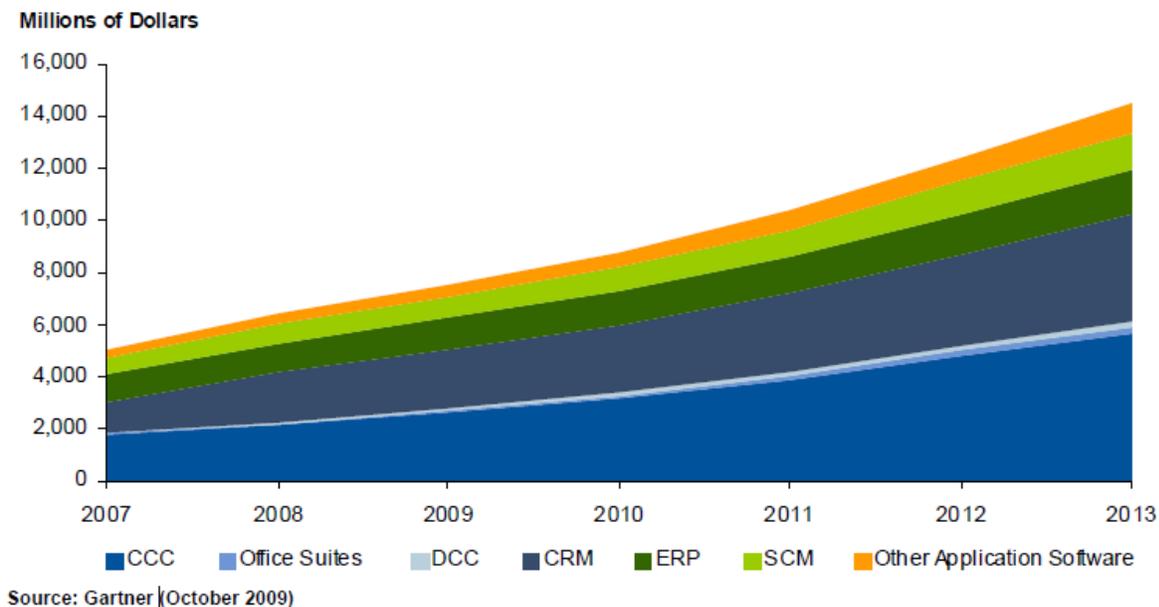

Source: Gartner (October 2009)

Figure 2. Projected Software as a Service revenue growth, 2007 through 2013. The Gartner Group, 2009.

3.7.2 Advantages of Platform as a Service

PaaS customers use a cloud to deploy an entire application and service platform. Primarily software and software application developers, PaaS customers can offer a full line of services to customers over the Internet, with full control over the applications, the Web interface, and products, if any, that are offered on the platform. For the most part, PaaS is not suited for off-the-shelf applications or day-to-day business use. It is, however, a highly dynamic and highly productive platform for software and application development.

3.7.3 Infrastructure as a Service

Infrastructure as a Service (IaaS) represents a flexible means for many businesses to adopt cloud computing. Companies can start small and grow their cloud-based businesses resources incrementally. In some of the largest implementations, IaaS can host an entire corporate data center on a cloud computing infrastructure. Replacing data center servers, disk arrays, network switches, and server-based applications, IaaS can grow to become the complete computing environment for any small, medium or enterprise business with an easy customization of any component or application. This deployment gives customers the best basis for a gradual cloud migration and also allows them plenty of room for growth at a fraction of the cost of legacy data center installations.
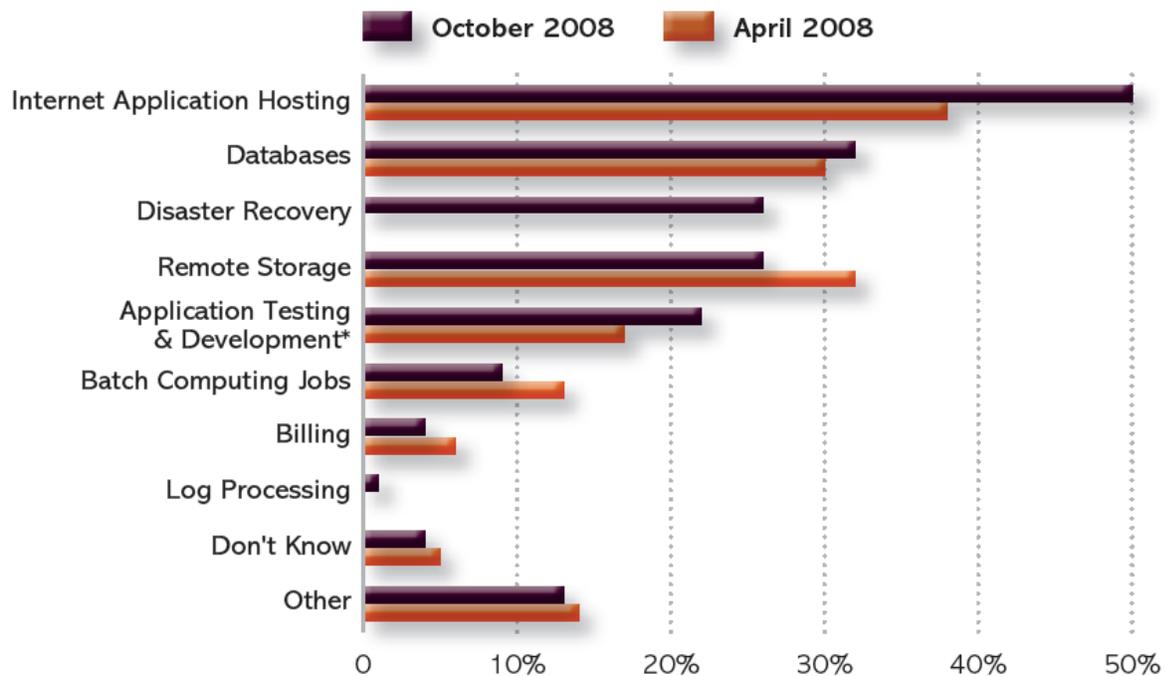

Figure 3. Customer Uses for Infrastructure as a Service. Source: Cloud Security Alliance, 2009, "Security Guidance for Areas of Focus in Cloud Computing V2.1"

3.8   Cloud Deployment Models

In addition to service levels, cloud computing is also classified into deployment models, each with its own strengths and applications depending on customer and corporate requirements.

Deployment Models

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.

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.

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.

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 for load-balancing between clouds).

Source: Cloud Security Alliance, 2009, "Security Guidance for Areas of Focus in Cloud Computing V2.1"

3.8.1   Private Cloud

Corporations deploy private clouds for a number of reasons. Some businesses prefer private clouds that are managed by third-party operators, thereby offloading management and headcount costs while retaining complete control. Private clouds that are based off premises with a cloud computing provider can insist that data and applications are spread among a number of cloud sites, mitigating any chance of single-site business failures. Private cloud infrastructures are the most expensive types of cloud computing in use today. They are typically used by the larger companies with severe regulation, compliance, and security requirements.

3.8.2   Community Cloud

Non-profit, social networking and affiliated groups often use community cloud infrastructures to leverage the one-size-fits-all templates for security, storage allocations, and other infrastructure components.

3.8.3   Public Cloud

The public cloud is merely any cloud computing platform open for use to the public—whether it be individuals or large corporations. Public clouds, however, ensure that individual cloud users are offered ample security and privacy. On properly deployed, maintained and secured public cloud offerings, customer data and resources should be as safe as any private LAN.

3.8.4   Hybrid Cloud

Many companies buy hybrid cloud services to get the greatest value from their hosted environment. Companies can buy extra public infrastructure that can be rolled out during peak access or when IT deployments are staged to offsite locations. Corporations often host their public-facing Web site and ecommerce front ends on public cloud infrastructures, while they reserve private clouds for data storage and internal and intranet computing services. These are typically used by companies with existing deployments, plus specific peak needs that may require additional infrastructure or applications. The public portion of the cloud accommodates bursts in traffic, while the private side of the cloud serves sustainable and stable applications and business functions.

4 Beyond Service and Deployment: Methods of Migration

Once a business has decided it can commit to a cloud computing infrastructure, it can begin to decide how it will migrate to the cloud. A number of considerations come into play, such as the size and complexity of current applications, the amount and number of applications, and whether the existing legacy platform is over-due for upgrades or replacements.

4.1 Incremental Cloud Deployment

Most companies start out incrementally, choosing a SaaS or IaaS application that would replace an in-house application, such as CRM, sales force automation, or email. After the new application settles into the business process, another cloud-based application can be added. In this incremental approach it is also advisable to choose the least disruptive application change-over first, or to migrate less business-sensitive applications early on. It is in the best interest of the company to carefully document the migration of each system or application and also, if possible, capture the difference between cost of premises ownership versus cost of cloud implementation.

4.2 Legacy Migration

With very entrenched legacy applications, equipment, and computing processes it may take time to migrate every application from one platform to the next, especially when application performance and reliability are at stake. It is imperative that businesses with a large base of legacy computing applications have a competent and experienced cloud computing provider to help them re-engineer their systems for optimum performance and reliability. Productivity, customer satisfaction, and business continuity cannot suffer during a migration. Companies should create mirror systems of key legacy applications – one on the new cloud platform, another on the existing platform, and compare performance, reliability, functionality before cutting over to the cloud-based version. Also, companies should consider moving the most critical legacy applications last.

4.3   Avoiding Costly Upgrades

When businesses are faced with costly and complicated upgrades to applications, it may be the right time to consider cloud computing alternatives. Rather than pay for costly computer, software, and storage upgrades and potentially greater outlays for hardware maintenance, companies facing upgrades can upload existing data from legacy applications to cloud computing alternatives, test the applications on live data, and then retire the legacy application once the platform has been fully tested.

4.4   Straight to the Cloud

Customers with relatively simple legacy applications, such as business productivity software and a few custom applications are better off making a complete changeover. The cloud infrastructure and applications can be configured, tested, and rolled out in tandem with the old systems, and cut over can occur fairly quickly. Again, an experienced cloud provider is essential in making a smooth transition.

5   Tata Communications' Cloud Computing

As one of the most experienced providers of global network services, Tata Communications hosts cloud computing centers throughout the world. Leveraging its extensive high-performance, highly-reliable network, Tata Communications is now offering a full range of cloud computing services to its customers.

Tata Communications' cloud computing builds upon its leadership position in specific SaaS based services, with India's first true IaaS environment for business, enabling customers to provision resources on demand via a portal and pay only for the resources they consume. Because the service is located in India, it offers minimal latency and maximum performance for Indian businesses.

Tata Communications offers customers a complete IT Services portfolio – spanning from global connectivity to hosting. Hosting options include traditional colocation, managed hosting, SaaS and IaaS.

All Tata Communications' Cloud Computing services provide the following:

- A comprehensive portfolio that makes Tata Communications the number one provider for service, support, and implementation planning.

- MPLS VPN connectivity into the cloud provides maximum security and QoS. The Tata Communications platform is known throughout the industry for its performance and reliability.

- Enhanced global reach, coupled with local service and expertise.   Contracts in local languages, local currency and multiple payment options, including prepaid credit card, post paid credit card, and corporate account and PO arrangements, position Tata Communications as unique in the industry. Tata Communications maintains India-based cloud customer data in India, ensuring regulatory compliance and peace of mind. With pricing and billing in rupees, U.S. or Singapore dollars, and Euros, and the ability to set up user alerts, customers can take advantage of better budget planning.

- All Tata Communications' cloud accounts employ the highest levels of security with master account and project account management, giving businesses the same security options and management flexibility they expect from an on-premises network. Accounts can accommodate multiple users. With Tata Communications' MPLS and cloud security and high availability, cloud customers have a more protected and safe environment than they could deploy on their own, and avoid significant investment in equipment, personnel, and training. Tata Communications' cloud management is local and available 24X7.

-Includes robust multiple projects governance with tight accountability and cost management where a master user can set up and administer multiple individual projects, each with a project lead and multiple users. The master user can set spending limits and automatic notifications when limits are approached.

5.1   Service End-to-End

Tata Communications offers an end-to-end solution for customers from high-speed, highly reliable MPLS connections to the data center cloud to a full array of business productivity applications, including word processing, group calendaring, video conferencing, and others. CRM and sales tracking applications, and other specialized business applications—custom designed or off the shelf—can easily be integrated into customer clouds at any time, with no disruption or costly upgrade.

With certified support teams, superior connectivity of a global Tier-1 IP backbone linking its datacenters, and—as a subsidiary of the Tata Group—a 150-year reputation for reliability and service, Tata Communications is prepared to be a trusted cloud computing provider and partner.

6 Conclusion

Companies must internally address any technology, business process, or security concerns they may have before considering a migration to cloud computing. Once they have made that decision, they should choose the right service and deployment method that best suits their business. Finally, they must select a provider with the experience, reliability, and expertise to make their move to cloud computing a smooth and productive experience.

Businesses adopting a cloud computing model can not only reduce costs, but also avoid the overhead and management of IT equipment. Tata Communication's cloud computing offerings combine the best in flexibility and scalability, whether for SMBs looking to quickly get web applications up and running or enterprises that need to move substantial applications from on-premises data centers into a cloud computing environment. Tata Communications will subsequently expand its cloud computing access geographically, building towards a global footprint, and offer new deployment models, to provide various cloud computing services to larger businesses that require enterprise-grade features.

7 References

- Definition of Cloud Computing, National Institute of Standards and Technology, Version 15, October, 2009.
- Cloud Security Alliance, 2009, "Security Guidance for Areas of Focus in Cloud Computing V2.1"